VASILE-DRAGOȘ BARTOȘ

Fabrici inteligente

și tehnologii convergente în era IIoT



U.T.PRESS
Cluj-Napoca, 2026
ISBN 978-606-737-870-2

Vasile-Dragoș BARTOȘ

Fabrici inteligente

și tehnologii convergente

în era IIoT

U.T. PRESS
Cluj-Napoca,2026
ISBN 978-606-737-870-2

Editura U.T.PRESS
Str. Observatorului nr. 34
400775 Cluj-Napoca
Tel.: 0264-401.999
e-mail: utpress@biblio.utcluj.ro
www.utcluj.ro/editura

Recenzia: Prof.dr.ing. Stelian Brad

Prof.dr.ing. Călin Neamțu

Pregătire format electronic on-line: Gabriela Groza

Copyright © 2026 Editura U.T.PRESS

Reproducerea integrală sau parțială a textului sau ilustrațiilor din această carte este posibilă numai cu acordul prealabil scris al editurii U.T.PRESS.

ISBN 978-606-737-870-2

CUPRINS

Glosar ... ix
Prefață ... xiv
1. INTRODUCERE ÎN INTERNETUL INDUSTRIAL AL LUCRURILOR ŞI TRANSFORMAREA DIGITALĂ A INDUSTRIEI ... 1
1.1. De la IoT la IIoT, Industria 4.0 şi fabricaţia inteligentă ... 3
1.1.1. De la mecanizare la sisteme ciber-fizice ... 4
1.1.2. Digitizare, digitalizare şi transformare digitală ... 5
1.1.3. Internetul Lucrurilor şi Internetul Industrial al Lucrurilor ... 7
1.1.4. Industria 4.0, fabricaţia inteligentă şi Industria 5.0 ... 9
1.2. Rolul datelor în lanţul valoric industrial ... 11
1.2.1. Date disponibile şi date utilizabile ... 11
1.2.2. Lanţul date – informaţie – decizie – acţiune ... 14
1.2.3. Datele în lanţul valoric industrial ... 15
1.2.4. Proprietatea, responsabilitatea şi păstrarea datelor industriale ... 17
1.3. Beneficii şi provocări în implementarea IIoT ... 19
1.3.1. Beneficii operaţionale şi strategice ... 20
1.3.2. Provocări tehnice, organizaţionale şi economice ... 21
1.3.3. Evaluarea economică a unui proiect-pilot IIoT ... 24
1.4. Scenariu didactic privind digitalizarea industrială ... 27
1.4.1. Contextul iniţial şi obiectivele proiectului ... 27
1.4.2. Arhitectura şi traseul datelor ... 29
1.4.3. Implementarea şi evaluarea soluţiei ... 31
1.4.4. Limitele scenariului didactic ... 32
1.5. Concluzii ... 34
1.6. Întrebări de verificare ... 35
2. ARHITECTURA UNEI COMPANII INDUSTRIALE ŞI FLUXUL COMENZII ÎN PRODUCŢIE ... 39
2.1. Structura organizaţională a unei companii industriale ... 40
2.1.1. Funcţiile operaţionale ... 41
2.1.2. Funcţiile de conducere şi suport ... 42
2.1.3. Colaborarea şi integrarea informaţională ... 43
2.1.4. Adaptarea structurii la dimensiunea şi domeniul companiei ... 45
2.2. Configuraţia funcţională a unei fabrici şi fluxul fizic al materialelor ... 47
2.2.1. Principalele zone funcţionale ... 48
2.2.2. Tipuri de configuraţie şi criterii de alegere ... 49
2.2.3. Organizarea fluxului fizic ... 50

2.2.4. Relaţia cu infrastructura de automatizare şi comunicaţie 51
2.3. Fluxul informaţional şi fizic al unei comenzi 52
2.3.1. Primirea şi validarea cererii clientului 53
2.3.2. Ofertarea şi confirmarea comenzii 53
2.3.3. Planificarea şi lansarea în producţie 53
2.3.4. Aprovizionarea şi recepţia materialelor 54
2.3.5. Execuţia şi urmărirea producţiei 54
2.3.6. Controlul calităţii şi gestionarea neconformităţilor 55
2.3.7. Ambalarea, expedierea şi facturarea 55
2.3.8. Serviciile post-vânzare şi utilizarea feedbackului 56
2.3.9. Durata totală de realizare a comenzii şi componentele acesteia 57
2.4. Interacţiunea companiei cu mediul extern 59
2.4.1. Relaţia cu clienţii 60
2.4.2. Relaţia cu furnizorii 60
2.4.3. Partenerii logistici şi prestatorii de servicii 62
2.4.4. Relaţia cu autorităţile şi organismele de reglementare 62
2.4.5. Digitalizarea colaborării şi integrarea orizontală 63
2.5. Scenariu didactic: structura funcţională şi fluxul operaţional într-o fabrică de mobilier modular 64
2.5.1. Structura funcţională a companiei 65
2.5.2. Configuraţia fabricii şi fluxul fizic 66
2.5.3. Fluxul informaţional al comenzii 67
2.5.4. Puncte de integrare digitală şi criterii de evaluare 68
2.6. Concluzii 70
2.7. Întrebări de verificare 71
3. TIPURI DE PRODUCŢIE ŞI MODELE DE FABRICAŢIE DIGITALĂ 75
3.1. Clasificarea proceselor de producţie 76
3.1.1. Producţia unicat 77
3.1.2. Producţia de serie 78
3.1.3. Producţia de masă 78
3.1.4. Producţia continuă 79
3.1.5. Punctul de decuplare a comenzii 80
3.2. Modele moderne de fabricaţie 81
3.2.1. Modelul Just-in-Time 83
3.2.2. Modelul Lean Manufacturing 84
3.2.3. Fabricaţia agilă 85
3.2.4. Personalizarea de masă 86
3.3. Corelarea tipului de producţie cu arhitectura IIoT 87
3.3.1. Arhitectura IIoT pentru producţia unicat 89
3.3.2. Arhitectura IIoT pentru producţia de serie 90

3.3.3. Arhitectura IIoT pentru producția de masă ... 91
3.3.4. Arhitectura IIoT pentru producția continuă ... 92
3.3.5. Dimensionarea fluxului de date și a lățimii de bandă ... 93
3.3.6. Metodă de evaluare a unei fabrici și de stabilire a priorităților ... 95
3.3.7. Aplicarea metodei într-un scenariu de fabricație a mobilierului modular ... 96
3.4. Concluzii ... 98
3.5. Întrebări de verificare ... 100
4. SISTEME FLEXIBILE ȘI RECONFIGURABILE DE FABRICAȚIE ... 103
4.1. Arhitectura sistemelor flexibile și reconfigurabile de fabricație ... 105
4.1.1. Sistemul flexibil de fabricație ... 105
4.1.2. Sistemul reconfigurabil de fabricație ... 107
4.1.3. Tipuri de flexibilitate și dimensionarea capacității ... 110
4.1.4. Dimensionarea capacității și costul treptei de scalare ... 111
4.2. Modularitate, interoperabilitate și adaptabilitate ... 113
4.2.1. Modularitatea ... 114
4.2.2. Interoperabilitatea ... 117
4.2.3. Adaptabilitatea ... 119
4.2.4. Bugetul de reconfigurare ... 121
4.3. Integrarea echipamentelor în rețele IIoT ... 123
4.3.1. Datele furnizate de echipamente ... 124
4.3.2. Integrarea unei celule robotizate ... 125
4.3.3. Distribuirea funcțiilor în arhitectură ... 127
4.3.4. Proiectarea și validarea integrării ... 129
4.4. Exercițiu aplicativ – Simularea unui sistem flexibil de fabricație într-un mediu tridimensional cu control prin PLC ... 130
4.4.1. Scenariul de fabricație și dimensionarea modelului ... 131
4.4.2. Configurarea modelului și a semnalelor ... 132
4.4.3. Programarea secvenței de control și interblocările ... 133
4.4.4. Testarea, criteriile de reușită și limitele transferului ... 135
4.4.5. Extinderea către integrarea IIoT și indicatorii locali ... 136
4.5. Concluzii ... 137
4.6. Întrebări de verificare ... 139
5. DISPOZITIVE INTELIGENTE INDUSTRIALE ȘI AUTOMATIZAREA PROCESELOR ... 143
5.1. Senzori industriali ... 145
5.1.1. Pt100 – senzor de temperatură cu rezistență ... 148
5.1.2. Senzori de presiune ... 149
5.1.3. Senzori fotoelectrici ... 149
5.1.4. Senzori inductivi ... 150
5.1.5. Senzori ultrasonici ... 151

5.1.6. Senzorii inteligenți și integrarea în IIoT 152
5.2. Actuatoare industriale 153
5.2.1. Valve de control 155
5.2.2. Servomotoare 156
5.2.3. Cilindri pneumatici 157
5.2.4. Robotul industrial ca sistem integrat de acționare 159
5.3. Automate programabile 161
5.3.1. Arhitectura unui automat programabil 161
5.3.2. Ciclul de scanare 163
5.3.3. Organizarea și programarea aplicației 165
5.3.4. Funcții de control și diagnosticare 167
5.3.5. Automatul programabil și sistemul de control distribuit 168
5.3.6. Rolul automatului programabil în IIoT 169
5.4. Gateway-urile industriale și prelucrarea edge 170
5.4.1. Rolul gateway-urilor industriale 171
5.4.2. Prelucrarea edge 172
5.4.3. Delimitarea dintre prelucrarea edge, fog și cloud 174
5.4.4. Proiectarea unui flux de date printr-un gateway industrial 175
5.4.5. Dimensionarea cantitativă a fluxului de date 177
5.5. Sisteme SCADA și interfețe om–mașină 179
5.5.1. Funcțiile unui sistem SCADA 180
5.5.2. Arhitectura unui sistem SCADA 181
5.5.3. Delimitarea dintre PLC, SCADA și Historian 183
5.5.4. Interfețele HMI 184
5.5.5. Alarme, evenimente și date istorice 186
5.5.6. Evoluția sistemelor SCADA 187
5.5.7. Integrarea SCADA în arhitectura IIoT 189
5.6. Exercițiu aplicativ – Configurarea unei interfețe HMI pentru monitorizare 191
5.6.1. Definirea etichetelor și a schimbului de date 191
5.6.2. Proiectarea ecranului și gestionarea alarmei 193
5.6.3. Comenzile, interblocările și simularea 195
5.6.4. Validarea interfeței 196
5.7. Exercițiu aplicativ – Integrarea unui senzor industrial cu PLC și SCADA 197
5.7.1. Scenariul și cerințele funcționale 198
5.7.2. Configurarea achiziției și scalarea valorii 199
5.7.3. Implementarea logicii în PLC 202
5.7.4. Integrarea cu sistemul SCADA 203
5.7.5. Testarea și validarea integrării 205

5.7.6. Rezultatul exercițiului și posibilitățile de extindere 206
5.8. Concluzii 207
5.9. Întrebări de verificare 209
6. PROTOCOALE DE COMUNICARE INDUSTRIALĂ ȘI IIOT 211
6.1. Protocoale industriale clasice 212
6.1.1. Determinismul și comunicarea în timp real 214
6.1.2. Magistralele de câmp și CAN 215
6.1.3. Modbus RTU și Modbus TCP 216
6.1.4. PROFIBUS și PROFINET 218
6.1.5. EtherNet/IP 219
6.1.6. EtherCAT 221
6.1.7. OPC Classic și tranziția către OPC UA 222
6.1.8. Poziționarea protocoalelor în arhitectura IIoT 223
6.2. Protocoale IIoT 224
6.2.1. OPC UA 225
6.2.2. MQTT 228
6.2.3. Sparkplug B 230
6.2.4. CoAP și HTTP/REST 231
6.2.5. AMQP 232
6.2.6. LoRaWAN și 5G industrial 233
6.2.7. Utilizarea complementară a OPC UA și MQTT 234
6.2.8. Convenția pentru subiectele MQTT și corespondența cu spațiul de adrese OPC UA 236
6.3. Stiva de comunicare în IIoT 238
6.3.1. Modelul stratificat al comunicației 239
6.3.2. Suprapunerea protocoalelor peste zonele arhitecturii 240
6.3.3. Exemple de stive de comunicație 241
6.3.4. Bugetul de latență pe lanțul de date 243
6.4. Considerații privind alegerea protocolului 245
6.4.1. Definirea cerințelor fluxului de comunicație 245
6.4.2. Criterii de selecție 246
6.4.3. Alegerea protocolului în funcție de scenariu 249
6.4.4. Metoda de selecție și validare 250
6.4.5. Dimensionarea lățimii de bandă necesare publicării datelor 251
6.5. Exerciții aplicative pentru validarea comunicațiilor industriale și IIoT 253
6.5.1. Validarea comunicației MQTT 254
6.5.2. Validarea schimbului de date între două automate programabile 255
6.5.3. Monitorizarea comunicației într-un sistem SCADA 256
6.5.4. Metoda comună de validare etapizată 257

6.6. Concluzii 258
6.7. Întrebări de verificare 260
7. ARHITECTURA ŞI INTEGRAREA UNUI SISTEM IIOT COMPLET 263
7.1. Componentele unei arhitecturi IIoT 265
7.1.1. Modelul funcţional de referinţă 265
7.1.2. Nivelurile procesului, câmpului şi controlului 267
7.1.3. Nivelurile operaţiunilor de fabricaţie şi întreprinderii 268
7.1.4. Determinismul şi comunicarea în timp real 270
7.1.5. Componentele transversale ale arhitecturii 272
7.1.6. Fluxurile şi limitele dintre niveluri 273
7.2. Interconectarea SCADA–MES–ERP 274
7.2.1. Delimitarea funcţională a sistemelor 275
7.2.2. Fluxurile bidirecţionale dintre niveluri 277
7.2.3. Contextualizarea datelor şi funcţiile MES 279
7.2.4. Proiectarea interfeţelor de integrare 281
7.2.5. Exemplu de integrare a unei comenzi de producţie 283
7.3. Modele de arhitectură IIoT 285
7.3.1. Arhitecturi centralizate, distribuite şi hibride 285
7.3.2. Continuumul marginea reţelei–nivel intermediar–cloud 288
7.3.3. Criterii pentru distribuirea funcţiilor 290
7.3.4. Geamănul digital 292
7.4. Platforme industriale care furnizează servicii de calcul în cloud 295
7.4.1. Lanţul funcţional al unei platforme IIoT 295
7.4.2. Recepţia datelor şi administrarea dispozitivelor 298
7.4.3. Rutarea, transformarea şi contextualizarea mesajelor 300
7.4.4. Persistenţa datelor industriale 301
7.4.5. Analiza, vizualizarea şi integrarea rezultatelor 303
7.4.6. Criterii pentru alegerea platformei 304
7.4.7. Exemple de platforme şi evoluţia serviciilor 306
7.5. Exerciţiu – Proiectarea unei arhitecturi IIoT pentru o linie de ambalare complet automatizată 307
7.5.1. Scenariul tehnologic 307
7.5.2. Cerinţele sistemului 309
7.5.3. Stiva tehnologică de referinţă 310
7.5.4. Convenţia de denumire a subiectelor şi structura mesajelor 311
7.5.5. Configurarea componentelor 314
7.5.6. Validarea etapizată 318
7.5.7. Livrabile şi criterii de reuşită 319
7.6. Concluzii 321
7.7. Întrebări de verificare 322

8. SECURITATE CIBERNETICĂ ÎN IIOT 325
8.1. Riscuri şi vulnerabilităţi în automatizările industriale 327
8.1.1. Specificul riscului în mediile OT 327
8.1.2. Suprafaţa de atac a unei arhitecturi IIoT 328
8.1.3. Atacuri asupra PLC-urilor şi sistemelor de supraveghere 331
8.1.4. Interceptarea şi manipularea comunicaţiilor 332
8.1.5. Vulnerabilităţi în stratul edge şi în serviciile cloud 334
8.1.6. Reţele wireless, acces fizic şi lanţul de aprovizionare 335
8.1.7. Incidente documentate şi evaluarea riscului 336
8.2. Măsuri de securitate – Autentificare, criptare, segmentare şi DMZ industrial 338
8.2.1. Principiile aplicării măsurilor de securitate 338
8.2.2. Identificarea, autentificarea şi autorizarea 339
8.2.3. Certificatele X.509 şi infrastructura cu chei publice 341
8.2.4. Protejarea comunicaţiilor şi a datelor 345
8.2.5. Segmentarea reţelei industriale 347
8.2.6. Zona demilitarizată industrială 349
8.2.7. Accesul la distanţă 350
8.2.8. Consolidarea configuraţiei, monitorizarea şi recuperarea 351
8.3. Standarde şi cadre relevante pentru securitatea IIoT 353
8.3.1. Familia ISA/IEC 62443 353
8.3.2. Zonele şi conductele de comunicaţie 354
8.3.3. Cerinţele fundamentale şi nivelurile de securitate 356
8.3.4. NIST Cybersecurity Framework 2.0 358
8.3.5. ISO/IEC 27001:2022 359
8.3.6. MITRE ATT&CK for ICS 360
8.3.7. Industrial Internet Security Framework 361
8.3.8. Utilizarea complementară a referinţelor 362
8.3.9. Cadrul de reglementare al Uniunii Europene 364
8.4. Exerciţii aplicative: identificarea riscurilor şi analiza securităţii unui sistem IIoT 365
8.4.1. Exerciţiul 1 – Evaluarea riscurilor unei linii de ambalare conectate IIoT 366
8.4.2. Exerciţiul 2. Analiza securităţii fluxului OPC UA – edge – MQTT – servicii cloud 369
8.4.3. Exerciţiul 3. Validarea controlată a măsurilor de securitate 373
8.5. Concluzii 375
8.6. Întrebări de verificare 376
9. APLICAŢII INDUSTRIALE ŞI MINI-PROIECTE GHIDATE 379
9.1. Exemple de aplicaţii IIoT 381
9.1.1. Mentenanţă predictivă 382

9.1.2. Monitorizarea consumului energetic 385
9.1.3. Automatizări agroindustriale 388
9.1.4. Regimul juridic al datelor generate de produsele conectate 391
9.1.5. Elemente comune și criterii de selecție a aplicației 393
9.2. Mini-proiecte ghidate 394
9.2.1. Mini-proiectul 1: Rețea de senzori pentru monitorizarea temperaturii și vibrațiilor 397
9.2.2. Mini-proiectul 2: Linie de transport automatizată 401
9.2.3. Mini-proiectul 3: Tablou de bord industrial cu date în timp real 406
9.2.4. Mini-proiectul 4: Celulă robotizată conectată IIoT 414
9.2.5. Evaluarea și documentarea mini-proiectelor 419
9.3. Concluzii 423
9.4. Întrebări de verificare 424
ANEXĂ – RĂSPUNSURI LA ÎNTREBĂRILE DE VERIFICARE 427
BIBLIOGRAFIE 428

Glosar

Actuator (*actuator*) – Dispozitiv care transformă un semnal de comandă într-o acţiune fizică asupra procesului, precum deplasarea unui mecanism, acţionarea unei valve sau reglarea unui debit.

API (*Application Programming Interface*) – Interfaţă software prin care aplicaţiile şi serviciile schimbă date sau solicită funcţii într-un mod standardizat şi controlat.

Automat programabil (PLC – *Programmable Logic Controller*) – Echipament industrial care achiziţionează semnale, execută determinist logica de control şi comandă actuatoarele. Controlul critic şi interblocările trebuie să rămână la nivel local.

Bază de date de serii temporale (*TSDB – time-series database*) – Bază de date optimizată pentru stocarea şi interogarea valorilor asociate unor mărci temporale, precum variabilele de proces, alarmele şi consumurile.

Broker MQTT (*MQTT broker*) – Componentă care primeşte mesajele publicate de clienţii MQTT şi le distribuie abonaţilor corespunzători, pe baza subiectelor şi a regulilor de acces configurate.

Calitatea serviciului (*QoS – Quality of Service*) – Nivel de garanţie asociat livrării mesajelor. În MQTT, nivelurile QoS 0, 1 şi 2 oferă mecanisme diferite privind confirmarea şi repetarea transmisiilor.

Date masive (*Big Data*) – Ansambluri de date al căror volum, ritm de generare sau diversitate necesită metode avansate de stocare, procesare şi analiză.

Determinism (*determinism*) – Proprietatea unui sistem de a răspunde într-un interval de timp limitat şi previzibil, indiferent de încărcare; este cerinţa centrală a funcţiilor de control şi de interblocare.

DMZ industrial (*industrial demilitarized zone*) – Zonă de reţea intermediară între infrastructura IT şi reţeaua OT, utilizată pentru controlarea şi securizarea schimburilor dintre cele două medii.

ERP (*Enterprise Resource Planning*) – Sistem informatic integrat pentru gestionarea comenzilor, aprovizionării, stocurilor, planificării, costurilor şi celorlalte resurse ale întreprinderii.

Ethernet industrial (*industrial Ethernet*) – Utilizarea tehnologiilor Ethernet în medii industriale, prin protocoale şi echipamente adaptate cerinţelor de disponibilitate, robusteţe, sincronizare şi timp de răspuns.

Fabrică inteligentă (*smart factory*) – Sistem de producţie în care echipamentele, produsele, oamenii şi aplicaţiile sunt conectate şi coordonate prin date pentru a susţine adaptarea şi optimizarea proceselor.

Gateway industrial (*industrial gateway*) – Echipament sau componentă software care conectează dispozitivele industriale la platformele IIoT şi poate realiza conversia protocoalelor, filtrarea, agregarea şi securizarea datelor.

Geamăn digital (*digital twin*) – Reprezentare digitală a unui activ, proces sau sistem fizic, actualizată prin date relevante şi utilizată pentru monitorizare, simulare, diagnosticare sau evaluarea unor scenarii.

Guvernanţa datelor (*data governance*) – Ansamblu de roluri, politici şi procese prin care sunt stabilite proprietatea, responsabilitatea, calitatea, accesul, păstrarea şi utilizarea datelor.

Historian (*data historian*) – Sistem care arhivează valorile variabilelor de proces, cu mărci temporale, pentru consultare, analiza tendinţelor şi raportare ulterioară.

HMI (*Human–Machine Interface*) – Interfaţă prin care operatorul urmăreşte starea procesului, consultă alarme şi tendinţe şi transmite comenzi către sistemul de automatizare.

IEC 62443 – Familie de standarde privind securitatea sistemelor industriale de automatizare şi control, care defineşte responsabilităţi, cerinţe tehnice, zone, conducte de comunicaţie şi niveluri de securitate.

IIoT (*Industrial Internet of Things*) – Ansamblu de echipamente, senzori, aplicaţii şi infrastructuri de comunicaţie care permit colectarea, schimbul şi valorificarea datelor industriale.

Industria 4.0 (*Industry 4.0*) – Paradigmă de transformare a producţiei bazată pe sisteme ciber-fizice, conectivitate, automatizare, date şi integrarea proceselor din lanţul valoric.

Industria 5.0 (*Industry 5.0*) – Orientare care completează digitalizarea industrială prin accentul pus pe factorul uman, sustenabilitate şi reziliență.

Inteligenţă artificială (*AI – artificial intelligence*) – Domeniu care dezvoltă sisteme capabile să recunoască tipare, să realizeze predicţii şi să sprijine luarea deciziilor pe baza datelor.

Interoperabilitate (*interoperability*) – Capacitatea unor echipamente şi aplicaţii diferite de a schimba şi utiliza coerent informaţii, pe baza unor reguli tehnice, sintactice şi semantice comune.

ISA-95 – Standard și model de referință pentru integrarea dintre sistemele de control și sistemele de management ale întreprinderii, inclusiv relațiile dintre ERP, MES și automatizare.

Învățare automată (*machine learning*) – Ramură a inteligenței artificiale în care modelele identifică tipare în date și generează clasificări, estimări sau predicții.

Just-in-Time (JIT) – Model de organizare prin care materialele și produsele sunt disponibile în cantitatea necesară și la momentul necesar, pentru reducerea stocurilor și a timpilor de așteptare.

Latență (*latency*) – Intervalul dintre producerea unui eveniment și disponibilitatea rezultatului la destinație. În IIoT, latența totală include toate etapele parcurse de date.

Lean (*lean manufacturing*) – Mod de organizare a producției orientat spre valoarea oferită clientului, eliminarea pierderilor și îmbunătățirea continuă a proceselor.

Magistrală de câmp (*fieldbus*) – Rețea industrială utilizată pentru comunicația digitală dintre controlere, senzori, actuatoare și alte dispozitive amplasate la nivelul procesului.

Mentenanță predictivă (*predictive maintenance*) – Strategie care utilizează datele despre starea echipamentelor pentru estimarea degradării și planificarea intervențiilor înaintea producerii defectării.

MES (*Manufacturing Execution System*) – Sistem care gestionează și urmărește execuția producției între nivelul ERP și automatizarea procesului.

MQTT (*Message Queuing Telemetry Transport*) – Protocol de mesagerie ușor, bazat pe modelul publicare–abonare și pe utilizarea unui broker, folosit frecvent pentru distribuirea datelor IIoT.

NIST Cybersecurity Framework (*NIST CSF*) – Cadru pentru organizarea managementului riscului cibernetic în jurul funcțiilor Govern, Identify, Protect, Detect, Respond și Recover.

OEE (*Overall Equipment Effectiveness*) – Indicator al eficacității globale a unui echipament, calculat ca produs între disponibilitate, performanță și calitate.

OPC UA (*Open Platform Communications Unified Architecture*) – Standard de interoperabilitate pentru schimbul securizat și contextualizat de date industriale, bazat pe servicii și modele informaționale.

Payload – Conținutul util transportat de un mesaj, separat de antetele și informațiile necesare transmisiei. Poate include valori, unități, mărci temporale și indicatori de calitate.

PKI (*Public Key Infrastructure*) – Ansamblu de autorități, certificate, politici și procese pentru emiterea, distribuirea, validarea și revocarea certificatelor digitale.

Procesare la edge (*edge computing*) – Executarea operațiilor de filtrare, agregare, analiză sau stocare temporară în apropierea sursei datelor, pentru reducerea latenței și a traficului către cloud.

PROFINET – Protocol Ethernet industrial utilizat pentru comunicația dintre controlere, dispozitive de câmp și alte componente ale sistemelor de automatizare.

PTP (*Precision Time Protocol, IEEE 1588*) – Protocol de sincronizare a ceasurilor într-o rețea locală, cu precizie de ordinul microsecundelor în configurații adecvate.

Publicare–abonare (*publish–subscribe*) – Model de comunicare în care producătorii publică mesaje, iar consumatorii primesc informațiile prin abonarea la subiectele relevante.

RAMI 4.0 (*Reference Architectural Model Industrie 4.0*) – Model tridimensional care corelează ciclul de viață al activelor, nivelurile ierarhice industriale și straturile funcționale ale unei arhitecturi.

SCADA (*Supervisory Control and Data Acquisition*) – Sistem pentru achiziția datelor, supravegherea proceselor, gestionarea alarmelor, afișarea tendințelor și transmiterea comenzilor de nivel superior.

Segmentare de rețea (*network segmentation*) – Împărțirea infrastructurii în zone cu roluri și politici de acces distincte, pentru limitarea incidentelor și controlarea fluxurilor de comunicație.

Senzor (*sensor*) – Dispozitiv care detectează o mărime fizică sau o stare și o transformă într-un semnal utilizabil de sistemul de control.

Servicii cloud (*cloud computing*) – Resurse de calcul, stocare, analiză și integrare furnizate printr-o infrastructură accesibilă în rețea.

Sistem ciber-fizic (CPS – *cyber-physical system*) – Sistem în care procesele fizice, calculul, comunicația și controlul sunt integrate prin bucle de măsurare și acțiune.

Sistem flexibil de fabricație (FMS – *Flexible Manufacturing System*) – Ansamblu automatizat capabil să producă o varietate definită de repere cu schimbări limitate de configurare.

Sistem reconfigurabil de fabricație (RMS – *Reconfigurable Manufacturing System*) – Sistem proiectat pentru modificarea controlată a structurii, capacității sau funcționalității sale atunci când cerințele de producție se schimbă.

Sistem în timp real (*real-time system*) – Sistem a cărui corectitudine depinde atât de rezultatul calculului, cât şi de respectarea termenului temporal asociat.

Sparkplug (*Sparkplug B*) – Specificaţie construită peste MQTT, care defineşte structura subiectelor, formatul mesajelor şi gestionarea stării dispozitivelor în aplicaţii industriale.

Tehnologie operaţională (OT – *Operational Technology*) – Ansamblu de sisteme hardware şi software care monitorizează sau controlează direct procese, echipamente şi infrastructuri fizice.

TLS (*Transport Layer Security*) – Protocol criptografic utilizat pentru autentificarea participanţilor şi protejarea confidenţialităţii şi integrităţii datelor transmise.

TSN (*Time-Sensitive Networking*) – Set de standarde IEEE 802.1 care adaugă reţelelor Ethernet sincronizare temporală, planificarea traficului şi latenţă limitată.

Trasabilitate (*traceability*) – Capacitatea de a reconstitui istoricul, localizarea şi transformările unui material, produs, lot sau ordin de producţie.

Transformare digitală (*digital transformation*) – Schimbare coordonată a proceselor, responsabilităţilor şi modelelor de operare prin utilizarea tehnologiilor şi datelor digitale.

Prefață

Cartea de față s-a născut la intersecția dintre experiența acumulată în industrie, activitatea didactică și preocuparea constantă pentru modul în care tehnologia transformă procesele, organizațiile și oamenii. Nu am ajuns la tema fabricilor inteligente și a Internetului Industrial al Lucrurilor doar prin studiul literaturii de specialitate. Am cunoscut industria mai întâi din apropierea utilajelor și a liniilor de producție, iar ulterior din perspectiva tehnicianului, inginerului, proiectantului, cercetătorului și cadrului didactic.

Lansarea acestei cărți coincide cu împlinirea a douăzeci de ani de activitate profesională. Pentru mine, acest moment reprezintă atât o bornă personală, cât și un prilej de reflecție asupra unui parcurs în care munca și studiul au evoluat împreună. Multe dintre ideile dezvoltate în paginile următoare își au originea în situații concrete întâlnite în fabrică: opriri de producție, probleme de calitate, modificări tehnice, instalarea unor echipamente, instruirea personalului sau necesitatea de a transforma datele disponibile în informații utile pentru decizie.

Primul contact cu mediul industrial a avut loc în cadrul unei companii multinaționale, unde am lucrat în timpul a două vacanțe de vară. După absolvirea liceului, m-am angajat ca operator al unui utilaj de debitare a firelor. Am trecut ulterior prin poziții de tehnician, inginer de testare electrică, inginer de producție, perioadă în care am coordonat și un proces, iar apoi inginer proiectant. Fiecare etapă mi-a oferit o perspectivă diferită asupra relației dintre oameni, echipamente, calitate, costuri și performanța proceselor industriale.

În această perioadă am colaborat cu numeroase persoane, din România și din alte țări, cu pregătiri, experiențe și caractere diferite. De la fiecare am avut ceva de învățat. Am înțeles astfel că performanța unei fabrici nu este determinată numai de nivelul tehnologic al echipamentelor sale, ci și de modul în care oamenii, procesele și informațiile funcționează împreună.

În anii în care am activat ca inginer de testare electrică și inginer de producție am avut oportunitatea de a participa la mai multe delegații în Germania. Aceste experiențe mi-au schimbat fundamental perspectiva asupra activității industriale. Am înțeles mai bine importanța standardizării, a documentării, a planificării și a responsabilității individuale. Am constatat, totodată, că transformarea unei organizații nu începe cu achiziția unei tehnologii, ci cu definirea corectă a problemelor și integrarea coerentă a soluțiilor în procesele existente.

Parcursul profesional a fost însoţit permanent de unul educaţional. După absolvirea unui profil economic, am urmat studiile de licenţă în Contabilitate şi Informatică de Gestiune şi studiile de masterat în Audit financiar. Dorinţa de a înţelege mai profund echipamentele şi procesele industriale m-a determinat să urmez apoi studiile de licenţă în domeniul Maşinilor-unelte şi masteratul în Robotică, în cadrul Universităţii Tehnice din Cluj-Napoca. Formarea mea a fost completată prin studiile psihopedagogice şi prin doctoratul în Inginerie şi management, finalizat cu calificativul Cum laude.

Pregătirea economică m-a ajutat să înţeleg întreprinderea, resursele şi procesele decizionale. Formarea inginerească mi-a oferit instrumentele necesare pentru analiza echipamentelor şi sistemelor de producţie, iar robotica şi cercetarea doctorală mi-au deschis perspectiva integrării dintre automatizare, informatică, inteligenţă artificială şi inovare. Din anul 2020, activitatea universitară mi-a oferit posibilitatea de a transforma experienţa acumulată în cunoaştere structurată şi de a o transmite mai departe.

Din această experienţă s-a conturat cartea Fabrici inteligente şi tehnologii convergente în era IIoT. Lucrarea prezintă transformarea digitală a industriei şi rolul Internetului Industrial al Lucrurilor (Industrial Internet of Things – IIoT) în dezvoltarea fabricilor inteligente. Tehnologiile nu sunt tratate izolat, ci în legătură cu structura întreprinderii, fluxurile de producţie, echipamentele de automatizare, comunicaţiile industriale, arhitecturile IIoT, securitatea cibernetică şi aplicaţiile practice.

Cartea se adresează studenţilor din domeniile inginereşti, inginerilor, tehnicienilor, managerilor şi tuturor celor care doresc să înţeleagă funcţionarea proceselor industriale moderne. Obiectivul său nu este doar transmiterea unor informaţii, ci formarea unor abilităţi durabile: capacitatea de a privi fabrica drept un sistem, de a identifica relaţiile dintre procese, de a transforma datele în informaţii relevante şi de a evalua critic soluţiile tehnologice.

La douăzeci de ani de la începutul acestui parcurs, privesc această carte ca pe o sinteză a experienţelor şi lecţiilor acumulate, dar şi ca pe un punct de plecare. Sper ca ea să îi ajute pe cititori să înţeleagă mai bine industria, să îşi dezvolte noi competenţe şi să abordeze cu încredere provocările transformării digitale. Îmi doresc să devină pentru cei aflaţi la început de drum, dar şi pentru cei care continuă să înveţe, un reper de orientare şi un far călăuzitor.

Vasile-Dragoş Bartoş

1. INTRODUCERE ÎN INTERNETUL INDUSTRIAL AL LUCRURILOR ȘI TRANSFORMAREA DIGITALĂ A INDUSTRIEI

Industria se află într-o etapă de transformare în care performanţa unei fabrici nu mai este determinată exclusiv de capacitatea mecanică a utilajelor, de viteza liniilor de producţie sau de gradul de automatizare locală. În fabricile moderne, valoarea este generată tot mai mult prin conectivitate, date, interoperabilitate şi prin capacitatea sistemelor de a susţine decizii rapide, întemeiate pe informaţii provenite din procesele reale. În acest context, Internetul industrial al lucrurilor (*Industrial Internet of Things – IIoT*), Industria 4.0 şi fabricaţia inteligentă (smart manufacturing), reprezentate în Figura 1.1, au devenit concepte de referinţă pentru modul în care sunt proiectate, operate şi optimizate sistemele industriale.

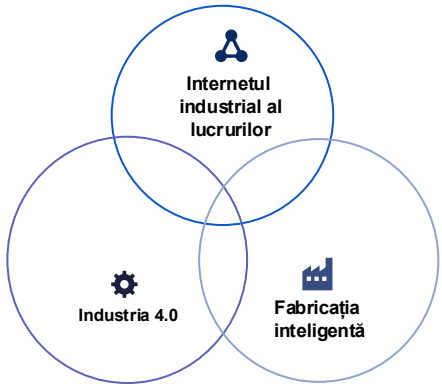


Figura 1.1 – IIoT, Industria 4.0 și fabricația inteligentă

Aplicarea acestor concepte în mediul industrial impune cerinţe ridicate privind fiabilitatea, disponibilitatea, securitatea, determinismul, integrarea echipamentelor existente şi continuitatea operaţională. Pierderea unor date, întârzierea unei comenzi sau compromiterea unei conexiuni nu reprezintă doar o problemă informatică, ci poate afecta direct calitatea produselor, siguranţa operatorilor şi disponibilitatea unei linii de producţie. Din această cauză, soluţiile preluate fără adaptare din zona aplicaţiilor destinate consumatorilor sunt rareori acceptabile într-o întreprindere de producţie (*industrial plant*).

Cele trei concepte sunt însă utilizate frecvent ca sinonime, atât în comunicarea comercială, cât şi în documentaţiile de proiect. Confuzia nu rămâne una terminologică: ea se transferă în specificaţii, în bugete şi în aşteptări, iar un proiect pornit de la premise neclare produce, de regulă, o infrastructură conectată fără efect

operațional măsurabil. Capitolul începe, prin urmare, cu delimitarea conceptelor și cu plasarea lor în evoluția sistemelor de producție, de la mecanizare la sisteme ciber-fizice.

A doua temă a capitolului o reprezintă datele privite ca resurse industriale. Într-o fabrică inteligentă, datele se adaugă materialelor, echipamentelor, timpului de lucru și energiei, dar valoarea lor nu rezultă din volumul colectat, ci din condițiile în care pot fi interpretate și utilizate. Sunt tratate distincția dintre datele disponibile și cele utilizabile, lanțul prin care ele devin acțiuni în proces, rolurile pe care le îndeplinesc de-a lungul lanțului valoric și, în final, cerințele de proprietate, responsabilitate și păstrare fără de care un ansamblu de date nu poate fi administrat pe termen lung.

A treia temă reunește beneficiile și dificultățile implementării IIoT, tratate împreună tocmai pentru că se condiționează reciproc: fiecare avantaj așteptat depinde de rezolvarea unei constrângeri tehnice, organizaționale sau economice. Discuția se încheie cu evaluarea economică a unui proiect-pilot, prezentată prin calcul explicit, deoarece decizia de a extinde sau de a opri o implementare se ia pe baza costurilor și a economiilor estimate, nu pe baza performanței tehnice în sine.

Capitolul se încheie cu un scenariu didactic de digitalizare a unei linii industriale, în care conceptele prezentate anterior sunt aplicate asupra unei situații caracteristice acestui tip de proiecte, împreună cu precizarea a ceea ce un asemenea scenariu poate și nu poate demonstra.

Capitolul stabilește astfel baza conceptuală a întregii lucrări. El răspunde la întrebările „*ce înseamnă*" și „*de ce*", în timp ce capitolele următoare tratează întrebarea „*cum*": organizarea companiei industriale și fluxul comenzii, tipurile de producție, sistemele flexibile de fabricație, dispozitivele și automatizarea, protocoalele de comunicație, arhitecturile IIoT, securitatea cibernetică și aplicațiile practice. Termenii introduși aici sunt utilizați consecvent în restul cărții, iar delimitările stabilite acum condiționează înțelegerea deciziilor tehnice discutate ulterior.

Obiectivele capitolului

La finalul acestui capitol, cititorul va putea:

- să diferențieze Internetul lucrurilor, Internetul industrial al lucrurilor, Industria 4.0, fabricația inteligentă și Industria 5.0, pe baza domeniului de aplicare, a obiectivelor urmărite și a cerințelor dominante;
- să distingă între digitizare, digitalizare și transformare digitală și să încadreze corect o intervenție industrială în categoria corespunzătoare;
- să diferențieze datele disponibile de datele utilizabile, să enumere elementele de context necesare interpretării unei valori măsurate și să descrie lanțul date–informație–decizie – acțiune;

- să identifice rolurile îndeplinite de date în etapele lanţului valoric industrial şi să stabilească cerinţele minime de proprietate, responsabilitate şi păstrare pentru un set de date industriale;
- să evalueze beneficiile şi provocările implementării IIoT şi să le asocieze cu indicatori măsurabili şi cu valori de referinţă stabilite înaintea intervenţiei;
- să calculeze costul total şi termenul de recuperare al unui proiect-pilot IIoT, pornind de la ipoteze declarate, şi să interpreteze limitele rezultatului obţinut;
- să explice rolul interoperabilităţii, al calităţii datelor, al securităţii cibernetice şi al colaborării dintre tehnologia informaţiei şi tehnologia operaţională;
- să analizeze un scenariu de digitalizare industrială şi să argumenteze necesitatea implementării graduale a unui proiect IIoT.

1.1. De la IoT la IIoT, Industria 4.0 și fabricația inteligentă

Pentru înţelegerea rolului IIoT în industria actuală este necesară plasarea acestuia în evoluţia mai amplă a sistemelor de producţie. Industria nu a devenit inteligentă printr-un salt izolat, ci prin acumularea succesivă a mai multor transformări: mecanizare, electrificare, automatizare, informatizare, conectivitate şi integrare digitală. Fiecare dintre acestea a păstrat şi a extins rezultatele etapei anterioare, ceea ce explică de ce o fabrică modernă conţine, simultan, echipamente aparţinând unor generaţii tehnologice diferite. Succesiunea acestor transformări este sintetizată în Figura 1.2.

Această coexistenţă nu este o abatere de la model, ci situaţia normală. Un utilaj pus în funcţiune în anii nouăzeci, comandat de un automat programabil fără interfaţă de reţea, funcţionează astăzi alături de o celulă robotizată recentă şi de un sistem de urmărire a producţiei care aşteaptă date de la amândouă. Orice discuţie despre fabrica inteligentă care presupune uniformitate tehnologică ratează, prin urmare, problema principală a implementării: nu construirea unui sistem nou, ci integrarea a ceea ce există deja.

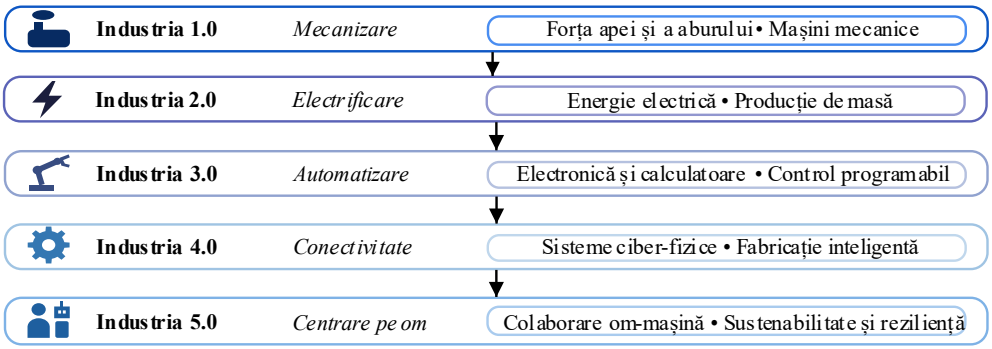


Figura 1.2 – Cronologia revoluțiilor industriale

1.1.1. De la mecanizare la sisteme ciber-fizice

Prima revoluţie industrială a fost asociată cu mecanizarea producţiei, utilizarea energiei aburului şi apariţia fabricii ca spaţiu organizat pentru producerea bunurilor. A doua revoluţie industrială a introdus electrificarea, producţia de masă şi liniile de asamblare, deplasând accentul către eficienţă, standardizare şi creşterea volumului de producţie [1].

A treia revoluţie industrială a adus automatizarea bazată pe electronică, informatică şi control programabil. Apariţia automatelor programabile (PLC-urilor), a sistemelor de comandă numerică, a roboţilor industriali şi a aplicaţiilor informatice pentru planificare şi control a permis creşterea flexibilităţii şi reducerea intervenţiei umane directe [1], [2]. Datele au devenit importante pentru procesele industriale, dar au rămas utilizate preponderent local, în bucle de reglare, în funcţii de monitorizare şi în raportări periodice. Fiecare sistem îşi administra propriile valori, iar corelarea lor între echipamente sau între departamente presupunea, de regulă, intervenţie umană.

Limitarea nu era una de capacitate de calcul, ci de accesibilitate a datelor. Informaţia exista în controler, dar nu putea fi obţinută fără efort disproporţionat: protocoale proprietare, absenţa unei referinţe comune de timp, lipsa unei identificări unitare a echipamentelor şi a loturilor. Aceasta este observaţia din care se înţelege cel mai bine ce anume schimbă etapa următoare.

A patra revoluţie industrială, asociată conceptului de Industria 4.0, a extins automatizarea prin conectarea, monitorizarea şi integrarea echipamentelor în sisteme capabile să participe la procese decizionale distribuite [3]. Termenul a fost formulat în 2011, în cadrul unei iniţiative strategice germane, şi a fost consolidat prin raportul final al grupului de lucru Industrie 4.0, care propune interconectarea sistemelor ciber-fizice, a oamenilor şi a resurselor de-a lungul întregului lanţ de valoare [4]. Analizele ulterioare au sistematizat această orientare în patru principii de proiectare: interconectarea, transparenţa informaţională, asistarea tehnică a operatorului şi descentralizarea deciziilor [5]. Modelul de arhitectură de referinţă elaborat pentru acest cadru, RAMI 4.0, ordonează aceleaşi elemente pe trei axe – nivelurile ierarhice ale întreprinderii, ciclul de viaţă al produsului şi straturile funcţionale, de la activul fizic până la funcţia de afacere [6], [7].

Elementul tehnic central al acestei etape este sistemul ciber-fizic (CPS), definit ca ansamblu în care componentele de calcul şi comunicaţie sunt integrate cu procese fizice pe care le monitorizează şi le controlează [8]. În producţie, sistemele ciber-fizice presupun existenţa unei reprezentări digitale actualizate a echipamentului sau a procesului, sincronizată cu starea reală a acestuia şi utilizabilă pentru analiză, predicţie şi decizie [9].

Construirea acestei reprezentări a fost descrisă printr-o succesiune de cinci niveluri, cunoscută ca arhitectura 5C, care indică ordinea în care capacităţile trebuie realizate: conectarea la sursa de date, conversia datelor în indicatori de stare,

constituirea imaginii coerente a echipamentului în raport cu celelalte, interpretarea rezultatelor în vederea deciziei şi, în final, reconfigurarea proceselor pe baza acestor decizii [10]. Ordinea are consecinţe practice: un nivel superior nu poate fi realizat înaintea celui inferior, iar proiectele care încep de la stratul de analiză, fără a rezolva conectarea şi calitatea datelor, produc rezultate care nu pot fi verificate. Trecerea de la automatizarea locală la sisteme ciber-fizice nu este, prin urmare, o problemă de dotare cu senzori suplimentari, ci de construire a legăturii permanente dintre proces şi modelul său informaţional. IIoT, procesarea la edge (*edge computing*), serviciile cloud, analiza datelor şi inteligenţa artificială reprezintă mijloacele prin care această legătură este realizată practic.

Industria 5.0 nu înlocuieşte Industria 4.0, ci îi adaugă o perspectivă orientată către colaborarea om–maşină, personalizare, reziliență şi sustenabilitate [11]. Formularea acestei orientări a fost determinată de constatarea că eficienţa şi gradul de automatizare nu sunt suficiente pentru a caracteriza performanţa industrială, în absenţa unor criterii privind rolul operatorului, consumul de resurse şi capacitatea de a rezista la perturbaţii [12]. Documentul de referinţă al Comisiei Europene formulează trei direcţii: centrarea pe om, sustenabilitatea şi reziliența, prima dintre ele fiind cea care are efect direct asupra proiectării sistemelor, întrucât impune ca tehnologia să fie adaptată operatorului, nu invers [11]. În robotică, această evoluţie accentuează rolul roboţilor colaborativi, al interfeţelor intuitive şi al sistemelor care sprijină operatorul uman, în locul înlocuirii lui [13]. Industria 5.0 exprimă astfel maturizarea modului în care tehnologiile digitale sunt integrate în procese industriale centrate pe valoare, siguranţă şi adaptabilitate.

1.1.2. Digitizare, digitalizare şi transformare digitală

Termenii „*digitizare*", „*digitalizare*" şi „*transformare digitală*" sunt utilizaţi frecvent ca sinonime, deşi descriu niveluri diferite de utilizare şi integrare a tehnologiilor digitale [14]. Delimitarea lor este necesară pentru înţelegerea şi proiectarea corectă a sistemelor IIoT, întrucât fiecare nivel presupune un alt efort, un alt tip de rezultat şi un alt mod de evaluare a reuşitei. Relaţia dintre cele trei concepte este sintetizată în Figura 1.3.

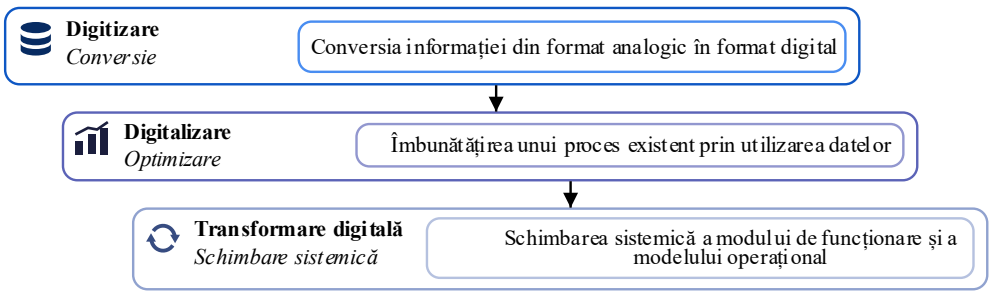


Figura 1.3 – Diferența dintre digitizare, digitalizare și transformare digitală

Digitizarea reprezintă conversia informației din format analogic în format digital. Transcrierea unei fișe de mentenanță de pe hârtie într-un fișier electronic sau conversia unui semnal analogic de temperatură într-o valoare digitală sunt exemple de digitizare. Informația devine astfel disponibilă pentru prelucrare informatică, fără ca procesul industrial să fie în mod necesar modificat. Rezultatul digitizării este un suport nou pentru aceeași informație, nu o schimbare a modului de lucru.

Digitalizarea presupune utilizarea datelor și a tehnologiilor digitale pentru îmbunătățirea unui proces existent [14]. De exemplu, colectarea automată a datelor privind temperatura, vibrațiile și consumul energetic al unui motor, afișarea acestora într-un sistem de supraveghere, control și achiziție de date (*SCADA*) și utilizarea lor pentru generarea alarmelor îmbunătățesc viteza, precizia și trasabilitatea monitorizării industriale. Procesul rămâne, în esență, același, dar se desfășoară cu mai puține intervenții manuale, cu întârzieri mai mici și cu o evidență verificabilă.

Transformarea digitală (TD) implică schimbarea modului de funcționare a organizației sau a sistemului industrial prin integrarea tehnologiilor digitale în procese, decizii și modele operaționale [15]. Datele sunt corelate cu obiectivele de producție, calitate, mentenanță, consum energetic și logistică. Un sistem IIoT poate anticipa defecțiuni, poate susține ajustarea parametrilor procesului, poate transmite unui sistem de execuție a fabricației (*MES*) informații despre desfășurarea producției și poate furniza indicatori pentru fundamentarea deciziilor. Analizele dedicate acestui nivel arată că elementul definitoriu nu este tehnologia utilizată, ci modificarea modului în care organizația creează și livrează valoare [16].

Distincția are consecințe practice imediate, pentru că fiecare nivel se verifică altfel. Un proiect definit ca digitizare se evaluează prin completitudinea și acuratețea datelor transferate în format electronic. Unul de digitalizare se evaluează prin performanța procesului îmbunătățit: durata unei operații, numărul de erori de transcriere, întârzierea cu care o abatere devine vizibilă. Unul de transformare digitală se evaluează prin modificarea indicatorilor operaționali și prin schimbarea efectivă a modului de organizare a activității. Formularea unui obiectiv de transformare digitală și evaluarea lui prin criterii de digitizare reprezintă una dintre cauzele frecvente ale nemulțumirii față de rezultatele proiectelor de acest tip.

Încadrarea corectă poate fi exersată pe situații concrete. Înlocuirea registrului de opriri completat pe hârtie cu un formular electronic pe o tabletă este digitizare – se schimbă suportul, nu procesul. Preluarea automată a opririlor din automatul programabil, clasificarea lor pe cauze și afișarea într-un tablou de bord actualizat continuu este digitalizare – același proces de urmărire a opririlor se desfășoară mai repede și mai exact. Utilizarea acelorași date pentru a decide ordinea intervențiilor de mentenanță, pentru a modifica planul de producție și pentru a renegocia termenele cu clientul reprezintă transformare digitală – se schimbă cel care decide, pe baza a ce și în ce moment. Aceeași infrastructură tehnică poate susține oricare dintre cele trei niveluri; ceea ce le deosebește este utilizarea, nu echipamentul.

Cele trei niveluri nu constituie o ierarhie de valoare, ci o succesiune de condiții. Nu există transformare digitală fără date disponibile în format digital și fără procese care le folosesc, iar ordinea este dictată de dependența dintre ele, nu de ambiția proiectului. Studiile privind adoptarea tehnologiilor din Industria 4.0 arată că întreprinderile care obțin rezultate consistente construiesc întâi stratul de conectare și de calitate a datelor și abia apoi funcțiile analitice și decizionale [17].

Deși în limba română termenul „*digitalizare*" este folosit frecvent ca termen general, care acoperă toate cele trei niveluri, este necesar ca într-un caiet de sarcini sau într-o specificație de proiect, unde imprecizia se transferă direct în obligațiile părților, să folosim termenii corecți, utilizați în sensul delimitat mai sus.

Simpla conectare a unor echipamente sau instalarea unor senzori suplimentari nu reprezintă transformare digitală și nu garantează existența unei fabrici inteligente. Valoarea este generată atunci când datele sunt contextualizate, corelate, analizate și utilizate pentru fundamentarea deciziilor operaționale sau strategice, aspect dezvoltat în secțiunea 1.2.

1.1.3. Internetul Lucrurilor și Internetul Industrial al Lucrurilor

Internetul lucrurilor (IoT) desemnează ansamblul obiectelor fizice echipate cu senzori, elemente de execuție, procesoare și interfețe de comunicație, capabile să colecteze și să transmită date prin intermediul rețelelor digitale [18]. Definiția normativă îl descrie ca o infrastructură globală care permite servicii avansate prin interconectarea obiectelor fizice și virtuale, pe baza tehnologiilor de informație și comunicație existente și în curs de dezvoltare [19], [20]. Aplicațiile uzuale se regăsesc în locuințe inteligente, dispozitive purtabile, transport urban, agricultură și servicii publice, unde accentul este pus frecvent pe confort, automatizare, eficiență energetică și servicii personalizate [21].

Internetul industrial al lucrurilor (IIoT) aplică același principiu în mediul industrial, dar introduce cerințe mai stricte privind fiabilitatea, disponibilitatea, securitatea, determinismul și continuitatea operațională [22]. Într-o fabrică, un senzor conectat poate participa la supravegherea unui proces critic, iar un gateway industrial (*industrial gateway*) poate filtra, agrega, securiza și transmite date către sisteme SCADA, MES, *sisteme de planificare a resurselor întreprinderii (ERP)* sau servicii cloud. Analizele de specialitate subliniază că elementul definitoriu al IIoT nu este conectarea în sine, ci integrarea acesteia în sisteme cu consecințe directe asupra siguranței fizice și a continuității producției [23]. Poziționarea IoT și IIoT în raport cu Industria 4.0 și fabricația inteligentă este ilustrată în Figura 1.4.

Diferența dintre IoT și IIoT poate fi evidențiată prin compararea unei locuințe inteligente cu o linie de producție automatizată. Într-o locuință, întârzierea cu câteva secunde a datelor transmise de un senzor de temperatură are, de regulă, consecințe minore. Într-o linie industrială, întârzierea, pierderea sau interpretarea

eronată a datelor privind temperatura, vibrațiile ori presiunea poate conduce la rebuturi, opriri neplanificate sau riscuri privind siguranța.

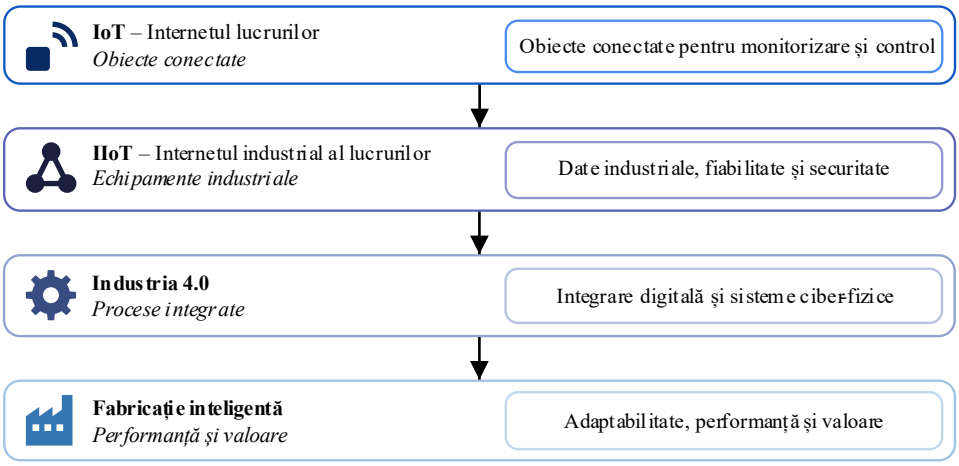


Figura 1.4 – Poziționarea IoT–IIoT–Industria 4.0 – Fabricație inteligentă

Deosebirea devine măsurabilă atunci când este exprimată prin cerințe. Buclele de reglare din automatizarea de proces operează la timpi de ciclu de ordinul zecilor de milisecunde, iar comanda coordonată a axelor sau sincronizarea mișcării impun timpi de livrare a mesajelor sub o milisecundă, cu abatere de sincronizare controlată; clasele de performanță pentru comunicația industrială în timp real sunt definite normativ tocmai pentru a face aceste cerințe verificabile [24]. O aplicație IoT destinată consumatorului nu formulează niciuna dintre aceste cerințe, pentru că nicio funcție a ei nu depinde de respectarea unui termen.

A doua deosebire privește ierarhia obiectivelor de securitate. În *tehnologia informației (IT)*, ordinea consacrată este confidențialitate, integritate, disponibilitate. În mediile de *tehnologie operațională (OT)*, ordinea se inversează: disponibilitatea procesului și integritatea datelor de proces devin criterii dominante, iar confidențialitatea, deși importantă, este subordonată acestora [25]. Inversarea nu este o preferință organizatorică, ci decurge din consecințele fizice ale unei opriri. Ea explică de ce practici curente în informatică – actualizarea automată a componentelor software, repornirea unui echipament pentru aplicarea unei corecții, blocarea preventivă a unui trafic suspect – nu pot fi transferate necondiționat într-o facilitate de producție (fabrică), unde aceleași acțiuni pot opri o linie sau pot lăsa un proces într-o stare nesigură. Consecințele acestei inversări pentru proiectarea măsurilor de protecție sunt tratate în capitolul 8.

Un al treilea element diferențiator este durata de viață a echipamentelor. Instalațiile industriale funcționează frecvent zece până la douăzeci de ani sau mai mult,

iar înlocuirea lor este condiționată de amortizarea investiției și de continuitatea producției. În consecință, o arhitectură IIoT trebuie proiectată pentru coexistența cu echipamente existente, care utilizează protocoale, formate de date și interfețe eterogene, și nu poate presupune uniformitatea tehnologică specifică rețelelor informatice de birou [26]. Această constrângere are un nume consacrat în practică: integrarea în fabrica existentă, spre deosebire de proiectarea unei instalații noi. Cea dintâi este situația obișnuită, iar costul principal al unui proiect IIoT provine, de regulă, din ea.

În consecință, IIoT trebuie tratat ca o infrastructură industrială critică, nu ca o simplă extindere a aplicațiilor IoT destinate consumatorilor. Alegerea componentelor și a protocoalelor de comunicație trebuie să țină seama de latență, fiabilitate, securitate, interoperabilitate și compatibilitate cu infrastructura existentă, cerințe esențiale pentru integrarea IT cu OT. Aceste criterii sunt reluate și dezvoltate în subcapitolul 6.4, la alegerea protocolului, și în capitolul 8, la tratarea securității.

1.1.4. Industria 4.0, fabricația inteligentă și Industria 5.0

Industria 4.0 reprezintă cadrul conceptual și strategic al transformării digitale industriale [3], [4]; în cadrul acesteia, IIoT furnizează infrastructura necesară conectării echipamentelor și colectării datelor, iar sistemele ciber-fizice, analiza datelor, inteligența artificială, procesarea la edge și serviciile cloud contribuie la transformarea datelor în informații și decizii. Arhitecturile de referință elaborate pentru acest domeniu tratează explicit separarea dintre nivelul echipamentelor, nivelul de conectivitate și nivelul aplicațiilor de întreprindere, tocmai pentru ca fiecare să poată evolua independent [27].

Cei doi termeni care descriu rezultatul, Industria 4.0 și fabricația inteligentă, provin din tradiții diferite și nu sunt interschimbabili. Primul s-a format în spațiul european, ca politică industrială, și pune accentul pe integrarea verticală și orizontală a lanțului de valoare. Al doilea s-a format în spațiul nord-american și asiatic, ca program tehnic, și pune accentul pe utilizarea datelor în conducerea proceselor de fabricație [28], [29]. Diferența se reflectă și în peisajul de standarde asociat fiecăruia, sistematizat în inventarele dedicate domeniului [30]. Cunoașterea acestei distincții este utilă practic: documentația unui furnizor european și cea a unui furnizor american descriu adesea aceeași funcționalitate în vocabulare diferite.

Fabricația inteligentă reprezintă aplicarea acestor principii în sistemele de producție [29]. O fabrică inteligentă nu este definită prin existența roboților, a senzorilor sau a aplicațiilor informatice, ci prin integrarea lor într-un sistem coerent. Echipamentele comunică, datele proceselor sunt disponibile în timp real, deciziile sunt susținute prin analiză, iar producția poate fi adaptată în funcție de cerere, calitate, disponibilitatea resurselor și starea echipamentelor [28], [31].

Cele două concepte se completează: *Industria 4.0 oferă direcția și principiile*, iar *fabricația inteligentă reprezintă sistemul de producție rezultat și folosirea concretă*

a datelor pentru conducerea proceselor [32]. Diferența are consecințe practice; un proiect Industria 4.0 pornește de la strategia organizației și se evaluează pe termen lung; unul de fabricație inteligentă urmărește indicatori de producție, calitate, mentenanță și consum, evaluați în luni. Confuzia poate duce la un eșec previzibil: unei investiții strategice i se cer, după punerea în funcțiune, rezultate operaționale pentru care nu a fost concepută.

Industria 5.0 completează acest model prin orientarea explicită către colaborarea om–mașină, reziliență și sustenabilitate. După cum s-a arătat în secțiunea 1.1.1, aceasta nu înlocuiește Industria 4.0, ci extinde utilizarea tehnologiilor digitale către sisteme industriale centrate pe om și pe crearea sustenabilă a valorii [11]. Pentru proiectarea tehnică, orientarea are consecințe verificabile: interfețele sunt evaluate și după efortul cognitiv impus operatorului, arhitecturile sunt evaluate și după comportamentul în regim degradat, iar soluțiile sunt evaluate și după consumul de resurse pe durata întregului ciclu de viață.

Principalele diferențe dintre conceptele analizate sunt sintetizate în Tabelul 1.1.

Relația dintre aceste concepte poate fi sintetizată astfel: IoT oferă principiul general al obiectelor conectate; IIoT îl adaptează cerințelor mediului industrial; Industria 4.0 asigură cadrul transformării digitale; fabricația inteligentă aplică aceste principii în producție; iar Industria 5.0 adaugă orientarea către om, reziliență și sustenabilitate. Elementul comun al tuturor acestor concepte este informația (datele), motiv pentru care rolul ei în lanțul valoric industrial constituie obiectul subcapitolului următor.

Tabelul 1.1 – Comparație între IoT, IIoT, Industria 4.0, fabricația inteligentă și Industria 5.0

Concept	Domeniu principal	Obiectiv	Exemple	Cerințe dominante
IoT	Aplicații generale, consum și servicii	Conectarea obiectelor și colectarea datelor	Locuințe inteligente, dispozitive purtabile, orașe inteligente	Conectivitate, cost redus, ușurință în utilizare
IIoT	Industrie, producție, energie și logistică	Monitorizare, control și optimizare industrială	Senzori industriali, PLC, SCADA, gateway-uri industriale, servicii cloud	Fiabilitate, securitate, disponibilitate, integrare OT–IT
Industria 4.0	Strategie industrială și transformare digitală	Integrarea sistemelor ciber-fizice și a datelor	Fabrică inteligentă, geamăn digital, inteligență artificială industrială	Interoperabilitate, date în timp real, automatizare adaptivă
Fabricația inteligentă	Aplicarea practică în fabricație	Producție flexibilă, eficientă și orientată către date	Linie de ambalare conectată, mentenanță predictivă, control digital al calității	Flexibilitate, trasabilitate, analiză și decizie rapidă
Industria 5.0	Industrie centrată pe om, rezilientă și sustenabilă	Integrarea tehnologiei cu nevoile operatorului și ale societății	Roboți colaborativi, producție personalizată, procese industriale reziliente	Siguranță, centrare pe om, sustenabilitate, reziliență

1.2. Rolul datelor în lanțul valoric industrial

Într-o fabrică tradiţională, valoarea este asociată în principal cu materialele, echipamentele, timpul de lucru, energia consumată şi produsele obţinute. Într-o fabrică inteligentă, acestor resurse li se adaugă datele, care descriu starea echipamentelor, condiţiile procesului, consumurile, calitatea produselor, timpii de ciclu, opririle, comenzile, loturile şi traseele materialelor [32].

Datele nu dobândesc valoare industrială prin simpla lor colectare. Pentru a deveni utile, acestea trebuie validate, contextualizate, interpretate şi corelate cu un obiectiv operaţional. În cadrul IIoT, datele brute sunt transformate în informaţii, informaţiile susţin decizii, iar deciziile determină acţiuni în procesul industrial.

Din această perspectivă, datele pot fi considerate o materie primă digitală. Asemenea unei resurse fizice, acestea trebuie colectate, transportate, filtrate, prelucrate şi integrate într-un flux de valoare. Analogia are însă trei limite care trebuie precizate, pentru că fiecare dintre ele schimbă modul de proiectare a sistemului. Datele nu se consumă prin utilizare, ceea ce face ca aceeaşi valoare colectată o singură dată să poată servi simultan mai multe scopuri. Costul lor principal nu este cel al achiziţiei, ci cel al menţinerii calităţii şi al integrării, iar acest cost se manifestă continuu, nu la punerea în funcţiune [33]. În sfârşit, spre deosebire de un material, o dată se depreciază prin trecerea timpului: o valoare de proces veche de o oră poate fi lipsită de utilitate pentru o decizie de reglare, deşi rămâne perfect utilizabilă pentru o analiză de tendinţă.

Senzorii, automatele programabile, sistemele SCADA, gateway-urile industriale şi platformele digitale susţin obiective operaţionale: reducerea opririlor neplanificate, creşterea calităţii, optimizarea consumului energetic, asigurarea trasabilităţii şi îmbunătăţirea deciziilor de producţie. Subcapitolul structurează transformarea datelor în patru etape: îndeplinirea condiţiilor de utilizare, conversia în acţiuni, îndeplinirea rolurilor în lanţul valoric şi stabilirea regulilor de proprietate, responsabilitate şi păstrare, indispensabile administrării ansamblului.

1.2.1. Date disponibile şi date utilizabile

O distincţie fundamentală în proiectarea sistemelor IIoT este cea dintre date disponibile şi date utilizabile (Figura 1.5). Datele disponibile sunt valorile care pot fi colectate dintr-un sistem: semnale provenite de la senzori, stări ale echipamentelor, alarme, parametri ai procesului, comenzi, timpi de funcţionare sau consumuri. Acestea pot fi accesate prin intermediul automatelor programabile, al sistemelor SCADA, al protocoalelor industriale sau al aplicaţiilor informatice.

Existenţa unei date nu garantează însă posibilitatea utilizării sale. De exemplu, valoarea 72,5 poate reprezenta o temperatură, o presiune, o viteză, un procent de încărcare, o umiditate relativă sau un indicator calculat. În absenţa contextului, aceasta nu poate fundamenta în siguranţă o decizie industrială.

O dată devine utilizabilă atunci când este însoţită de elementele necesare interpretării:

- *eticheta şi sursa*, care indică variabila măsurată şi echipamentul de proveniență;
- *marca temporală*, care precizează momentul achiziției;
- *unitatea de măsură*, care permite interpretarea corectă a valorii;
- *calitatea datei*, care indică dacă valoarea este validă, estimată, incertă, indisponibilă sau afectată de o eroare.

Aceste patru atribute nu constituie o convenţie didactică, ci reproduc structura utilizată efectiv de protocoalele industriale moderne. În OPC UA, orice valoare citită dintr-un nod este transmisă împreună cu un cod de stare care exprimă calitatea şi cu mărci temporale distincte pentru momentul achiziției la sursă şi pentru cel al transmiterii de către server [34]. Existența unei mărci temporale (*timestamp*) generate la sursă este esențială atunci când datele provenite de la echipamente diferite trebuie corelate: fără o referință de timp comună, o alarmă şi cauza ei pot apărea în ordine inversă în înregistrare. Sincronizarea ceasurilor între dispozitivele unei rețele industriale se realizează prin protocoale dedicate, care asigură abateri de ordinul microsecundelor şi fac astfel posibilă compararea evenimentelor provenite din surse diferite [35].

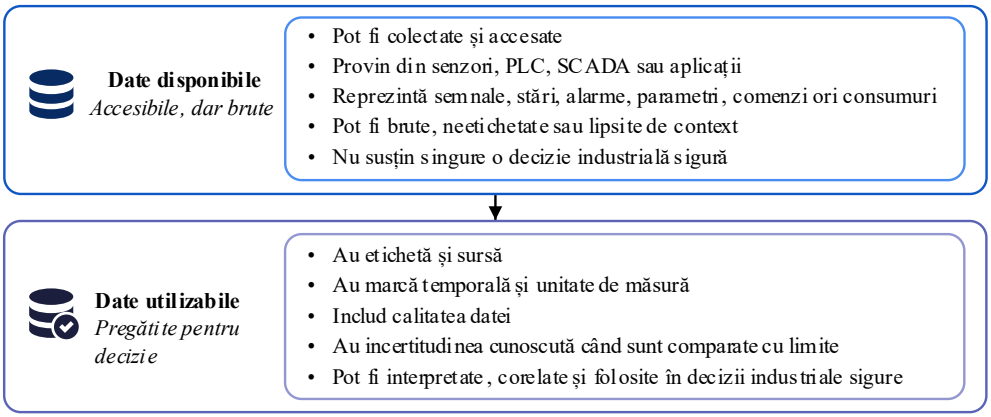


Figura 1.5 – Date disponibile versus date utilizabile

Astfel, valoarea 72,5 devine relevantă dacă este identificată drept temperatura motorului Motor_01, exprimată în grade Celsius, înregistrată la un moment cunoscut şi validată ca fiind de calitate bună. În această formă, ea poate fi comparată cu limitele admise, utilizată pentru calcularea unei tendinţe sau transmisă unei aplicaţii de monitorizare ori mentenanţă.

Un al cincilea element este necesar atunci când valoarea urmează să fie comparată cu o limită sau folosită într-o decizie de acceptare: incertitudinea de măsurare. O temperatură raportată ca 72,5 °C de un traductor cu eroare admisă de ±1,5 °C nu

permite afirmația că limita de 73 °C a fost respectată. Ghidurile de metrologie tratează exprimarea incertitudinii ca parte inseparabilă a rezultatului măsurării, nu ca informație suplimentară opțională [36]. În practica industrială, incertitudinea nu însoțește fiecare valoare transmisă, ci este consemnată în documentația punctului de măsurare; important este ca ea să fie cunoscută atunci când se stabilesc pragurile de alarmare, altfel sistemul generează alarme false sau, dimpotrivă, ratează depășiri reale.

Literatura privind calitatea datelor extinde această listă cu dimensiuni relevante pentru utilizarea industrială: acuratețea, completitudinea, consecvența, actualitatea și accesibilitatea [37], [38]. Fiecare dintre ele corespunde unui mod concret de eșec. O valoare exactă, dar transmisă cu întârziere, nu mai poate susține o decizie de reglare. O serie completă, dar cu unități neuniforme între echipamente, produce comparații false. O valoare corectă, dar inaccesibilă aplicației care ar avea nevoie de ea, rămâne fără efect operațional. Aceste moduri de eșec sunt sintetizate în Figura 1.6.

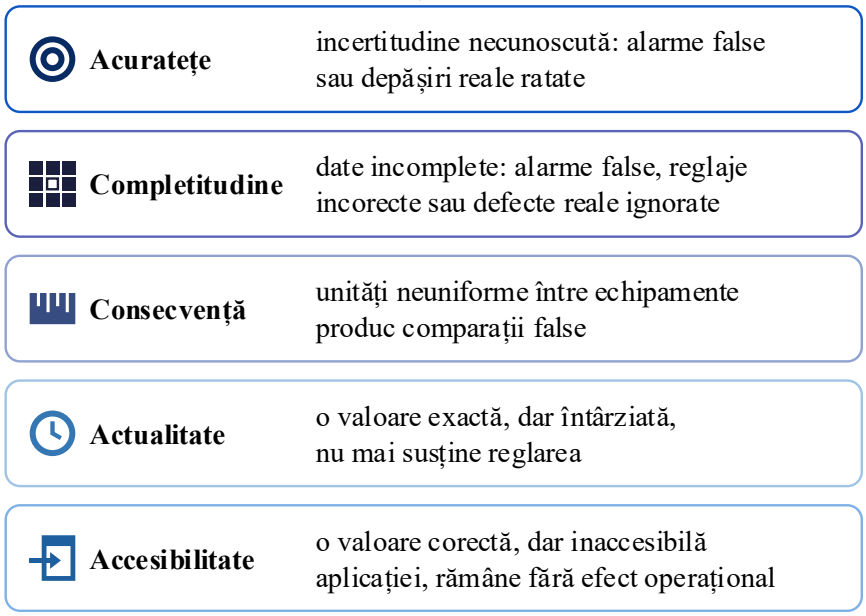


Figura 1.6 – Moduri de eșec asociate dimensiunilor calității datelor

Datele incomplete sau interpretate greșit pot conduce la alarme false, reglaje incorecte, opriri inutile ori ignorarea unor defecte reale. Costul acestor erori nu este proporțional cu numărul valorilor afectate, ci cu importanța deciziei pe care au influențat-o: o singură marcă temporală eronată într-un lot analizat pentru o neconformitate poate invalida întreaga investigație. Prin urmare, una dintre funcțiile esențiale ale infrastructurii IIoT este transformarea datelor disponibile în date

utilizabile, capabile să susțină decizii și acțiuni sigure. Modul concret în care această transformare este realizată prin structura mesajelor transmise este tratat în subcapitolul 6.2, iar componentele care o execută sunt descrise în subcapitolele 5.3 și 5.4.

1.2.2. Lanțul date – informație – decizie – acțiune

Rolul datelor în IIoT poate fi explicat printr-un lanț logic format din patru etape: date, informație, decizie și acțiune. Modelul are ca origine ierarhia date–informație–cunoaștere din teoria sistemelor informaționale [39], [40], adaptată aici prin adăugarea etapei finale de acțiune, care este specifică mediului industrial: într-o fabrică, valoarea nu se realizează în momentul înțelegerii unei situații, ci în momentul intervenției asupra procesului.

Datele brute provin din senzori, elemente de execuție, automate programabile, sisteme SCADA, roboți industriali, echipamente de măsurare și aplicații informatice. În această formă, ele pot fi fragmentate, distribuite și dependente de sistemele care le generează.

Prin contextualizare, filtrare, agregare și comparare cu limitele stabilite sau cu valorile istorice, datele sunt transformate în informații. De exemplu, o temperatură măsurată devine relevantă atunci când este analizată în raport cu regimul de funcționare, nivelul de încărcare și istoricul echipamentului. Sistemul poate identifica astfel o funcționare normală, o tendință de supraîncălzire sau o posibilă anomalie.

Informațiile obținute susțin luarea unei decizii de către un operator, un inginer, un sistem expert sau o aplicație automată. Decizia poate conduce la declanșarea unei alarme, ajustarea parametrilor procesului, programarea unei intervenții de mentenanță ori modificarea ritmului de producție.

Valoarea industrială este realizată prin acțiunea rezultată: reglarea procesului, oprirea controlată a unui echipament, emiterea unui ordin de lucru, reducerea consumului energetic, respingerea unui produs neconform sau actualizarea planului de producție.

Aplicarea lanțului asupra unui caz concret arată ce se produce la fiecare trecere. Un traductor de vibrații montat pe lagărul unui motor furnizează o valoare eficace a vitezei de vibrație, exprimată în milimetri pe secundă, împreună cu marca temporală și indicatorul de calitate: acestea sunt datele. Comparată cu domeniile de evaluare stabilite pentru clasa de mașini respectivă și corelată cu regimul de funcționare și cu istoricul propriu al echipamentului, valoarea devine o caracterizare a stării – funcționare acceptabilă, degradare incipientă sau condiție inacceptabilă; aceasta este informația [41]. Compararea cu evoluția din ultimele săptămâni și cu pragurile stabilite intern conduce la decizia de a programa o intervenție la următoarea oprire planificată, în locul unei opriri imediate. Acțiunea este emiterea ordinului de lucru, alocarea piesei de schimb și modificarea corespunzătoare a planului de producție. Standardele dedicate monitorizării stării descriu această succesiune

ca pe un proces cu etape distincte: achiziţia datelor, prelucrarea, detecţia stării, evaluarea sănătăţii, prognoza şi, în final, recomandarea acţiunii [42], [43].

Cerinţele temporale determină distribuirea funcţiilor în arhitectură: reglarea procesului operează în milisecunde, local, în automatul programabil; detectarea degradării utilizează ore sau zile de date istorice; planificarea producţiei vizează schimbul sau săptămâna. Condiţionarea unei acţiuni de siguranţă de răspunsul unui serviciu extern constituie o alocare greşită a funcţiei şi o eroare de proiectare. Funcţiile critice, interblocările şi siguranţa se execută permanent local, prin componente dedicate, evaluate conform cerinţelor aplicabile de siguranţă funcţională. Infrastructura IIoT îndeplineşte funcţiile de colectare, stocare, analiză şi vizualizare a datelor [44], [45]. Distribuirea pe niveluri este detaliată în secţiunea 7.3.3.

O a doua proprietate este că lanţul se poate întrerupe în oricare dintre punctele sale, iar întreruperea are efect identic: absenţa rezultatului operaţional. Un sistem care colectează date fără a le contextualiza se opreşte la prima etapă. Unul care produce rapoarte pe care nimeni nu le utilizează se opreşte la a doua. Unul în care alarmele sunt generate corect, dar nu există o procedură de intervenţie asociată, se opreşte la a treia. Ultima situaţie este cea mai frecventă şi cea mai costisitoare, pentru că sistemul pare să funcţioneze: alarmele apar, sunt confirmate de operator şi sunt închise fără nicio acţiune asupra procesului. Practica de proiectare a sistemelor de alarmare tratează explicit acest risc, cerând ca fiecare alarmă configurată să aibă un destinatar, un timp disponibil pentru reacţie şi o acţiune posibilă; o alarmă care nu îndeplineşte aceste condiţii trebuie eliminată, nu tolerată [46], [47].

Verificarea continuităţii acestui lanţ constituie, în practică, un criteriu util de evaluare a unui proiect IIoT înainte de extinderea lui. Întrebarea de control nu este ce date se colectează, ci ce decizie se ia altfel decât înainte şi cine o ia.

1.2.3. Datele în lanţul valoric industrial

Lanţul valoric industrial transformă resursele în produse sau servicii cu valoare pentru client [48]. Acesta cuprinde proiectarea, ofertarea, planificarea, aprovizionarea, producţia, controlul calităţii, mentenanţa şi logistica, urmate de livrare, asistenţă tehnică şi valorificarea informaţiilor post-vânzare. Figura 1.7. ilustrează relaţia dintre transformarea datelor şi etapele acestui lanţ.

Datele au roluri specifice în fiecare etapă a lanţului. În *proiectare şi industrializare*, susţin analiza cerinţelor produsului, simularea proceselor, estimarea costurilor şi definirea parametrilor tehnologici. În *planificare şi aprovizionare*, permit alocarea resurselor, programarea comenzilor, estimarea capacităţii şi corelarea necesarului de materiale cu disponibilitatea echipamentelor şi a personalului. În *producţie*, descriu în timp real timpii de ciclu, parametrii tehnologici, stările echipamentelor, alarmele, consumurile şi cantităţile realizate. În *controlul calităţii*, asigură trasabilitatea şi corelează neconformităţile cu loturile, echipamentele, sculele, operatorii şi condiţiile procesului. În *mentenanţă*, vibraţiile, temperatura, curentul

absorbit, presiunea, numărul de cicluri şi istoricul alarmelor pot indica degradarea progresivă a echipamentelor. În *logistică şi livrare*, susţin gestionarea depozitelor, urmărirea comenzilor, optimizarea transportului şi trasabilitatea produselor până la client. În *asistenţa tehnică şi etapa post-vânzare*, sprijină îmbunătăţirea produselor, optimizarea mentenanţei şi dezvoltarea de servicii noi.

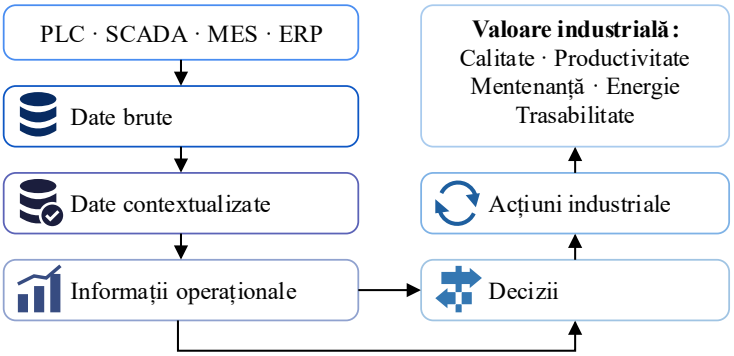


Figura 1.7 – Lanțul valoric industrial

Aceste roluri nu sunt independente; aceeaşi valoare colectată o singură dată poate fi utilizată în etape diferite şi în scopuri diferite. Durata unui ciclu de prelucrare susţine în producţie urmărirea ritmului, în calitate corelarea cu abaterile dimensionale, în mentenanţă identificarea creşterii lente a timpului de execuţie ca indiciu al uzurii, iar în planificare actualizarea normelor de timp. Reutilizarea aceleiaşi date în mai multe scopuri constituie principalul argument economic al unei arhitecturi IIoT integrate, comparativ cu soluţiile punctuale, în care fiecare aplicaţie îşi colectează separat propriile valori. Diferenţa nu este de cost al senzorilor, ci de cost al integrării: patru achiziţii separate ale aceleiaşi mărimi înseamnă patru puncte de măsurare de întreţinut, patru definiţii posibil divergente şi patru surse care se pot contrazice în faţa aceleiaşi întrebări.

Reutilizarea presupune însă o condiţie care nu este întotdeauna îndeplinită: identificarea consecventă a obiectelor la care datele se referă. Un lot, un echipament sau un produs trebuie să poarte acelaşi identificator în sistemul de producţie, în cel de calitate şi în cel de logistică, altfel corelarea nu poate fi realizată automat, iar trasabilitatea rămâne parţială. Modelul ISA-95 stabileşte structurile de informaţie schimbate între sistemele de conducere a producţiei şi cele de gestiune a întreprinderii, tocmai pentru a asigura corespondenţa dintre obiectele descrise la niveluri diferite [49]. Standardele privind indicatorii de performanţă în producţie tratează aceeaşi cerinţă din perspectiva măsurării, definind atât modul de calcul al indicatorilor, cât şi elementele de date pe baza cărora aceştia se determină [50], [51]. În schimburile dintre organizaţii, unde identificatorii interni nu mai sunt recunoscuţi, aceeaşi funcţie este îndeplinită de sistemele de identificare standardizate pentru produse, unităţi logistice şi locaţii [52].

Consecinţa practică este că decizia privind identificatorii se ia la începutul proiectului, nu la final. Un identificator de lot introdus după punerea în funcţiune nu poate fi aplicat retroactiv datelor deja colectate, iar istoricul acumulat între timp rămâne neutilizabil: valorile există, dar nu pot fi legate de obiectele la care se referă. Aceasta este una dintre puţinele decizii de proiectare din IIoT care nu admit corecţie ulterioară fără pierdere.

Datele creează astfel o legătură între etapele lanţului valoric. Informaţiile obţinute în producţie şi în exploatarea produselor pot reveni către proiectare şi planificare, contribuind la evitarea problemelor recurente şi la îmbunătăţirea continuă a produselor şi proceselor [32]. Această buclă de întoarcere este cea care deosebeşte un sistem de raportare de un sistem de îmbunătăţire: în primul caz datele descriu ce s-a întâmplat, în al doilea ele modifică modul în care se va lucra ulterior. Ea presupune însă o condiţie organizatorică, nu tehnică – existenţa unui moment stabilit în care rezultatele sunt analizate şi a unei persoane responsabile de transformarea concluziei în modificare de proces. În absenţa acestui mecanism, bucla rămâne deschisă, indiferent de calitatea infrastructurii.

Lanţul valoric nu se încheie, prin urmare, la livrarea produsului, ci se extinde asupra întregului ciclu de viaţă al acestuia. Modul în care aceste fluxuri se reflectă în structura organizatorică a unei companii industriale şi în parcursul concret al unei comenzi este tratat în capitolul 2. Secţiunea următoare tratează condiţiile în care ansamblul de date astfel constituit poate fi administrat pe termen lung.

1.2.4. Proprietatea, responsabilitatea şi păstrarea datelor industriale

Un ansamblu de date industriale supravieţuieşte proiectului care l-a creat. Echipamentul monitorizat rămâne în funcţiune zece sau douăzeci de ani, personalul se schimbă, furnizorul platformei poate fi înlocuit, iar valorile acumulate îşi păstrează utilitatea numai dacă se ştie în continuare ce reprezintă, cui aparţin şi cine răspunde de ele. Aceste întrebări nu sunt administrative: ele determină dacă istoricul acumulat va putea fi folosit peste cinci ani sau va deveni un volum de valori neinterpretabile.

Proprietatea – datele generate de procesul de producţie aparţin organizaţiei care exploatează instalaţia, dar această afirmaţie trebuie transformată în clauze verificabile în contractele cu furnizorii de echipamente şi de servicii. Trei elemente se stabilesc înainte de punerea în funcţiune: dreptul de acces al furnizorului la datele colectate şi scopul în care le poate utiliza, dreptul organizaţiei de a exporta integral datele proprii într-un format documentat şi situaţia datelor la încetarea contractului. Al doilea element este cel mai frecvent omis, deşi distincţia dintre portabilitatea datelor şi portabilitatea aplicaţiilor este tratată explicit în documentele normative: posibilitatea de a exporta un fişier nu înseamnă că structura, contextul şi relaţiile dintre valori se transferă odată cu el [53]. Consecinţele practice ale acestei distincţii pentru alegerea unei platforme sunt tratate în secţiunea 7.4.6.

Responsabilitatea – guvernanța datelor presupune atribuirea explicită a trei roluri distincte pentru fiecare domeniu de date – proces, calitate, mentenanță, energie [54], [55]. Proprietarul domeniului decide ce se colectează, cu ce nivel de detaliu și cine are acces; este, de regulă, responsabilul funcției care utilizează datele, nu un specialist informatic. Responsabilul de date răspunde de definiții, de unități, de reguli de validare și de consecvența identificatorilor; el este cel care stabilește ce înseamnă exact „oprire neplanificată" și menține această definiție neschimbată în timp. Administratorul tehnic asigură funcționarea infrastructurii de colectare, stocare și acces. Confuzia dintre aceste roluri produce o situație recunoscută cu ușurință în practică: nimeni nu poate răspunde de ce doi indicatori care ar trebui să coincidă arată valori diferite.

Datele cu caracter personal – o parte dintre datele colectate în producție identifică persoane: operatorul care a executat o operație, cel care a confirmat un control, cel care a închis o alarmă. Din momentul în care o valoare de proces poate fi asociată unei persoane identificabile, prelucrarea intră sub incidența reglementării europene privind protecția datelor, cu obligațiile aferente privind temeiul prelucrării, minimizarea datelor, durata păstrării și informarea persoanelor vizate [56]. Soluția uzuală nu este renunțarea la trasabilitate, ci separarea nivelurilor: identificatorul persoanei se păstrează acolo unde este necesar pentru trasabilitate, iar analizele de performanță se realizează pe date agregate sau pseudonimizate. Utilizarea datelor de producție pentru evaluarea individuală a personalului este o decizie distinctă, care depinde de temeiul legal și de dialogul social, nu de disponibilitatea tehnică a informației.

Păstrarea – datele industriale au trei orizonturi de utilizare, cu cerințe diferite. Orizontul operațional acoperă zile sau săptămâni, cu rezoluție completă, și susține reglarea, alarmarea și analiza incidentelor recente. Orizontul analitic acoperă luni sau ani, de regulă cu date agregate, și susține analiza tendințelor, mentenanța bazată pe stare și evaluarea îmbunătățirilor. Orizontul de conformitate este impus din exterior – de reglementări sectoriale, de cerințe contractuale sau de obligații de garanție – și fixează atât durata minimă, cât și forma în care înregistrările trebuie să rămână lizibile și verificabile [57].

Decizia critică este cea de agregare, pentru că este ireversibilă. Trecerea de la valori la interval de o secundă la medii pe cinci minute reduce volumul de stocare cu peste două ordine de mărime, dar elimină definitiv posibilitatea de a analiza ulterior un fenomen tranzitoriu: un vârf de curent, o oscilație scurtă a presiunii, o abatere de câteva secunde care explică un rebut. Regula practică este ca rezoluția completă să fie păstrată pentru mărimile asociate echipamentelor critice și pentru intervalele care conțin evenimente – alarme, opriri, schimbări de lot – iar agregarea să se aplice regimului de funcționare normală.

Documentația – elementul care leagă toate cele de mai sus este registrul punctelor de măsurare, întocmit la punerea în funcțiune și actualizat la fiecare modificare. Pentru fiecare mărime colectată, acesta consemnează: identificatorul, echipamentul-sursă, semnificația în limbaj clar, unitatea de măsură, domeniul și incertitudinea, frecvența de achiziție, regula de validare, orizontul de păstrare,

proprietarul domeniului și aplicațiile care o utilizează. Registrul este un document de câteva pagini pentru un proiect-pilot și singurul instrument prin care semnificația datelor supraviețuiește schimbărilor de personal. Absența lui este cauza obișnuită a situației în care un istoric de câțiva ani nu mai poate fi folosit, pentru că nimeni nu mai poate spune cu certitudine ce reprezintă fiecare serie.

1.3. Beneficii și provocări în implementarea IIoT

Implementarea IIoT poate îmbunătăți performanța industrială prin conectarea echipamentelor, integrarea datelor și utilizarea informațiilor în procesele decizionale.

Rezultatele nu sunt însă generate automat de tehnologie, ci depind de alegerea unor obiective clare, de calitatea datelor, de compatibilitatea cu infrastructura existentă și de capacitatea organizației de a transforma informațiile obținute în acțiuni [17]. Studiile privind adoptarea tehnologiilor din Industria 4.0 arată că beneficiile și barierele se manifestă simultan și că întreprinderile care obțin rezultatele așteptate sunt, de regulă, cele care au tratat explicit constrângerile înainte de extinderea soluției [58].

Subcapitolul tratează cele două laturi împreună și se încheie cu evaluarea economică, pentru că decizia de a continua sau de a opri o implementare se ia comparând beneficiile estimate cu costul total, nu apreciind separat fiecare latură. Echilibrul dintre avantajele urmărite și constrângerile care condiționează obținerea lor este ilustrat în Figura 1.8.

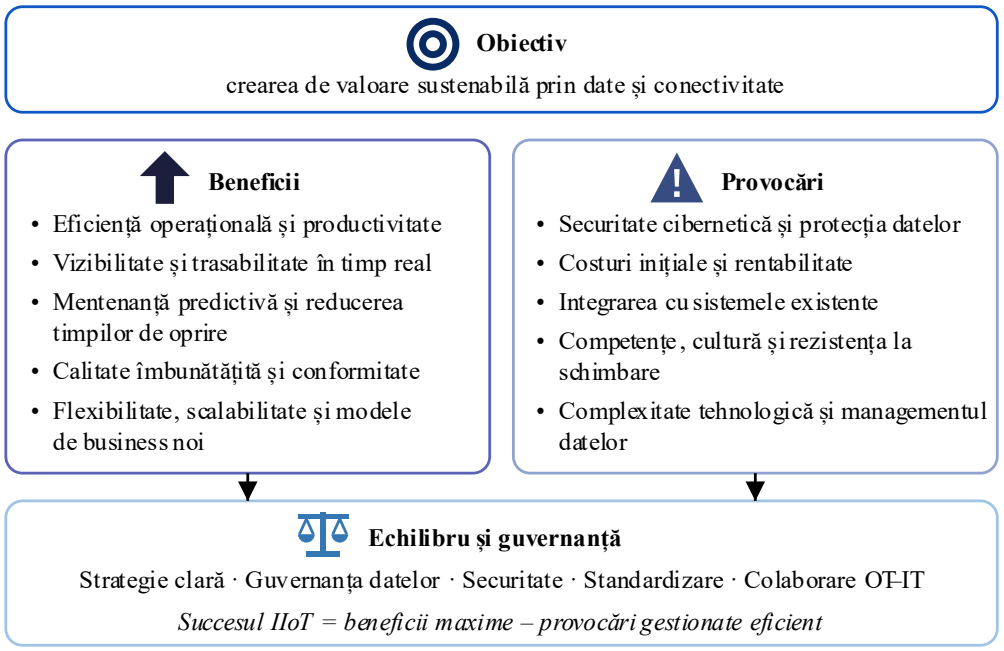


Figura 1.8 – Balanța implementării IIoT

1.3.1. Beneficii operaționale și strategice

Unul dintre principalele beneficii ale IIoT este creșterea vizibilității asupra proceselor industriale. Monitorizarea stării echipamentelor, a parametrilor tehnologici, a consumurilor și a producției realizate permite identificarea rapidă a abaterilor și fundamentarea deciziilor pe date actualizate. Managementul și personalul tehnic pot urmări astfel performanța proceselor fără a depinde exclusiv de rapoarte întocmite manual sau de observații izolate.

Disponibilitatea echipamentelor poate fi îmbunătățită prin identificarea timpurie a degradării și prin planificarea intervențiilor de mentenanță. Datele privind vibrațiile, temperatura, curentul absorbit, numărul de cicluri și istoricul alarmelor permit trecerea graduală de la mentenanța reactivă la cea preventivă și, ulterior, la mentenanța bazată pe stare și predictivă [59], [60]. Deosebirea dintre ultimele două este relevantă pentru proiectare, pentru că ele cer date diferite: mentenanța bazată pe stare declanșează intervenția la depășirea unui prag măsurat și necesită doar valoarea curentă, comparată cu o limită; mentenanța predictivă estimează durata de funcționare rămasă pe baza evoluției istorice și necesită serii lungi, consecvente, însoțite de evidența intervențiilor executate [61], [62]. A doua nu poate fi realizată fără prima, iar organizațiile care încearcă să o atingă direct constată, de regulă, că nu dispun de istoricul necesar antrenării niciunui model.

IIoT contribuie și la îmbunătățirea calității și a trasabilității. Corelarea parametrilor procesului cu loturile de materiale, echipamentele, operatorii și rezultatele controlului permite identificarea cauzelor neconformităților. Abaterile pot fi detectate înainte de acumularea unui volum mare de produse neconforme, iar istoricul digital facilitează analiza problemelor și demonstrarea respectării cerințelor de fabricație, inclusiv în domeniile în care aceasta este impusă prin reglementări. Efectul cel mai vizibil nu este creșterea nivelului de calitate în sine, ci reducerea drastică a timpului necesar investigării unei neconformități: identificarea loturilor afectate și a condițiilor în care au fost fabricate devine o interogare, nu o reconstituire.

Monitorizarea detaliată a consumurilor permite identificarea pierderilor de energie, a funcționării în gol și a utilizării ineficiente a resurselor. Datele pot evidenția diferențe între echipamente, schimburi de lucru, produse sau regimuri de funcționare și pot susține măsuri de reducere a consumurilor fără afectarea calității ori a capacității de producție. Un sistem de management al energiei presupune tocmai existența unei baze de măsurare care să permită stabilirea consumului de referință și verificarea efectului măsurilor aplicate [63], [64]. Fără această bază, o reducere observată nu poate fi separată de variația volumului de producție sau de sezonalitate.

La nivel strategic, integrarea datelor din producție, mentenanță, calitate și logistică sprijină adaptarea mai rapidă la schimbarea comenzilor și a condițiilor de funcționare. Organizația poate evalua mai precis capacitatea disponibilă, poate urmări comenzile și poate coordona resursele pe baza situației reale din fabrică, nu pe baza unei imagini reconstituite ulterior.

Pentru ca aceste beneficii să poată fi demonstrate, proiectele IIoT trebuie asociate cu indicatori măsurabili, precum disponibilitatea echipamentelor, durata

opririlor, rata produselor neconforme, consumul specific de energie, timpul de ciclu, eficacitatea globală a echipamentelor (OEE) sau respectarea termenelor de livrare [51], [65]. Condiţia esenţială este stabilirea valorilor de referinţă înainte de implementare: în absenţa unei situaţii iniţiale măsurate, îmbunătăţirea nu poate fi separată de variaţia normală a procesului sau de efectul altor intervenţii desfăşurate în aceeaşi perioadă. La fel de importantă este fixarea definiţiilor de calcul odată cu valorile de referinţă – ce intervale intră în timpul planificat, care opriri se clasifică drept planificate, cum se tratează schimbările de reper – pentru că o valoare de referinţă calculată după alte reguli decât valoarea finală produce o îmbunătăţire aparentă care nu există. Modul de calcul al indicatorului OEE şi efectul acestor convenţii asupra rezultatului sunt tratate numeric în secţiunile 4.4.5 şi 7.2.3.

Compararea rezultatelor implementării cu valorile iniţiale arată contribuţia reală a soluţiei şi justifică extinderea acesteia. Secţiunea 1.3.3 explică modul în care comparaţia susţine decizia de investiţie.

1.3.2. Provocări tehnice, organizaționale și economice

Una dintre principalele provocări tehnice ale implementării IIoT este integrarea echipamentelor existente. Fabricile utilizează frecvent utilaje provenite de la furnizori diferiţi, instalate în perioade distincte şi bazate pe protocoale, formate de date şi interfeţe incompatibile. Înlocuirea simultană a acestora este rareori justificată economic, ceea ce impune utilizarea gateway-urilor industriale, a convertoarelor de protocol şi a mecanismelor de interoperabilitate [26]. Interoperabilitatea nu se rezumă la posibilitatea transmiterii datelor între sisteme, ci presupune şi interpretarea identică a semnificaţiei acestora, condiţie pe care modelele informaţionale standardizate încearcă să o asigure [49], [66]. Distincţia este operaţională: două sisteme pot schimba corect octeţi şi, în acelaşi timp, să atribuie înţelesuri diferite aceleiaşi valori – „*piese realizate*" poate include sau exclude reprelucrările, iar rezultatul nu este semnalat de niciun mecanism de comunicaţie.

O parte dintre echipamentele existente nu expun nicio interfaţă de date utilizabilă. În aceste situaţii, soluţiile practicate sunt achiziţia indirectă – măsurarea curentului absorbit pentru deducerea stării de funcţionare, contorizarea pieselor prin senzor extern, citirea semnalelor de la lămpile de semnalizare – sau intercalarea unui modul de intrări-ieşiri paralel cu comanda existentă. Aceste metode nu modifică programul automatului şi nu intervin în funcţiile de siguranţă, dar au precizie limitată şi trebuie declarate ca atare în registrul punctelor de măsurare, întrucât un timp de funcţionare dedus din consumul de curent nu are aceeaşi calitate cu unul raportat direct de controler.

Infrastructura de comunicaţii trebuie să asigure transmiterea fiabilă a datelor în condiţiile specifice mediului industrial. Latenţa, pierderea pachetelor, interferenţele, indisponibilitatea reţelei sau sincronizarea necorespunzătoare pot afecta monitorizarea şi controlul proceselor [22]. Mediul industrial adaugă constrângeri absente în reţelele de birou: perturbaţii electromagnetice generate de convertoare de frecvenţă şi de comutaţii de putere, temperaturi şi vibraţii care depăşesc condiţiile de utilizare ale echipamentelor comerciale, cerinţe de imunitate stabilite normativ

[67]. Arhitectura trebuie, de asemenea, proiectată pentru extindere, astfel încât adăugarea unor echipamente, puncte de măsurare sau aplicaţii să nu necesite restructurarea integrală a sistemului. Dimensionarea cantitativă a acestor cerinţe – bugetul de latenţă pe traseul datelor şi necesarul de lăţime de bandă – este tratată în secţiunile 3.3.5 şi 6.3.4.

Calibrarea necorespunzătoare a senzorilor, mărcile temporale incorecte, valorile lipsă, unităţile neuniforme şi absenţa contextului compromit calitatea datelor şi pot genera concluzii eronate (secţiunea 1.2.1). Proiectul IIoT impune reguli de validare, contextualizare, păstrare şi utilizare, cu responsabilităţi explicite (secţiunea 1.2.4). Controlul calităţii este continuu: dereglarea senzorilor şi modificarea echipamentelor necesită verificări, iar schimbările neconsemnate ale definiţiilor invalidează comparaţiile istorice.

Conectarea sistemelor de producţie extinde suprafaţa expusă ameninţărilor cibernetice. Dispozitivele insuficient protejate, configuraţiile implicite, actualizările necontrolate şi conexiunile dintre reţelele OT şi IT pot introduce vulnerabilităţi cu efect direct asupra continuităţii şi siguranţei proceselor [25]. Securitatea trebuie integrată încă din etapa de proiectare, nu adăugată după punerea în funcţiune, iar cerinţele aplicabile sunt formulate pe zone funcţionale şi pe niveluri de securitate [68]. Pentru fabricanţii şi integratorii de produse industriale conectate, cerinţele au devenit şi obligaţii legale: regulamentul european privind cerinţele orizontale de securitate cibernetică pentru produsele cu elemente digitale impune securitatea pe durata ciclului de viaţă, gestionarea vulnerabilităţilor şi raportarea incidentelor [69]. Regulamentul a intrat în vigoare la 10 decembrie 2024; obligaţiile de raportare se aplică din 11 septembrie 2026, iar ansamblul cerinţelor, din 11 decembrie 2027. Măsurile tehnice şi cadrele de referinţă sunt tratate în subcapitolul 8.3, iar obligaţiile de reglementare ale Uniunii Europene, în secţiunea 8.3.9.

Provocările organizaţionale sunt generate de modificarea proceselor, a responsabilităţilor şi a modului de luare a deciziilor. Implementarea IIoT necesită colaborarea dintre specialiştii în automatizări, tehnologia informaţiei, mentenanţă, producţie, calitate şi management. Separarea rigidă dintre aceste funcţii poate conduce la soluţii tehnic corecte, dar insuficient corelate cu necesităţile operaţionale. Diferenţa de priorităţi dintre echipele IT şi OT, semnalată în secţiunea 1.1.3, se manifestă practic în decizii curente privind actualizările, accesul de la distanţă şi ferestrele de intervenţie, iar rezolvarea ei presupune reguli convenite în prealabil, nu arbitraje punctuale.

Deficitul de competenţe poate limita utilizarea sistemului după finalizarea implementării [70]. Personalul trebuie să înţeleagă atât procesul industrial, cât şi elementele de comunicaţie, prelucrare a datelor şi securitate. Formarea utilizatorilor şi implicarea operatorilor încă din etapa de definire a cerinţelor reduc rezistenţa la schimbare şi facilitează integrarea soluţiei în activitatea curentă. Un aspect subestimat este modul în care sistemul este perceput de operatori: dacă datele colectate sunt utilizate vizibil pentru evaluarea individuală a performanţei, calitatea raportărilor manuale asociate – clasificarea cauzelor de oprire, confirmarea

intervenţiilor – se degradează rapid, iar sistemul îşi pierde tocmai informaţia pe care nu o poate obţine automat.

Din perspectivă economică, costurile nu se limitează la achiziţia senzorilor şi a aplicaţiilor. Acestea includ integrarea, modernizarea reţelelor, licenţele, stocarea datelor, securitatea, mentenanţa, formarea personalului şi actualizarea periodică a componentelor [71]. Alegerea unor soluţii închise poate genera, în plus, dependenţă faţă de un anumit furnizor şi poate limita extinderea ulterioară, motiv pentru care utilizarea protocoalelor şi a formatelor deschise reprezintă un criteriu de selecţie cu efect pe termen lung. Structura detaliată a acestor costuri şi modul de calcul al termenului de recuperare sunt tratate în secţiunea următoare.

Reducerea acestor riscuri necesită definirea unor obiective măsurabile şi implementarea graduală a soluţiei. Un proiect-pilot bine delimitat, aplicat unei linii sau unui grup restrâns de echipamente, permite verificarea arhitecturii, a calităţii datelor şi a beneficiilor înaintea extinderii, cu un cost al eventualei corecţii mult mai redus. Etapele acestei abordări sunt sintetizate în Figura 1.9.

IIoT trebuie abordat, prin urmare, ca un proces de transformare organizaţională şi tehnologică, nu ca o achiziţie izolată de echipamente şi aplicaţii.

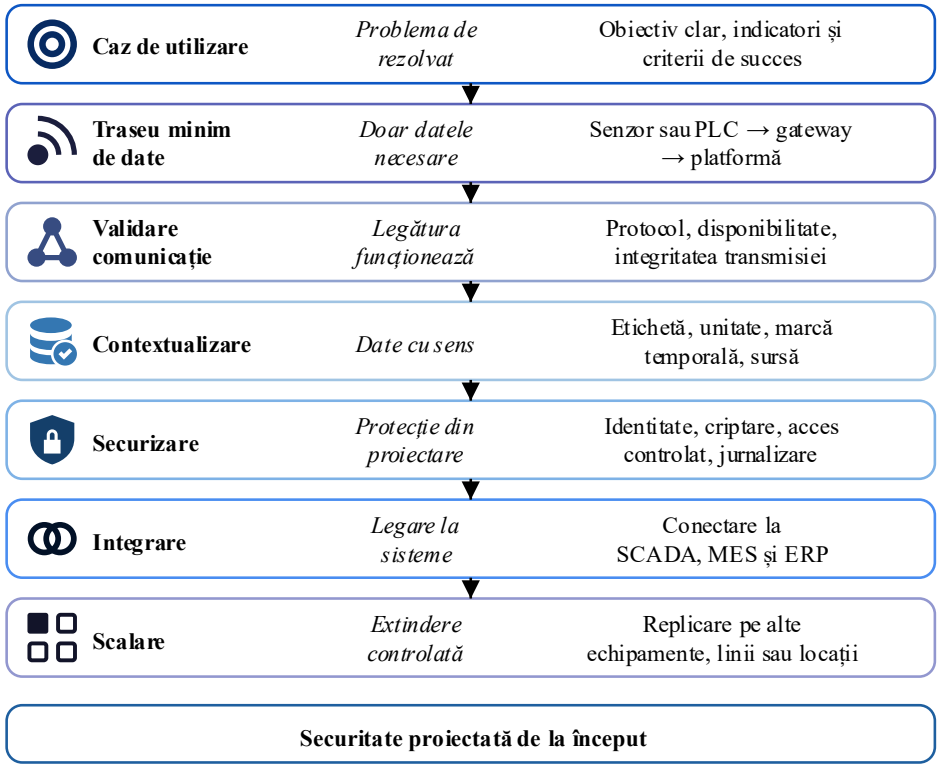


Figura 1.9 – Implementarea graduală a unui proiect IIoT

1.3.3. Evaluarea economică a unui proiect-pilot IIoT

Decizia de a extinde sau de a opri o implementare nu se ia pe baza performanţei tehnice, ci comparând beneficiile estimate cu costul total. Metoda este cea a analizei economice inginereşti, aplicată aici în cea mai simplă formă utilă: costul total pe durata de viaţă, beneficiul anual net, termenul simplu de recuperare şi valoarea actualizată netă [72], [73].

Calculul de mai jos este un ***scenariu didactic***. Valorile sunt ipoteze de lucru, alese pentru a face raţionamentul verificabil; ele nu provin dintr-o măsurare şi nu descriu o instalaţie reală. Ceea ce trebuie reţinut este structura calculului şi sensibilitatea rezultatului, nu cifrele.

Datele de intrare – se consideră o linie de ambalare care funcţionează în două schimburi, 230 de zile pe an, cu 3.680 de ore de timp planificat de producţie. Ipotezele declarate sunt prezentate în Tabelul 1.2.

Marja de contribuţie, nu cifra de afaceri, este mărimea corectă pentru evaluarea unei ore de oprire: veniturile neîncasate sunt însoţite de costuri variabile care nu se mai produc.

Tabelul 1.2 – Ipotezele de lucru ale evaluării economice

Mărime	Valoare	Unitate
Timp planificat de producție	3.680	h/an
Ponderea opririlor neplanificate	6	% din timpul planificat
Marja de contribuție pierdută pe oră de oprire	180	€/h
Producție anuală	420.000	piese/an
Rata produselor neconforme	1,8	%
Cost unitar al unui rebut	2,10	€/piesă
Consum energetic al liniei	310.000	kWh/an
Preț mediu al energiei electrice	0,145	€/kWh
Rata de actualizare	10	%/an
Orizont de analiză	5	ani

Beneficiile anuale estimate – beneficiul anual brut se obţine prin însumarea reducerilor estimate, fiecare exprimată în aceeaşi unitate monetară:

$$B = \Sigma\,(\Delta i \times vi)$$

unde Δi este reducerea estimată a pierderii de tip i, iar vi este valoarea unitară asociată.

Opriri neplanificate. Pierderea actuală: 3.680 h × 6 % = 220,8 h/an, adică 220,8 × 180 = 39.744 €/an. La o reducere estimată de 15 %, beneficiul este 0,15 × 39.744 = 5.962 €/an.

Rebuturi. Pierderea actuală: 420.000 × 1,8 % = 7.560 piese/an, adică 7.560 × 2,10 = 15.876 €/an. La o reducere estimată de 10 %, beneficiul este 1.588 €/an.

Energie. Costul actual: 310.000 × 0,145 = 44.950 €/an. La o reducere estimată de 4 %, beneficiul este 1.798 €/an.

Beneficiul anual brut este, prin urmare, B = 5.962 + 1.588 + 1.798 = 9.348 €/an.

Costurile – structura investiției inițiale și a costurilor anuale de exploatare este prezentată în Tabelul 1.3.

Componentele software ale stivei sunt deschise, deci nu generează cost de achiziție, dar generează cost de suport și de administrare. Ponderea dominantă a investiției – 9.500 € din 17.520 €, adică 54 % – revine muncii de integrare, formare și documentare, nu echipamentelor.

Indicatorii. Beneficiul anual net rezultă din diferența dintre beneficiul brut și costul anual de exploatare:

$$Bnet = B - Cop = 9.348 - 4.450 = 4.898 \text{ €/an}$$

Termenul simplu de recuperare este raportul dintre investiția inițială și beneficiul anual net:

$$T = I / Bnet = 17.520 / 4.898 = 3,58 \text{ ani}$$

Valoarea actualizată netă, calculată la o rată de actualizare de 10 % pe un orizont de cinci ani, cu factorul de anuitate 3,7908, este:

$$VAN = Bnet \times 3,7908 - I = 4.898 \times 3,7908 - 17.520 = 18.567 - 17.520 = 1.047 \text{ €}$$

Tabelul 1.3 – Structura costurilor proiectului-pilot

Element	Investiție inițială (€)	Cost anual (€)
Instrumentație: 6 puncte de măsurare (vibrații, temperatură, energie, contorizare)	2.520	–
Gateway industrial și modul de intrări-ieșiri	1.900	–
Comutator industrial administrabil, cablare, tablou	1.400	–
Calculator industrial pentru procesarea la edge	2.200	–
Integrare, configurare, punere în funcțiune (120 h × 55 €/h)	6.600	–
Formare (6 persoane × 2 zile)	1.800	–
Documentație, registrul punctelor de măsurare, teste de recepție (20 h × 55 €/h)	1.100	–
Suport software și actualizări	–	900
Stocare și administrare a datelor	–	600
Mentenanța instrumentației, verificări metrologice	–	700
Timp intern de administrare (0,05 din norma unui inginer)	–	2.250
Total	17.520	4.450

Interpretarea. Pilotul are o rentabilitate marginală: recuperare în circa trei ani și jumătate și valoare actualizată netă aproape nulă. Justificarea investiției presupune extinderea pe alte linii. Costul dominant, integrarea, este suportat o singură dată; infrastructura de colectare, baza de date, tablourile de bord, convențiile de denumire și competențele dobândite sunt reutilizabile pentru fiecare linie adăugată ulterior.

Pentru o a doua linie comparabilă, costul marginal cuprinde instrumentația (2.520 €), gateway-ul (1.900 €), integrarea redusă la 40 h × 55 €/h (2.200 €) și instruirea suplimentară (300 €), în total 6.920 €, cu un cost anual suplimentar de

circa 1.200 €. Beneficiul net marginal devine 9.348 − 1.200 = 8.148 €/an, iar termenul de recuperare 6.920 / 8.148 = 0,85 ani, adică zece luni.

Extins la cinci linii, ansamblul înseamnă o investiție de 17.520 + 4 × 6.920 = 45.200 € și un beneficiu net anual de 4.898 + 4 × 8.148 = 37.490 €/an, cu un termen de recuperare de 1,21 ani și o valoare actualizată netă de 37.490 × 3,7908 − 45.200 = 96.917 €. Aceasta este forma corectă a argumentului economic al unui proiect IIoT: pilotul cumpără informația necesară deciziei de extindere, iar rentabilitatea se realizează la scară.

Sensibilitatea – rezultatul depinde aproape integral de o singură ipoteză. Dacă reducerea opririlor neplanificate este de 8 % în loc de 15 %, beneficiul brut scade la 6.567 €/an, beneficiul net la 2.117 €/an, termenul de recuperare al pilotului urcă la 8,3 ani, iar valoarea actualizată netă devine negativă: 2.117 × 3,7908 − 17.520 = −9.495 €. Proiectul care părea acceptabil devine, la o modificare de șapte puncte procentuale a unei estimări, o pierdere. Din acest motiv, orice evaluare de acest tip se prezintă cu un interval, nu cu o valoare unică, iar reducerea opririlor se măsoară în perioada-pilot, nu se presupune.

Limitele calculului – rezultatul obținut trebuie citit împreună cu următoarele restricții:

- beneficiile sunt estimări, nu măsurători; ele devin verificabile numai prin comparație cu valorile de referință stabilite înaintea implementării, conform secțiunii 1.3.1;
- reducerea opririlor produce valoare doar dacă linia este strangulare și dacă există cerere pentru capacitatea eliberată; pe o linie care lucrează sub capacitate, aceeași reducere nu generează venit suplimentar, ci doar timp neutilizat, iar marja de contribuție nu se aplică;
- îmbunătățirea observată nu se datorează exclusiv sistemului, ci include efectul analizei zilnice a opririlor și al atenției sporite acordate liniei, care însoțesc de regulă implementarea;
- îmbunătățirea observată nu se datorează exclusiv sistemului, ci include efectul analizei zilnice a opririlor și al atenției sporite acordate liniei, care însoțesc de regulă implementarea;
- calculul ignoră costurile de oportunitate ale personalului intern implicat și eventualele întreruperi ale producției în perioada de punere în funcțiune;
- termenul simplu de recuperare nu ține seama de valoarea în timp a banilor și nu trebuie folosit singur; el este util pentru comparație rapidă, iar valoarea actualizată netă pentru decizie;
- valoarea informațională a pilotului – reducerea incertitudinii pentru decizia de extindere – nu apare în niciunul dintre cei doi indicatori, deși este, adesea, principalul lui rezultat.

1.4. Scenariu didactic privind digitalizarea industrială

Pentru aplicarea conceptelor prezentate în acest capitol este analizat un **scenariu didactic** privind digitalizarea unei linii industriale. Acesta nu descrie o companie reală și nu prezintă rezultate experimentale, ci reunește elemente caracteristice proiectelor IIoT de dimensiune medie, într-o formă care permite urmărirea deciziilor de proiectare. Valorile numerice utilizate sunt ipoteze de lucru, alese pentru a face raționamentul verificabil, nu măsurători.

Scenariul este construit astfel încât să parcurgă întregul lanț tratat în subcapitolele anterioare: identificarea problemei operaționale, stabilirea datelor necesare, contextualizarea acestora, transformarea lor în informații și în decizii și, în final, evaluarea rezultatului prin indicatori. Transformarea propusă, de la echipamente automatizate local la un sistem IIoT integrat, este ilustrată în Figura 1.10.

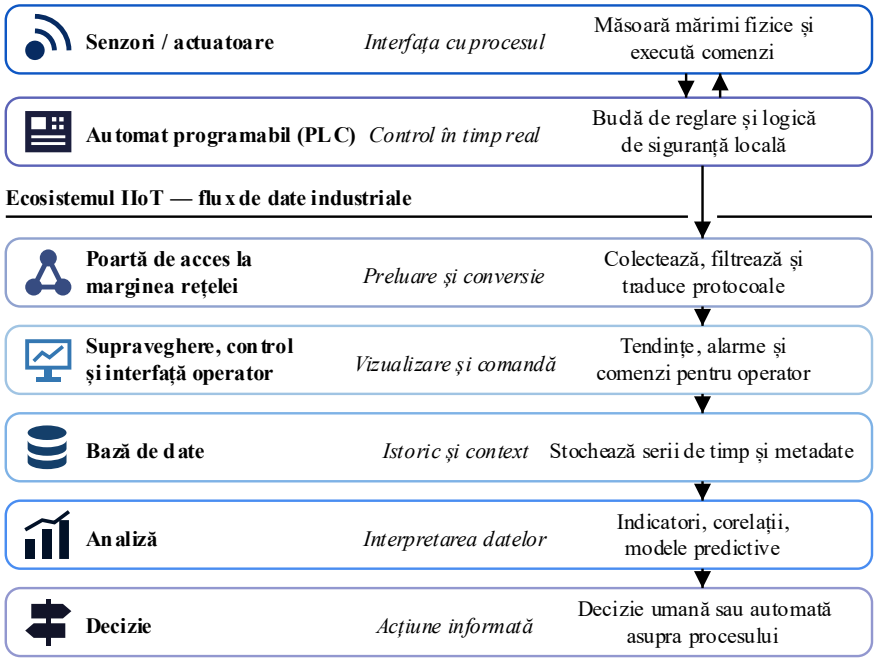


Figura 1.10 – Digitalizarea unei linii industriale: de la echipament local la ecosistem IIoT

1.4.1. Contextul inițial și obiectivele proiectului

Se consideră o fabrică de dimensiune medie care produce componente ambalate individual pentru clienți industriali. Fabrica include o zonă de alimentare cu semifabricate, o linie de prelucrare, o stație de verificare dimensională, o zonă de ambalare și un depozit temporar. Producția este organizată pe loturi, în două schimburi.

Echipamentele sunt automatizate local, dar slab integrate informațional. Automatele programabile provin din perioade diferite, fiecare utilaj având propria interfață de operare. Opririle, rebuturile și mentenanța se înregistrează manual, datele de calitate se introduc periodic într-un fișier, iar consumul energetic se monitorizează doar pe secție.

Deficiențele inițiale sunt: vizibilitate redusă asupra procesului, trasabilitate incompletă a loturilor, mentenanță predominant reactivă, monitorizare energetică insuficientă și colaborare IT–OT limitată. Circulația datelor între utilaje, operatori, mentenanță, calitate și conducere este incoerentă. Lipsa contextului, a mărcii temporale comune și a identificării consecvente a loturilor face datele disponibile în echipamente în mare parte neutilizabile, conform distincției din secțiunea 1.2.1.

Consecințele se pot formula în termeni verificabili. Durata medie necesară pentru a stabili cauza unei neconformități este de câteva zile, pentru că presupune confruntarea unui registru de opriri completat manual cu un fișier de calitate și cu memoria operatorilor din schimbul respectiv.

Clasificarea cauzelor de oprire diferă între schimburi, întrucât nu există o listă convenită. Consumul energetic nu poate fi atribuit unui utilaj sau unui produs, ci doar secției, ceea ce face imposibilă identificarea pierderilor. Niciuna dintre aceste probleme nu este de natură tehnologică în sens strict: toate provin din absența contextului și a identificatorilor comuni.

Proiectul de digitalizare urmărește:

- creșterea vizibilității asupra stării liniei de producție;
- reducerea timpului de reacție la opriri și alarme;
- corelarea loturilor cu parametrii procesului și rezultatele controlului calității;
- monitorizarea condițiilor de funcționare ale echipamentelor critice;
- urmărirea consumului energetic pe zone și utilaje;
- constituirea unei baze de date pentru analize ulterioare;
- păstrarea stabilității sistemului de control existent.

Fiecărui obiectiv i se asociază, încă din această etapă, un indicator și o valoare de referință măsurată înainte de intervenție, conform cerinței formulate în secțiunea 1.3.1. Fără această asociere, evaluarea ulterioară a proiectului rămâne o apreciere calitativă, iar extinderea soluției nu poate fi justificată economic. Corespondența este redată în Tabelul 1.4.

Punctul de pornire al proiectului nu este, prin urmare, alegerea unei platforme, ci identificarea problemelor industriale, a indicatorilor care trebuie îmbunătățiți și a datelor necesare pentru fundamentarea soluției. Ordinea inversă – selectarea tehnologiei înaintea definirii problemei – conduce frecvent la sisteme corect instalate, dar fără efect operațional, situație descrisă în secțiunea 1.1.2 drept confuzie între digitizare și transformare digitală.

Tabelul 1.4 – Obiectivele proiectului, indicatorii asociați și modul de măsurare a situației inițiale

Obiectiv	Indicator	Modul de stabilire a valorii de referință
Vizibilitate asupra liniei	Ponderea timpului de funcționare pentru care există date înregistrate automat	Inventarul punctelor de măsurare existente, înainte de intervenție
Reacție la opriri și alarme	Durata medie de la apariția opririi până la începerea intervenției	Măsurare pe patru săptămâni, cu înregistrare manuală controlată
Trasabilitate	Ponderea loturilor pentru care parametrii de proces pot fi reconstituiți integral	Verificare pe un eșantion de loturi din ultimele trei luni
Starea echipamentelor critice	Numărul opririlor neplanificate cauzate de defecte mecanice	Extras din registrul de mentenanță, ultimele douăsprezece luni
Consum energetic	Consum specific, exprimat în kWh la o mie de piese	Facturi și producție realizată, ultimele douăsprezece luni
Bază de date pentru analiză	Durata medie de investigare a unei neconformități	Măsurare pe ultimele zece neconformități documentate

1.4.2. Arhitectura şi traseul datelor

Soluţia reutilizează senzorii, elementele de execuţie, automatele programabile, interfeţele HMI şi sistemele locale de control. Astfel, reduce costurile şi păstrează reglarea şi siguranţa independente de disponibilitatea infrastructurii noi. Se adaugă senzori şi gateway-uri industriale care convertesc protocoalele, filtrează şi agregă datele, apoi le transmit controlat.

Traseul datelor cuprinde patru niveluri. La nivelul echipamentului, valorile sunt achiziţionate de automatul programabil şi utilizate local pentru comandă, interblocări şi alarme. La nivelul gateway-ului industrial, ele sunt citite fără a interveni în programul de comandă, li se ataşează contextul necesar interpretării şi sunt convertite într-un format unitar. La nivelul de agregare, datele sunt stocate, corelate între utilaje şi puse la dispoziţia aplicaţiilor. La nivelul aplicaţiilor, sunt calculaţi indicatorii, sunt analizate opririle şi sunt urmărite calitatea şi consumurile.

Separarea acestor niveluri respectă principiul enunţat în secţiunea 1.2.2: funcţiile critice, interblocările şi siguranţa rămân locale, iar infrastructura adăugată este utilizată exclusiv pentru colectare, stocare, analiză şi vizualizare. O întrerupere a legăturii către nivelurile superioare determină pierderea vizibilităţii şi a analizei, nu pierderea controlului asupra procesului. Sensul citirii este, de asemenea, unic: în această etapă, gateway-ul citeşte din automatul programabil, dar nu scrie în el. Orice scriere dinspre nivelurile superioare către controler introduce o cale prin care o defecţiune sau un acces neautorizat poate afecta procesul şi se tratează separat, cu măsurile din capitolul 8. Cerinţa de independenţă se verifică explicit la punerea în funcţiune, prin simularea deconectării.

Prelucrarea la marginea reţelei diferenţiază datele operaţional: valorile normale se agregă sau se înregistrează mai rar; depăşirile limitelor critice declanşează transmiterea imediată a alarmelor. Dimensionarea infrastructurii reflectă această

diferenţiere. Cele 42 de mărimi colectate sunt grupate astfel: 6 indicatori de vibraţii şi curent, calculaţi local şi preluaţi de gateway la 100 ms; 24 de mărimi de proces, la 1 s; 12 mărimi lente — consumuri, contoare cumulative şi stări de sinteză —, la 10 s. Intervalul de 100 ms defineşte preluarea indicatorilor disponibili, precum valoarea efectivă sau de vârf, nu eşantionarea semnalelor brute. Achiziţia acestora se realizează local, la frecvenţe determinate de banda urmărită şi analiza necesară. Frecvenţa de eşantionare, durata ferestrei de calcul şi intervalul de preluare sunt distincte; citirea repetată nu confirmă recalcularea indicatorului (secţiunea 9.2.1). Banda de insensibilitate condiţionează transmiterea de depăşirea unui prag al diferenţei faţă de ultima valoare transmisă. În regim staţionar, reduce traficul mărimilor de proces cu un ordin de mărime, fără pierderea informaţiei relevante. Dimensionarea cantitativă a traficului este prezentată în secţiunea 3.3.5; mecanismele de comunicaţie, în subcapitolul 6.2.

Sistemele SCADA şi HMI prezintă stările utilajelor, alarmele şi tendinţele, iar aplicaţiile de nivel superior permit calcularea indicatorilor, analizarea opririlor şi urmărirea calităţii şi a consumurilor.

Conform principiilor prezentate în secţiunea 1.2.1, valorile colectate sunt însoţite de contextul necesar interpretării. O înregistrare poate avea forma:

Motor_02 – temperatura rulmentului – 68,4 °C – 10:42:15 – calitate bună

Cele cinci elemente corespund atributelor definite anterior: sursa, eticheta variabilei, valoarea împreună cu unitatea de măsură, marca temporală generată la achiziţie şi indicatorul de calitate. Valoarea poate fi astfel comparată cu limitele admise, corelată cu regimul de funcţionare, inclusă într-un grafic de evoluţie şi utilizată pentru identificarea degradării. Aceeaşi logică este aplicată vibraţiilor, presiunii, consumului energetic, timpilor de ciclu şi rezultatelor controlului calităţii.

Forma de mai sus este cea lizibilă pentru cititor; în transmisie, aceleaşi elemente sunt structurate într-un format prelucrabil automat, cu câmpuri denumite explicit, iar mărcile temporale se exprimă într-o referinţă unică de timp pentru întreaga instalaţie. Structura completă a mesajelor, convenţia de denumire a subiectelor şi tratarea calităţii sunt dezvoltate în subcapitolul 6.2.

Pentru corelarea între niveluri, fiecare înregistrare este asociată identificatorului lotului aflat în execuţie la momentul respectiv. Această asociere, aparent minoră, condiţionează întreaga trasabilitate ulterioară: în lipsa ei, o neconformitate constatată la control nu poate fi legată automat de parametrii procesului în care a apărut, iar analiza cauzelor rămâne manuală. Identificatorul se ataşează cât mai aproape de sursă – la nivelul gateway-ului, pe baza lotului activ raportat de controler – şi nu se reconstituie ulterior din intervale de timp, metodă care produce asocieri greşite la schimbarea de lot şi la reprelucrări.

Registrul punctelor de măsurare, descris în secţiunea 1.2.4, se întocmeşte în această etapă şi se recepţionează odată cu instalaţia. El consemnează, pentru fiecare dintre cele 42 de mărimi, semnificaţia, unitatea, domeniul, incertitudinea,

frecvența de achiziție, regula de validare și orizontul de păstrare, și constituie documentul pe baza căruia datele rămân interpretabile după schimbarea personalului.

1.4.3. Implementarea și evaluarea soluției

Implementarea se desfășoară în etape succesive, fiecare încheiată cu o verificare care condiționează trecerea la următoarea. Etapele sunt sintetizate în Figura 1.9.

Etapa 1 – Delimitarea perimetrului – asociate unei decizii identificate, conform secțiunii 1.2.2. Înaintea intervenției, se măsoară valorile de referință din Tabelul 1.4, Criteriul de trecere este întocmirea registrului punctelor de măsurare și nominalizarea unui utilizator pentru fiecare mărime.

Etapa 2 – Colectarea – se instalează instrumentația și gateway-urile fără modificarea programelor de comandă. Validarea precede analiza și verifică citirea valorilor, unitățile de măsură, sincronizarea temporală între gateway-uri și consecvența identificatorilor de echipament și lot. Erorile de context invalidează concluziile derivate. Criteriul de trecere: pe durata unei săptămâni, ponderea valorilor lipsă sau cu o calitate necorespunzătoare rămâne sub pragul stabilit; o probă comparativă confirmă identitatea dintre valoarea afișată la echipament și cea stocată în baza de date.

Etapa 3 – Vizualizarea și alarmarea – se pornesc tablourile de bord și se stabilesc, pentru fiecare alarmă, pragul, destinatarul și procedura de intervenție. Fără procedură, lanțul se întrerupe la decizie (secțiunea 1.2.2). Etapa este încheiată când operatorul poate gestiona efectiv alarmele pe schimb, fiecare având un destinatar, timp disponibil pentru reacție și o acțiune posibilă.

Tabelul 1.5 – Sinteza scenariului didactic privind digitalizarea industrială

Element analizat	**Situație inițială**	**Intervenție IIoT**	**Rezultat urmărit**
Monitorizare proces	Date locale și rapoarte întârziate	Sisteme SCADA și HMI, tablouri de bord	Creșterea vizibilității operaționale
Mentenanță	Intervenții predominant reactive	Monitorizarea vibrațiilor, a temperaturii și a alarmelor	Detectarea timpurie a degradării
Calitate	Date introduse manual	Corelarea loturilor cu parametrii procesului și rezultatele controlului	Îmbunătățirea trasabilității și analizarea cauzelor
Energie	Consum urmărit global	Măsurarea consumului pe utilaje și intervale	Identificarea pierderilor energetice
Date	Valori izolate	Contextualizarea datelor și registrul punctelor de măsurare	Obținerea informațiilor utilizabile pentru decizii
Securitate	Separarea rețelelor fără politici formalizate	Segmentarea rețelelor, controlul accesului, politici de securitate	Reducerea riscurilor
Organizație	Colaborare limitată între echipele IT și OT	Echipe mixte și obiective comune	Implementare coerentă și durabilă

Etapa 4 – Analiza pe istoric – se analizează seriile de date privind temperatura şi vibraţiile echipamentelor critice, distribuţia opririlor pe cauze, corelaţiile neconformităţi–parametri de proces şi profilul energetic pe schimburi. Analizele permit trecerea de la mentenanţa reactivă la cea bazată pe stare. Criteriul de trecere: clasificare stabilă a cauzelor opririlor între schimburi şi investigarea integrală a unei neconformităţi folosind datele înregistrate.

Etapa 5 – Evaluarea şi decizia de extindere – se evaluează indicatorii faţă de referinţe şi se recalculează rezultatele economice cu reducerile măsurate (secţiunea 1.3.3). Testul de independenţă presupune deconectarea controlată a gateway-ului: producţie şi funcţii de siguranţă neafectate, urmate de transmiterea datelor acumulate local după restabilirea legăturii.

Principalele elemente ale scenariului sunt sintetizate în Tabelul 1.5.

Beneficiile prezentate în secţiunea 1.3.1 reprezintă, în acest scenariu, rezultate urmărite, nu rezultate demonstrate. Evaluarea unei implementări reale necesită valori de referinţă măsurate înainte de intervenţie şi indicatori definiţi unitar: durata opririlor neplanificate, timpul de reacţie la alarme, rata produselor neconforme, consumul energetic specific, disponibilitatea echipamentelor şi timpul necesar analizării unei neconformităţi. Pentru fiecare indicator trebuie precizate perioada de referinţă, modul de calcul şi regulile de clasificare a evenimentelor; compararea unor valori obţinute prin reguli diferite conduce la concluzii eronate chiar şi atunci când formulele par identice, aspect dezvoltat în secţiunile 4.4.5 şi 7.2.3.

Evaluarea trebuie să distingă, de asemenea, între efectul soluţiei tehnice şi efectul schimbărilor organizatorice care o însoţesc. Introducerea unui tablou de bord este de regulă simultană cu instituirea unei analize zilnice a opririlor; îmbunătăţirea observată rezultă din ambele, iar atribuirea ei exclusiv tehnologiei supraestimează contribuţia acesteia şi denaturează justificarea extinderii.

Implementarea graduală permite verificarea funcţionării tehnice şi a utilităţii operaţionale înaintea extinderii arhitecturii. În fiecare etapă trebuie validate comunicaţia, calitatea datelor, securitatea şi efectul asupra procesului, cu participarea operatorilor, inginerilor, personalului de mentenanţă, echipelor IT şi OT şi a conducerii. Scenariul confirmă astfel concluzia formulată în secţiunea 1.3.2: rezultatele nu sunt produse de tehnologie, ci de utilizarea consecventă a informaţiilor pe care aceasta le pune la dispoziţie.

1.4.4. Limitele scenariului didactic

Un scenariu construit are o funcţie precisă şi una singură: să arate cum se leagă între ele conceptele prezentate. El nu poate proba nimic. Delimitarea acestor limite face parte din onestitatea metodei, iar cititorul trebuie să o poată face şi în situaţiile în care întâlneşte, în literatura comercială, exemple prezentate ca dovezi.

Ce arată scenariul – elementele transferabile sunt: ordinea deciziilor de proiectare – problema operaţională şi indicatorii, datele necesare, arhitectura, tehnologia;

traseul datelor pe patru niveluri și separarea funcțiilor critice de infrastructura de colectare; relația dintre contextul valorilor și utilizarea lor decizională; construirea calculului economic și identificarea ipotezei determinante. Aceste principii se aplică, cu valori adaptate, oricărei implementări de acest tip.

Ce nu arată scenariul – în primul rând, nu arată că beneficiile enunțate se produc. Reducerile de 15 %, 10 % și 4 % din secțiunea 1.3.3 sunt ipoteze necesare calculului, nu rezultate; ele au fost alese pentru a fi plauzibile, nu pentru că ar fi fost măsurate. În al doilea rând, nu arată că soluția funcționează, pentru că nu a fost pusă în funcțiune: dificultățile reale de integrare – un protocol nedocumentat, un automat programabil fără capacitate de calcul disponibilă, o rețea care nu suportă traficul suplimentar – apar la instalare, nu la proiectare. În al treilea rând, nu arată dacă organizația va folosi informația obținută, ceea ce este, conform secțiunii 1.2.2, condiția de care depinde totul.

De ce nu poate fi tratat ca studiu de caz – un studiu de caz este o descriere a ceva ce s-a întâmplat, cu o sursă verificabilă a datelor. El precizează contextul real, configurația efectiv instalată, valorile măsurate înainte și după, perioada de măsurare, regulile de calcul și problemele întâmpinate, inclusiv cele nerezolvate. Un exemplu construit nu îndeplinește niciuna dintre aceste condiții, indiferent cât de detaliat este redactat, iar prezentarea lui ca studiu de caz este o eroare de metodă, nu o convenție de expunere.

Cum se citește un caz publicat – aceleași criterii se aplică materialelor întâlnite în practică. Un caz care afirmă o îmbunătățire de douăzeci la sută fără a preciza valoarea inițială, perioada de măsurare, definiția indicatorului și ce altceva s-a schimbat în aceeași perioadă nu conține o măsurătoare, ci o afirmație. Întrebările utile sunt puține și aceleași de fiecare dată: cine a măsurat, cu ce definiție, pe ce interval, față de ce referință și ce alte intervenții s-au desfășurat simultan. Absența răspunsurilor nu înseamnă că rezultatul este fals, ci că nu poate fi verificat, iar un rezultat neverificabil nu poate fundamenta o decizie de investiție.

Ce ar completa scenariul – valori reale, obținute dintr-o implementare documentată, cu acordul organizației și cu nivelul de anonimizare convenit. În lipsa lor, capitolul își păstrează funcția didactică, dar nu poate susține afirmații despre rezultate obținute. Această limitare este declarată aici pentru ca nicio parte a lucrării să nu fie citită ca dovadă a unui efect industrial pe care autorul nu l-a măsurat.

Distincția dintre exemplul construit și cazul documentat revine în capitolul 9, unde mini-proiectele ghidate sunt tratate cu aceeași convenție: ele descriu ceea ce cititorul poate realiza și verifica singur, nu ceea ce s-a obținut în altă parte.

1.5. Concluzii

Transformarea digitală a industriei reprezintă integrarea coerentă a conectivității, datelor și tehnologiilor digitale în procesele de producție și în mecanismele decizionale ale organizației. IoT oferă principiul general al obiectelor conectate, IIoT îl adaptează cerințelor industriale, Industria 4.0 definește cadrul transformării, iar fabricația inteligentă concretizează aceste principii în sisteme de producție integrate. Industria 5.0 completează evoluția prin orientarea către om, reziliență și sustenabilitate. Delimitarea acestor concepte nu are valoare pur terminologică: nivelul la care este formulat un proiect determină criteriile după care el va fi evaluat, iar evaluarea unei transformări digitale prin criterii de digitizare explică o parte însemnată a nemulțumirii față de rezultatele proiectelor industriale de acest tip.

Diferența dintre IoT și IIoT nu constă în tehnologiile utilizate, ci în ierarhia cerințelor. În mediul industrial, disponibilitatea procesului și integritatea datelor de proces devin criterii dominante, cerințele de timp sunt exprimate prin clase normative verificabile, durata de viață a echipamentelor impune coexistența unor generații tehnologice diferite, iar consecințele unei erori se manifestă asupra calității, siguranței și continuității producției. Din acest motiv, IIoT este tratat ca infrastructură industrială, nu ca extindere a aplicațiilor destinate consumatorilor.

Valoarea unui sistem IIoT nu rezultă din conectarea echipamentelor, ci din transformarea datelor disponibile în date utilizabile. O valoare devine utilizabilă atunci când este însoțită de sursă, marcă temporală, unitate de măsură și indicator de calitate, iar identificarea consecventă a echipamentelor și a loturilor condiționează întreaga trasabilitate ulterioară. Prin lanțul date–informație–decizie–acțiune, informațiile provenite din procese susțin monitorizarea, mentenanța, controlul calității, eficiența energetică și planificarea producției. Lanțul se poate întrerupe în oricare dintre punctele sale, cu același efect: absența rezultatului operațional. Verificarea continuității lui constituie un criteriu practic de evaluare a unui proiect înainte de extindere, iar întrebarea de control nu este ce date se colectează, ci ce decizie se ia altfel decât înainte și cine o ia.

Datele leagă între ele etapele lanțului valoric industrial, iar aceeași valoare colectată o singură dată poate servi în producție, calitate, mentenanță și planificare. Această reutilizare reprezintă principalul argument economic al unei arhitecturi integrate, în raport cu soluțiile punctuale. Ea presupune însă decizii care nu admit corecție ulterioară – în primul rând cea privind identificatorii – și un cadru de administrare care stabilește proprietatea asupra datelor, responsabilitățile pentru definiții și calitate, tratamentul datelor cu caracter personal și orizonturile de păstrare. Registrul punctelor de măsurare este instrumentul prin care semnificația datelor supraviețuiește schimbărilor de personal și de furnizor.

Beneficiile IIoT depind de integrarea echipamentelor existente, de interoperabilitate, de calitatea datelor, de securitatea cibernetică și de colaborarea dintre echipele IT și OT. Demonstrarea lor presupune indicatori definiți unitar și valori de

referinţă stabilite înaintea intervenţiei; în absenţa unei situaţii iniţiale măsurate, îmbunătăţirea nu poate fi separată de variaţia normală a procesului sau de efectul schimbărilor organizatorice care însoţesc implementarea.

Evaluarea economică arată de ce implementarea graduală nu este doar o precauţie, ci forma corectă a investiţiei. Costul dominant al unui proiect-pilot este cel de integrare, plătit o singură dată, în timp ce beneficiile se acumulează proporţional cu numărul echipamentelor conectate. Un pilot izolat se recuperează greu şi poate deveni nerentabil la o modificare modestă a ipotezelor; acelaşi proiect, extins pe mai multe linii care reutilizează infrastructura şi competenţa dobândită, se recuperează în circa un an. Pilotul cumpără, în esenţă, informaţia necesară deciziei de extindere, iar acesta este principalul lui rezultat.

Scenariul didactic a ilustrat trecerea de la automatizarea locală la un sistem industrial conectat, cu păstrarea neschimbată a funcţiilor critice de control. Principiul de proiectare care rezultă din el este aplicabil dincolo de exemplul analizat: funcţiile de comandă, interblocările şi siguranţa rămân locale, infrastructura adăugată deserveşte colectarea, stocarea, analiza şi vizualizarea datelor, iar independenţa procesului faţă de această infrastructură se verifică la recepţie, nu se presupune. Scenariul arată însă ordinea deciziilor de proiectare, nu efectele obţinute; distincţia dintre exemplul construit şi cazul documentat rămâne valabilă în toată lucrarea.

Aplicarea acestor concepte presupune cunoaşterea contextului în care ele sunt utilizate. Pentru înţelegerea modului în care tehnologiile IIoT se integrează în activitatea unei organizaţii, capitolul următor prezintă structura unei companii industriale, configuraţia funcţională a fabricii şi parcursul unei comenzi, de la client până la livrare, urmărind în paralel fluxul fizic al materialelor şi fluxul informaţional care îl însoţeşte.

1.6. Întrebări de verificare

1. Care este ordinea în care, conform arhitecturii 5C, trebuie realizate capacităţile unui sistem ciber-fizic?

a) interpretarea rezultatelor, conectare la sursa de date, conversia datelor, imaginea coerentă, reconfigurare;

b) conversia datelor în indicatori de stare, conectare, reconfigurare, interpretarea rezultatelor, imaginea coerentă;

c) conectare la sursa de date, conversia datelor în indicatori de stare, imaginea coerentă a echipamentului, interpretarea rezultatelor, reconfigurare;

d) imaginea coerentă a echipamentului, conectare, interpretarea rezultatelor, conversia datelor, reconfigurare.

2. Ce raport există între Industria 5.0 şi Industria 4.0?

a) Industria 5.0 reprezintă doar o denumire comercială pentru IIoT, fără elemente conceptuale noi;

b) Industria 5.0 înlocuieşte Industria 4.0, renunţând la sistemele ciber-fizice şi la analiza datelor;
c) Industria 5.0 se referă exclusiv la creşterea gradului de automatizare şi la reducerea intervenţiei operatorului;
d) Industria 5.0 nu înlocuieşte Industria 4.0, ci îi adaugă orientarea către colaborarea om–maşină, reziliență şi sustenabilitate.

3. Înlocuirea registrului de opriri completat pe hârtie cu un formular electronic pe o tabletă reprezintă:
a) transformare digitală, deoarece se modifică modul de funcţionare al organizaţiei;
b) digitalizare, deoarece datele sunt utilizate pentru îmbunătăţirea procesului existent;
c) fabricaţie inteligentă, deoarece datele devin disponibile în timp real;
d) digitizare, deoarece se schimbă suportul informaţiei, nu procesul.

4. Care este ordinea priorităţilor de securitate în mediile de tehnologie operaţională (OT), spre deosebire de mediile IT?
a) niciun obiectiv nu are prioritate, deoarece cele trei se tratează întotdeauna cu aceeaşi pondere;
b) confidenţialitatea este prioritatea absolută, deoarece datele de proces sunt secrete industriale;
c) disponibilitatea procesului şi integritatea datelor de proces sunt dominante, iar confidenţialitatea este subordonată lor;
d) confidenţialitatea, integritatea, disponibilitatea – aceeaşi ordine ca în IT.

5. Un traductor cu eroare admisă de ±1,5 °C raportează 72,5 °C, iar limita de acceptare este 73 °C. Ce se poate afirma corect?
a) Nu se poate afirma că limita a fost respectată, deoarece incertitudinea de măsurare depăşeşte marja de 0,5 °C faţă de limită;
b) Limita a fost depăşită, deoarece eroarea de +1,5 °C aduce valoarea la 74 °C;
c) Limita a fost respectată, deoarece 72,5 °C este mai mic decât 73 °C;
d) Valoarea este inutilizabilă în orice situaţie, deoarece traductorul are o eroare admisă.

6. Un sistem generează corect alarme, dar nu există o procedură de intervenţie asociată fiecărei alarme. În care etapă a lanţului date–informaţie–decizie–acţiune se întrerupe lanţul?
a) la informaţie, deoarece alarma nu este contextualizată;
b) la decizie, deoarece nu este stabilit cine şi ce hotărăşte la apariţia alarmei;
c) la date, deoarece alarmele nu pot fi colectate fără procedură;
d) la acţiune, deoarece alarma generată reprezintă ea însăşi acţiunea.

7. De ce trebuie stabiliţi identificatorii de lot şi de echipament înaintea începerii colectării datelor?

a) deoarece identificatorii reduc automat volumul de date stocate;
b) deoarece un identificator introdus ulterior nu poate fi aplicat retroactiv datelor deja colectate, iar istoricul rămâne neutilizabil pentru trasabilitate;
c) deoarece identificatorii înlocuiesc marca temporală și calitatea datei;
d) deoarece protocoalele industriale nu permit transmiterea valorilor fără identificator de lot.

8. De ce este ireversibilă decizia de agregare a datelor (de exemplu, trecerea de la valori la interval de o secundă la medii pe cinci minute)?
a) deoarece datele agregate nu mai pot fi afișate în sistemele SCADA;
b) deoarece agregarea modifică identificatorii echipamentelor;
c) deoarece se elimină definitiv posibilitatea de a analiza ulterior fenomene tranzitorii, precum un vârf de curent sau o oscilație scurtă de presiune;
d) deoarece datele agregate nu pot fi păstrate mai mult de câteva zile.

9. Un proiect-pilot IIoT are o investiție inițială de 17.520 €, un beneficiu anual brut de 9.348 € și un cost anual de exploatare de 4.450 €. Care este termenul simplu de recuperare?
a) aproximativ 3,58 ani;
b) aproximativ 1,21 ani;
c) aproximativ 1,87 ani;
d) aproximativ 8,30 ani.

10. Un material de prezentare afirmă că o soluție IIoT a redus opririle neplanificate cu 20 %. Ce trebuie verificat pentru a stabili dacă afirmația este o măsurătoare?
a) doar dacă materialul conține un grafic și o diagramă a arhitecturii;
b) valoarea inițială, perioada de măsurare, definiția indicatorului și ce alte schimbări au avut loc în aceeași perioadă;
c) doar dacă procentul a fost rotunjit la o cifră întreagă;
d) doar numele furnizorului platformei și numărul de senzori instalați.

2. ARHITECTURA UNEI COMPANII INDUSTRIALE ȘI FLUXUL COMENZII ÎN PRODUCȚIE

Un sistem IIoT nu se proiectează pornind de la lista echipamentelor disponibile, ci de la activităţile pe care datele urmează să le susţină. Care mărimi merită măsurate, la ce interval, cine le utilizează şi ce decizie devine posibilă prin ele sunt întrebări cu răspuns organizaţional, nu tehnologic. În lipsa acestei raportări, o instalare corectă din punct de vedere tehnic poate produce volume mari de date fără destinatar, fără prag de reacţie şi fără efect asupra rezultatelor fabricii.

Perspectiva adoptată aici tratează compania industrială ca sistem de prelucrare a informaţiei, nu ca sumă de departamente. Formularea nu este o metaforă: o organizaţie poate fi descrisă prin capacitatea sa de a colecta, transmite şi utiliza informaţie în condiţii de incertitudine, iar structurile organizatorice pot fi interpretate ca mecanisme de reducere a nevoii de comunicare sau, dimpotrivă, de creştere a capacităţii de a o susţine [74]. Un proiect IIoT intervine exact în acest punct: el modifică volumul, viteza şi fidelitatea informaţiei care circulă între funcţii.

Capitolul analizează patru planuri suprapuse. Structura organizaţională arată cine decide şi cine execută; configuraţia funcţională a fabricii determină traseul fizic al materialelor şi locul în care se instalează echipamentele de automatizare; fluxul informaţional al comenzii leagă cerinţa clientului de operaţiile executate şi de înregistrările rezultate; relaţiile cu mediul extern extind aceste dependenţe dincolo de limitele fabricii. Cele patru planuri se condiţionează reciproc: o repartizare clară a responsabilităţilor nu compensează o amplasare care obligă materialele să traverseze hala de mai multe ori, iar o configuraţie eficientă a spaţiului nu compensează o informaţie care ajunge târziu sau eronat la punctul de execuţie.

Această ordine de expunere este mai puţin obişnuită într-o carte despre IIoT, unde tratarea începe de regulă de la senzori şi protocoale, însă necesară din trei motive:

- Datele utile sunt generate de procese, iar identificarea lor presupune cunoaşterea proceselor.
- Sistemele care urmează să fie interconectate – ERP, MES, SCADA şi HMI – corespund unor funcţii organizaţionale distincte, iar interfeţele dintre ele reproduc graniţele dintre aceste funcţii; modelul de referinţă care formalizează corespondenţa, seria ISA-95, este utilizat în Capitolul 7 [75].
- Proprietăţile invocate în legătură cu IIoT – trasabilitate, vizibilitate, timp de răspuns – sunt proprietăţi ale fluxului, nu ale unui echipament luat separat, iar comportamentul fluxului urmează legităţi proprii, independente de tehnologia de măsurare utilizată [76].

Expunerea urmează parcursul unei comenzi. Secţiunea 2.1 prezintă funcţiile companiei şi modul în care acestea se modifică odată cu dimensiunea şi domeniul organizaţiei. Secţiunea 2.2 trece de la organigramă la spaţiul fizic al fabricii. Secţiunea 2.3 urmăreşte o comandă de la solicitarea clientului până la livrare şi la valorificarea feedbackului, cu o tratare cantitativă a duratei totale. Secţiunea 2.4 completează imaginea cu relaţiile externe şi cu integrarea orizontală. Secţiunea 2.5 reuneşte aceste elemente într-un scenariu didactic construit pentru prezenta lucrare.

Capitolul nu descrie soluţii tehnice; acestea sunt tratate începând cu Capitolul 5. Rolul său este de a furniza cadrul în care soluţiile capătă sens. Capitolul 3 utilizează direct acest cadru, corelând tipul de producţie cu cerinţele arhitecturii IIoT, iar Capitolele 7 şi 9 revin asupra fluxului comenzii pentru a-i asocia o arhitectură concretă şi aplicaţii executabile.

Obiectivele capitolului

La finalul acestui capitol, cititorul va fi capabil:

- să descrie funcţiile operaţionale, comerciale, de suport şi de conducere ale unei companii industriale şi să explice interdependenţa dintre ele;
- să coreleze fiecare funcţie cu sistemele informatice industriale asociate – ERP, MES, SCADA şi HMI – şi cu datele pe care le generează sau le consumă;
- să compare configuraţiile funcţionale de bază ale unei fabrici şi să explice influenţa lor asupra traseului materialelor, a timpilor de aşteptare şi a amplasării infrastructurii de automatizare;
- să diferenţieze fluxul fizic de fluxul informaţional al unei comenzi şi să identifice consecinţele desincronizării acestora;
- să urmărească parcursul unei comenzi de la solicitarea clientului până la livrare şi la valorificarea feedbackului post-vânzare;
- să calculeze eficienţa fluxului pentru o comandă dată şi să argumenteze, pe baza rezultatului, ordinea intervenţiilor de digitalizare;
- să descrie relaţiile companiei cu clienţii, furnizorii, partenerii logistici şi autorităţile şi cerinţele integrării orizontale privind schimbul de date;
- să identifice, într-un flux industrial dat, punctele în care IIoT poate îmbunătăţi vizibilitatea, trasabilitatea, calitatea şi fundamentarea deciziilor.

2.1. Structura organizaţională a unei companii industriale

Structura organizaţională defineşte modul în care sunt repartizate responsabilităţile, resursele şi drepturile de decizie necesare realizării produselor. Într-o companie industrială, compartimentele nu funcţionează independent, ci contribuie împreună la îndeplinirea obiectivelor privind producţia, calitatea, costurile şi termenele de livrare. Din perspectiva prezentei lucrări, structura prezintă un interes

suplimentar: ea indică unde sunt generate datele industriale, cine le utilizează şi ce decizie devine posibilă atunci când acestea sunt disponibile la timp.

Gruparea utilizată aici – funcţii operaţionale, funcţii de conducere şi funcţii de suport – este descriptivă şi corespunde practicii curente din industria prelucrătoare [74]. Ea nu descrie un tip organizatoric unic: aceleaşi funcţii pot fi coordonate prin supraveghere directă, prin standardizarea proceselor sau prin standardizarea rezultatelor, iar mecanismul dominant de coordonare diferă în funcţie de mărimea organizaţiei şi de stabilitatea mediului în care operează [77]. Gruparea funcţională nu trebuie confundată nici cu ierarhia sistemelor de automatizare, tratată în Capitolul 7 pe baza modelului ISA-95: o funcţie organizaţională poate fi susţinută de sisteme aflate pe niveluri diferite, iar un singur sistem poate deservi mai multe funcţii. Structura funcţională şi principalele relaţii dintre compartimente sunt ilustrate în Figura 2.1.

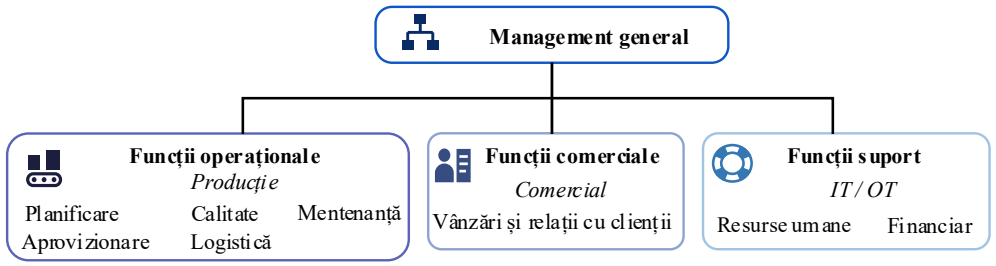


Figura 2.1 – Organigramă funcțională tipică a unei companii industriale

2.1.1. Funcțiile operaționale

Producţia reprezintă nucleul activităţii industriale. În cadrul secţiilor, liniilor şi celulelor de fabricaţie, materiile prime şi componentele sunt transformate în produse finite prin operaţii de prelucrare, asamblare, verificare şi ambalare. Activităţile sunt realizate de operatori, tehnicieni şi ingineri, cu ajutorul utilajelor, instalaţiilor şi sistemelor de automatizare. Producţia este, totodată, principala sursă de date operaţionale: stări ale echipamentelor, timpi de ciclu, cantităţi realizate, parametri tehnologici, opriri şi alarme.

Planificarea şi controlul producţiei transformă comenzile clienţilor în ordine de lucru şi stabileşte succesiunea operaţiilor, resursele necesare şi termenele de execuţie. Această funcţie corelează cererea cu disponibilitatea materialelor, capacitatea echipamentelor şi necesarul de personal, urmărind evitarea blocajelor şi respectarea termenelor de livrare [78]. Calitatea planificării depinde direct de exactitatea datelor de intrare: un timp de ciclu estimat greşit sau un stoc raportat incorect se propagă în întregul plan. Dependenţa este cu atât mai importantă cu cât planificarea operează, prin natura ei, cu valori medii, în timp ce execuţia este afectată de variabilitate; ignorarea acestei diferenţe conduce la planuri care par realizabile în calcul şi eşuează sistematic în execuţie [76].

Achiziţiile şi aprovizionarea asigură materiile prime, componentele, materialele auxiliare şi serviciile necesare. Deciziile de aprovizionare trebuie corelate cu planul de producţie, nivelul stocurilor, termenele furnizorilor şi cerinţele de calitate. Alegerea între stocuri mai mari şi livrări mai frecvente este, în esenţă, un compromis între costul imobilizării şi costul comenzii, iar termenul de livrare al furnizorului determină cât din acest compromis poate fi controlat de companie [79].

Logistica gestionează recepţia, depozitarea şi deplasarea materialelor între zonele fabricii, precum şi pregătirea şi expedierea produselor finite. Eficienţa acestei funcţii influenţează direct continuitatea producţiei, nivelul stocurilor şi durata totală de realizare a comenzilor.

Funcţia de calitate verifică respectarea cerinţelor aplicabile materiilor prime, proceselor şi produselor. Activitatea sa include controlul la recepţie, verificările intermediare, inspecţia finală, gestionarea neconformităţilor şi păstrarea înregistrărilor necesare trasabilităţii. Cerinţa de a menţine informaţii documentate privind conformitatea şi de a identifica elementele de ieşire ale proceselor atunci când trasabilitatea este necesară este formulată explicit în ISO 9001 [80]; ea determină, în practică, o parte importantă a datelor care trebuie colectate şi păstrate într-o implementare IIoT. Valoarea acestor înregistrări depinde însă de proprietăţi care nu se obţin automat prin conectarea echipamentelor: acurateţe, completitudine, consecvenţă a unităţilor şi a denumirilor, actualitate şi accesibilitate pentru aplicaţia care are nevoie de ele [37].

Mentenanţa asigură disponibilitatea şi funcţionarea sigură a echipamentelor. Pe lângă remedierea defecţiunilor, aceasta include inspecţii, revizii, activităţi preventive şi analiza datelor privind starea utilajelor. Integrarea mentenanţei cu producţia permite programarea intervenţiilor astfel încât efectul asupra comenzilor aflate în desfăşurare să fie limitat. Corelarea sistematică dintre exploatarea echipamentului şi îngrijirea lui, împreună cu urmărirea pierderilor de disponibilitate, de performanţă şi de calitate, constituie fundamentul mentenanţei productive totale [65].

Trecerea mai departe, către mentenanţa bazată pe stare, presupune disponibilitatea unor date continue despre echipament – condiţie tehnică tratată în Capitolul 5 şi aplicată în Capitolul 9.

2.1.2. Funcțiile de conducere și suport

Conducerea stabileşte obiectivele organizaţiei, alocă resursele şi urmăreşte performanţa activităţilor. Deciziile sale trebuie fundamentate prin informaţii provenite din vânzări, producţie, calitate, mentenanţă, logistică şi situaţia financiară. Pentru ca aceste informaţii să fie comparabile între perioade şi între secţii, indicatorii utilizaţi trebuie definiţi unitar; seria ISO 22400 stabileşte terminologia şi conceptele comune [50], iar partea a doua defineşte setul de indicatori şi regulile lor de calcul [51]. În absenţa unei astfel de referinţe, acelaşi indicator ajunge să fie

determinat diferit de aplicaţii diferite, iar comparaţiile pe care se sprijină deciziile devin lipsite de fundament.

Vânzările şi relaţiile cu clienţii constituie legătura dintre piaţă şi sistemul de producţie. Acestea preiau cerinţele, formulează ofertele, înregistrează comenzile şi comunică termenele de livrare. Confirmarea unei comenzi necesită verificarea capacităţii de producţie, a materialelor disponibile şi a cerinţelor tehnice.

Proiectarea şi industrializarea definesc specificaţiile, desenele, listele de materiale, instrucţiunile şi parametrii de proces conform cerinţelor clientului. Materialele, toleranţele şi succesiunea operaţiilor determină o parte importantă a costului final [1]. Modificările produsului se comunică controlat către planificare, aprovizionare, producţie şi calitate, prevenind folosirea documentaţiei neactualizate. Controlul deficitar al versiunilor generează frecvent neconformităţi în producţia personalizată: execuţie corectă după specificaţii depăşite, fără erori imediat vizibile.

Funcţia financiar-contabilă gestionează bugetele, costurile, plăţile, încasările şi raportările economice. Datele privind consumurile, timpii de fabricaţie, rebuturile şi utilizarea echipamentelor contribuie la determinarea costului real al produselor şi la evaluarea rentabilităţii comenzilor.

Resursele umane asigură recrutarea, formarea şi dezvoltarea personalului. În contextul digitalizării industriale, această funcţie trebuie să sprijine dobândirea competenţelor necesare utilizării echipamentelor conectate, interpretării datelor şi colaborării dintre IT şi OT.

Departamentul IT administrează infrastructura informatică, aplicaţiile, conturile, stocarea şi securitatea. Pentru integrarea producţiei, colaborează permanent cu specialiştii în automatizări, care cunosc cerinţele de control, disponibilitate şi siguranţă. Priorităţile diferă: IT urmăreşte confidenţialitatea şi actualizarea rapidă, iar tehnologia operaţională pune accent pe disponibilitatea procesului şi integritatea datelor. Diferenţa ţine de criterii, nu de competenţă: o repornire sau o corecţie automată poate fi inacceptabilă în timpul funcţionării instalaţiei [25]. Capitolul 8 explică aceste consecinţe.

2.1.3. Colaborarea şi integrarea informaţională

Realizarea unei comenzi necesită colaborarea tuturor funcţiilor; vânzările preiau cerinţa clientului, proiectarea defineşte soluţia tehnică, planificarea stabileşte ordinea de execuţie, achiziţiile asigură materialele, iar producţia realizează produsul. Calitatea verifică respectarea cerinţelor, mentenanţa menţine echipamentele disponibile, logistica gestionează materialele şi livrarea, iar funcţia financiară urmăreşte costurile şi încasările.

Această succesiune nu este strict liniară. O întârziere a unui furnizor poate impune modificarea planului de producţie, o defecţiune poate necesita reprogramarea unei comenzi, iar identificarea unei neconformităţi poate determina revenirea

la proiectare, aprovizionare sau reglarea procesului. Fiecare astfel de abatere generează o nevoie suplimentară de comunicare între funcţii, iar organizaţia trebuie să reducă această nevoie prin reguli şi rezerve sau să îşi mărească explicit capacitatea de a o susține prin sisteme informaționale [74]. Un proiect IIoT aparține celei de-a doua categorii de soluții și trebuie evaluat ca atare: nu prin numărul de mărimi colectate, ci prin numărul de decizii pe care le face posibile mai devreme.

Tabelul 2.1 – Funcțiile companiei industriale în context digital

Funcție	**Rol în companie**	**Date generate sau utilizate**	**Sisteme digitale asociate și relevanță pentru IIoT**
Producție	Transformă materialele și componentele în produse	Stări ale utilajelor, timpi de ciclu, cantități, parametri tehnologici, alarme	Automate programabile (PLC), HMI, SCADA și MES; principala sursă de date operaționale
Planificare	Organizează comenzile, capacitățile și resursele	Ordine de producție, capacități, priorități, termene	ERP, MES și sisteme de planificare și programare avansată; conectează cererea cu execuția
Aprovizionare	Asigură materialele, componentele și serviciile necesare	Stocuri, furnizori, consumuri, termene de livrare	ERP și sisteme de gestiune a stocurilor; utilizează datele reale privind consumul și ritmul producției
Logistică	Gestionează fluxul materialelor și produselor	Poziții, mișcări, stocuri intermediare, livrări	ERP, MES, sisteme de management al depozitului și identificare prin radiofrecvență (RFID); susține trasabilitatea fluxului fizic
Asigurarea calității	Verifică respectarea specificațiilor	Măsurători, neconformități, defecte, loturi	MES, baze de date și sisteme de management al calității; corelează parametrii procesului cu rezultatele
Mentenanță	Menține echipamentele în stare de funcționare	Alarme, defecte, intervenții, starea activelor	SCADA, servere istorice de date și sisteme computerizate de management al mentenanței; furnizează baza pentru mentenanța bazată pe stare și predictivă
Comercial	Gestionează relația cu piața și clientul	Cereri, oferte, comenzi, specificații, modificări	ERP și sisteme de gestionare a relațiilor cu clienții; declanșează fluxul intern al comenzii
Financiar	Urmărește costurile și performanța economică	Costuri, facturi, bugete, investiții, indicatori	ERP și aplicații de analiză a datelor; utilizează date agregate pentru calcularea costurilor și fundamentarea deciziilor
Resurse umane	Gestionează personalul și competențele	Competențe, instruire, program de lucru, responsabilități	Sisteme informatice pentru resurse umane; susține dezvoltarea competențelor necesare transformării digitale
IT și OT	Asigură infrastructura digitală și funcționarea proceselor	Utilizatori, rețele, servere, drepturi de acces, alarme, configurații	Infrastructură IT–OT, sisteme de administrare și securitate; asigură integrarea, disponibilitatea și protecția datelor
Conducere	Stabilește direcția, obiectivele și investițiile	Indicatori, costuri, performanță, prognoze	ERP, MES și aplicații de analiză; utilizează informații agregate pentru decizii tactice și strategice

Sistemele ERP, MES și SCADA susțin niveluri diferite ale acestei colaborări. ERP gestionează comenzile, materialele și resursele întreprinderii; MES coordonează execuția producției, iar SCADA furnizează informații despre starea proceselor și a echipamentelor. Delimitarea responsabilităților dintre gestionarea operațiunilor de fabricație și activitățile întreprinderii, împreună cu categoriile de informații schimbate între ele, este formalizată de seria ISA-95 [75]; relația tehnică dintre sisteme, inclusiv fluxurile bidirecționale, este prezentată în secțiunea 7.2.

Sistemele digitale asociate acestor funcții sunt distribuite pe mai multe niveluri. La nivelul procesului se află senzorii, actuatoarele, automatele programabile, roboții, sistemele de acționare și echipamentele de măsurare. La nivelul supravegherii se află interfețele om–mașină (HMI) și SCADA, care permit operatorilor să monitorizeze și să controleze procesul. MES conectează planificarea cu realitatea din fabrică, iar ERP gestionează comenzile, stocurile, achizițiile, activitatea financiară și celelalte resurse ale organizației. IIoT asigură infrastructura prin care datele pot circula controlat între aceste niveluri.

Corespondența dintre funcțiile companiei, datele pe care le generează sau le utilizează și sistemele digitale asociate este sintetizată în Tabelul 2.1.

O companie industrială performantă nu funcționează prin departamente izolate. Producția depinde de planificare, planificarea de comenzi și stocuri, aprovizionarea de cererea viitoare, calitatea de parametrii procesului, mentenanța de starea echipamentelor, iar conducerea de informații corecte și actualizate. IIoT poate susține aceste legături prin colectarea datelor din teren și transmiterea lor către sistemele și persoanele care le pot transforma în decizii, dar nu poate compensa o organizare incoerentă. O arhitectură digitală slab proiectată amplifică problemele existente prin date duplicate, denumiri neunitare, alarme inutile, rapoarte contradictorii și responsabilități neclare – toate fiind, de fapt, eșecuri ale dimensiunilor calității datelor, nu ale echipamentelor de colectare [37].

2.1.4. Adaptarea structurii la dimensiunea și domeniul companiei

Structura organizațională diferă în funcție de dimensiunea companiei, complexitatea produselor și specificul industriei. În întreprinderile mici și mijlocii, aceeași persoană poate îndeplini mai multe roluri, iar coordonarea se realizează în bună măsură prin supraveghere directă și comunicare informală. În companiile mari, responsabilitățile sunt specializate, iar coordonarea migrează către standardizarea proceselor, a rezultatelor și a competențelor, susținută de proceduri, sisteme informatice și niveluri decizionale clar definite [77].

Industriile puternic reglementate acordă o importanță sporită calității, trasabilității și documentării, în timp ce producția de serie mare pune accent pe continuitatea fluxului, automatizare și utilizarea capacității. Structura trebuie să rămână suficient de flexibilă pentru a se adapta modificării produselor, volumelor de producție și tehnologiilor utilizate.

Aceste diferențe au consecințe directe asupra modului în care se abordează o implementare IIoT. Într-o organizaţie mică, avantajul îl constituie viteza deciziei şi numărul redus de interfeţe dintre sisteme; limitarea principală este lipsa unui compartiment IT dedicat şi absenţa unei evidenţe riguroase a activelor. Într-o organizaţie mare, datele sunt mai bine structurate, dar orice modificare atinge mai multe funcţii şi necesită coordonare formală. Tabelul 2.2 sintetizează aceste diferenţe şi punctul de pornire recomandat pentru fiecare situaţie.

Datele din tabel nu descriu praguri fixe, ci tendinţe: o companie mică dintr-un domeniu reglementat poate avea o documentare mai riguroasă decât o companie mare din producţia de serie. Criteriul practic nu este numărul de angajaţi, ci numărul de interfeţe dintre funcţii care trebuie menţinute coerente.

Organizarea funcţională este completată de amplasarea fizică a activităţilor. Structura organizaţională explică cine participă la transformarea unei comenzi în produs şi ce rol are fiecare funcţie, însă activitatea industrială se desfăşoară într-un spaţiu concret, format din hale, linii, celule de fabricaţie, depozite, zone de control şi infrastructuri de comunicaţie. Modul în care sunt dispuse aceste zone determină traseul materialelor, influenţează eficienţa întregului sistem şi condiţionează amplasarea echipamentelor de automatizare. Secţiunea următoare analizează configuraţia funcţională a fabricii din această perspectivă.

Tabelul 2.2 – Influența dimensiunii companiei asupra structurii și a abordării unei implementări IIoT

Element	Companie mică	Companie mijlocie	Companie mare
Repartizarea rolurilor	Roluri cumulate; aceeași persoană acoperă planificare, achiziții și calitate	Compartimente distincte, cu roluri parțial cumulate în funcțiile de suport	Compartimente specializate, cu roluri și competențe delimitate
Mecanismul dominant de coordonare	Supraveghere directă și ajustare reciprocă	Standardizarea proceselor pentru fluxurile principale	Standardizarea proceselor, a rezultatelor și a competențelor
Sisteme informatice tipice	Aplicație de contabilitate, foi de calcul, eventual ERP de bază	ERP funcțional, SCADA la nivelul liniilor, MES parțial sau absent	ERP, MES, SCADA, sisteme de management al calității și al mentenanței, integrate
Responsabilitatea IT–OT	Nedelimitată; frecvent asigurată de un furnizor extern	Compartiment IT restrâns, colaborare punctuală cu automatiștii	Compartimente distincte, cu proceduri comune de gestionare a modificărilor
Riscul principal în digitalizare	Dependența de furnizor și de o singură persoană-cheie	Coexistența unor sisteme neintegrate și a evidențelor paralele	Durata deciziei și rigiditatea sistemelor existente
Punct de pornire recomandat	O linie sau un utilaj critic, cu un număr redus de mărimi și un indicator urmărit	Un flux complet al unei familii de produse, de la lansare la expediere	Un proiect-pilot pe o secție, cu reguli de denumire și de securitate stabilite de la început

2.2. Configurația funcțională a unei fabrici și fluxul fizic al materialelor

Configuraţia funcţională a fabricii (engl. *factory layout*) descrie amplasarea zonelor de lucru, a echipamentelor, a spaţiilor de depozitare şi a căilor de circulaţie [81]. Aceasta trebuie să reflecte succesiunea proceselor tehnologice şi să permită deplasarea eficientă şi sigură a materialelor, produselor, personalului şi mijloacelor de manipulare.

O configuraţie adecvată reduce distanţele de transport, timpii de aşteptare şi manipulările inutile; în acelaşi timp, facilitează supravegherea proceselor, izolarea zonelor periculoase, efectuarea intervenţiilor de mentenanţă şi adaptarea capacităţii de producţie. O amplasare necorespunzătoare poate genera intersectarea fluxurilor, acumularea stocurilor intermediare, blocaje şi dificultăţi în urmărirea comenzilor. Deciziile de amplasare au, în plus, un caracter durabil: modificarea lor ulterioară implică oprirea producţiei, relocarea utilajelor şi refacerea instalaţiilor, motiv pentru care efectele unei configuraţii greşite sunt suportate ani la rând [81]. Procesele pe care această configuraţie trebuie să le deservească – intrări, procese principale, ieşiri şi procese de suport – sunt reprezentate în Figura 2.2.

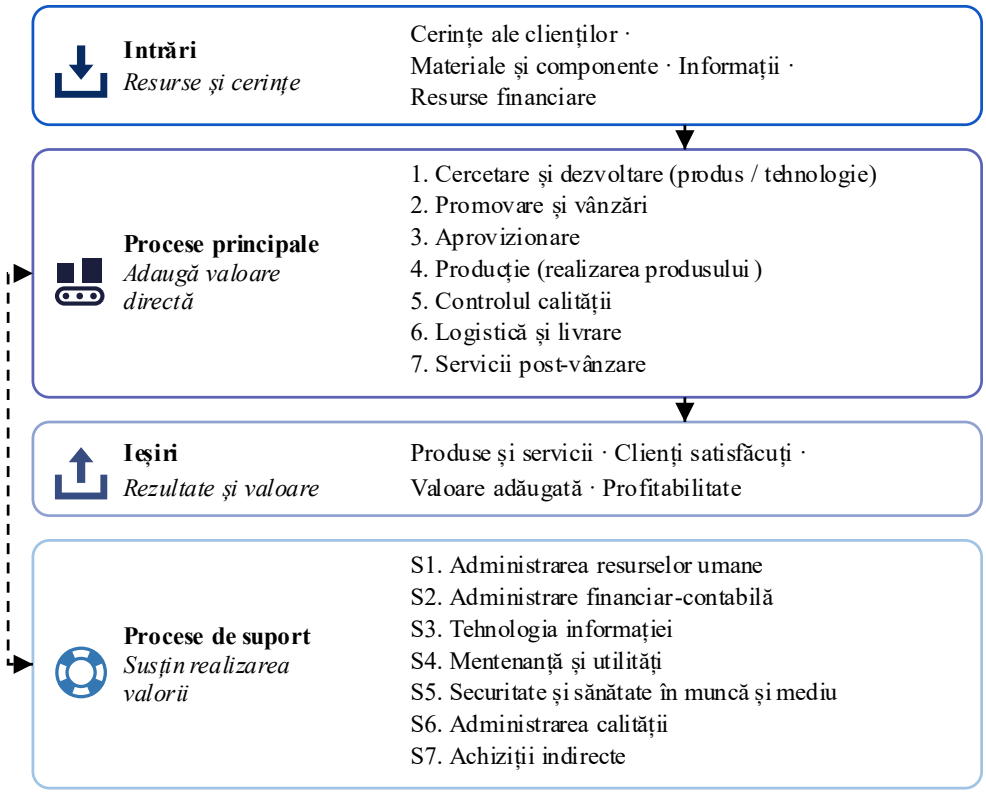


Figura 2.2 – Harta proceselor unei companii industriale: intrări, procese principale, ieșiri și procese de suport

2.2.1. Principalele zone funcționale

Zonele descrise în continuare corespund funcţiilor care apar, în forme diferite, în majoritatea unităţilor de producţie discretă; gruparea lor urmează practica planificării instalaţiilor industriale.

Recepţia materialelor constituie intrarea în fabrică pentru materii prime şi componente, cu descărcare, verificarea documentelor de livrare şi controale cantitative şi, după caz, calitative. Amplasarea trebuie să asigure accesul mijloacelor de transport şi transferul rapid către depozit.

Depozitul de materii prime asigură păstrarea materialelor până la introducerea lor în producţie. Organizarea acestuia trebuie să ţină seama de tipul materialelor, frecvenţa utilizării, condiţiile de depozitare şi cerinţele de trasabilitate. Identificarea clară a poziţiilor şi actualizarea stocurilor reduc riscul utilizării unor materiale greşite sau indisponibile.

Zona de pregătire poate include debitarea preliminară, sortarea, dozarea, pregătirea sculelor ori formarea loturilor care urmează să fie introduse în proces. Separarea acestor activităţi de operaţiile principale contribuie la alimentarea ritmică a producţiei.

Zona de producţie cuprinde utilajele, liniile, celulele şi posturile în care materialele sunt transformate. Configuraţia sa depinde de succesiunea operaţiilor, dimensiunea produselor, volumul producţiei şi nivelul de automatizare. Echipamentele trebuie amplasate astfel încât să permită operarea, alimentarea, evacuarea produselor şi efectuarea în siguranţă a intervenţiilor.

Controlul calităţii poate fi integrat în fluxul de producţie sau organizat în spaţii dedicate. Verificările intermediare permit identificarea abaterilor înainte ca produsele să parcurgă operaţii suplimentare, iar controlul final confirmă îndeplinirea cerinţelor înaintea ambalării şi livrării.

Zona de ambalare asigură protejarea, etichetarea şi pregătirea produselor pentru depozitare ori expediere. Aceasta trebuie corelată cu ritmul producţiei şi cu cerinţele logistice, pentru a evita acumularea produselor neambalate.

Depozitul de produse finite reprezintă punctul de păstrare temporară a produselor înaintea livrării. Organizarea sa trebuie să permită identificarea comenzilor, formarea loturilor şi aplicarea regulii primul intrat–primul ieşit (FIFO), atunci când aceasta este necesară.

Expedierea constituie punctul final al fluxului fizic. Aici sunt verificate comenzile, sunt pregătite documentele şi sunt încărcate produsele în mijloacele de transport. Amplasarea zonei în apropierea depozitului de produse finite reduce manipulările suplimentare.

Funcţiile suport, precum mentenanţa, laboratoarele, depozitele de scule, utilităţile şi spaţiile tehnice, nu fac parte întotdeauna din traseul principal al produsului,

dar trebuie amplasate astfel încât să poată deservi rapid zonele de producţie fără a perturba fluxul materialelor.

2.2.2. Tipuri de configurație și criterii de alegere

Amplasarea zonelor admite patru configuraţii de bază, definite prin gruparea echipamentelor după succesiunea operaţiilor, natura tehnologică a acestora, familia de produse sau poziţia fixă a obiectului fabricat [1]. Alegerea depinde de volumul producţiei, varietatea produselor şi repetabilitatea operaţiilor, influenţând direct lungimea traseelor, volumul producţiei în curs de execuţie şi complexitatea sistemului de urmărire.

Amplasarea nu se alege doar calitativ. Planificarea sistematică utilizează o matrice care exprimă intensitatea relaţiilor dintre zone prin volumul deplasărilor şi motivele lor [82]. Variantele se compară combinând intensitatea cu distanţa: efortul total de transport este proporţional cu suma produselor dintre numărul deplasărilor şi distanţa parcursă pe fiecare relaţie. Apropierea zonelor între care circulaţia este intensă reduce efortul, chiar dacă zonele rar conectate se îndepărtează. Cele patru configuraţii sunt comparate în Tabelul 2.3.

În practică, fabricile utilizează rareori o configuraţie pură. Combinaţia cea mai frecventă asociază o secvenţă principală de tip linie cu celule funcţionale destinate operaţiilor cu variabilitate ridicată sau cu timpi de pregătire mari. Această soluţie mixtă păstrează avantajul unui traseu principal previzibil şi permite, în acelaşi timp, tratarea diferenţiată a comenzilor personalizate.

Tabelul 2.3 – Configurații funcționale de bază și implicațiile lor asupra fluxului și a colectării datelor

Configurație	**Criteriu de grupare**	**Domeniu tipic**	**Caracteristici ale fluxului**	**Implicații pentru colectarea datelor**
Pe produs (linie)	Succesiunea operațiilor unui produs	Volum mare, varietate redusă	Traseu scurt și liniar, ritm impus, producție în curs redusă	Puncte de măsurare fixe; datele se pot asocia cu poziția din linie; oprirea unui post afectează întreaga linie
Pe proces (funcțională)	Natura tehnologică a operației	Volum redus, varietate mare	Trasee lungi și variabile, stocuri intermediare între ateliere	Necesară identificarea individuală a pieselor; datele nu pot fi deduse din poziția în flux
Celulară	Familii de produse cu operații similare	Volum mediu, varietate medie	Flux scurt în interiorul celulei, autonomie relativă a acesteia	Colectare la nivel de celulă; indicatorii pot fi calculați pentru fiecare celulă separat
Cu poziție fixă	Produsul rămâne pe loc, resursele se deplasează	Produse mari sau grele, unicat	Deplasarea materialelor, sculelor și personalului către produs	Măsurarea urmărește resursele și operațiile, nu poziția produsului; frecvent necesare echipamente mobile

Alegerea depășește criteriile tehnologice. Traseele scurte pot crea dependențe critice: defectarea unui post oprește întreaga linie. O configurație flexibilă, cu redundanță, implică trasee mai lungi și stocuri intermediare mai mari. Stocurile reduse fac fluxul mai sensibil la variabilitate. Pentru păstrarea debitului când variabilitatea crește, sunt necesare rezerve de capacitate, de stoc sau acceptarea unor durate de trecere mai lungi [76]. Aceste efecte se compară cu tipul de producție, prezentat în Capitolul 3.

2.2.3. Organizarea fluxului fizic

Fluxul fizic reprezintă deplasarea materiilor prime, semifabricatelor și produselor prin fabrică, ilustrată schematic în Figura 2.3.

În practică, traseul poate include reveniri pentru reprelucrare, zone-tampon, operații executate în paralel și puncte suplimentare de verificare. Aceste abateri trebuie controlate pentru a nu produce deplasări inutile, confuzii între loturi sau acumulări nejustificate de producție în curs.

Corelarea configurației fizice cu succesiunea tehnologică reduce distanțele parcurse și timpul dintre operații. Căile destinate personalului trebuie separate, pe cât posibil, de traseele stivuitoarelor, roboților mobili și altor mijloace de manipulare. Zonele-tampon trebuie dimensionate și delimitate clar, astfel încât să susțină continuitatea procesului fără a ascunde blocajele; o zonă-tampon nedimensionată transformă o problemă de sincronizare într-un stoc permanent, iar cauza inițială devine invizibilă [83].

Schimbările de stare, identitate sau responsabil al materialului definesc punctele de înregistrare: recepție, eliberare din depozit, început și sfârșit de operație, rezultate ale verificărilor, transfer în ambalare și confirmarea expedierii. Acestea conectează traseul fizic cu cel informațional. Standardele de vizibilitate în lanțul de aprovizionare structurează evenimentele pe patru dimensiuni — obiect, moment, loc și context de proces, permițând corelarea înregistrărilor din puncte și sisteme diferite [84]. Punctele se stabilesc înaintea selectării echipamentelor de colectare, pentru amplasarea senzorilor în funcție de valoarea datelor pentru urmărirea comenzii, nu de comoditatea instalării.

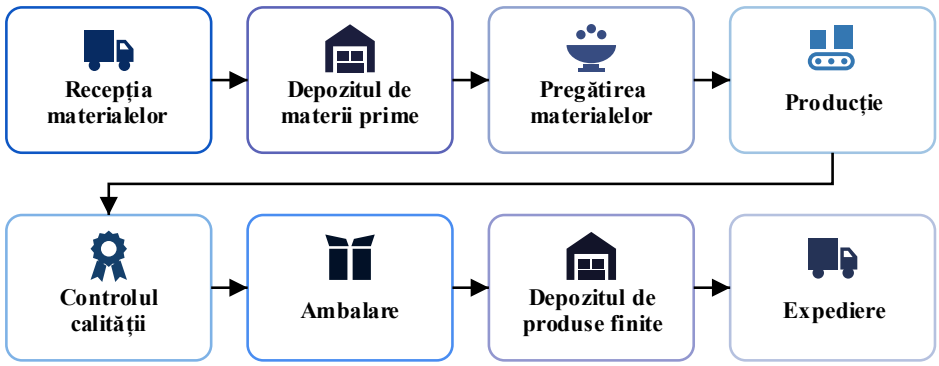


Figura 2.3 – Fluxul fizic al materialelor, de la recepție la expediere

2.2.4. Relația cu infrastructura de automatizare și comunicație

Amplasarea fizică a proceselor influențează și arhitectura sistemelor de automatizare și comunicație. Senzorii și actuatoarele sunt instalate în apropierea procesului monitorizat sau controlat, iar automatele programabile și echipamentele de comunicație sunt amplasate, de regulă, în dulapuri electrice asociate utilajelor, liniilor ori celulelor de producție.

Comutatoarele industriale, gateway-urile industriale și punctele de interconectare trebuie distribuite astfel încât lungimea cablurilor, expunerea la perturbații și numărul legăturilor vulnerabile să fie limitate. Echipamentele destinate procesării edge pot fi amplasate în apropierea celulelor pe care le deservesc, în timp ce serverele SCADA, bazele de date și celelalte sisteme centralizate sunt instalate, de regulă, în spații tehnice protejate. Rolul funcțional al acestor echipamente este tratat în Capitolul 5, iar modul în care se organizează într-o arhitectură completă, în Cap. 7.

Zonele fizice ale fabricii pot constitui punctul de plecare pentru segmentarea rețelei industriale. O linie de producție, o celulă robotizată sau o instalație tehnologică poate fi organizată ca zonă distinctă de comunicație, cu acces controlat către celelalte sisteme. Configurația rețelei nu trebuie însă să reproducă automat amplasarea fizică. Delimitarea zonelor și a rețelei de comunicație rezultă dintr-o evaluare a riscului, în care se analizează funcția, criticitatea, expunerea și consecințele compromiterii activelor, nu poziția lor în hală [85]; două utilaje aflate unul lângă altul pot aparține unor zone distincte, iar echipamente aflate în hale diferite pot avea aceleași cerințe de securitate. Criteriile de aplicare sunt tratate în secțiunea 8.3.

Locul instalării expune echipamentele la temperatură, umiditate, vibrații, praf, agenți de răcire și câmpurile electromagnetice ale motoarelor și convertizoarelor. Protecția necesară se verifică prin codul IP al carcasei, pentru corpuri solide și apă [86], și prin nivelurile de imunitate electromagnetică industrială [67]. Condițiile influențează cablurile, ecranarea, separarea traseelor de forță și semnal și, uneori, alegerea comunicației fără fir. Neglijarea lor poate provoca defectări premature și întreruperi intermitente ale comunicației, dificil de identificat când dispar la verificarea instalației oprite.

Proiectarea spațiilor, a fluxului materialelor și a infrastructurii digitale trebuie realizată coordonat. Configurația fabricii arată unde se află materialele și unde pot fi ele observate; ea nu explică însă cum ajunge o cerință a clientului să se transforme într-un ordin de lucru și într-o operație executată. Secțiunea următoare va prezenta fluxul informațional care însoțește o comandă, de la solicitarea clientului până la producție, livrare și feedback.

2.3. Fluxul informațional și fizic al unei comenzi

O comandă industrială declanşează o succesiune de activităţi comerciale, tehnice, logistice şi productive. Parcursul acesteia este susţinut de fluxul informaţional, prin care sunt transmise cerinţele clientului, documentaţia produsului, necesarul de materiale, planurile de producţie, instrucţiunile de lucru, starea execuţiei şi rezultatele verificărilor. Traseul complet al comenzii, de la cerinţa clientului până la livrare şi feedback, este ilustrat în Figura 2.4.

Fluxul informaţional trebuie corelat permanent cu fluxul fizic prezentat în secţiunea 2.2; orice diferenţă dintre informaţia disponibilă în sistem şi situaţia reală din fabrică poate conduce la utilizarea unor materiale necorespunzătoare, executarea unei versiuni greşite a produsului, întârzieri sau pierderea trasabilităţii. Corelarea este obiectul explicit al modelelor de integrare a funcţiilor întreprinderii cu cele de control al fabricaţiei, care definesc categoriile de informaţii schimbate între planificarea comenzii şi execuţia ei [75], iar activităţile prin care aceste informaţii sunt produse şi consumate în interiorul fabricii – programarea detaliată, lansarea, execuţia, colectarea datelor, urmărirea şi analiza performanţei – sunt descrise ca model de referinţă în partea a treia a aceleiaşi serii [87].

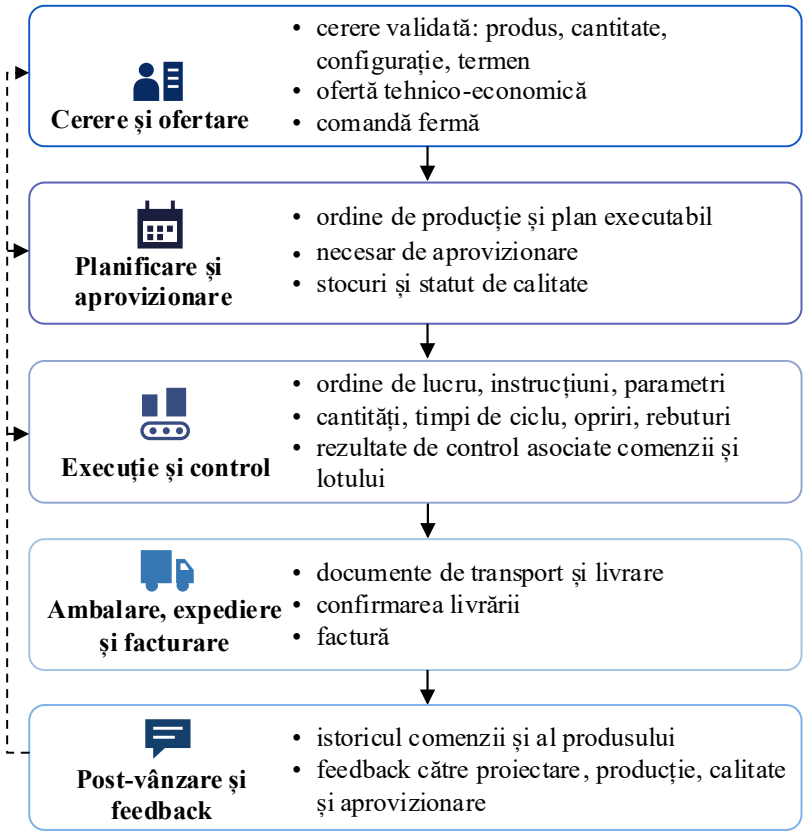


Figura 2.4 – Fluxul informațional al unei comenzi

Un element determină, mai mult decât altele, forma întregului flux: momentul în care comanda clientului se atașează produsului. Acest punct de decuplare separă zona în care activitatea este condusă de prognoză de zona în care este condusă de comandă, iar poziția lui distinge fabricația pe stoc, asamblarea la comandă, fabricația la comandă și proiectarea la comandă [88]. Poziția punctului de decuplare stabilește, implicit, și locul din flux în care identificatorul comenzii trebuie atașat fizic materialului, aspect reluat în secțiunea 2.5.2 și dezvoltat în Capitolul 3.

2.3.1. Primirea și validarea cererii clientului

Fluxul începe prin primirea unei solicitări de ofertă sau a unei comenzi. Departamentul de vânzări înregistrează informațiile într-un sistem pentru gestionarea relațiilor cu clienții (CRM) sau în sistemul ERP.

Cererea trebuie să precizeze produsul, cantitatea, configurația, materialele, cerințele de calitate, termenul și condițiile de livrare. Pentru produsele standard, validarea poate fi realizată rapid. În cazul produselor personalizate, proiectarea, producția, calitatea și aprovizionarea trebuie să confirme fezabilitatea tehnică și disponibilitatea resurselor.

Clarificarea cerințelor în această etapă reduce riscul modificărilor ulterioare, când materialele pot fi deja comandate, iar capacitatea de producție rezervată.

2.3.2. Ofertarea și confirmarea comenzii

Pe baza cerințelor validate este elaborată oferta tehnico-economică. Stabilirea prețului și a termenului necesită estimarea consumurilor, a timpilor de fabricație, a costurilor materialelor și a capacității disponibile.

Acceptarea ofertei conduce la înregistrarea unei comenzi ferme. Specificațiile aprobate, cantitățile, termenul și versiunea documentației trebuie păstrate într-o formă controlată. Orice modificare ulterioară trebuie evaluată și comunicată compartimentelor afectate înainte de introducerea sa în producție.

Exactitatea estimărilor din această etapă depinde direct de calitatea datelor istorice privind timpii de execuție, consumurile și rebuturile, deoarece încărcarea capacității se calculează pornind de la aceste valori [78].

O companie care nu colectează sistematic aceste date ofertează pe baza experienței individuale, iar abaterile rezultate se descoperă abia la închiderea comenzii. Efectul este cumulativ: o estimare optimistă nu produce doar o marjă mai mică pe comanda respectivă, ci și o încărcare a capacității care nu corespunde realității, cu consecințe asupra tuturor comenzilor programate în aceeași perioadă.

2.3.3. Planificarea și lansarea în producție

Comanda clientului este transformată în unul sau mai multe ordine de producție. Planificarea stabilește operațiile necesare, succesiunea acestora, termenele, materialele, echipamentele și personalul implicat.

Sistemul ERP gestionează comanda, necesarul de materiale şi resursele întreprinderii, iar sistemul MES poate detalia şi urmări execuţia la nivelul secţiilor, liniilor şi utilajelor. Planificarea trebuie să ţină seama de:

- capacitatea disponibilă a echipamentelor;
- existenţa materialelor şi componentelor;
- disponibilitatea sculelor şi dispozitivelor;
- timpii de pregătire şi de prelucrare;
- operaţiile subcontractate;
- activităţile de control şi mentenanţă;
- comenzile aflate deja în desfăşurare.

Rezultatul acestei etape este un plan executabil, corelat cu situaţia reală din fabrică [78]. Un plan construit pe capacităţi teoretice, care ignoră opririle, timpii de pregătire şi intervenţiile de mentenanţă, devine nerealizabil din primele zile şi este înlocuit, în practică, de decizii luate direct în secţie. Sursa dificultăţii nu este calculul, ci variabilitatea: pe măsură ce gradul de încărcare se apropie de capacitatea nominală, timpul de aşteptare creşte neliniar, astfel încât ultimele procente de utilizare se plătesc prin creşteri disproporţionate ale duratei de trecere [76].

2.3.4. Aprovizionarea şi recepţia materialelor

Dacă materialele necesare nu sunt disponibile, sistemul generează un necesar de aprovizionare. Aprovizionarea selectează furnizorii, transmite comenzile şi urmăreşte termenele de livrare.

La recepţie se verifică cantitatea, documentele şi, după caz, caracteristicile materialelor, actualizând stocurile şi statutul de calitate. Materialele supuse verificării intră în producţie numai după confirmarea conformităţii.

Întârzierile furnizorilor sau respingerea unui lot pot impune replanificarea comenzii. Variabilitatea termenelor de livrare, nu doar valoarea lor medie, determină mărimea stocului de siguranţă necesar pentru a menţine acelaşi nivel de serviciu [79]. Informaţia trebuie transmisă rapid către planificare, producţie, vânzări şi, dacă termenul este afectat, către client.

2.3.5. Execuţia şi urmărirea producţiei

După asigurarea materialelor şi eliberarea documentaţiei, comanda intră în execuţie. Operatorii şi echipamentele primesc ordinele de lucru, instrucţiunile, desenele şi parametrii necesari fiecărei operaţii.

Pe parcursul producţiei sunt înregistrate cantităţile realizate, timpii de ciclu, opririle, consumurile, alarmele, rebuturile şi starea operaţiilor. Datele pot proveni din raportări ale operatorilor, automate programabile, interfeţe HMI, sisteme SCADA şi aplicaţii MES. Colectarea datelor de producţie şi urmărirea execuţiei constituie activităţi distincte în modelul de referinţă al gestionării operaţiunilor de fabricaţie, cu intrări, ieşiri şi responsabilităţi proprii [87]; tratarea lor ca simplă consecinţă a instalării unor senzori este una dintre confuziile frecvente ale proiectelor de digitalizare.

Aceste informaţii permit compararea progresului real cu planul. Apariţia unei defecţiuni, a unei lipse de materiale sau a unei întârzieri poate determina reprogramarea operaţiilor şi actualizarea termenului estimat de finalizare. Diferenţa dintre o raportare manuală, efectuată la sfârşitul schimbului, şi o raportare automată, disponibilă în câteva secunde, nu constă în volumul datelor, ci în intervalul în care mai este posibilă o corecţie.

2.3.6. Controlul calității și gestionarea neconformităților

Controlul calităţii poate fi realizat la recepţia materialelor, pe parcursul procesului şi înaintea livrării. Rezultatele verificărilor trebuie asociate comenzii, lotului, materialelor şi operaţiilor executate.

Identificarea unei neconformităţi poate conduce la reprelucrare, sortare, derogare sau respingerea produsului. Decizia şi rezultatul intervenţiei trebuie înregistrate pentru menţinerea trasabilităţii; păstrarea unor informaţii documentate care permit identificarea elementelor de ieşire ale proceselor este o cerinţă explicită a sistemelor de management al calităţii [80].

Corelarea datelor privind calitatea cu parametrii procesului permite identificarea cauzelor şi prevenirea repetării problemelor la comenzile următoare; această corelare este posibilă numai dacă măsurătoarea de calitate şi parametrii de proces pot fi asociaţi aceleiaşi piese sau aceluiaşi lot, printr-un identificator comun şi o marcă temporală comparabilă – condiţie tratată în Capitolul 7. Fără ea, datele de calitate şi datele de proces rămân două colecţii paralele, fiecare corectă în sine şi niciuna utilizabilă pentru stabilirea unei cauze.

2.3.7. Ambalarea, expedierea și facturarea

Produsele declarate conforme sunt ambalate, etichetate şi transferate în depozitul de produse finite. Logistica grupează produsele în funcţie de comandă şi pregătește documentele de transport şi livrare.

Înaintea expedierii trebuie verificată concordanţa dintre comanda clientului, produsele pregătite, cantităţile, etichetele şi documentele asociate. Această verificare finală, împreună cu înregistrarea rezultatului ei, face parte din controlul elementelor de ieşire cerut sistemelor de management al calităţii [80]. Confirmarea livrării actualizează starea comenzii în sistemul ERP şi permite emiterea facturii.

Trasabilitatea trebuie păstrată până la client, astfel încât produsul livrat să poată fi asociat loturilor de materiale, operaţiilor, verificărilor şi documentelor utilizate. Continuitatea acestei asocieri dincolo de poarta fabricii presupune identificatori care îşi păstrează semnificaţia la partenerii din lanţ: identificatorul articolului comercial, al unităţii logistice şi al locaţiei [52]. Un cod intern, oricât de bine construit, nu poate îndeplini această funcţie decât prin conversii, care sunt ele însele o sursă de erori.

2.3.8. Serviciile post-vânzare şi utilizarea feedbackului

După livrare pot fi necesare instalarea, punerea în funcţiune, mentenanţa, furnizarea pieselor de schimb sau soluţionarea reclamaţiilor. Informaţiile obţinute în această etapă completează istoricul comenzii şi al produsului.

Tabelul 2.4 – Etapele fluxului comenzii, sistemele implicate și riscurile asociate

Etapă	Declanșator	Compartiment responsabil	Sistem principal	Informații esențiale	Risc tipic în lipsa datelor
Primirea și validarea cererii	Solicitarea clientului	Vânzări	CRM sau ERP	Produs, cantitate, configurație, termen	Acceptarea unei cerințe nefezabile tehnic
Ofertarea și confirmarea	Cerință validată	Vânzări, proiectare, planificare	ERP	Costuri estimate, timpi, capacitate disponibilă	Termen și preț stabilite pe estimări nefundamentate
Planificarea și lansarea	Comandă fermă	Planificare	ERP și MES	Ordine de producție, operații, resurse, termene	Plan bazat pe capacitate teoretică, nerealizabil
Aprovizionarea și recepția	Necesar de materiale	Achiziții, logistică, calitate	ERP	Stocuri, termene furnizori, statut de calitate	Lansare în producție cu materiale neconfirmate
Execuția și urmărirea	Eliberarea documentației	Producție	MES, SCADA, HMI, PLC	Cantități, timpi de ciclu, opriri, alarme, consumuri	Abaterea față de plan se descoperă prea târziu
Controlul calității	Finalizarea unei operații	Calitate	MES și sisteme de management al calității	Măsurători, neconformități, decizii, loturi	Imposibilitatea identificării cauzei unui defect
Ambalarea și expedierea	Produse conforme	Logistică	ERP și sisteme de management al depozitului	Componență set, etichete, documente de transport	Livrare incompletă sau etichetată greșit
Facturarea	Confirmarea livrării	Financiar	ERP	Cantități livrate, prețuri, termene de plată	Facturare neconcordantă cu livrarea reală
Serviciile post-vânzare	Utilizarea produsului	Service, calitate, proiectare	CRM și ERP	Defecte, intervenții, reclamații, piese consumate	Repetarea acelorași cauze la comenzile următoare

Feedbackul privind funcţionarea, defectele şi experienţa clientului trebuie transmis către proiectare, producţie, calitate şi aprovizionare. Astfel, informaţiile post-

vânzare pot contribui la îmbunătățirea produselor, actualizarea instrucțiunilor și eliminarea cauzelor unor probleme recurente.

Sistemele informatice care susțin etapele acestui traseu, de la preluarea comenzii până la livrare, sunt reprezentate în Figura 2.5. Etapele parcurse, sistemele implicate și riscurile asociate fiecărei tranziții sunt sintetizate în Tabelul 2.4.

Coerența dintre fluxul informațional și cel fizic permite urmărirea comenzii, menținerea documentației actualizate și coordonarea activităților.

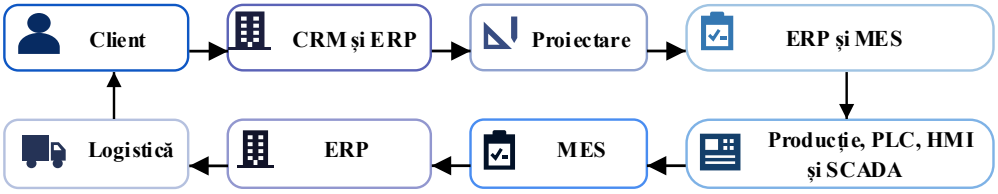


Figura 2.5 – Sistemele informatice care susțin fluxul comenzii

2.3.9. Durata totală de realizare a comenzii și componentele acesteia

Durata totală de realizare a comenzii, măsurată din momentul primirii cererii până la livrare, se compune din intervale de natură foarte diferită: timp de decizie, de așteptare, de aprovizionare, de pregătire și timp de transformare efectivă a materialului. Distincția are consecințe practice directe, deoarece fiecare categorie răspunde la alt tip de intervenție. Separarea activităților care modifică produsul de cele care doar îl deplasează, îl păstrează sau îl așteaptă constituie, de altfel, punctul de plecare al analizei fluxului de valoare [83].

Raportul dintre timpul în care produsul este efectiv transformat și durata totală se numește eficiență a fluxului și se calculează cu relația:

$$E_{flux} = T_{transformare} / T_{total} \cdot 100 \quad [\%] \qquad (2.1)$$

Tabelul 2.5 – Descompunerea duratei de realizare a unei comenzi (valori orientative)

Etapă	Natura intervalului	Durată [h]
Primirea și validarea cererii	Decizie	4
Ofertarea și confirmarea	Decizie	16
Proiectarea și pregătirea documentației	Pregătire	12
Planificarea și lansarea	Decizie	4
Aprovizionarea materialelor lipsă	Așteptare externă	40
Așteptarea în coadă înaintea execuției	Așteptare internă	24
Execuția operațiilor de prelucrare și asamblare	Transformare	6
Controlul calității	Transformare (confirmare)	2
Ambalarea	Transformare	1
Așteptarea expedierii	Așteptare internă	8
Transportul la client	Transfer	12
Total	—	129

în care termenul de la numărător reprezintă suma duratelor operațiilor care modifică produsul sau confirmă conformitatea acestuia, iar numitorul este durata totală măsurată de la primirea cererii până la livrarea către client, adică suma tuturor etapelor din Tabelul 2.5.

Pentru ilustrare se consideră o comandă de produse personalizate, cu materiale parțial indisponibile în stoc. Valorile din Tabelul 2.5 sunt exprimate în ore lucrătoare și au caracter orientativ; nu provin dintr-o măsurătoare, ci sunt alese pentru a evidenția proporțiile tipice.

Înlocuind în relația (2.1):

$$E_{flux} = (6 + 2 + 1) / 129 \cdot 100 = 9 / 129 \cdot 100 = 6{,}98\ \% \approx 7\ \%$$

Rezultatul arată că produsul este efectiv transformat în aproximativ 7 % din durata totală. Restul de 93 % este format din decizii, așteptări și transferuri. Consecința pentru un proiect IIoT este directă și adesea contraintuitivă: o reducere cu 20 % a timpului de prelucrare, obținută prin optimizarea regimurilor de așchiere sau prin creșterea vitezei unui utilaj, scurtează durata totală cu 1,2 h, adică sub 1 %. În schimb, reducerea la jumătate a celor 24 h de așteptare în coadă înaintea execuției scurtează durata totală cu 12 h, adică 9,3 % – de zece ori mai mult, cu o investiție tehnologică incomparabil mai mică.

Efectul poate fi exprimat și în comenzi, nu doar în ore, printr-o relație valabilă pentru orice sistem stabil, indiferent de distribuția sosirilor sau de disciplina cozii [89]:

$$L = \lambda \cdot W \qquad (2.2)$$

în care L este numărul mediu de comenzi aflate simultan în sistem, λ este ritmul mediu de lansare, iar W este durata medie de trecere. Pentru o fabrică ce lansează în medie 3 comenzi pe zi lucrătoare, cu W = 129 h ≈ 16,1 zile, rezultă:

$$L = 3 \cdot 16{,}1 \approx 48 \text{ comenzi}$$

Reducerea așteptării în coadă de la 24 h la 12 h coboară durata de trecere la 117 h ≈ 14,6 zile, deci L ≈ 44 comenzi. Aproximativ patru comenzi și jumătate dispar permanent din fabrică: mai puține materiale imobilizate, mai puține poziții de urmărit, mai puține componente care se pot amesteca. Relația arată și reciproca, utilă în practică: reducerea deliberată a numărului de comenzi lansate simultan scurtează durata de trecere fără nicio intervenție asupra echipamentelor.

Interpretarea nu diminuează importanța disponibilității utilajelor, care rămâne esențială atunci când echipamentul constituie o restricție de capacitate. Ea indică însă unde trebuie căutate primele câștiguri: în vizibilitatea asupra cozilor, a stocurilor intermediare, a stadiului aprovizionării și a momentului în care o comandă poate fi lansată – mărimi care se obțin din date de stare și de identificare, nu din măsurători de proces rapide.

Limitele calculului trebuie precizate. Valorile sunt orientative şi diferă semnificativ între tipurile de producţie; într-o producţie de masă cu materiale în stoc, eficienţa fluxului poate depăşi 30 %, iar în producţia unicat cu componente de import poate coborî sub 2 %. Calculul presupune, de asemenea, o succesiune strict secvenţială, în timp ce în practică unele activităţi se desfăşoară în paralel, iar orele lucrătoare nu coincid cu timpul calendaristic perceput de client. Relaţia (2.2) este valabilă pentru un sistem în regim stabil, pe intervale suficient de lungi; aplicarea ei la o perioadă cu variaţii mari ale ritmului de lansare produce rezultate lipsite de semnificaţie. Pentru o utilizare corectă, ambele mărimi trebuie determinate pe date proprii, pe o familie de produse omogenă şi pe un număr suficient de comenzi.

Parcursul comenzii nu se limitează la interiorul fabricii, deoarece realizarea şi livrarea produsului depind şi de relaţiile companiei cu furnizorii, transportatorii, subcontractanţii şi ceilalţi parteneri externi. Aşa cum arată Tabelul 2.5, cel mai lung interval al exemplului analizat (aprovizionarea materialelor lipsă, de 40 h) este generat în afara fabricii. Secţiunea următoare tratează aceste relaţii.

2.4. Interacțiunea companiei cu mediul extern

O companie industrială nu funcţionează izolat, ci ca parte a unui ecosistem format din clienţi, furnizori, transportatori, prestatori de servicii, autorităţi şi alţi parteneri. Performanţa sa depinde atât de eficienţa proceselor interne, cât şi de capacitatea de a coordona fluxurile de materiale, informaţii şi documente care depăşesc limitele fabricii [79].

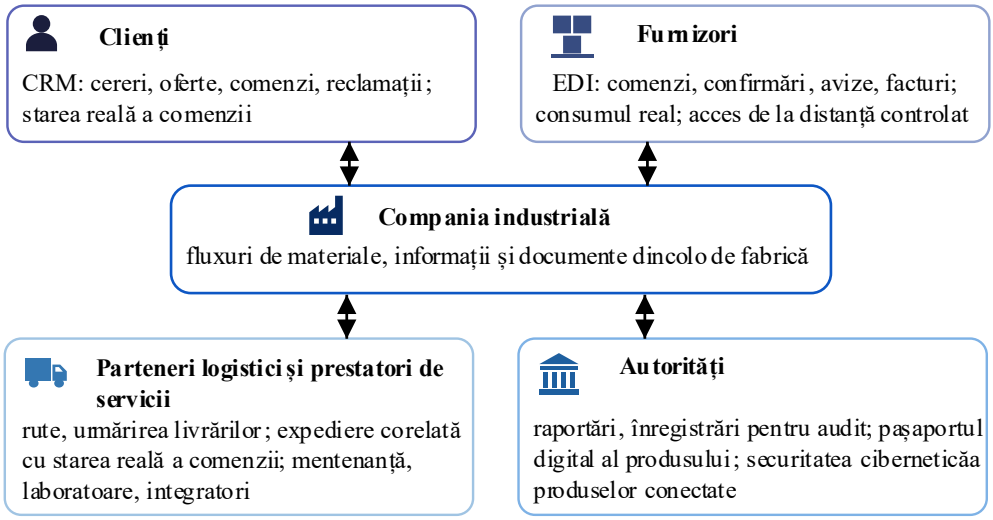


Figura 2.6 – Relațiile companiei industriale cu mediul extern

Relaţiile externe influenţează cererea, disponibilitatea materialelor, costurile, termenele de livrare, conformitatea şi continuitatea producţiei. Integrarea acestora cu procesele interne completează fluxul comenzii prezentat în secţiunea 2.3. Descompunerea din secţiunea 2.3.9 a arătat, de altfel, că cel mai lung interval al unei comenzi poate fi generat în afara fabricii; prin urmare, o parte importantă a câştigurilor de timp nu se obţine prin intervenţii asupra utilajelor, ci prin ameliorarea schimbului de informaţii cu partenerii externi. Principalele relaţii sunt sintetizate în Figura 2.6.

2.4.1. Relaţia cu clienţii

Clienţii reprezintă sursa cererii şi punctul final al lanţului valoric. Relaţia începe prin identificarea necesităţilor şi definirea cerinţelor tehnice şi comerciale, dar continuă pe parcursul proiectării, producţiei, livrării şi utilizării produsului.

Principalele activităţi asociate acestei relaţii includ:

- analizarea cererilor şi acordarea consultanţei tehnice;
- elaborarea şi negocierea ofertelor;
- validarea specificaţiilor şi a termenelor;
- comunicarea stării comenzilor;
- gestionarea modificărilor şi reclamaţiilor;
- furnizarea serviciilor post-vânzare.

În cazul produselor personalizate, clientul poate participa direct la definirea soluţiei, verificarea etapelor intermediare şi aprobarea configuraţiei finale. Informaţiile rezultate trebuie transmise controlat către proiectare, planificare, producţie şi calitate.

Sistemele pentru gestionarea relaţiilor cu clienţii (CRM) permit centralizarea solicitărilor, ofertelor, comenzilor, reclamaţiilor şi istoricului interacţiunilor. Corelarea acestora cu sistemul ERP asigură concordanţa dintre angajamentele comerciale şi capacitatea reală de producţie.

Un aspect frecvent subestimat priveşte momentul în care starea comenzii devine vizibilă pentru client. O informare bazată pe estimări comunicate telefonic diferă esenţial de una derivată din stadiul real al operaţiilor. A doua variantă presupune însă ca datele din producţie să fie corecte, complete şi actualizate, deoarece o stare eronată transmisă automat produce mai multe pagube decât absenţa informaţiei: clientul îşi organizează propriile activităţi în funcţie de ea.

2.4.2. Relaţia cu furnizorii

Furnizorii asigură materiile prime, componentele, echipamentele şi serviciile necesare realizării produselor. Calitatea, costul şi punctualitatea livrărilor influenţează direct continuitatea procesului şi conformitatea produsului final. Evaluarea, selectarea, monitorizarea performanţei şi reevaluarea furnizorilor externi, pe baza

capacității lor de a livra conform cerințelor, constituie o cerință explicită a sistemelor de management al calității [80].

Selectarea furnizorilor trebuie realizată pe baza unor criterii precum:

- capacitatea tehnică;
- calitatea produselor și serviciilor;
- respectarea termenelor;
- costul total al aprovizionării;
- flexibilitatea în cazul modificării cererii;
- respectarea cerințelor de mediu și securitate;
- capacitatea de integrare informațională.

Performanța furnizorilor trebuie evaluată periodic prin indicatori privind livrările la termen, loturile neconforme, timpul de răspuns și respectarea condițiilor contractuale. Pentru componentele critice pot fi necesare audituri, aprobări tehnice și mecanisme suplimentare de trasabilitate.

Dependența de un singur furnizor, întârzierile de transport sau indisponibilitatea unor materiale pot afecta întregul plan de producție. Aceste riscuri pot fi reduse prin diversificarea surselor, stabilirea unor alternative aprobate, utilizarea stocurilor de siguranță și monitorizarea anticipată a perturbărilor.

Există însă și o categorie de perturbări generate chiar de modul în care circulă informația între partenerii lanțului. Atunci când fiecare verigă își construiește previziunile exclusiv pe comenzile primite de la veriga imediat următoare, variația cererii se amplifică pe măsura îndepărtării de client, fenomen cunoscut ca efect de bici; printre cauzele identificate se numără prelucrarea locală a semnalului cererii, comenzile în loturi, fluctuațiile de preț și raționalizarea în perioadele de penurie [90]. Consecința practică este importantă pentru un proiect IIoT: transmiterea către furnizori a consumului real, nu doar a comenzilor agregate, reduce amplificarea și, implicit, stocurile necesare pe întregul lanț. Efectul se obține prin schimb de informație, nu prin capacitate suplimentară.

Schimbul electronic de date (EDI) permite transmiterea standardizată a comenzilor, confirmărilor, avizelor și facturilor. Integrarea acestor informații cu sistemele interne reduce introducerea manuală a datelor și facilitează actualizarea planurilor în funcție de situația reală a aprovizionării.

Colaborarea cu furnizorii de echipamente și servicii tehnice aduce riscuri suplimentare în sistemele conectate. Actualizările software, diagnoza la distanță și intervențiile producătorului creează acces din exterior către echipamentele de control. Ghidurile de securitate OT identifică accesul terților de la distanță printre căile de compromitere cel mai probabil utilizate [25]. Pentru furnizorii de servicii de automatizare și control industrial, seria IEC 62443 prevede un program de securitate privind conturile, accesul la distanță, copiile de siguranță și modificările [91]. Înainte punerii în funcțiune, contractul și soluția tehnică trebuie să precizeze cine

iniţiază accesul, prin ce canal, pentru cât timp şi cum se înregistrează activitatea. Secţiunea 8.2 detaliază măsurile tehnice.

2.4.3. Partenerii logistici şi prestatorii de servicii

Transportatorii şi operatorii logistici asigură legătura fizică dintre companie, furnizori şi clienţi. Atunci când activităţile sunt externalizate, compania poate colabora cu furnizori terţi de servicii logistice. Decizia de externalizare urmează aceleaşi criterii ca orice alegere privind structura lanţului de aprovizionare: costul total, gradul de control asupra serviciului şi capacitatea de a răspunde la variaţii ale cererii [79].

Coordonarea logistică trebuie să ţină seama de disponibilitatea produselor, ferestrele de încărcare, capacitatea mijloacelor de transport, condiţiile de manipulare şi termenele asumate faţă de client. Informaţiile privind expedierea trebuie corelate cu starea reală a comenzii, pentru a evita programarea transportului înaintea finalizării producţiei sau menţinerea inutilă a produselor în depozit.

Sistemele pentru gestionarea transportului pot susține planificarea rutelor, selectarea transportatorilor, urmărirea livrărilor şi evaluarea costurilor. Datele privind poziţia transportului, întârzierile sau confirmarea livrării completează trasabilitatea comenzii în afara fabricii.

Companiile pot colabora şi cu laboratoare, firme de mentenanţă, integratori de sisteme, furnizori de servicii informatice sau subcontractanţi. Accesul acestora la echipamente, documente şi sisteme trebuie delimitat prin responsabilităţi, condiţii contractuale şi măsuri de securitate clar definite.

2.4.4. Relația cu autoritățile și organismele de reglementare

Activitatea industrială trebuie să respecte cerinţele privind fiscalitatea, protecţia mediului, sănătatea şi securitatea în muncă, trasabilitatea, protecţia datelor şi comercializarea produselor. În funcţie de domeniu, pot fi necesare autorizaţii, certificări, inspecţii şi raportări periodice.

Compania trebuie să păstreze înregistrări care demonstrează conformitatea materialelor, proceselor şi produselor. Datele privind consumurile, emisiile, deşeurile, incidentele şi rezultatele verificărilor trebuie să fie corecte, complete şi disponibile pentru audit.

Digitalizarea raportărilor poate reduce volumul documentelor şi timpul necesar pregătirii informaţiilor, dar impune reguli privind validarea, păstrarea şi protejarea datelor. Automatizarea colectării nu elimină responsabilitatea companiei de a verifica exactitatea informaţiilor transmise.

Cadrul de reglementare european a evoluat în două direcţii cu efect direct asupra sistemelor conectate. Prima priveşte securitatea produselor cu elemente digitale: Regulamentul (UE) 2024/2847 stabileşte obligaţii pentru fabricanţi privind

securitatea pe durata ciclului de viaţă, gestionarea vulnerabilităţilor şi raportarea incidentelor [69]. Obligaţiile de raportare se aplică din 11 septembrie 2026, iar ansamblul cerinţelor, din 11 decembrie 2027. Cerinţele privesc atât companiile care fabrică echipamente conectate, cât şi pe cele care le integrează în propriile produse. Acestea sunt tratate în secţiunea 8.3.9.

A doua direcţie priveşte informaţia despre produs. Regulamentul (UE) 2024/1781 instituie cadrul pentru cerinţele de proiectare ecologică şi introduce paşaportul digital al produsului, un set structurat de informaţii despre compoziţie, durabilitate, reparabilitate şi trasabilitate, accesibil pe tot parcursul ciclului de viaţă [92]. Cerinţele concrete se stabilesc pe grupe de produse, prin acte delegate. Pentru o companie industrială, consecinţa practică este că o parte dintre datele colectate astăzi pentru uz intern – provenienţa materialelor, componenţa produsului, operaţiile executate – devin informaţii care trebuie păstrate într-o formă structurată şi puse la dispoziţie în afara organizaţiei.

2.4.5. Digitalizarea colaborării și integrarea orizontală

Digitalizarea relaţiilor externe poate fi realizată prin portaluri pentru clienţi şi furnizori, schimb electronic de documente, platforme colaborative și sisteme pentru urmărirea comenzilor şi transporturilor. Aceste instrumente reduc întârzierile informaţionale și permit actualizarea mai rapidă a planurilor. Nivelurile posibile ale acestei colaborări diferă prin efort, prin beneficii şi prin riscurile pe care le introduc. Ele sunt comparate în Tabelul 2.6.

Integrarea orizontală, introdusă în Capitolul 1, extinde conectarea proceselor dincolo de limitele companiei. Cererea clientului, capacitatea furnizorului, disponibilitatea materialelor, starea producţiei şi situaţia transportului pot fi corelate într-un flux informaţional comun. O întârziere confirmată de furnizor poate determina replanificarea producţiei, iar finalizarea unei comenzi poate declanșa automat pregătirea transportului și notificarea clientului.

Schimbul de date între organizaţii trebuie să utilizeze identificatori, formate şi reguli comune. Utilizarea unor sisteme de identificare standardizate pentru produse, unităţi logistice şi locaţii permite ca aceeaşi entitate fizică să fie recunoscută identic de partenerii din lanţ, fără conversii manuale şi fără riscul asocierilor greşite [52], iar structurarea evenimentelor de vizibilitate după dimensiunile obiect–moment–loc–context face ca înregistrările provenite de la parteneri diferiţi să poată fi reunite într-un istoric coerent al produsului [84]. Fără o astfel de convenţie, integrarea se reduce la transferul unor fişiere pe care fiecare parte le reinterpretează după reguli proprii.

Sunt necesare, de asemenea, stabilirea responsabilităţii pentru actualizarea informaţiilor, controlul accesului şi protejarea datelor comerciale şi tehnice. Integrarea nu trebuie să ofere partenerilor acces necontrolat la sistemele interne, ci numai la informaţiile necesare relaţiei contractuale. Principiul aplicabil este acordarea

drepturilor minime necesare îndeplinirii unei funcţii determinate, pentru un interval determinat.

Alegerea nivelului nu trebuie făcută după gradul de noutate tehnologică, ci după frecvenţa schimbului, volumul datelor şi consecinţele unei informaţii întârziate. Pentru un furnizor de la care se comandă de două ori pe an, transmiterea prin poştă electronică rămâne rezonabilă; pentru un furnizor care livrează zilnic componente critice, aceeaşi soluţie devine o sursă permanentă de erori.

Prin conectarea proceselor interne cu cele ale clienţilor, furnizorilor şi partenerilor logistici, compania poate obţine o imagine mai completă asupra lanţului de aprovizionare şi poate reacţiona mai rapid la perturbări. Elementele prezentate până aici – structura organizaţională, configuraţia fabricii, fluxul comenzii şi relaţiile externe – se manifestă însă simultan într-o companie reală. Secţiunea următoare le reunește într-un scenariu didactic construit pentru această lucrare.

Tabelul 2.6 – Niveluri de digitalizare a colaborării cu partenerii externi

Nivel	Mod de schimb	Efort de implementare	Beneficiu principal	Risc și limitare
Documente transmise prin poștă electronică	Fișiere atașate, formate neuniforme	Minim	Nu necesită investiții	Reintroducere manuală, versiuni necontrolate, erori de transcriere
Portal pentru clienți sau furnizori	Acces la o interfață pusă la dispoziție de una dintre părți	Redus spre mediu	Informație unică, actualizată, fără schimb de fișiere	Partenerul trebuie să consulte activ portalul; date nepreluate automat în sistemele proprii
Schimb electronic structurat (EDI)	Mesaje standardizate între sisteme	Mediu	Preluare automată a comenzilor, avizelor și facturilor	Necesită acord asupra formatelor; modificările se negociază bilateral
Interfețe de programare a aplicațiilor	Interogare directă între sisteme, în timp aproape real	Mediu spre ridicat	Stare actualizată permanent; declanșarea automată a acțiunilor	Expunere sporită; necesită autentificare, limitarea drepturilor și monitorizarea accesului
Platformă colaborativă comună	Spațiu de date partajat între mai mulți parteneri	Ridicat	Vizibilitate asupra întregului lanț, replanificare coordonată	Guvernanța datelor, proprietatea informațiilor și dependența de un operator terț

2.5. Scenariu didactic: structura funcțională și fluxul operațional într-o fabrică de mobilier modular

Scenariul prezentat în continuare este construit în scop didactic; el nu descrie o companie identificabilă şi nu conţine date măsurate într-o fabrică reală. Configuraţia, succesiunea operaţiilor şi tipurile de date au fost alese astfel încât să reunească, într-un singur exemplu coerent, elementele tratate în secţiunile 2.1–2.4. Valorile

care apar în text au rol ilustrativ; ele nu trebuie preluate ca repere de proiectare și nu susțin nicio comparație de performanță între soluții.

Scenariul se referă la o fabrică de dimensiune medie, orientată către realizarea mobilierului modular personalizat pentru clienți rezidențiali și comerciali. Produsele diferă prin dimensiuni, configurație și finisaje, dar utilizează materiale comune, precum plăci aglomerate din lemn melaminate, plăci din fibre de densitate medie și elemente standardizate de feronerie.

Personalizarea necesită flexibilitate în proiectare și producție; materialele și operațiile comune susțin standardizarea parțială. Fabrica gestionează varietatea produselor, termenele de livrare, disponibilitatea materialelor și trasabilitatea componentelor pe comandă. Punctul de decuplare (secțiunea 2.3) definește regimul de fabricație la comandă: aprovizionare pe baza prognozei și prelucrare numai după confirmarea configurației. Varietatea ridicată a produselor finale și repetitivitatea operațiilor vor fundamenta, în Capitolul 3, corelarea tipului de producție cu arhitectura IIoT.

2.5.1. Structura funcțională a companiei

Departamentul de vânzări preia solicitările clienților, clarifică cerințele și elaborează ofertele tehnico-economice. După confirmarea comenzii, proiectarea pregătește modelele tridimensionale, desenele de execuție, listele de materiale și fișierele necesare echipamentelor de prelucrare.

Planificarea transformă documentația aprobată în ordine de producție și stabilește succesiunea operațiilor, termenele și resursele necesare. Achizițiile asigură plăcile, feroneria, materialele pentru ambalare și componentele speciale, corelând termenele furnizorilor cu planul de fabricație.

Producția este organizată în zone sau celule destinate debitării, aplicării canturilor, găuririi și frezării, controlului, grupării componentelor și asamblării parțiale. Funcția de calitate verifică dimensiunile, poziția prelucrărilor, aspectul suprafețelor și concordanța componentelor cu documentația comenzii. Logistica pregătește ambalarea, etichetarea, depozitarea temporară și expedierea.

Finanțele, resursele umane, IT și mentenanța susțin operațiunile. Prioritatea mentenanței o constituie utilajele critice de debitare și aplicare a canturilor: deservind întregul flux, oprirea oricăruia blochează rapid toate comenzile, indiferent de configurație. Ca resurse-restricție, disponibilitatea lor afectează direct debitul sistemului; la utilajele cu rezervă de capacitate, fluxul poate absorbi opriri de aceeași durată [76].

Dimensiunea companiei corespunde categoriei mijlocii din Tabelul 2.2. Compartimentul IT este restrâns, iar responsabilitatea asupra echipamentelor de automatizare revine mentenanței, în colaborare cu furnizorii utilajelor. Această repartizare, frecventă în industria prelucrării lemnului, explică de ce o eventuală

implementare IIoT trebuie să pornească de la un domeniu restrâns şi bine delimitat, cu reguli de denumire şi de acces stabilite înainte de prima conectare.

2.5.2. Configuraţia fabricii şi fluxul fizic

Fabrica utilizează o configuraţie semiliniară, completată de celule funcţionale – soluţia mixtă descrisă în secţiunea 2.2.2. Această organizare permite păstrarea unei succesiuni clare a operaţiilor şi prelucrarea simultană a unor comenzi diferite. Traseul rezultat este prezentat în Figura 2.7.

Zona de recepţie este amplasată în apropierea depozitului de materii prime şi permite descărcarea plăcilor, a feroneriei şi a materialelor auxiliare. Materialele sunt verificate, identificate şi transferate în poziţii de depozitare codificate. Înaintea lansării în producţie, componentele necesare sunt alocate comenzilor şi pregătite în funcţie de planul de execuţie.

După debitare, fiecare piesă trebuie identificată şi asociată comenzii din care face parte. Aplicarea unei etichete cu cod de bare sau cod bidimensional permite păstrarea identităţii piesei pe parcursul operaţiilor şi reduce riscul amestecării componentelor provenite din comenzi diferite; utilizarea structurilor de identificare consacrate, în locul unor coduri interne construite ad-hoc, asigură totodată compatibilitatea cu partenerii externi [52].

Momentul etichetării este determinant. Până la debitare, materialul este un lot omogen şi poate fi urmărit la nivel de placă; după debitare, el devine un ansamblu de piese distincte, aparţinând unor comenzi diferite, care nu mai pot fi deosebite vizual. Punctul de debitare coincide astfel cu punctul de decuplare identificat anterior şi constituie locul în care trasabilitatea individuală trebuie să înceapă. O identificare introdusă mai târziu în flux nu poate reconstitui asocierile pierdute; una introdusă mai devreme aplică efort inutil unui material încă nediferenţiat.

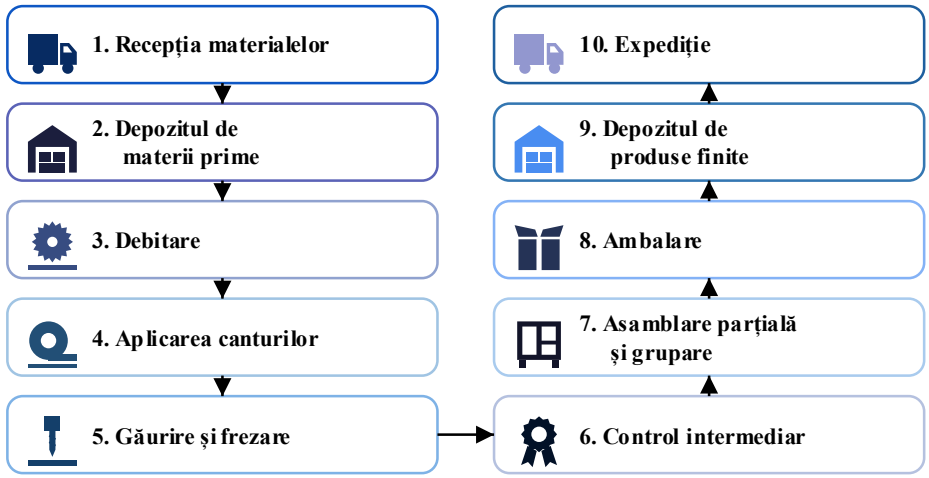


Figura 2.7 – Fluxul fizic principal în scenariul fabricii de mobilier

Componentele sunt verificate înaintea ambalării, apoi sunt grupate în seturi complete. În cazul mobilierului livrat neasamblat, ambalajul trebuie să conţină toate piesele, elementele de feronerie şi instrucţiunile necesare montajului. O componentă lipsă sau etichetată greşit poate face inutilizabil întregul produs, chiar dacă operaţiile de prelucrare au fost executate corect. Verificarea completitudinii setului constituie astfel un punct de control cu efect disproporţionat asupra satisfacţiei clientului, deoarece consecinţa unei erori nu este o abatere dimensională, ci imposibilitatea montajului.

2.5.3. Fluxul informațional al comenzii

Clientul transmite cererea prin poştă electronică, printr-o platformă electronică sau direct către departamentul de vânzări. Informaţiile sunt înregistrate în sistemul CRM şi preluate în ERP după confirmarea configuraţiei, cantităţii, preţului şi termenului.

Proiectarea generează documentaţia produsului, lista de materiale şi fişierele pentru echipamentele cu comandă numerică. Versiunea aprobată este asociată comenzii şi transmisă către planificare şi producţie. Orice modificare ulterioară trebuie controlată, deoarece poate afecta materialele comandate, programele utilajelor, etichetele şi termenul de livrare. În producţia personalizată, modificările solicitate după lansare reprezintă una dintre cauzele principale ale rebuturilor: o piesă debitată conform versiunii anterioare nu poate fi corectată, ci numai refabricată.

ERP verifică disponibilitatea materialelor şi generează necesarul de aprovizionare, iar MES coordonează lansarea şi urmărirea operaţiilor. La nivelul producţiei, automatele programabile, interfeţele HMI şi sistemele SCADA pot furniza date privind starea echipamentelor, timpii de funcţionare, opririle, alarmele şi cantităţile prelucrate. Traseul informațional urmează schema generală prezentată în secțiunea 2.3.8.

Datele raportate din producţie actualizează starea comenzii şi permit identificarea întârzierilor. Rezultatele controlului calităţii sunt asociate pieselor şi loturilor, iar produsele neconforme sunt direcţionate către reprelucrare sau refabricare. După finalizarea şi verificarea tuturor componentelor, sistemul confirmă disponibilitatea comenzii pentru ambalare şi expediere. Circuitul informațional corespunzător este ilustrat în Figura 2.8.

Specificul acestui tip de producţie introduce o dificultate care nu apare în fabricaţia de serie: starea unei comenzi nu poate fi dedusă din poziţia fizică a produsului, deoarece piesele aceleiaşi comenzi se află simultan în etape diferite ale fluxului. O comandă este finalizată numai atunci când toate componentele sale au parcurs toate operaţiile prevăzute. Urmărirea trebuie, prin urmare, să opereze la nivel de piesă şi să calculeze starea comenzii prin agregare, nu invers. Consecinţa asupra modelului de date este directă: entitatea urmărită este piesa, identificată individual,

iar comanda devine o mulţime de piese cu o regulă de completitudine, nu un obiect cu stare proprie.

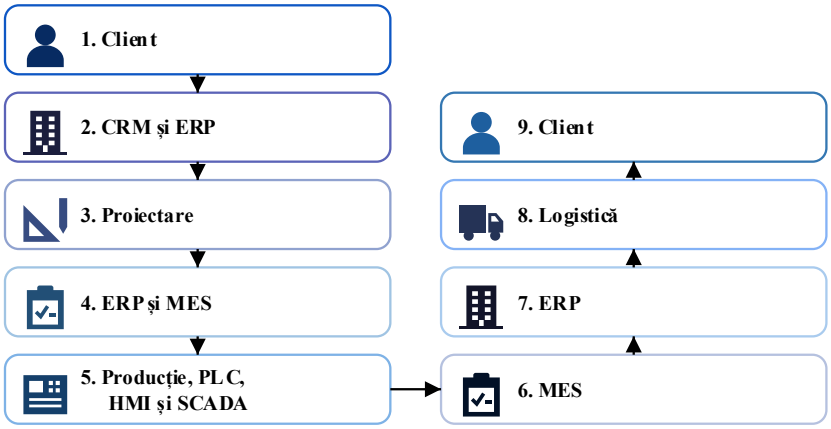


Figura 2.8 – Fluxul informațional în scenariul fabricii de mobilier

2.5.4. Puncte de integrare digitală şi criterii de evaluare

Integrarea dintre proiectare, ERP, MES şi echipamentele de producţie reduce introducerea repetată a datelor şi riscul utilizării unei documentaţii neactualizate. Identificarea automată a pieselor susţine trasabilitatea, iar monitorizarea stării utilajelor permite raportarea opririlor şi planificarea intervenţiilor de mentenanţă.

Principalele puncte în care digitalizarea poate îmbunătăţi fluxul, împreună cu datele necesare şi cu efectul urmărit, sunt sintetizate în Tabelul 2.7.

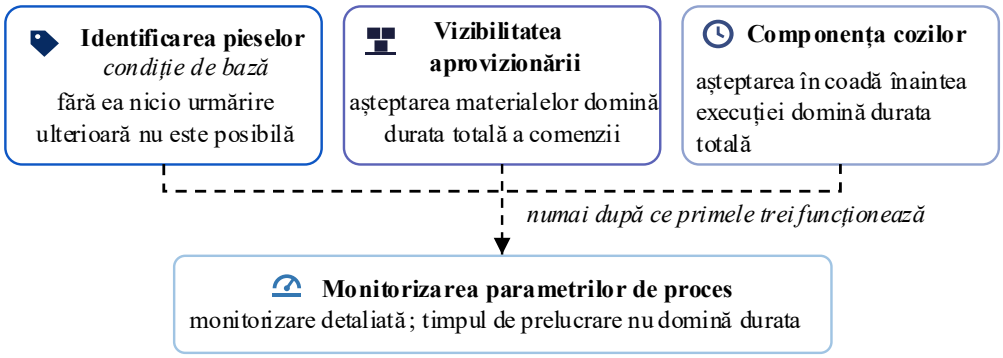


Figura 2.9 – Ordinea de implementare a intervențiilor digitale în scenariul analizat

Ordinea de implementare are, în acest scenariu, o justificare cantitativă. Aplicând raţionamentul din secţiunea 2.3.9, se observă că intervalele care domină durata totală sunt aşteptarea materialelor şi aşteptarea în coadă înaintea execuţiei, nu timpul de prelucrare. Primele intervenţii cu efect măsurabil sunt, prin urmare, cele care fac vizibile stadiul aprovizionării şi componenţa cozilor, împreună cu

identificarea pieselor – condiția tehnică fără de care nicio urmărire ulterioară nu este posibilă. Monitorizarea detaliată a parametrilor de proces are sens numai după ce aceste elemente funcționează (Figura 2.9).

Tabelul 2.7 – Puncte de integrare digitală în scenariul analizat

Punct de integrare	Locul în flux	Date necesare	Efect urmărit
Preluarea controlată a configurației aprobate	Vânzări – proiectare	Configurație, dimensiuni, finisaje, versiune aprobată	Eliminarea reintroducerii manuale și a interpretărilor divergente
Transferul listelor de materiale și al fișierelor de prelucrare	Proiectare – producție	Listă de materiale, programe pentru comandă numerică, versiune	Excluderea utilizării unei documentații depășite
Identificarea pieselor la debitare	Debitare	Identificator unic al piesei, ordin de producție, poziție în ansamblu	Trasabilitate individuală de la prima operație
Urmărirea progresului fiecărei comenzi	Toate operațiile	Citiri ale identificatorului, marcă temporală, post de lucru	Stare reală a comenzii, calculată prin agregarea pieselor
Înregistrarea opririlor și a cauzelor	Utilaje critice	Stare utilaj, durata opririi, motiv codificat	Baza pentru calculul disponibilității și pentru planificarea mentenanței
Corelarea neconformităților cu procesul	Control intermediar și final	Rezultatul verificării, identificator piesă, parametri de proces, utilaj	Identificarea cauzei, nu numai a efectului
Verificarea completitudinii seturilor	Înaintea ambalării	Componență teoretică a setului, piese confirmate ca prezente	Prevenirea livrărilor incomplete
Actualizarea stării comenzii și a documentelor de livrare	Expediere	Confirmarea ambalării, cantități, documente asociate	Informare corectă a clientului și facturare concordantă

Un ultim element ține de evoluția cerințelor externe. Mobilierul figurează printre grupele de produse prioritare din primul plan de lucru adoptat în temeiul reglementării privind proiectarea ecologică [93], ceea ce înseamnă că informațiile despre compoziția produsului, proveniența materialelor și posibilitatea de dezasamblare pot deveni obligatorii într-o formă structurată.

Datele colectate pentru trasabilitatea internă și cele necesare conformării la aceste cerințe provin, în bună măsură, din aceleași înregistrări; proiectarea sistemului de identificare ținând seama de ambele utilizări evită o intervenție ulterioară costisitoare.

Scenariul evidențiază faptul că performanța fabricii nu depinde numai de viteza fiecărui utilaj. Rezultatul este determinat de sincronizarea proiectării, aprovizionării, producției, controlului și logisticii, precum și de concordanța permanentă dintre informațiile din sistem și situația fizică a materialelor și produselor.

2.6. Concluzii

Funcţionarea companiei industriale presupune coordonarea continuă a structurii organizaţionale, configuraţiei fizice şi fluxurilor materiale şi informaţionale. Execuţia comenzii conectează succesiv vânzările, proiectarea, planificarea, aprovizionarea, producţia, calitatea, mentenanţa şi logistica prin dependenţe şi schimburi de date. Cartografierea acestor schimburi fundamentează proiectul IIoT. Implementarea dezvoltă capacitatea de prelucrare a informaţiilor în punctele unde coordonarea activităţilor o impune.

Amplasarea fizică a activităţilor condiţionează atât eficienţa fluxului de materiale, cât şi arhitectura infrastructurii de automatizare. Alegerea unei configuraţii – pe produs, pe proces, celulară sau cu poziţie fixă – determină lungimea traseelor, volumul producţiei în curs şi modul în care pot fi colectate datele, iar compararea variantelor se poate face cantitativ, prin intensitatea legăturilor dintre zone şi distanţele parcurse. Punctele în care materialul îşi schimbă starea, identitatea sau responsabilul sunt şi punctele naturale de înregistrare. Delimitarea zonelor de comunicaţie poate porni de la zonele fizice, dar nu trebuie să le reproducă automat, deoarece criteriul determinant este funcţia, criticitatea şi expunerea activelor, nu poziţia lor în hală.

Parcursul comenzii evidenţiază prioritatea coerenţei dintre informaţie şi realitate faţă de viteza etapelor individuale. Punctul asocierii comenzii cu produsul structurează fluxul şi stabileşte începutul trasabilităţii individuale. Transformarea efectivă ocupă o mică parte din durata percepută de client, dominată de decizii, aşteptări şi transferuri. Relaţia dintre numărul comenzilor simultane, ritmul lansării şi durata de trecere indică posibilitatea unor îmbunătăţiri fără modificarea echipamentelor. Astfel, primele rezultate ale implementării conectate provin, de regulă, din vizibilitatea asupra cozilor, stocurilor şi stadiului aprovizionării, mai degrabă decât din accelerarea prelucrării.

Performanţa nu este determinată exclusiv de capacitatea echipamentelor, ci şi de continuitatea fluxului, disponibilitatea informaţiilor corecte şi capacitatea organizaţiei de a reacţiona la modificări, întârzieri, defecţiuni şi neconformităţi. Relaţiile cu furnizorii, clienţii şi partenerii logistici extind aceste dependenţe dincolo de limitele fabricii, iar modul în care circulă informaţia între verigile lanţului poate genera el însuşi perturbări, independent de capacitatea de producţie. Nivelul de digitalizare a colaborării externe trebuie ales după frecvenţa schimbului şi consecinţele unei informaţii întârziate, nu după gradul de noutate tehnologică, iar deschiderea către parteneri presupune identificatori comuni, drepturi minime necesare şi responsabilităţi explicite. Accesul de la distanţă al furnizorilor de echipamente rămâne o cale de expunere care trebuie reglementată contractual şi tehnic înainte de punerea în funcţiune.

Scenariul didactic al fabricii de mobilier modular a reunit aceste elemente şi a evidenţiat necesitatea corelării fiecărei componente fizice cu ordinul de producţie,

documentația tehnică și rezultatele verificărilor. El a arătat, de asemenea, că într-o producție personalizată starea unei comenzi nu poate fi dedusă din poziția fizică a produsului, ci trebuie calculată prin agregarea stărilor individuale ale pieselor, ceea ce face din piesă, nu din comandă, entitatea urmărită. Integrarea sistemelor CRM, ERP, MES și SCADA, împreună cu identificarea automată și colectarea datelor din producție, poate îmbunătăți trasabilitatea, coordonarea și utilizarea resurselor, dar nu poate compensa o organizare incoerentă.

Înțelegerea acestor relații constituie baza pentru analizarea tipurilor de producție și a modelelor de fabricație. Modul de organizare a fluxurilor, volumul datelor generate și cerințele privind infrastructura digitală diferă substanțial în funcție de varietatea produselor, volumul producției și gradul de flexibilitate necesar. Capitolul următor tratează aceste diferențe și corelează fiecare tip de producție cu arhitectura IIoT corespunzătoare.

2.7. Întrebări de verificare

1. *Într-o comandă de produse personalizate, timpul de transformare efectivă a materialului reprezintă aproximativ 7 % din durata totală de realizare. Cu cât se scurtează, aproximativ, durata totală dacă timpul de prelucrare se reduce cu 20 %?*

a) cu aproximativ 20 %, deoarece durata totală scade proporțional cu timpul de prelucrare;
b) cu aproximativ 7 %, deoarece se reduce întreaga componentă productivă;
c) cu aproximativ 93 %, deoarece restul duratei devine inutil;
d) cu aproximativ 1,4 %, deoarece 20 % din 7 % este 1,4 %.

2. *O fabrică lansează în medie 3 comenzi pe zi lucrătoare, iar durata medie de trecere a unei comenzi este de 14,6 zile. Folosind relația $L = \lambda \cdot W$, câte comenzi se află, în medie, simultan în sistem?*

a) aproximativ 17,6 comenzi;
b) aproximativ 4,9 comenzi;
c) aproximativ 44 de comenzi;
d) aproximativ 48 de comenzi.

3. *Ce reprezintă punctul de decuplare într-un flux de comandă?*

a) momentul în care sistemul MES transmite datele către sistemul ERP;
b) punctul în care se oprește fluxul fizic al materialelor din cauza unui blo-caj;
c) momentul în care comanda clientului se atașează produsului, separând zona condusă de prognoză de zona condusă de comandă;
d) locul în care produsul trece din depozitul de materii prime în zona de producție.

4. *Care sunt criteriile după care sunt definite cele patru configurații de bază ale amplasării zonelor într-o fabrică?*

a) numărul de clienți, numărul de furnizori, distanța până la autorități și numărul de schimburi;
b) succesiunea operațiilor, natura tehnologică a operațiilor, familia de pro-duse și poziția fixă a obiectului fabricat;
c) tipul de energie utilizată, nivelul de zgomot, temperatura mediului și co-dul IP al carcaselor;
d) numărul de angajați, suprafața halei, valoarea utilajelor și nivelul stocuri-lor.

5. Care este soluția de amplasare întâlnită cel mai frecvent în practică, deoare-ce fabricile folosesc rareori o configurație pură?

a) o secvență principală de tip linie, combinată cu celule funcționale pentru operațiile cu variabilitate ridicată sau cu timpi de pregătire mari;
b) o configurație exclusiv funcțională, fără traseu principal al produsului;
c) o linie unică, fără celule, pentru toate comenzile personalizate;
d) o configurație cu poziție fixă pentru toate produsele, indiferent de volum.

6. Care este corespondența corectă dintre sistemele ERP, MES și SCADA și funcțiile lor?

a) ERP monitorizează starea proceselor; MES gestionează resursele între-prinderii; SCADA coordonează execuția producției;
b) ERP comandă direct actuatoarele; MES gestionează facturarea; SCADA planifică aprovizionarea;
c) ERP, MES și SCADA îndeplinesc aceeași funcție și diferă doar prin produ-cătorul software;
d) ERP gestionează comenzile, materialele și resursele întreprinderii; MES coordonează execuția producției; SCADA furnizează informații despre starea proceselor și echipamentelor.

7. Ce explică efectul de bici într-un lanț de aprovizionare?

a) cererea scade uniform pe măsură ce produsul se apropie de clientul final;
b) termenele de livrare devin mai previzibile pe măsură ce lanțul se lungeș-te;
c) furnizorii își măresc prețurile proporțional cu distanța față de fabrică;
d) variația cererii se amplifică pe măsura îndepărtării de client, deoarece fi-ecare verigă își construiește previziunile numai pe comenzile primite de la veriga imediat următoare.

8. De ce depinde în principal mărimea stocului de siguranță necesar pentru a menține același nivel de serviciu?

a) exclusiv de valoarea medie a termenului de livrare;
b) de variabilitatea termenelor de livrare ale furnizorilor, nu doar de valoa-rea lor medie;
c) de numărul de angajați din departamentul de aprovizionare;
d) de numărul de linii de producție din fabrică.

9. *În ce condiție pot fi corelate datele de calitate cu parametrii procesului pen-tru a identifica cauzele neconformităților?*

a) dacă măsurătoarea de calitate și parametrii de proces pot fi asociați ace-leiași piese sau aceluiași lot printr-un identificator comun și o marcă temporală comparabilă;
b) dacă fiecare departament folosește propria convenție de denumire;
c) dacă datele sunt agregate lunar înainte de a fi comparate;
d) dacă datele de calitate sunt stocate într-un sistem diferit de cel al datelor de proces.

10. *În scenariul fabricii de mobilier modular, de ce este determinant momen-tul etichetării pieselor?*

a) deoarece etichetele reduc timpul de uscare al plăcilor melaminate;
b) deoarece până la debitare fiecare placă aparține deja unei singure piese finite;
c) deoarece după debitare materialul devine un ansamblu de piese distincte din comenzi diferite, care nu mai pot fi deosebite vizual, iar trasabilitatea se pierde dacă nu sunt etichetate;
d) deoarece etichetarea înlocuiește controlul dimensional al pieselor.

3. TIPURI DE PRODUCȚIE ȘI MODELE DE FABRICAȚIE DIGITALĂ

Proiectarea unei infrastructuri IIoT nu începe de la tehnologie, ci de la procesul industrial pe care aceasta urmează să îl deservească. Ceea ce se fabrică, în ce cantitate, cu ce varietate, cu ce ritm și cu ce consecințe în cazul unei opriri determină mai mult din configurația finală decât alegerea unui protocol sau a unei platforme. Două fabrici pot utiliza același tip de automat programabil (PLC), același broker de mesaje și același serviciu de analiză, dar au nevoie de arhitecturi diferite, pentru că entitatea urmărită, frecvența datelor și timpul admis pentru reacție diferă.

Capitolul 2 a descris compania industrială ca organizație: compartimentele, configurația spațiilor, traseul fizic al materialelor și circulația informației asociate unei comenzi. Capitolul de față coboară un nivel, către procesul de fabricație propriu-zis, și pregătește terenul pentru capitolele tehnice care urmează. Fără o clasificare a producției, discuția despre sisteme flexibile, senzori, automate programabile, protocoale sau arhitecturi integrate rămâne fără criterii de selecție: orice soluție pare acceptabilă, pentru că nimic nu precizează ce anume trebuie măsurat, cât de des și cu ce grad de autonomie față de rețea.

Capitolul tratează trei teme, în această ordine. Prima este clasificarea proceselor de producție, prezentată din două perspective complementare – cea managerială, construită pe volum, varietate și repetabilitate, și cea tehnologică, construită pe modul de curgere a procesului. Cele două nu se suprapun și confundarea lor produce erori de dimensionare. A doua temă o constituie modelele de organizare a producției – JIT, lean, agil și personalizarea de masă – analizate nu ca metode de management, ci din perspectiva datelor pe care fiecare le presupune și pe care infrastructura digitală trebuie să le furnizeze. A treia temă, care ocupă cea mai mare parte a capitolului, este corelarea explicită dintre tipul de producție și arhitectura IIoT: entitatea urmărită, profilul de date, timpul admis pentru detectarea unui eveniment, nivelul de autonomie locală și integrarea cu sistemele de execuție și planificare.

Utilitatea practică a acestei corelări este directă. Ea oferă un set de criterii verificabile pentru evaluarea unei fabrici existente și pentru stabilirea priorităților de digitalizare, înainte de a alege echipamente sau furnizori. Un cititor cu responsabilități tehnice va găsi aici baza dimensionării pe care capitolele 5, 6 și 7 o vor detalia; un cititor cu responsabilități manageriale va găsi criteriile după care poate judeca dacă o propunere de investiție corespunde procesului pe care îl conduce.

O precizare care traversează întregul capitol: funcțiile de control și de siguranță rămân locale, indiferent de tipul de producție. Infrastructura IIoT adaugă colectare, contextualizare, analiză și vizibilitate, dar nu preia responsabilitatea menținerii

procesului în limite sigure. Această delimitare, reluată în capitolele 7 și 8, condiționează toate recomandările formulate în continuare.

Obiectivele capitolului

La finalul acestui capitol, cititorul va putea:

- să diferențieze producția unicat, de serie, de masă și continuă, pe baza volumului, varietății și repetabilității;
- să explice deosebirea dintre perspectiva managerială și perspectiva tehnologică asupra procesului de producție;
- să descrie procesele discrete, în loturi, semicontinue și continue și să identifice tipul de control adecvat fiecăruia;
- să coreleze tipul de producție cu cerințele privind flexibilitatea, standardizarea, trasabilitatea și continuitatea funcționării;
- să explice rolul datelor în modelele JIT, lean și agil, precum și în personalizarea de masă;
- să selecteze, pentru un tip de producție dat, entitatea urmărită, profilul datelor și prioritățile arhitecturii IIoT;
- să calculeze volumul de date și lățimea de bandă necesare pentru un set dat de semnale și o frecvență dată de eșantionare;
- să argumenteze de ce arhitectura IIoT trebuie adaptată procesului industrial și să aplice raționamentul asupra unui exemplu de fabricație.

3.1. Clasificarea proceselor de producție

Procesele de producție admit două perspective complementare: managerială, care distinge producția unicat, de serie și de masă prin volum, varietate și repetabilitate; tehnologică, care diferențiază procesele discrete, în loturi, semicontinue și continue după desfășurare. Matricea produs–proces formalizează corespondența dintre caracteristicile produsului și configurația procesului [94], iar Groover dezvoltă abordarea inginerească, axată pe echipamente și automatizare [1]. Figura 3.1. prezintă relația dintre volumul producției, varietatea produselor și cerințele IIoT.

Cele două clasificări nu se suprapun integral. Producția unicat este, de regulă, discretă, producția de serie poate fi discretă sau organizată în loturi, iar producția de masă poate utiliza linii repetitive pentru produse discrete. Producția continuă descrie atât modul de curgere a procesului, cât și o formă distinctă de organizare industrială. Procesele în loturi ocupă o poziție intermediară și dispun de un model propriu de descriere, definit prin standardul de control al proceselor în loturi, care separă modelul fizic al instalației de modelul procedural al rețetei [95].

Delimitarea nu este un exercițiu taxonomic. Ea determină direct patru mărimi de care depinde orice dimensionare ulterioară: entitatea la care se atașează datele, volumul și frecvența acestora, timpul admis pentru detectarea și tratarea unui

eveniment şi efectul unei opriri. O linie de îmbuteliere şi un atelier de echipamente speciale pot avea acelaşi număr de utilaje şi un cost de investiţie comparabil, dar generează profiluri de date care nu se aseamănă în niciun punct.

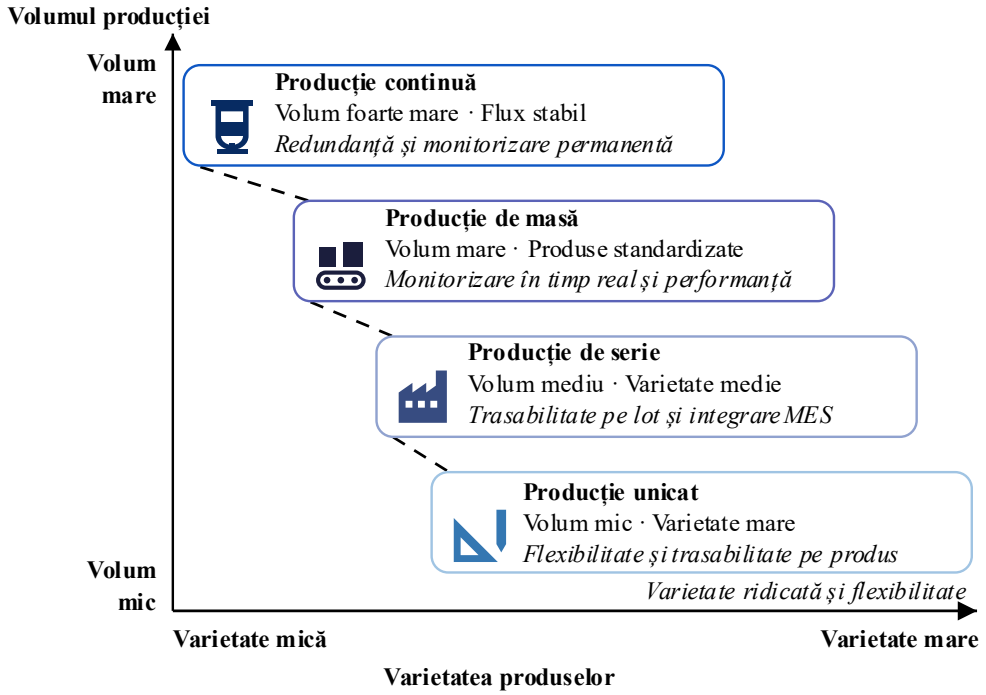


Figura 3.1 – Matrice volum–varietate și cerințe IIoT

3.1.1. Producţia unicat

Producţia unicat presupune realizarea unui produs individual sau a unui număr foarte redus de produse, pe baza unor cerinţe specifice. Este întâlnită în fabricaţia echipamentelor speciale, a instalaţiilor industriale, a prototipurilor, a construcţiilor complexe şi a produselor realizate la comandă.

Produsele pot avea documentaţie, liste de materiale şi operaţii proprii. Traseele se schimbă frecvent, iar activitatea depinde de competenţa operatorilor, tehnicienilor şi inginerilor. Realizarea durează şi costă, de regulă, mai mult decât în producţia repetitivă.

Profilul datelor este discontinuu şi neomogen. Nu există un ciclu care să se repete la intervale previzibile, deci nu există nici un flux constant de valori de proces. Datele apar la momente determinate de evenimente – încheierea unei operaţii, o măsurătoare de recepţie, o observaţie a operatorului, o modificare de documentaţie – şi îşi pierd sensul dacă nu sunt însoţite de contextul care le-a generat: proiectul, componenta, versiunea desenului şi operaţia.

Digitalizarea acestui mediu nu urmărește în primul rând automatizarea completă, ci gestionarea documentației, asistarea personalului și menținerea trasabilității. Datele trebuie asociate produsului, componentelor, versiunii documentației și operațiilor executate. Interfețele de lucru și sistemele de colectare trebuie să poată fi adaptate fără modificări costisitoare la fiecare proiect nou; costul dominant al unei soluții IIoT în producția unicat este costul reconfigurării, nu cel al infrastructurii de transport al datelor.

3.1.2. Producția de serie

Producția de serie constă în fabricarea repetată a unui număr determinat de produse identice sau asemănătoare. În funcție de volumul loturilor și de frecvența repetării, se poate vorbi despre serie mică, mijlocie sau mare.

Operațiile sunt stabile pe durata realizării unui lot, dar trecerea la o altă serie poate necesita schimbarea sculelor, programelor, materialelor și parametrilor procesului. Performanța depinde atât de eficiența execuției, cât și de reducerea timpilor necesari pregătirii și schimbării fabricației. Metodele sistematice de reducere a acestor timpi, dezvoltate inițial în industria de automobile, tratează schimbarea fabricației ca pe o operație care poate fi proiectată și măsurată, nu ca pe o pierdere inevitabilă [96].

În cadrul lotului, valorile se repetă la intervale cunoscute, permițând stabilirea limitelor de variație și compararea cu ciclurile anterioare. Schimbarea seriei întrerupe acest tipar și invalidează limitele. Dacă sistemul nu recunoaște schimbarea, poate raporta abateri false sau ascunde abateri reale într-o medie care combină datele a două configurații diferite.

În acest mediu, sistemele IIoT susțin identificarea loturilor și produselor, urmărirea progresului comenzilor și colectarea parametrilor de proces. Integrarea cu sistemele MES permite corelarea datelor provenite de la echipamente cu ordinele de producție, materialele și rezultatele verificărilor, pe baza modelului de schimb informațional dintre nivelul de execuție și cel de planificare definit de seria de standarde ISA-95 [49]. Analiza datelor poate evidenția variațiile procesului, cauzele opririlor și oportunitățile de reducere a timpului de trecere între serii.

Fabrica de mobilier modular prezentată în secțiunea 2.5 reprezintă un exemplu de producție de serie cu un nivel ridicat de personalizare. Componentele utilizează operații repetabile, dar configurația fiecărei comenzi impune gestionarea controlată a documentației și identificarea individuală a pieselor.

3.1.3. Producția de masă

Producția de masă urmărește realizarea unui volum foarte mare de produse standardizate, prin operații repetitive și timpi de ciclu reduși. Este specifică produselor de larg consum, componentelor standardizate, ambalajelor și altor domenii în care cererea justifică utilizarea unor linii dedicate.

Echipamentele, dispozitivele și metodele de lucru sunt optimizate pentru un flux stabil. Gradul de automatizare este, de regulă, ridicat, iar variațiile procesului trebuie menținute în limite restrânse. Avantajul principal îl reprezintă reducerea costului unitar, însă o defecțiune sau o abatere nedetectată poate afecta într-un interval scurt un număr mare de produse. Consecința este asimetrică: valoarea unei detecții rapide crește proporțional cu ritmul liniei, în timp ce costul unei detecții întârziate crește cu numărul de unități produse între momentul apariției abaterii și momentul identificării ei.

Profilul datelor este dens, regulat și dominat de volum. O linie cu timp de ciclu de câteva secunde produce, într-un schimb, un număr de evenimente cu ordin de mărime superior celui generat într-un an de un atelier de producție unicat. Transmiterea integrală a valorilor brute către nivelurile superioare devine nu doar costisitoare, ci și inutilă: informația necesară deciziei este, în majoritatea cazurilor, agregată sau declanșată de eveniment.

Soluțiile IIoT trebuie să colecteze și să prelucreze volume mari de date fără a perturba funcțiile de control. Monitorizarea stării echipamentelor, controlul calității în flux și detectarea rapidă a abaterilor devin prioritare. Arhitectura trebuie să asigure disponibilitate ridicată, latență redusă pentru funcțiile operaționale și integrarea datelor agregate cu sistemele de planificare și analiză. Filtrarea, agregarea și detecția locală a evenimentelor prin prelucrare la marginea rețelei reprezintă aici o cerință de dimensionare, nu o opțiune de arhitectură [22].

3.1.4. Producția continuă

Producția continuă este specifică proceselor în care materiile prime sunt transformate într-un flux neîntrerupt. Se întâlnește în producerea energiei, petrochimie, tratarea apei, industria alimentară, industria farmaceutică și fabricarea materialelor precum cimentul sau sticla.

Controlul vizează în principal temperatura, presiunea, debitul, nivelul, concentrația sau pH-ul. Buclele de reglare mențin aceste variabile aproape de valorile prescrise, compensând continuu perturbațiile [97]. Instalațiile pot funcționa permanent, cu opriri planificate pentru mentenanță, revizii sau modificări tehnologice.

Aici dispare noțiunea de unitate de produs ca purtător al datelor. Trasabilitatea nu se atașează unui obiect, ci unui interval de timp și unei porțiuni de flux, ceea ce schimbă complet modul de construire a istoricului: identificarea unui lot de produs finit cu materiile prime din care provine presupune reconstituirea timpilor de rezidență în instalație, nu citirea unui identificator.

În acest context, sistemele de control distribuit (DCS), automatele programabile, sistemele SCADA și istoricele de proces trebuie să funcționeze coordonat. Infrastructura IIoT completează sistemele de control prin integrarea datelor, analiza stării instalațiilor, monitorizarea consumurilor și transmiterea informațiilor către nivelurile superioare. Funcțiile critice trebuie să rămână disponibile local, inclusiv în

cazul întreruperii conexiunii cu serviciile de calcul în cloud – cerință formulată explicit și în ghidurile de securitate pentru OT, care tratează disponibilitatea locală a controlului ca pe o condiție de proiectare, nu ca pe o măsură de rezervă [25].

Cerințele de disponibilitate, redundanță și securitate sunt ridicate, deoarece o comandă incorectă sau o întrerupere poate afecta siguranța personalului, instalația și mediul. Datele trebuie păstrate împreună cu marca temporală, unitatea de măsură, starea semnalului și contextul operațional necesar interpretării.

3.1.5. Punctul de decuplare a comenzii

Cele patru tipuri de producție descriu modul în care se fabrică. O a treia distincție, complementară, descrie momentul în care comanda clientului intervine în fluxul de fabricație. Punctul de decuplare a comenzii separă porțiunea de flux realizată pe bază de previziune de porțiunea realizată pe bază de comandă fermă [88].

Poziționarea acestui punct generează patru situații uzuale, reprezentate în Figura 3.2: fabricație pe stoc, când produsul finit este realizat integral înaintea comenzii; asamblare la comandă, când subansamblurile există, iar comanda determină configurația finală; fabricație la comandă, când operațiile de prelucrare încep după primirea comenzii; și proiectare la comandă, când însăși documentația produsului este elaborată pentru comanda respectivă.

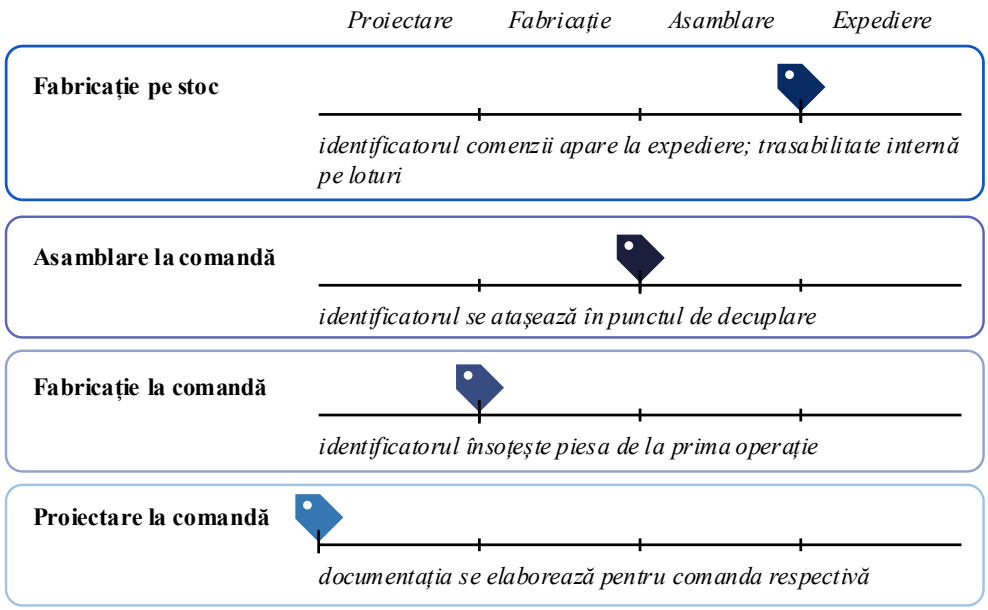


Figura 3.2 – Cele patru poziții uzuale ale punctului de decuplare a comenzii

Distincția are consecințe informaționale directe, care nu decurg din tipul de producție. În fabricația pe stoc, identificatorul comenzii apare abia la expediere, iar

trasabilitatea internă se construieşte pe loturi. În asamblarea la comandă, identificatorul comenzii trebuie asociat produsului exact în punctul de decuplare, iar înaintea acestuia rămân relevante doar loturile de subansambluri. În fabricaţia şi proiectarea la comandă, identificatorul comenzii însoţeşte piesa de la prima operaţie şi devine cheia sub care se adună toate datele ulterioare.

Acelaşi tip de producţie poate necesita puncte diferite de identificare. Pentru mobilierul fabricat la comandă, etichetarea poate începe după debitare, odată cu particularizarea configuraţiei. Pentru componentele standardizate produse pe stoc, absenţa identificatorilor de comandă impune trasabilitatea pe lot de material şi interval de producţie. Punctul de decuplare se defineşte astfel printre primele decizii ale proiectului de digitalizare, înaintea selectării echipamentelor de identificare.

Relaţia dintre tipul de producţie şi cerinţele principale ale infrastructurii IIoT este sintetizată în Tabelul 3.1. Tipul de producţie stabileşte cadrul operaţional, dar nu determină singur performanţa fabricii. Modul în care materialele sunt aprovizionate, activităţile sunt planificate şi procesele sunt îmbunătăţite depinde şi de modelul de organizare adoptat. Principalele modele relevante pentru fabricaţia digitală sunt prezentate în secţiunea 3.2.

Tabelul 3.1 – Relația dintre tipul de producție și cerințele principale ale infrastructurii IIoT

Tipul de producție	**Caracteristici operaționale**	**Profilul datelor**	**Cerințe IIoT prioritare**
Unicat	Volum redus, varietate ridicată, trasee variabile	Date punctuale, generate de evenimente, dependente de proiect și operație	Trasabilitate individuală, documentație controlată, configurare flexibilă a punctelor de colectare
Serie	Loturi repetabile, schimbări între serii	Date ciclice, asociate lotului și produsului, cu discontinuități la schimbarea fabricației	Integrare MES, urmărirea loturilor, controlul variației și al schimbărilor de fabricație
Masă	Volum foarte mare, standardizare și ritm ridicat	Fluxuri dense și frecvente, dominate de volum	Monitorizare continuă, control în flux, agregare și detecție la edge, disponibilitate ridicată
Continuă	Proces neîntrerupt, parametri interdependenți	Date continue, cu frecvență și criticitate ridicate, atașate intervalului de timp	Control local robust, redundanță, istoric de proces, sincronizare temporală și securitate

3.2. Modele moderne de fabricație

Modelele moderne de organizare a producţiei urmăresc optimizarea consumului de resurse, îmbunătăţirea fluxului şi adaptarea la cererea pieţei. Producţia exact la timp (*engl. just-in-time, JIT*), organizarea lean şi fabricaţia agilă (*engl. agile manufacturing*) abordează aceste obiective din perspective diferite, dar complementare, iar personalizarea de masă descrie rezultatul urmărit atunci când varietatea

trebuie obținută fără costul specific producției unicat. În Figura 3.3 sunt reprezentate aceste modele.

JIT sincronizează aprovizionarea și producția cu necesarul real. Termenul lean desemnează un model de organizare orientat către crearea valorii pentru client prin eliminarea sistematică a activităților care consumă resurse fără a contribui la rezultatul solicitat; denumirea s-a impus în literatura de management după studiul comparativ al industriei mondiale de automobile realizat de Womack et al. [98] și este utilizată ca atare în practica industrială din România. Modelul agil dezvoltă capacitatea organizației de a răspunde rapid la variația cererii, la personalizarea produselor și la apariția unor cerințe noi.

Conceptele sunt adesea confundate, inclusiv comercial. JIT sincronizează materialele, lean organizează activitatea folosind și JIT, iar agilitatea arată cât costă și durează schimbarea sistemului, nu cât de eficient funcționează într-o configurație stabilă. Distincția contează pentru infrastructura digitală: sincronizarea materialelor, identificarea risipei și reconfigurarea se bazează pe date diferite.

Aplicarea acestor modele nu depinde exclusiv de tehnologie. Stabilitatea proceselor, disciplina operațională, calitatea datelor și colaborarea dintre compartimente rămân condiții esențiale. Soluțiile IIoT susțin aceste modele prin vizibilitate asupra proceselor, colectarea automată a datelor și transmiterea rapidă a informațiilor necesare deciziei; ele nu înlocuiesc însă niciunul dintre mecanismele organizaționale pe care modelele le presupun.

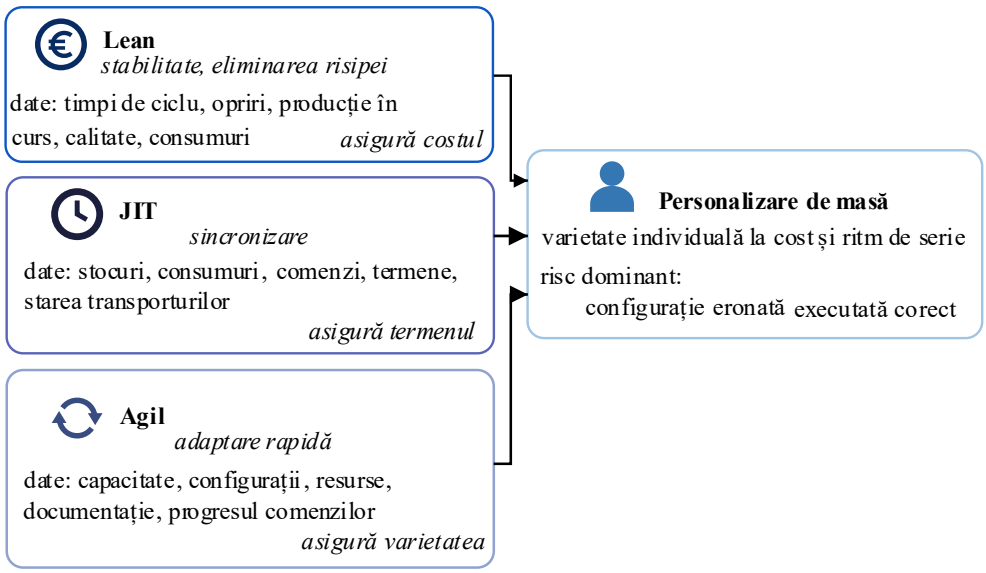


Figura 3.3 – Modele moderne de fabricație

3.2.1. Modelul Just-in-Time

Modelul JIT urmăreşte asigurarea materialelor, componentelor şi produselor în cantitatea necesară şi la momentul în care acestea sunt solicitate de proces. Producţia este declanşată de cererea reală, nu exclusiv de estimări sau de utilizarea capacităţii disponibile. Descrierea originală a modelului, formulată în contextul sistemului de producţie Toyota, asociază acest principiu cu un mecanism explicit de semnalizare între posturile de lucru, prin care operaţia din aval solicită operaţiei din amonte exact cantitatea consumată [99].

Reducerea stocurilor diminuează costurile de depozitare şi evidenţiază mai rapid problemele procesului. În acelaşi timp, aceasta limitează capacitatea fabricii de a absorbi întârzierile furnizorilor, variaţiile neprevăzute ale cererii şi defecţiunile echipamentelor. Relaţia dintre variabilitate, stocuri şi timp de traversare este demonstrabilă cantitativ: o variabilitate mai mare impune fie stocuri mai mari, fie capacitate suplimentară, fie timpi de traversare mai lungi, iar eliminarea simultană a tuturor celor trei nu este posibilă [76]. Aplicarea JIT presupune, prin urmare:

- procese stabile şi timpi de ciclu cunoscuţi;
- furnizori capabili să respecte cantitatea, calitatea şi termenul;
- timpi reduşi pentru schimbarea fabricaţiei;
- identificarea şi urmărirea materialelor;
- actualizarea corectă a consumurilor şi stocurilor;
- reacţie rapidă la abateri şi perturbări.

Infrastructura IIoT poate furniza informaţiile necesare sincronizării fluxurilor. Materialele şi containerele pot fi identificate prin coduri de bare, coduri bidimensionale sau identificare prin radiofrecvenţă (RFID). Cantităţile disponibile pot fi actualizate pe baza recepţiilor, consumurilor şi transferurilor dintre zonele fabricii.

Datele provenite din producţie permit compararea consumului real cu planul şi estimarea momentului în care un material trebuie reaprovizionat. Integrarea sistemelor MES şi ERP poate corela starea ordinelor de producţie cu necesarul de materiale, comenzile transmise furnizorilor şi termenele confirmate de livrare.

Vizibilitatea asupra transporturilor şi schimbul electronic de informaţii cu furnizorii permit identificarea anticipată a întârzierilor. Planificarea poate fi astfel ajustată înainte ca lipsa materialelor să oprească producţia. Pentru componentele critice, decizia privind nivelul stocului de siguranţă trebuie fundamentată pe variabilitatea consumului, timpul de aprovizionare şi riscul asociat întreruperii procesului.

Automatizarea reaprovizionării trebuie aplicată controlat. Datele incorecte privind stocurile, consumurile sau termenele furnizorilor pot genera comenzi nejustificate ori lipsuri de materiale. Din acest motiv, sistemul trebuie să asigure validarea informaţiilor, trasabilitatea modificărilor şi mecanisme de confirmare pentru deciziile cu impact ridicat. Un semnal de consum eronat, propagat automat, produce într-un sistem JIT o perturbare mai mare decât într-un sistem cu stocuri, tocmai pentru că stocul intermediar care ar fi absorbit eroarea a fost eliminat.

3.2.2. Modelul Lean Manufacturing

Organizarea lean este orientată către crearea valorii pentru client prin reducerea activităţilor care utilizează resurse fără a contribui la rezultatul solicitat; aceste activităţi sunt considerate forme de risipă şi pot apărea sub forma supraproducţiei, a aşteptării, transportului inutil, prelucrării excesive, stocurilor prea mari, mişcărilor inutile şi defectelor [100].

Aplicarea modelului presupune înţelegerea valorii din perspectiva clientului, analiza fluxului prin care aceasta este creată, eliminarea întreruperilor, producţia în funcţie de cerere şi îmbunătăţirea continuă [101]. Rezultatele nu provin dintr-o intervenţie izolată, ci din observarea repetată a procesului şi implicarea personalului în identificarea cauzelor problemelor [102].

Datele colectate prin infrastructura IIoT pot susţine această analiză prin măsurarea obiectivă a:

- timpilor de ciclu şi de aşteptare;
- cantităţii de producţie în curs;
- frecvenţei şi duratei opririlor;
- consumurilor de materiale şi energie;
- cantităţilor conforme, reprelucrate şi rebutate;
- timpilor necesari transportului şi schimbării fabricaţiei;
- gradului de utilizare şi disponibilităţii echipamentelor.

Cartografierea fluxului valorii (VSM) poate fi completată cu date reale provenite din echipamente şi sisteme informatice [103]. Compararea timpilor efectivi cu cei planificaţi evidenţiază blocajele, acumulările şi activităţile care nu adaugă valoare. Avantajul datelor automate faţă de observarea manuală nu constă numai în precizie, ci în acoperirea temporală: o cartografiere realizată prin cronometrare surprinde o zi, în timp ce datele colectate continuu surprind variabilitatea între schimburi, zile ale săptămânii şi configuraţii de produs.

Sistemele digitale de semnalizare de tip Andon permit operatorilor sau echipamentelor să raporteze o problemă şi să transmită informaţia către persoanele responsabile. Alerta trebuie să precizeze locul, momentul, echipamentul şi natura abaterii, astfel încât intervenţia să poată fi prioritizată şi analizată ulterior.

Datele privind funcţionarea echipamentelor permit calcularea automată a unor indicatori precum disponibilitatea, performanţa şi calitatea. Aceştia pot fi integraţi în eficacitatea globală a echipamentelor (OEE), indicator introdus în cadrul mentenanţei productive totale [65] şi definit ulterior formal, împreună cu regulile de compunere a timpilor, în seria de standarde dedicată indicatorilor de performanţă în gestionarea operaţiunilor de fabricaţie [51]. Condiţia de validitate este ca regulile de calcul şi clasificarea opririlor să fie definite unitar; formula dezvoltată şi aplicată numeric este prezentată în secţiunea 7.2.3.

Tehnologia nu trebuie utilizată pentru a reproduce digital un proces ineficient. Înaintea automatizării colectării şi transmiterii datelor trebuie analizate necesitatea activităţilor, succesiunea operaţiilor şi modul în care informaţiile vor susţine o decizie. Colectarea unui volum mare de date fără un obiectiv operaţional clar poate introduce costuri şi complexitate fără a reduce risipa – situaţie care poate fi descrisă ca forma digitală a supraproducţiei: date produse înaintea existenţei unei cereri pentru ele.

3.2.3. Fabricaţia agilă

Fabricaţia agilă urmăreşte capacitatea sistemului de producţie de a răspunde rapid la modificarea cererii, la personalizarea produselor şi la introducerea unor variante noi. Conceptul a fost formulat iniţial ca strategie industrială pentru medii caracterizate prin schimbare imprevizibilă [104] şi dezvoltat ulterior ca model care integrează structura organizaţională, tehnologia, personalul şi sistemele informatice [105]. Este relevant în mediile caracterizate prin volume variabile, cicluri de viaţă scurte şi cerinţe dificil de anticipat.

Agilitatea nu înlocuieşte modelul lean sau JIT. Un proces stabil şi lipsit de activităţi inutile poate fi reconfigurat mai uşor, iar informaţiile privind cererea şi disponibilitatea resurselor permit adaptarea planului fără formarea unor stocuri excesive. Diferenţa principală constă în accentul pus pe gestionarea schimbării, nu numai pe eficienţa unei configuraţii stabile. Distincţia este importantă şi pentru dimensionare: un sistem optimizat exclusiv pentru eficienţă poate deveni rigid, deoarece fiecare eliminare de rezervă reduce simultan şi marja disponibilă pentru reconfigurare.

Principalele caracteristici ale fabricaţiei agile sunt:

- personalizarea produselor şi realizarea eficientă a loturilor mici;
- introducerea rapidă a produselor şi variantelor noi;
- reconfigurarea echipamentelor şi a fluxurilor de producţie;
- utilizarea unor componente şi interfeţe modulare;
- colaborarea dintre proiectare, planificare, producţie şi logistică;
- actualizarea rapidă a documentaţiei şi parametrilor de proces.

Infrastructura IIoT susţine agilitatea prin furnizarea unei imagini actualizate asupra capacităţii, stării echipamentelor, materialelor şi progresului comenzilor. Sistemele MES pot reprograma operaţiile în funcţie de disponibilitatea resurselor, iar reţetele şi parametrii de fabricaţie pot fi transferaţi controlat către echipamentele compatibile.

Echipamentele modulare, roboţii reprogramabili şi staţiile configurabile permit adaptarea fizică a procesului. Capacitatea de a modifica structura sistemului prin adăugarea, eliminarea sau înlocuirea de module, în locul supradimensionării iniţiale a funcţiilor, constituie principiul sistemelor reconfigurabile de fabricaţie tratate în capitolul 4 [106]. Interoperabilitatea este esenţială, deoarece înlocuirea sau

adăugarea unui modul nu trebuie să impună reconstruirea întregii infrastructuri de comunicație și integrare.

Gemenii digitali pot fi utilizați pentru simularea unei configurații, verificarea capacității și evaluarea efectelor unei modificări înaintea aplicării acesteia în fabrică [107]. Rezultatele simulării trebuie validate însă prin date provenite din procesul real, deoarece un model neactualizat poate conduce la estimări incorecte.

Agilitatea presupune și controlul riguros al versiunilor. Schimbarea rapidă a produselor și parametrilor poate genera erori dacă documentația, programele, sculele și materialele nu sunt corelate. Fiecare set de date trebuie asociat produsului, ordinului de producție și configurației aprobate.

3.2.4. Personalizarea de masă

Personalizarea de masă oferă produse adaptate fiecărui client, la costuri și într-un ritm apropiate producției de masă [108]. Ea combină cele trei abordări: stabilitatea și eliminarea risipei controlează costul, sincronizarea susține respectarea termenului, iar agilitatea permite diversitatea produselor.

Realizarea sa depinde de trei capacități organizaționale distincte: identificarea corectă a spațiului de opțiuni pe care clienții îl solicită efectiv, proiectarea unui produs a cărui varietate se obține prin combinarea unor module standardizate, și existența unui proces capabil să execute configurația comandată fără intervenție de inginerie pentru fiecare comandă [109]. Absența oricăreia dintre ele transformă personalizarea de masă în producție unicat cu preț de producție de serie, adică într-un model nesustenabil economic.

Consecința tehnică cea mai importantă este poziționarea varietății. Într-un produs corect proiectat pentru personalizare, componentele diferă între comenzi în puține puncte controlate, iar restul rămâne comun. Aceasta permite menținerea operațiilor repetitive până în apropierea punctului de decuplare a comenzii, discutat în secțiunea 3.1.5, și limitarea zonei în care sunt necesare trasabilitate individuală și documentație specifică.

Din perspectiva infrastructurii digitale, personalizarea de masă impune un ansamblu de cerințe care nu se regăsește integral în niciunul dintre modelele anterioare considerate separat. Acesta presupune utilizarea unui configurator care validează combinațiile admisibile înainte de acceptarea comenzii și transmite configurația rezultată către proiectare și planificare, precum și generarea automată a listei de materiale și a programelor de fabricație pe baza configurației comandate, fără reintroducerea manuală a datelor. Sunt necesare identificarea individuală a componentelor din momentul în care acestea devin specifice unei comenzi și menținerea asocierii dintre piesa fizică, configurația aprobată și versiunea documentației. Totodată, infrastructura trebuie să permită verificarea completitudinii setului înaintea ambalării sau a asamblării finale și păstrarea configurației efectiv livrate, necesară pentru service, furnizarea pieselor de schimb și tratarea reclamațiilor.

Riscul dominant nu este de natură tehnologică, ci informațională. O eroare de configurare nu se manifestă ca defect de execuție, ci ca produs executat corect după

o specificaţie greşită, care trece de controlul dimensional şi de cel funcţional şi este identificată abia la client. Din acest motiv, validarea configuraţiei la intrare şi trasabilitatea versiunilor au, în acest model, o valoare mai mare decât creşterea densităţii de senzori în procesul de fabricaţie.

Cele patru modele, comparate în Tabelul 3.2, pot fi aplicate simultan. O fabrică poate utiliza principiile lean pentru stabilizarea proceselor, JIT pentru sincronizarea materialelor şi organizarea agilă pentru adaptarea la modificarea portofoliului de produse, obţinând, în ansamblu, capacitatea de personalizare de masă. Configuraţia infrastructurii IIoT trebuie stabilită în funcţie de combinaţia dintre modelul de organizare şi tipul de producţie, relaţie analizată în secţiunea 3.3.

Tabelul 3.2 – Comparația modelelor JIT, lean, agil și personalizare de masă

Model	Obiectiv principal	Date necesare	Contribuția infrastructurii IIoT	Riscuri principale
JIT	Sincronizarea aprovizionării și producției cu cererea reală	Stocuri, consumuri, comenzi, termene și starea transporturilor	Urmărirea materialelor, actualizarea stocurilor și semnalarea necesarului de reaprovizionare	Întreruperea producției, propagarea datelor incorecte și dependența de furnizori
Lean	Crearea valorii prin eliminarea risipei	Timpi de ciclu, opriri, producție în curs, calitate și consumuri	Identificarea pierderilor, monitorizarea indicatorilor și alertarea rapidă	Digitalizarea proceselor ineficiente și colectarea datelor fără utilizare operațională
Agil	Adaptarea rapidă la schimbarea cererii și a produselor	Capacitate, configurații, resurse, documentație și progresul comenzilor	Replanificare, reconfigurare, simulare și transfer controlat al parametrilor	Pierderea controlului versiunilor, integrarea insuficientă și creșterea complexității
Personalizare de masă	Varietate individuală la cost și ritm de serie	Opțiuni admisibile, configurația comandată, liste de materiale generate, identificatori de componentă	Validarea configurației, generarea automată a documentației și trasabilitatea individuală până la livrare	Configurații eronate executate corect, seturi incomplete și proliferarea necontrolată a variantelor

3.3. Corelarea tipului de producție cu arhitectura IIoT

Arhitectura IIoT trebuie proiectată în funcţie de caracteristicile procesului industrial pe care îl deserveşte. Volumul producţiei, varietatea produselor, frecvenţa schimbărilor, criticitatea operaţiilor şi cerinţele de trasabilitate determină modul de colectare, prelucrare, transmitere şi păstrare a datelor.

Caracteristicile tipurilor de producţie au fost prezentate în secţiunea 3.1. Din perspectiva proiectării arhitecturii, acestea trebuie transpuse în opt cerinţe care constituie, împreună, specificaţia de pornire a oricărui proiect de digitalizare:

- entitatea urmărită: produs, componentă, lot, comandă sau interval de proces;
- volumul, frecvenţa şi granularitatea datelor;

- timpul admis pentru detectarea şi tratarea unui eveniment;
- nivelul de autonomie necesar în cazul pierderii conectivităţii;
- frecvenţa reconfigurării echipamentelor şi fluxurilor;
- integrarea cu sistemele de proiectare, control, execuţie şi planificare;
- disponibilitatea, redundanţa şi securitatea infrastructurii;
- perioada şi contextul în care datele trebuie păstrate.

Ordinea acestor cerinţe nu este arbitrară. Prima determină modelul de date, a doua determină dimensionarea reţelei şi a stocării, a treia determină locul prelucrării, iar a patra determină ce anume poate fi delegat unui serviciu extern. Un proiect care începe de la alegerea platformei şi abia apoi stabileşte entitatea urmărită ajunge, în general, să colecteze valori corecte care nu pot fi atribuite niciunui obiect gestionat în producţie.

Funcţiile de control şi siguranţă se menţin la nivel local, în PLC-uri şi în sistemele industriale dedicate. Infrastructura IIoT completează aceste funcţii prin integrarea datelor, monitorizare, analiză şi transmiterea informaţiilor către nivelurile superioare. O conexiune cu un serviciu de calcul în cloud nu trebuie să devină o condiţie pentru funcţionarea sigură a procesului. Această separare – între bucla de control, care rămâne deterministă şi locală, şi fluxul informaţional, care poate fi asincron şi distribuit – reprezintă principiul arhitectural care distinge un sistem ciber-fizic industrial de o simplă reţea de senzori conectaţi [9].

Relaţia dintre modelele de organizare a producţiei şi categoriile de date pe care acestea le presupun este sintetizată în Figura 3.4.

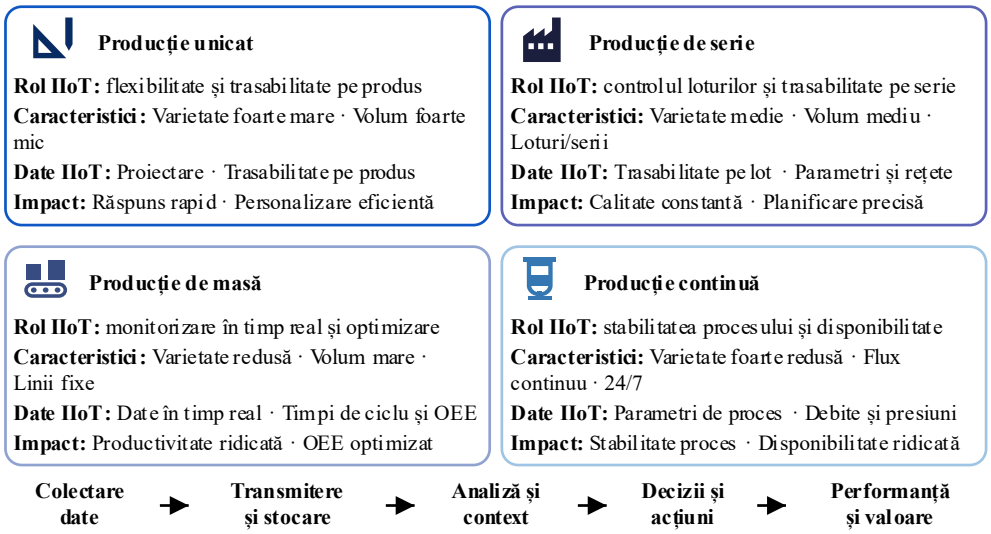


Figura 3.4 – Relația dintre modelele moderne de fabricație și rolul datelor IIoT

Convenţia de reprezentare a datelor este a doua decizie transversală. Indiferent de tipul de producţie, o valoare transmisă fără identificatorul sursei, marca temporală a măsurării, unitatea de măsură şi indicatorul de calitate a semnalului nu poate fi interpretată ulterior. Modelele informaţionale care asociază explicit aceste atribute unei valori, precum spaţiul de adrese definit de OPC UA [66], sau convenţiile de structurare a mesajelor peste protocoale de tip publicare–abonare [110], rezolvă această cerinţă prin construcţie. Tratarea detaliată a protocoalelor şi a structurii mesajelor face obiectul capitolului 6.

3.3.1. Arhitectura IIoT pentru producţia unicat

În producţia unicat, arhitectura trebuie orientată către flexibilitate şi trasabilitate individuală. Fiecare produs poate utiliza o configuraţie, o documentaţie şi un traseu tehnologic diferite, iar datele trebuie asociate versiunii aprobate şi operaţiilor efectiv executate.

Integrarea cu aplicaţiile pentru proiectare asistată de calculator (CAD) şi cu sistemele pentru gestionarea ciclului de viaţă al produsului (PLM) permite transmiterea controlată a desenelor, listelor de materiale şi instrucţiunilor către producţie. Modificările trebuie propagate fără pierderea legăturii dintre versiunea documentaţiei şi stadiul fizic al produsului.

Punctele de colectare a datelor trebuie să poată fi reconfigurate uşor. Pot fi utilizate staţii mobile, instrumente digitale de măsurare, formulare configurabile şi gateway-uri industriale care integrează echipamente eterogene. Atunci când produsul este realizat în mai multe zone, stocarea locală temporară permite păstrarea datelor şi sincronizarea lor ulterioară.

Arhitectura trebuie să susţină:

- identificarea individuală a produselor şi componentelor;
- asocierea măsurătorilor cu operaţia şi documentaţia utilizată;
- introducerea controlată a observaţiilor operatorilor;
- adăugarea rapidă a unor noi tipuri de date;
- accesul contextual la instrucţiuni şi criterii de verificare;
- păstrarea istoricului modificărilor.

Datele introduse de personal ridică o problemă specifică acestui mediu. Într-o producţie dominată de evenimente rare şi de decizii de inginerie, o parte importantă a informaţiei valoroase nu provine din senzori, ci din observaţii umane: cauza unei reprelucrări, motivul unei abateri acceptate, dificultatea întâmpinată la montaj. Aceste date trebuie colectate în formă structurată, cu liste de opţiuni predefinite şi cu asociere automată la operaţie şi la persoană, altfel devin text liber neexploatabil. Cerinţa de proiectare rezultată este ca timpul necesar înregistrării să rămână sub un prag la care operatorul o percepe ca pe o întrerupere a lucrului.

În acest mediu, valoarea infrastructurii IIoT rezultă în principal din gestionarea complexității și coordonarea informațiilor, nu din colectarea unui volum foarte mare de date repetitive. Criteriul de evaluare a unei investiții nu este numărul de puncte de măsurare adăugate, ci reducerea timpului necesar pentru a răspunde la întrebarea „ce configurație a fost efectiv executată și pe baza cărei documentații".

3.3.2. Arhitectura IIoT pentru producția de serie

În producția de serie, lotul, ordinul de producție și configurația produsului constituie principalele elemente de corelare. Arhitectura trebuie să combine repetabilitatea operațiilor cu posibilitatea schimbării controlate a materialelor, programelor, sculelor și parametrilor.

Automatele programabile și SCADA monitorizează și controlează operațiunile, iar MES leagă datele de ordinele de producție, loturi și resurse. Prin ERP se actualizează progresul, consumurile și disponibilitatea materialelor. Modelul integrării dintre control și gestiune stabilește responsabilitățile și informațiile schimbate între niveluri [49].Momentul critic al acestei arhitecturi este schimbarea fabricației. La trecerea de la o serie la alta, arhitectura trebuie să asigure:

- selectarea și validarea rețetei sau configurației corecte;
- confirmarea materialelor și sculelor utilizate;
- transmiterea controlată a parametrilor către echipamente;
- identificarea primei și ultimei unități din lot;
- asocierea rezultatelor verificărilor cu lotul și produsul;
- înregistrarea timpilor și problemelor apărute la schimbarea fabricației.

Marcarea explicită a momentului schimbării are o consecință care depășește trasabilitatea. Toate mecanismele de detectare a abaterilor prin comparație cu istoricul – limite de variație, praguri de consum, timpi de ciclu de referință – devin invalide dacă seria de date nu este segmentată pe configurații. Un sistem care nu primește semnalul de schimbare a fabricației va calcula medii pe două populații diferite și va produce simultan alarme false și abateri nesemnalate. Din acest motiv, evenimentul de schimbare a configurației trebuie tratat ca dată de proces, nu ca informație administrativă, și trebuie să circule pe același canal și cu aceeași marcă temporală ca valorile măsurate.

Pentru procesele organizate în loturi, separarea dintre modelul fizic al instalației și modelul procedural al rețetei oferă un cadru consacrat de structurare a acestor informații, în care aceeași instalație poate executa rețete diferite fără modificarea programelor de control [95].

Echipamentele moștenite tehnologic pot fi conectate prin gateway-uri industriale și convertoare de protocol, fără înlocuirea imediată a sistemelor locale de control. Datele relevante sunt preluate, contextualizate și transmise către SCADA sau MES, menținând separarea dintre funcțiile de comandă și cele de analiză. Această soluție trebuie tratată însă ca decizie de arhitectură, nu ca improvizație: gateway-

ul devine punct unic de defect pentru vizibilitatea asupra echipamentului şi, dacă este conectat bidirecţional, punct de intrare către reţeaua de automatizare.

3.3.3. Arhitectura IIoT pentru producţia de masă

Producţia de masă generează fluxuri dense de date şi necesită detectarea rapidă a opririlor, variaţiilor şi neconformităţilor. Arhitectura trebuie să fie scalabilă, să susţină un număr mare de echipamente şi să evite transmiterea necontrolată a tuturor valorilor brute către nivelurile superioare.

Prelucrarea la marginea reţelei devine, în acest context, o cerinţă de dimensionare. Filtrarea, agregarea, detectarea evenimentelor şi calculul indicatorilor pot fi realizate în apropierea echipamentelor, astfel încât către nivelurile superioare să circule informaţia necesară deciziei, nu întregul flux de valori [111]. Avantajele sunt simultane: reducerea traficului, reducerea latenţei de detectare şi menţinerea funcţionării atunci când legătura către serviciile externe este indisponibilă.

Regula practică de repartizare a prelucrării poate fi formulată prin timpul admis pentru reacţie. Ceea ce trebuie să producă un efect în milisecunde rămâne în automatul programabil. Ceea ce trebuie detectat în secunde se prelucrează la nivelul echipamentului sau al gateway-ului industrial. Ceea ce susţine decizii la nivel de schimb, zi sau săptămână poate fi transmis către MES, către istoricul de proces sau către servicii de calcul în cloud. Aplicarea inversă a acestei reguli – trimiterea unei valori într-un serviciu extern pentru a decide o acţiune care trebuie executată în câteva zeci de milisecunde – reprezintă eroarea de proiectare cea mai frecventă în acest tip de producţie. Timpii de reacţie sunt reprezentaţi în Figura 3.5.

Arhitectura trebuie să asigure:

- colectarea sincronizată de la un număr mare de surse, cu marcă temporală comună;
- agregarea şi filtrarea locală, cu păstrarea valorilor brute numai în intervalele relevante;

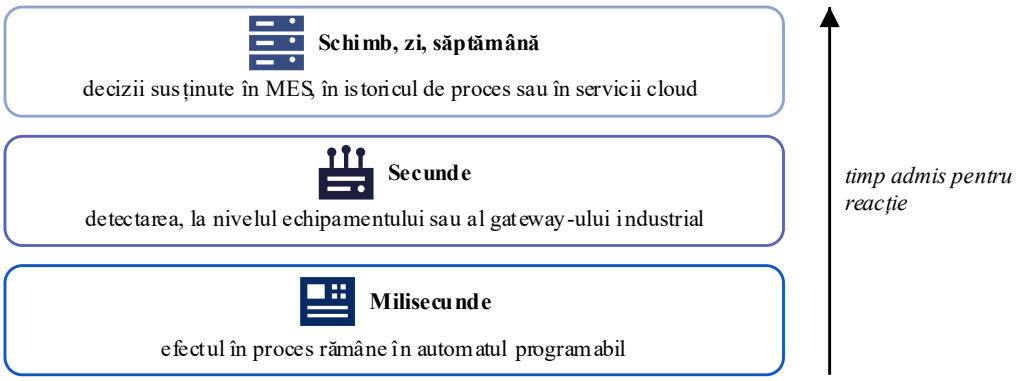


Figura 3.5 – Nivelul de prelucrare a datelor în funcţie de timpul admis pentru reacţie

- transmiterea prin excepţie a evenimentelor şi a depăşirilor de prag;
- separarea traficului de analiză de traficul de control, prin segmentare de reţea;
- scalarea orizontală a colectării, fără reproiectarea modelului de date;
- calculul indicatorilor de disponibilitate, performanţă şi calitate pe fiecare linie şi schimb.

Transmiterea prin excepţie merită o precizare, pentru că este adesea confundată cu reducerea eşantionării. Reducerea eşantionării scade rezoluţia în orice condiţii, inclusiv atunci când procesul se abate; transmiterea prin excepţie păstrează rezoluţia completă în intervalele în care se produce ceva relevant şi o reduce în rest. Pentru detectarea unei abateri tranzitorii, cele două strategii nu sunt echivalente, deşi pot produce acelaşi trafic mediu.

Structurile de mesaje care transportă simultan valoarea, identitatea sursei, marca temporală şi starea semnalului permit reconstituirea contextului fără interogări suplimentare. Convenţiile de organizare a subiectelor şi de compunere a sarcinii utile (engl. payload) sunt tratate în capitolul 6; la nivelul acestui capitol este important doar că alegerea lor condiţionează scalabilitatea, nu doar lizibilitatea.

3.3.4. Arhitectura IIoT pentru producţia continuă

În producţia continuă, entitatea urmărită nu este un obiect, ci o variabilă de proces observată pe un interval de timp. Datele sunt continue, corelate între ele şi interpretabile numai împreună cu regimul de funcţionare al instalaţiei: aceeaşi temperatură poate fi normală într-o fază şi inacceptabilă în alta.

Sistemele de control distribuit, automatele programabile, sistemele SCADA şi istoricele de proces constituie nucleul operaţional, iar sistemele instrumentate de siguranţă funcţionează separat de acestea. Infrastructura IIoT se adaugă acestui nucleu pentru integrare, analiză şi vizibilitate, fără a interveni în buclele de reglare.

Arhitectura trebuie să asigure:

- redundanţa componentelor şi căilor de comunicaţie critice;
- sincronizarea temporală a surselor de date;
- stocarea locală în cazul întreruperii conexiunilor;
- separarea funcţiilor de analiză de cele de control şi siguranţă;
- gestionarea alarmelor şi a evenimentelor;
- validarea calităţii datelor;
- păstrarea istoricului necesar auditului şi investigării incidentelor.

Sincronizarea temporală este deosebit de importantă în procesele cu variabile interdependente, unde identificarea cauzelor perturbărilor depinde de succesiunea evenimentelor. Dacă decalajul ceasurilor depăşeşte timpul de propagare a perturbării, ordinea reconstruită poate fi inversată, conducând la concluzii cauzale

greşite. Marca temporală se aplică astfel cât mai aproape de măsurare şi se păstrează separat de cea a recepţiei în platformă, pentru conservarea diferenţei dintre ele.

Separarea reţelelor este a doua cerinţă structurală. Zona de proces, zona de supraveghere şi zona informaţională sunt segmentate, iar schimbul dintre ele se realizează controlat, printr-o zonă demilitarizată industrială (engl. industrial DMZ), cu fluxuri iniţiate dinspre interior. Cerinţele de zonare, de definire a conductelor de comunicaţie şi de niveluri de securitate sunt detaliate în seria de standarde dedicată securităţii sistemelor de automatizare şi control industrial [68], tratată pe larg în capitolul 8. Corelarea celor patru tipuri de producţie cu principalele componente ale arhitecturii IIoT este sintetizată în Tabelul 3.3.

Deciziile de siguranţă şi comenzile cu impact direct asupra instalaţiei nu trebuie să depindă de serviciile de calcul în cloud. Rezultatele analizelor pot susţine operatorii sau pot genera recomandări, dar aplicarea automată a unei modificări trebuie realizată numai prin mecanisme validate şi controlate, cu înregistrarea deciziei, a valorii aplicate şi a persoanei sau sistemului care a autorizat-o.

Tabelul 3.3 – Corelarea tipului de producție cu principalele componente ale arhitecturii IIoT

Tipul de producție	**Entitatea urmărită**	**Nucleul operațional**	**Integrarea informațională**	**Priorități arhitecturale**
Unicat	Produs, componentă și versiune	Echipamente configurabile și puncte flexibile de colectare	CAD, PLM, MES și documentație digitală	Trasabilitate individuală, flexibilitate și integrarea datelor eterogene
Serie	Lot, ordin de producție și configurație	PLC, HMI și SCADA	MES și ERP	Schimbare controlată a fabricației, urmărirea loturilor și controlul calității
Masă	Unitate, ciclu și linie	Control automatizat și prelucrare la edge	MES, platforme de analiză și servicii cloud	Scalabilitate, latență redusă, disponibilitate și filtrarea volumelor mari de date
Continuă	Variabilă și stare a procesului	DCS, PLC, SCADA și sisteme de siguranță	Istoric de proces și platforme de analiză	Redundanță, continuitate, sincronizare temporală și separarea funcțiilor critice

3.3.5. Dimensionarea fluxului de date şi a lăţimii de bandă

Cerinţele formulate până aici sunt calitative. Trecerea de la o arhitectură descrisă la una dimensionată presupune estimarea numerică a fluxului de date pe care procesul îl generează, deoarece de această mărime depind alegerea reţelei, locul prelucrării şi costul stocării. Calculul de mai jos este orientativ, dar structura sa se aplică oricărei configuraţii.

Datele problemei: Se consideră o linie de producție de masă cu 12 echipamente. Fiecare echipament furnizează 20 de semnale analogice (temperaturi, presiuni, curenți, viteze) și 30 de semnale binare (stări, confirmări, alarme). Semnalele analogice se eșantionează la 10 Hz, adică o valoare la 100 ms. Semnalele binare se transmit la schimbarea stării, cu o frecvență medie estimată de 2 schimbări pe minut pentru fiecare semnal.

Ipoteze de calcul: Fiecare valoare transmisă trebuie să conțină identificatorul sursei, valoarea propriu-zisă, marca temporală a măsurării, unitatea de măsură și indicatorul de calitate a semnalului. Se compară două convenții de transport:

- convenția A – un mesaj textual independent pentru fiecare valoare, cu numele complet al variabilei repetat în fiecare mesaj: 180 de octeți de sarcină utilă;
- convenția B – un mesaj pe echipament la fiecare perioadă de eșantionare, cu valori codificate binar și cu descrierea variabilelor transmisă separat, o singură dată, la stabilirea conexiunii: 12 octeți pe valoare și 24 de octeți antet de grup.

Pentru ambele convenții se consideră o suprasarcină de protocol de 80 de octeți pe mesaj, corespunzătoare antetelor MQTT, TCP/IP și înregistrării TLS. Traficul de control al procesului, imaginile de inspecție și fluxurile video nu sunt incluse.

Formula. Debitul binar necesar, exprimat în biți pe secundă, se obține însumând contribuția fiecărei categorii de semnale:

$$D = 8 \cdot \Sigma\, m_i \cdot (p_i + h)$$

unde m_i este numărul de mesaje pe secundă din categoria i, p_i este dimensiunea sarcinii utile în octeți, iar h este suprasarcina de protocol pe mesaj, în octeți.

Înlocuirea numerică – convenția A. Numărul de valori analogice pe secundă este 12 × 20 × 10 = 2 400. Numărul de valori binare pe secundă este 12 × 30 × 2 / 60 = 12. Fiecare valoare generează un mesaj de 180 + 80 = 260 de octeți.

$$D_A = 8 \times (2\,400 + 12) \times 260 = 5\,016\,960 \text{ bit/s} \approx 5{,}0 \text{ Mbit/s}$$

Înlocuirea numerică – convenția B. Valorile analogice se grupează pe echipament: 12 × 10 = 120 de mesaje pe secundă, fiecare cu 20 × 12 + 24 = 264 de octeți de sarcină utilă, deci 344 de octeți cu suprasarcină. Valorile binare rămân transmise prin excepție, 12 mesaje pe secundă a 92 de octeți.

$$D_B = 8 \times (120 \times 344 + 12 \times 92) = 8 \times 42\,384 = 339\,072 \text{ bit/s} \approx 0{,}34 \text{ Mbit/s}$$

Rezultatul. Aceeași informație, provenită din același proces, necesită 5,0 Mbit/s în prima convenție și 0,34 Mbit/s în a doua. Raportul este de aproximativ 15:1 și nu provine dintr-o reducere a datelor utile, ci exclusiv din modul de reprezentare și grupare a mesajelor.

Volumul stocat. Cele 2 412 valori pe secundă înseamnă aproximativ $2{,}08 \times 10^8$ valori pe zi. La 16 octeți pe valoare stocată, incluzând indexul, rezultă circa 3,3 GB pe zi și aproximativ 1,2 TB pe an pentru o singură linie. Istoricele de proces aplică metode de comprimare specifice seriilor temporale, cu factori uzuali între 5 și 10,

ceea ce conduce la 120–250 GB pe an. Pentru o fabrică cu opt linii comparabile, ordinul de mărime al debitului agregat este de 2,7 Mbit/s, iar al volumului anual comprimat, de 1–2 TB.

Interpretarea. Trei concluzii de proiectare decurg din acest calcul. Prima: pentru procese de acest tip, lățimea de bandă în rețeaua locală nu constituie o restricție, iar o infrastructură Ethernet obișnuită acoperă cerința cu o marjă confortabilă în ambele convenții. A doua: restricția reală apare pe legătura către serviciile externe, unde 5 Mbit/s permanenți reprezintă o cerință semnificativ diferită de 0,34 Mbit/s, atât ca disponibilitate, cât și ca cost, iar diferența se obține fără nicio pierdere de informație. A treia: decizia privind convenția de reprezentare a datelor, adesea tratată ca detaliu de implementare, are un efect de dimensionare mai mare decât alegerea echipamentelor de rețea.

Limitele calculului. Debitul calculat este o medie, însă rețeaua trebuie dimensionată pentru vârfuri, cu o marjă suplimentară. Pornirea instalației, oprirea generală sau propagarea alarmelor pot schimba simultan numeroase semnale binare, crescând traficul de 10–100 de ori față de medie. Cei 80 de octeți suplimentari sunt estimați: valoarea depinde de lungimea subiectelor, reutilizarea conexiunii securizate și gruparea pachetelor în stiva de comunicație. Cele 2 schimbări/minut presupuse pentru semnalele binare trebuie verificate și înlocuite cu valori măsurate. Estimarea include doar telemetria; imaginile inspecției vizuale pot depăși singure acest volum. Capitolul 6 explică mesajele și organizarea subiectelor, iar capitolul 7, dimensionarea completă și latența pe lanțul senzor–PLC–gateway–broker–bază de date.

3.3.6. Metodă de evaluare a unei fabrici și de stabilire a priorităților

Criteriile prezentate în secțiunile 3.3.1–3.3.5 pot fi transformate într-o procedură aplicabilă unei fabrici existente, înaintea oricărei decizii privind echipamentele sau furnizorii. Procedura parcurge șase pași:

Pasul 1 – Încadrarea procesului. Se stabilește tipul de producție dominant, conform secțiunii 3.1, și se identifică zonele care fac excepție. Puține fabrici au un singur tip de producție: o hală de serie poate conține un atelier de scule care funcționează în regim unicat și o instalație de tratament termic care funcționează continuu. Fiecare zonă se tratează separat.

Pasul 2 – Localizarea punctului de decuplare. Se determină momentul în care comanda clientului intervine în flux, conform secțiunii 3.1.5. Acest punct stabilește locul fizic în care identificatorul comenzii trebuie atașat produsului și separă zona în care trasabilitatea se construiește pe loturi de zona în care se construiește pe unități individuale.

Pasul 3 – Definirea entității urmărite și a modelului de date. Pentru fiecare zonă se stabilește la ce obiect se atașează datele: produs, componentă, lot, ordin de producție sau interval de proces. Se definesc atributele obligatorii ale oricărei valori –

identificator, marcă temporală a măsurării, unitate, calitate – şi regulile de asociere cu ordinul şi configuraţia.

Pasul 4 – Stabilirea timpului admis pentru reacţie. Pentru fiecare categorie de eveniment se determină intervalul în care detectarea are încă valoare operaţională. Rezultatul repartizează prelucrarea între automatul programabil, nivelul de la marginea reţelei şi nivelurile superioare, conform regulii formulate în secţiunea 3.3.3.

Pasul 5 – Dimensionarea fluxului. Se aplică metoda din secţiunea 3.3.5 pentru numărul real de semnale şi frecvenţele reale de eşantionare, cu estimarea vârfurilor şi a volumului de stocare pe durata de păstrare cerută.

Pasul 6 – Ierarhizarea intervenţiilor. Punctele de digitalizare se ordonează după raportul dintre pierderea produsă astăzi de lipsa informaţiei şi efortul de conectare. Criteriul nu este gradul de modernitate al echipamentului, ci frecvenţa cu care absenţa unei date generează o decizie greşită, o căutare manuală sau o reprelucrare.

Aplicarea grilei din Tabelul 3.4 nu produce o soluţie tehnică, ci o specificaţie. Valoarea ei constă în faptul că poate fi completată înaintea consultării unui furnizor şi permite compararea ofertelor pe criterii derivate din proces, nu din catalog.

Tabelul 3.4 – Grilă de evaluare a unei zone de producție în vederea digitalizării

Element evaluat	Întrebarea de verificare	Sursa criteriului
Tipul de producție	Care este regimul dominant al zonei și ce excepții conține?	Secțiunea 3.1
Punctul de decuplare	În ce operație devine produsul specific unei comenzi?	Secțiunea 3.1.5
Modelul de organizare	Ce combinație de JIT, lean, agil și personalizare este aplicată efectiv?	Secțiunea 3.2
Entitatea urmărită	La ce obiect se atașează datele colectate în această zonă?	Secțiunea 3.3
Timpul admis pentru reacție	În cât timp trebuie detectat fiecare tip de eveniment ca detecția să mai fie utilă?	Secțiunea 3.3.3
Autonomia locală	Ce funcții trebuie să rămână operaționale la pierderea legăturii externe?	Secțiunile 3.3.4 și 3.1.4
Volumul și frecvența datelor	Care este debitul mediu, debitul de vârf și volumul stocat anual?	Secțiunea 3.3.5
Prioritatea intervenției	Unde produce astăzi lipsa informației cea mai mare pierdere?	Pasul 6

3.3.7. Aplicarea metodei într-un scenariu de fabricație a mobilierului modular

Scenariul didactic al fabricii de mobilier modular din secţiunea 2.5 ilustrează aplicarea integrală a metodei şi raţionamentul aferent, fără a descrie o instalaţie documentată prin măsurători proprii.

Încadrarea şi punctul de decuplare. Zona de prelucrare funcţionează în producţie de serie cu personalizare ridicată, iar modelul comercial corespunde fabricaţiei la comandă: panourile brute şi feroneria sunt materiale standardizate, dar

dimensiunile, finisajele și combinațiile rezultă din configurația comandată. Punctul de decuplare se află la debitare, prima operație specifică unei comenzi – din acel moment piesa nu mai este interschimbabilă și trebuie identificată individual.

Entitatea urmărită și modelul de date. Înainte de debitare, entitatea este lotul de panouri, caracterizat prin material, grosime, furnizor și dată de recepție. După debitare, entitatea devine piesa, identificată prin cod bidimensional și asociată ordinului de producție, poziției din lista de materiale, versiunii documentației și programului utilizat de echipamentul cu comandă numerică.

Timpul admis pentru reacție. Trei categorii de evenimente au orizonturi diferite. Oprirea unui utilaj trebuie semnalată în secunde, pentru ca intervenția să înceapă înainte de blocarea fluxului din aval. O abatere dimensională trebuie detectată în cadrul aceluiași lot, adică în minute, altfel se propagă asupra întregii comenzi. Întârzierea unei comenzi trebuie identificată la nivel de zi, pentru ca planul să poată fi reordonat. Nicio decizie nu impune un timp de reacție sub 100 ms în afara buclelor locale de control ale utilajelor.

Dimensionarea fluxului. Față de linia din secțiunea 3.3.5, fabrica prezintă un flux de date semnificativ redus: mai puține semnale, eșantionare la 1 Hz posibilă pentru majoritatea mărimilor și trafic dominat de identificarea pieselor. Restricția critică privește acoperirea și fiabilitatea citirii codurilor în mediu cu praf de lemn, nu lățimea de bandă.

Evoluția arhitecturii. Arhitectura poate evolua gradual prin trei niveluri; acestea sunt reprezentate în Figura 3.6.

Primul nivel presupune funcționare locală și raportare manuală a ordinelor, timpilor și cantităților. ERP gestionează comenzile și materialele, fără preluare automată din producție. Datele fragmentate necesită verificări în surse multiple pentru identificarea cauzelor întârzierilor sau neconformităților.

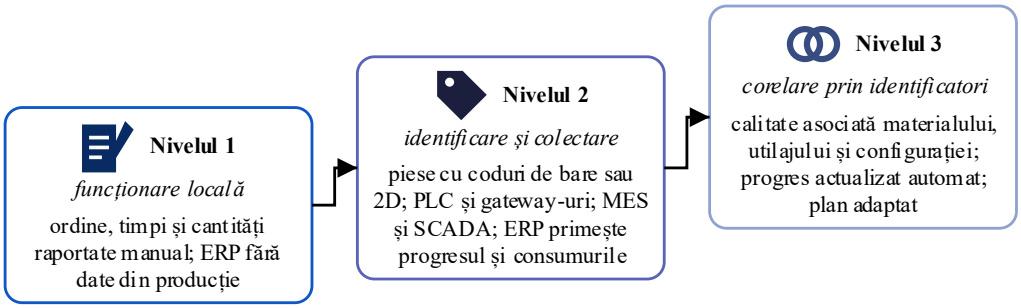


Figura 3.6 – Cele trei niveluri de conectare

La al doilea nivel, piesele sunt identificate prin coduri de bare sau coduri bidimensionale, iar stările utilajelor sunt colectate prin automate programabile și gateway-uri industriale. MES urmărește operațiile și ordinele de producție, SCADA monitorizează echipamentele, iar ERP primește informații privind progresul și

consumurile. Fabrica obține astfel vizibilitate asupra fluxului și poate localiza mai rapid opririle și comenzile întârziate.

La al treilea nivel, datele de proiectare, programele echipamentelor, materialele, parametrii procesului și rezultatele verificărilor sunt corelate prin identificatorul comenzii și al piesei. Abaterile de calitate pot fi asociate materialului, utilajului și configurației utilizate, iar datele privind starea echipamentelor susțin planificarea mentenanței. Finalizarea operațiilor actualizează automat progresul comenzii și permite adaptarea planului de producție.

Ierarhizarea intervențiilor. Evoluția dintre cele trei niveluri nu presupune înlocuirea simultană a tuturor echipamentelor. Conectarea poate începe în punctele în care lipsa informațiilor produce cele mai mari pierderi: identificarea pieselor după debitare, urmărirea comenzilor, înregistrarea opririlor și verificarea completitudinii seturilor înaintea ambalării.

Corelarea dintre tipul de producție, modelul de organizare și arhitectura IIoT este sintetizată în Figura 3.7. Ultimul punct este specific modelului de personalizare discutat în secțiunea 3.2.4 – o componentă lipsă face inutilizabil un produs executat corect în rest, iar costul remedierii apare la client, nu în fabrică.

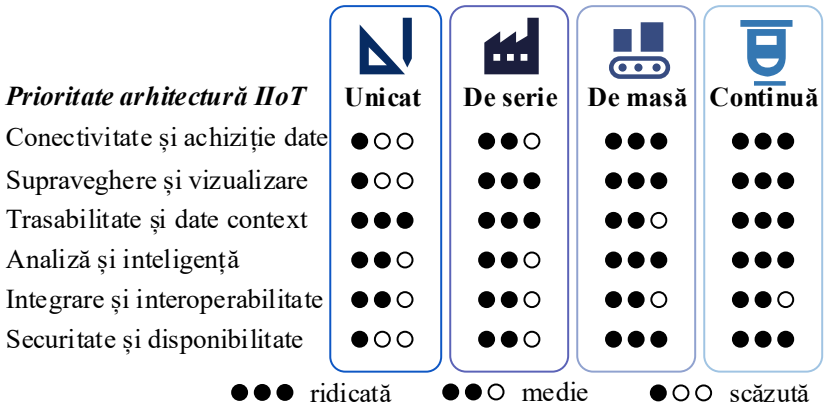


Figura 3.7 – Corelarea tipului de producție cu prioritățile arhitecturii IIoT

3.4. Concluzii

Tipul de producție determină cerințele privind automatizarea, trasabilitatea, frecvența colectării datelor și continuitatea funcționării. Producția unicat necesită flexibilitate și gestionarea riguroasă a documentației, producția de serie impune urmărirea loturilor și schimbarea controlată a configurațiilor, producția de masă solicită monitorizare continuă și disponibilitate ridicată, iar producția continuă necesită redundanță, sincronizare temporală și menținerea locală a funcțiilor critice.

Cele două perspective asupra procesului – cea managerială, construită pe volum, varietate și repetabilitate, și cea tehnologică, construită pe modul de curgere – nu

se suprapun și nu se pot substitui. Confundarea lor conduce la soluții dimensionate pentru un profil de date care nu corespunde procesului real. La acestea se adaugă o a treia distincție, independentă de primele două: poziția punctului de decuplare a comenzii, care stabilește operația din care produsul devine specific unei comenzi și, implicit, locul fizic în care trasabilitatea individuală devine posibilă și necesară.

Modelele JIT, lean și agil pot fi susținute prin colectarea și integrarea datelor, dar nu sunt înlocuite de tehnologie. Eficiența lor depinde de stabilitatea proceselor, calitatea informațiilor și capacitatea organizației de a transforma datele în decizii operaționale. Fiecare model solicită o categorie distinctă de date, iar personalizarea de masă rezultă din aplicarea lor simultană: costul provine din stabilitate și din eliminarea risipei, termenul din sincronizare, varietatea din agilitate. Riscul dominant al acestui din urmă model nu este de execuție, ci de configurare – un produs realizat corect după o specificație greșită trece de toate verificările interne.

Arhitectura IIoT trebuie proiectată pornind de la procesul industrial, de la entitatea urmărită și de la timpul disponibil pentru reacție. Acest ultim criteriu repartizează prelucrarea între automatul programabil, nivelul de la marginea rețelei și nivelurile superioare, iar aplicarea sa inversă – condiționarea unei acțiuni rapide de răspunsul unui serviciu extern – rămâne eroarea de proiectare cea mai frecventă. Funcțiile de control și de siguranță se mențin local, iar integrarea cu sistemele MES, ERP și cu platformele de analiză se realizează gradual, în funcție de utilitatea informațiilor și de riscurile operaționale.

Dimensionarea numerică a fluxului de date arată că modul de reprezentare și de grupare a mesajelor influențează debitul necesar mai mult decât alegerea echipamentelor de rețea, la volum de informație utilă identic. Concluzia practică este că decizia asupra convenției de date aparține fazei de proiectare a arhitecturii, nu fazei de implementare.

Metoda de evaluare în șase pași și grila asociată transformă aceste criterii într-o specificație care poate fi completată înaintea consultării unui furnizor. Valoarea ei constă în ordinea impusă: încadrarea procesului, localizarea punctului de decuplare, definirea entității urmărite, stabilirea timpilor de reacție, dimensionarea fluxului și abia apoi ierarhizarea intervențiilor. Un proiect care începe de la alegerea platformei ajunge, de regulă, să colecteze valori corecte care nu pot fi atribuite niciunui obiect gestionat în producție.

Corelațiile stabilite în acest capitol descriu ce trebuie să realizeze infrastructura, dar nu și cum trebuie construit sistemul fizic care execută producția. Capacitatea unei fabrici de a susține varietatea, schimbarea configurației și reconfigurarea fluxului depinde de proprietățile constructive ale echipamentelor și ale liniei: modularitate, interoperabilitate și adaptabilitate. Capitolul 4 tratează aceste proprietăți prin sistemele flexibile și reconfigurabile de fabricație, arătând cum cerințele formulate aici se traduc în arhitectura fizică a sistemului de producție și în modul de integrare a echipamentelor în rețele IIoT.

3.5. Întrebări de verificare

1. *Care este deosebirea dintre perspectiva managerială și cea tehnologică asupra procesului de producție?*

a) perspectiva managerială se aplică numai producției continue, iar cea tehnologică numai producției unicat;
b) perspectiva managerială distinge procesele după tipul de energie utilizată, iar cea tehnologică după numărul de angajați;
c) cele două perspective sunt echivalente și se pot înlocui una cu alta fără erori de dimensionare;
d) perspectiva managerială distinge unicat, serie și masă după volum, varietate și repetabilitate; cea tehnologică distinge procesele discrete, în loturi, semi continue și continue după modul de curgere.

2. *Care este entitatea urmărită și cum se construiește trasabilitatea în producția continuă?*

a) entitatea este piesa individuală, iar trasabilitatea se construiește prin cod bidimensional aplicat fiecărui produs;
b) entitatea este o variabilă de proces observată pe un interval de timp, iar trasabilitatea se atașează unui interval de timp și unei porțiuni de flux, nu unui obiect;
c) entitatea este comanda clientului, iar trasabilitatea se construiește pe numărul facturii;
d) nu există entitate urmărită, deoarece producția continuă nu necesită trasabilitate.

3. *Ce se poate întâmpla într-o producție de serie dacă sistemul de monitorizare nu primește semnalul de schimbare a fabricației?*

a) valorile de proces sunt șterse din istoric la schimbarea seriei;
b) poate raporta abateri false sau poate ascunde abateri reale într-o medie care combină datele a două configurații diferite;
c) sistemul oprește automat linia până la introducerea manuală a noii serii;
d) nimic, deoarece limitele de variație rămân valabile pentru orice serie.

4. *Cum se construiește trasabilitatea internă în fabricația pe stoc?*

a) pe piese individuale, cu identificatorul comenzii atașat de la debitare;
b) pe comenzi, deoarece produsul finit este realizat după primirea comenzii;
c) nu se construiește, deoarece produsele sunt realizate fără comandă;
d) pe loturi de material și intervale de producție, deoarece identificatorul comenzii apare abia la expediere.

5. *Care este corespondența corectă între modelele JIT, lean și agil și obiectivul principal al fiecăruia?*

a) JIT asigură personalizarea produselor; lean reconfigurează echipamentele; agilitatea elimină stocurile;

b) JIT elimină risipa; lean sincronizează materialele; agilitatea reduce costul unitar în producţia de masă;
c) JIT sincronizează materialele cu cererea reală; lean elimină risipa şi organizează activitatea; agilitatea indică cât costă şi durează schimbarea sistemului;
d) cele trei modele au acelaşi obiectiv şi diferă numai prin denumirea comercială.

6. Care dintre următoarele grupuri conţine numai forme de risipă (muda) descrise în modelul lean?

a) supraproducţia, aşteptarea, transportul inutil, prelucrarea excesivă, stocurile prea mari, mişcările inutile şi defectele;
b) supraproducţia, redundanţa reţelei, segmentarea zonelor, criptarea şi autentificarea;
c) timpul de ciclu, timpul de pregătire, disponibilitatea echipamentului şi rata produselor conforme;
d) stocurile de siguranţă, instruirea personalului, mentenanţa preventivă şi calibrarea senzorilor.

7. Care este riscul dominant al personalizării de masă şi de ce nu este detectat de controlul calităţii execuţiei?

a) este de natură informaţională: produsul este executat corect după o specificaţie greşită, deci trece de controlul dimensional şi funcţional şi este identificat abia la client;
b) este de natură energetică: consumul creşte proporţional cu varietatea produselor;
c) este de natură tehnologică: utilajele nu pot prelucra niciodată piese diferite;
d) este de natură juridică: produsele personalizate nu pot fi trasate.

8. Conform regulii practice de repartizare a prelucrării după timpul admis pentru reacţie, unde se prelucrează ceea ce trebuie să producă un efect în milisecunde?

a) în automatul programabil, local;
b) în sistemul MES, la nivel de schimb;
c) în gateway-ul industrial, prin agregare la edge;
d) într-un serviciu de calcul în cloud, pentru scalabilitate.

9. O linie de producţie de masă are 12 echipamente, fiecare cu 20 de semnale analogice eşantionate la 10 Hz şi 30 de semnale binare cu o schimbare medie de 2 ori pe minut. Fiecare valoare se transmite într-un mesaj de 180 de octeţi de sarcină utilă plus 80 de octeţi de suprasarcină de protocol. Care este debitul binar aproximativ?

a) aproximativ 0,63 Mbit/s;
b) aproximativ 0,34 Mbit/s;
c) aproximativ 50 Mbit/s;
d) aproximativ 5,0 Mbit/s.

10. Prin ce diferă transmiterea prin excepţie de simpla reducere a eşantionării?

a) transmiterea prin excepţie se aplică numai semnalelor analogice, iar reducerea eşantionării numai celor binare;
b) nu diferă: ambele scad rezoluţia în mod egal, indiferent de comportamentul procesului;
c) transmiterea prin excepţie păstrează rezoluţia completă în intervalele în care se produce ceva relevant şi o reduce în rest, în timp ce reducerea eşantionării scade rezoluţia în orice condiţii;
d) transmiterea prin excepţie elimină definitiv valorile brute, iar reducerea eşantionării le păstrează.

4. SISTEME FLEXIBILE ȘI RECONFIGURABILE DE FABRICAȚIE

Capitolul 3 a stabilit că arhitectura IIoT se deduce din procesul de producţie: din entitatea urmărită, din profilul datelor şi din timpul admis pentru reacţie. Corelarea rezultată rămâne valabilă atâta vreme cât produsul, volumul şi varietatea rămân stabile. Fabricile actuale funcţionează rar în asemenea condiţii. Cererea variază pe intervale scurte, ciclurile de viaţă ale produselor se scurtează, nivelul de personalizare creşte, iar variantele noi trebuie introduse fără oprirea producţiei curente. Întrebarea acestui capitol nu mai este ce arhitectură corespunde unui proces dat, ci ce trebuie să aibă sistemul fizic de producţie pentru ca schimbarea procesului să nu impună reconstruirea lui.

Sistemele rigide, dedicate unei game restrânse, asigură cost unitar redus şi performanţă previzibilă. Depăşirea ipotezelor de proiectare generează investiţii suplimentare sau capacitate neutilizată. Alternativele sunt sistemul flexibil de fabricaţie (FMS), bazat pe reprogramarea echipamentelor versatile şi trasee alternative pentru produse anticipate, şi sistemul reconfigurabil (RMS), care adaptează structura, capacitatea şi funcţionalitatea prin adăugarea, eliminarea sau reorganizarea modulelor, inclusiv la cerinţe iniţial nedefinite [106], [112]. Paradigmele tratează tipuri distincte de incertitudine, cu structuri diferite ale investiţiilor şi cerinţe specifice de gestionare a datelor şi configuraţiilor.

Capitolul tratează aceste sisteme din perspectiva integrării digitale, nu din cea a proiectării mecanice; relaţia dintre cele două este de condiţionare reciprocă. Infrastructura IIoT nu face un sistem flexibil, dar condiţionează valorificarea flexibilităţii existente: fără identificarea modulelor, fără date contextualizate şi fără verificarea configuraţiei active, o linie modulară rămâne un ansamblu de echipamente care se reconfigurează manual şi se validează de fiecare dată de la zero. Reciproc, un sistem bine instrumentat, dar cu module incompatibile mecanic sau informaţional, nu poate fi reorganizat oricât de bogate ar fi datele colectate. Această dublă dependenţă este motivul pentru care proprietăţile constructive şi cele informaţionale sunt tratate aici împreună.

Structura capitolului urmează această logică. Secţiunea 4.1 delimitează cele două paradigme, distinge tipurile de flexibilitate care se ascund sub acelaşi cuvânt şi transformă decizia de scalare într-un calcul cu variante comparabile. Secţiunea 4.2 tratează cele trei proprietăţi care condiţionează funcţionarea sistemelor flexibile – modularitatea, interoperabilitatea şi adaptabilitatea – şi arată de ce niciuna nu compensează absenţa celorlalte; tot aici se descompune cantitativ efortul unei reconfigurări, mărimea cel mai frecvent subestimată în justificările economice. Secţiunea 4.3 descrie integrarea efectivă a echipamentelor într-o reţea IIoT: ce date furnizează o celulă, cum se distribuie funcţiile între echipament, nivelul edge,

SCADA, MES și platformele de analiză și ce trebuie validat înaintea extinderii. Secțiunea 4.4 aplică aceste principii într-un exercițiu de simulare a unei linii flexibile controlate printr-un automat programabil.

Două precizări traversează întregul capitol. Prima: funcțiile de comandă critică, interblocările și funcțiile de siguranță rămân locale. Sistemele externe colectează, contextualizează, analizează și afișează, dar indisponibilitatea lor nu trebuie să determine pierderea controlului asupra procesului – regulă care are aici prima formulare tehnică detaliată și care revine în capitolele 5, 7 și 8. A doua: valorile numerice din exemplele de calcul sunt ipoteze de lucru declarate, alese pentru claritatea raționamentului, iar exercițiul din secțiunea 4.4 este un scenariu didactic, nu o instalație documentată.

Obiectivele capitolului

La finalul acestui capitol, cititorul va putea:

- să diferențieze sistemul flexibil de fabricație de sistemul reconfigurabil de fabricație, pe baza sursei flexibilității, a domeniului de variație acoperit și a tipului de modificare admis;
- să descrie componentele arhitecturale ale unui FMS și să explice de ce flexibilitatea ansamblului este limitată de componenta cea mai puțin adaptabilă;
- să distingă cele șase tipuri de flexibilitate tratate în capitol și să indice, pentru o cerință operațională dată, care dintre ele este efectiv solicitată și prin ce mijloc se obține;
- să calculeze numărul de stații necesare unei cereri date, capacitatea și gradul de utilizare rezultate și să compare variantele de acoperire a cererii înainte de a propune o investiție;
- să descompună efortul unei reconfigurări pe componente și să argumenteze de ce durata validării, nu cea a intervenției mecanice, determină pragul economic al schimbării;
- să argumenteze rolul modularității fizice, logice și informaționale și să identifice cele șase categorii de interfețe pe care trebuie să le expună un modul de producție;
- să distingă compatibilitatea tehnică, sintactică, semantică și operațională și să identifice etapa proiectului în care absența fiecăreia produce consecințe;
- să selecteze datele pe care o celulă flexibilă trebuie să le transmită într-o rețea IIoT, pornind de la decizia pe care o susține, și să întocmească fișa de specificație a unei categorii de date;
- să proiecteze și să valideze o logică de control pentru un sistem flexibil simulat, incluzând separarea dintre logică și rețetă, tratarea blocajelor și reluarea controlată a funcționării.

4.1. Arhitectura sistemelor flexibile și reconfigurabile de fabricație

Sistemele flexibile şi cele reconfigurabile de fabricaţie urmăresc acelaşi rezultat – adaptarea producţiei la variaţia produselor şi a cererii – prin mecanisme diferite. Într-un FMS, flexibilitatea este prevăzută în etapa de proiectare şi se manifestă în limitele gamei de produse, ale proceselor şi ale echipamentelor configurate; sistemul oferă o flexibilitate generalizată, construită în avans pentru variaţiile anticipate. Într-un RMS, structura poate fi modificată pentru a adapta capacitatea şi funcţionalitatea la cerinţe care nu au fost definite integral iniţial, ceea ce literatura de referinţă descrie ca flexibilitate personalizată, furnizată atunci când devine necesară şi în măsura în care devine necesară [112]. Distincţia a fost formulată sistematic în lucrarea care a introdus paradigma reconfigurabilă [106] şi a fost dezvoltată ulterior într-un corp consistent de literatură [113], [114], [115].

Distincţia are implicaţii economice directe. FMS concentrează costurile în investiţia iniţială, reducând costul marginal al schimbării în gama prevăzută. RMS porneşte cu investiţie şi capacitate mai mici, dar necesită extinderi ulterioare în trepte costisitoare. Alegerea depinde de natura incertitudinii: varietatea cunoscută şi volumul incert favorizează RMS; volumul stabil şi varietatea dificil de anticipat într-o familie de produse favorizează FMS. În comparaţiile cu linia dedicată, justificarea economică a RMS presupune ca totalul costurilor treptelor de capacitate, pe durata de viaţă estimată, să rămână inferior costului capacităţii instalate anticipat şi neutilizate [115], [116].

4.1.1. Sistemul flexibil de fabricație

Un FMS integrează staţii automate de prelucrare sau de asamblare, sisteme pentru manipularea materialelor şi o infrastructură de control capabilă să coordoneze realizarea mai multor produse dintr-o familie [1], [117]. Trecerea de la un produs la altul se realizează prin schimbarea programelor, sculelor, parametrilor şi traseelor, fără reconstruirea sistemului. Arhitectura funcţională a unui asemenea sistem este reprezentată în Figura 4.1.

Arhitectura include şapte categorii: staţii de lucru — maşini-unelte cu comandă numerică, roboţi industriali, inspecţie automată; transport şi stocare temporară — transportoare, vehicule ghidate automat, roboţi mobili autonomi — pentru decuplarea staţiilor; dispozitive de fixare, magazii şi schimbătoare automate de scule; senzori şi identificare pentru urmărirea pieselor, resurselor şi stării echipamentelor; controlere locale pentru secvenţele staţiilor; coordonare pentru alocarea operaţiilor, definirea traseelor şi sincronizarea resurselor; integrare SCADA–MES–ERP pentru supraveghere, execuţie şi planificare [1].

Identificarea piesei sau lotului la intrare permite stabilirea traseului după operaţii şi disponibilitatea resurselor. Staţiile echivalente funcţional oferă rute alternative pentru echilibrarea încărcării şi ocolirea echipamentelor indisponibile. Flexibilitatea de rutare, definită în clasificarea sistemelor flexibile [117] şi invocată

frecvent pentru justificarea investiției, presupune coordonare capabilă de realocare în timp util. Această condiție este rar verificată explicit. Redundanța stațiilor cu trasee fixe în programul de control înseamnă doar capacitate suplimentară. Figura 4.2 identifică elementul care limitează flexibilitatea celulei.

Roboții industriali contribuie la flexibilitate prin posibilitatea reprogramării mișcărilor și a sarcinilor. Flexibilitatea unei celule robotizate nu depinde însă numai de robot, ci și de dispozitivul de prindere, de dispozitivele de fixare, de alimentarea cu piese, de senzori, de programe și de sistemele de siguranță. Regula practică este că ansamblul nu poate fi mai flexibil decât componenta sa cea mai puțin adaptabilă: o celulă cu robot reprogramabil, dar cu dispozitiv de prindere dedicat unei singure geometrii, nu poate prelua o variantă nouă fără intervenție mecanică, iar reprogramarea robotului rămâne fără efect. Aceeași regulă se aplică și părții informaționale a celulei, discutată în secțiunea 4.3.2.

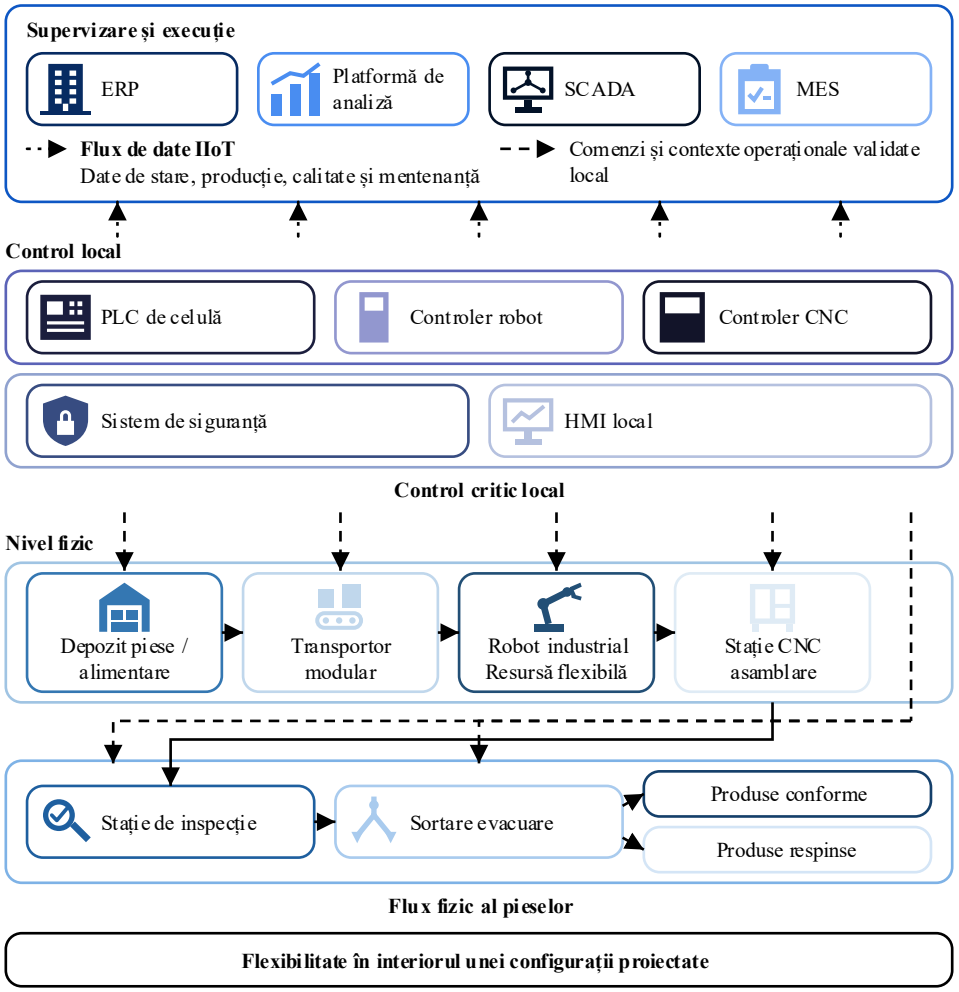


Figura 4.1 – Arhitectura celulei flexibile de fabricație

Infrastructura IIoT permite colectarea datelor privind starea echipamentelor, timpii de ciclu, poziţia pieselor, nivelul cozilor de aşteptare, uzura sculelor, consumurile şi alarmele. Procesarea locală a acestor date poate susţine identificarea blocajelor, redistribuirea controlată a comenzilor şi planificarea mentenanţei. MES corelează informaţiile operaţionale cu ordinele de producţie, iar ERP utilizează datele agregate pentru planificarea materialelor şi a capacităţii, potrivit repartizării funcţionale definite normativ pentru schimbul de informaţii dintre nivelul de execuţie şi cel de planificare [75], [49].

FMS oferă schimbări rapide de fabricaţie, utilizare eficientă a echipamentelor, varietate şi trasabilitate îmbunătăţită [1]. Cerinţele includ investiţii ridicate, integrarea echipamentelor eterogene şi personal calificat. Beneficiile scad când flexibilitatea disponibilă rămâne neutilizată sau gama produselor depăşeşte limitele proiectate. Complexitatea excesivă generează costuri pentru flexibilitate nevalorificată şi robusteţe inferioară unei linii dedicate [113]. Criteriul investiţional este numărul variantelor realizate efectiv într-un interval de referinţă, raportat la posibilităţile sistemului.

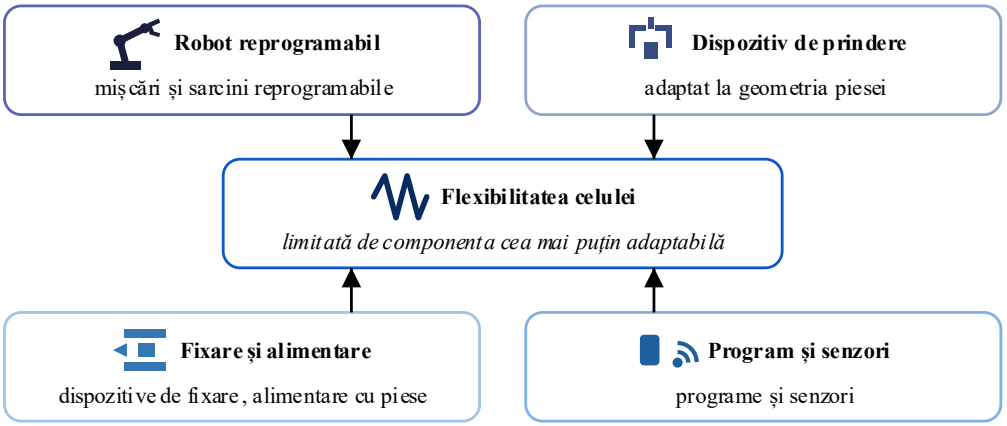


Figura 4.2 – Componenta limitativă a flexibilităţii celulei

4.1.2. Sistemul reconfigurabil de fabricaţie

Un RMS este proiectat astfel încât structura, capacitatea şi funcţionalitatea sa să poată fi modificate prin adăugarea, eliminarea, înlocuirea sau reorganizarea modulelor [106]. Reconfigurarea poate viza o staţie, o celulă, sistemul de transport, infrastructura de control sau succesiunea operaţiilor.

Arhitectura unui asemenea sistem se bazează pe module de producţie cu funcţii clar definite, pe interfeţe mecanice, electrice şi de comunicaţie standardizate, pe control local suficient de autonom pentru fiecare modul, pe mecanisme pentru identificarea şi înregistrarea configuraţiei active, pe gestionarea versiunilor programelor, parametrilor şi documentaţiei, pe diagnosticarea stării şi a compatibilităţii modulelor şi pe validarea configuraţiei înaintea reluării producţiei [106],

[116]. Ultimele patru elemente sunt de natură informaţională, ceea ce explică de ce un sistem reconfigurabil nu poate fi construit fără o infrastructură de date proiectată odată cu el. Deosebirile dintre cele două categorii de sisteme sunt sintetizate în Tabelul 4.1.

Tabelul 4.1 – Comparația dintre sistemele FMS și RMS

Criteriu	FMS	RMS
Obiectiv principal	Realizarea flexibilă a unei game cunoscute de produse	Adaptarea capacității și a funcționalității la cerințe noi
Sursa flexibilității	Reprogramarea și utilizarea versatilă a echipamentelor	Modificarea structurii și a configurației sistemului
Domeniul de variație	Stabilit în mare parte la proiectare	Extensibil prin înlocuirea sau adăugarea modulelor
Modificări caracteristice	Schimbarea programelor, sculelor, parametrilor și traseelor	Adăugarea, eliminarea sau reorganizarea stațiilor și modulelor
Structură	Integrată și relativ stabilă	Modulară și proiectată pentru modificare
Structura costului	Investiție inițială ridicată, cost marginal redus al schimbării	Investiție inițială moderată, cost pe treaptă de extindere
Tipul de incertitudine acoperit	Varietate anticipată în interiorul familiei de produse	Volum și funcționalitate nedefinite la proiectare
Limitare principală	Flexibilitate restrânsă la domeniul prevăzut inițial	Complexitatea interfețelor, a validării și a gestionării configurațiilor
Rolul infrastructurii IIoT	Monitorizarea și optimizarea utilizării resurselor	Identificarea, coordonarea și verificarea modulelor și configurațiilor

Literatura de referinţă delimitează şase caracteristici de proiectare care fac un sistem efectiv reconfigurabil (Figura 4.3): modularitatea, integrabilitatea, personalizarea capabilităţilor în raport cu familia de produse, convertibilitatea, scalabilitatea şi diagnosticabilitatea [106], [112], [115]. Primele trei se decid la proiectare şi sunt vizibile în specificaţia tehnică. Ultimele trei se manifestă abia la prima schimbare şi sunt, din acest motiv, cel mai des subestimate. Convertibilitatea priveşte trecerea rapidă la o funcţionalitate nouă şi se măsoară prin durata dintre decizia de schimbare şi prima piesă conformă.

Scalabilitatea priveşte modificarea capacităţii în trepte economice şi se măsoară prin mărimea şi costul treptei, mărimi calculate în secţiunea 4.1.4. Diagnosticabilitatea condiţionează durata rampei de pornire după reconfigurare: un sistem care nu îşi poate identifica singur abaterile de configuraţie transferă această sarcină punerii în funcţiune, unde costul orar este cel mai ridicat, iar rampa de pornire este intervalul în care se concentrează cea mai mare parte a pierderilor asociate unei schimbări [118].

Scalarea capacităţii poate fi realizată prin introducerea unei staţii suplimentare, iar extinderea funcţionalităţii prin adăugarea unui modul nou de prelucrare, asamblare sau control [116]. Un modul defect poate fi izolat sau înlocuit dacă arhitectura

permite redistribuirea operaţiilor şi dacă sunt menţinute condiţiile de siguranţă şi calitate [115].

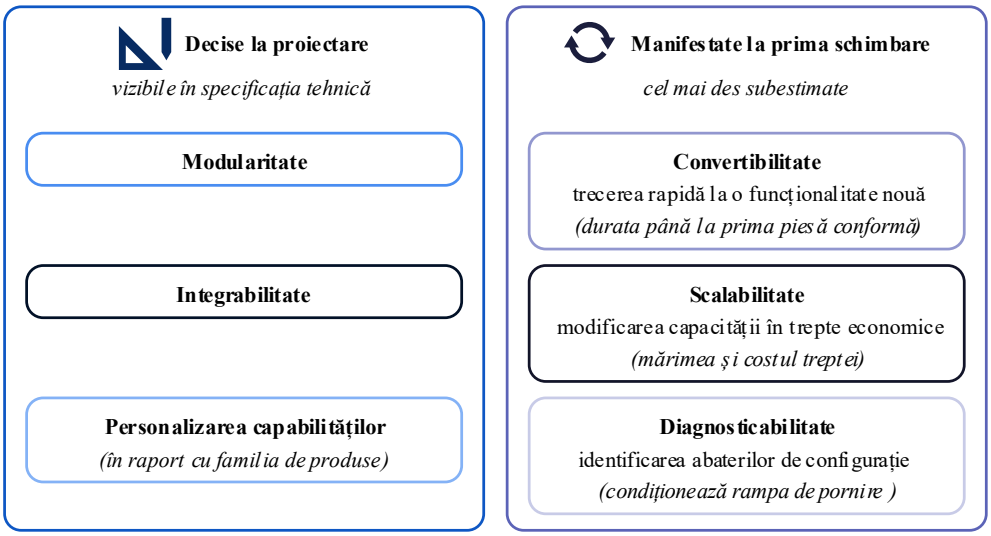


Figura 4.3 – Caracteristicile de proiectare ale sistemelor reconfigurabile

Reconfigurarea cuprinde intervenţii fizice şi logice: programe de controlere şi roboţi, comunicaţii, modele de date, reguli de coordonare şi configuraţie MES. Delimitarea modificărilor echipamentelor de cele software şi informaţionale fundamentează estimarea efortului [112], [119]. Validarea înaintea reluării producţiei acoperă compatibilitatea modulelor, funcţiile de siguranţă, precizia, timpul de ciclu şi corectitudinea transmiterii datelor.

Infrastructura IIoT susţine acest proces prin furnizarea informaţiilor privind identitatea, capabilităţile, starea şi disponibilitatea fiecărui modul. Configuraţia activă poate fi comparată cu cea aprobată, iar abaterile privind conexiunile, parametrii sau versiunile software pot fi semnalate înaintea lansării producţiei. Standardizarea acestor descrieri face obiectul unor lucrări normative recente: structura reprezentării digitale uniforme a activului industrial expune identitatea, capabilităţile şi datele acestuia într-o formă exploatabilă de aplicaţii diferite, independent de furnizorul echipamentului [120]. Modelul de referinţă pentru arhitecturile Industriei 4.0 plasează aceeaşi descriere pe axele de ierarhie, de ciclu de viaţă şi de strat funcţional, ceea ce permite verificarea faptului că un proiect acoperă efectiv toate interfeţele necesare, nu doar pe cele de comunicaţie [6]. Datele colectate după reconfigurare permit verificarea stabilităţii procesului şi compararea performanţei cu rezultatele estimate.

O aplicaţie recentă a acestei logici o constituie utilizarea unui model digital al sistemului pentru verificarea configuraţiei înaintea execuţiei fizice. Un geamăn digital al liniei, alimentat cu datele reale ale modulelor, permite evaluarea unei

configuraţii propuse – timpi de ciclu, interferenţe, echilibrarea posturilor – fără oprirea producţiei curente [107]. Valoarea acestei practici nu constă în eliminarea validării fizice, care rămâne obligatorie, ci în reducerea numărului de iteraţii efectuate pe instalaţia reală.

Funcţiile critice de comandă şi de siguranţă trebuie să rămână locale. Platformele IIoT pot sprijini selectarea configuraţiei, monitorizarea şi analiza, dar nu înlocuiesc validarea tehnică a modificărilor şi nici mecanismele industriale de control. Într-un sistem reconfigurabil, cerinţa are o consecinţă suplimentară faţă de o linie fixă: funcţiile de siguranţă trebuie revalidate la fiecare schimbare de configuraţie, întrucât zonele de risc, distanţele de siguranţă şi logica de interblocare se modifică odată cu amplasarea modulelor.

4.1.3. Tipuri de flexibilitate şi dimensionarea capacităţii

Termenul „*flexibilitate*" acoperă proprietăţi care nu se obţin prin aceleaşi mijloace, nu au acelaşi cost şi nu se măsoară prin aceiaşi indicatori. Clasificările consacrate delimitează opt tipuri de flexibilitate pentru sistemele de fabricaţie [117] şi extind analiza la unsprezece dimensiuni, grupate pe niveluri de agregare [121]. Capitolul de faţă reţine şase dintre acestea – de maşină, de proces, de produs, de rutare, de volum şi de expansiune, întrucât ele sunt cele care influenţează direct arhitectura sistemului şi profilul datelor colectate; celelalte, între care flexibilitatea operaţiilor, a manipulării materialelor şi a programului de fabricaţie, sunt cuprinse implicit în primele sau se manifestă la nivelul planificării, tratat în capitolele 2 şi 7.

Distincţia este operaţională, nu academică. O cerinţă de „*mai multă flexibilitate*" formulată de producţie înseamnă, aproape întotdeauna, una singură dintre acestea, iar investiţia potrivită diferă radical: flexibilitatea de rutare se obţine prin staţii redundante şi printr-un nivel de coordonare capabil să realoce, în timp ce flexibilitatea de produs se obţine prin interfeţe mecanice şi prin modele de date pregătite pentru variante încă nedefinite. Confundarea lor produce sistematic acelaşi rezultat – un sistem capabil de altceva decât ceea ce i se cere.

Tabelul 4.2 asociază fiecărui tip de flexibilitate întrebarea la care răspunde, mijlocul prin care se obţine şi indicatorul prin care poate fi verificat. Ultima coloană are o consecinţă directă asupra proiectării infrastructurii de date: dacă un indicator nu poate fi calculat din datele colectate, proprietatea corespunzătoare nu poate fi demonstrată, nici îmbunătăţită.

Primele trei tipuri sunt, prin natura lor, atribute ale unui FMS: ele descriu ce poate face sistemul în interiorul unui domeniu stabilit. Ultimele trei sunt atribute ale unui RMS: ele descriu cum poate fi modificat domeniul însuşi. Criteriul practic de alegere între paradigme rezultă din această repartiţie. Dacă cerinţele operaţionale se concentrează în primele trei rânduri ale tabelului, sistemul trebuie proiectat pentru versatilitate; dacă se concentrează în ultimele trei, trebuie proiectat pentru

modificare. Cele două nu se exclud, dar nici nu se obţin gratuit împreună: fiecare tip de flexibilitate adăugat consumă investiţie şi adaugă complexitate de validare.

În practică, paradigmele se combină. O fabrică poate utiliza un FMS pentru realizarea curentă a mai multor variante şi poate proiecta anumite celule după principiile RMS, astfel încât acestea să poată fi extinse sau transformate [112], [119]. Decizia de repartizare urmează, de regulă, poziţia în flux: zonele apropiate de punctul de decuplare a comenzii, discutat în secţiunea 3.1.5, sunt cele care beneficiază de versatilitate, întrucât acolo se manifestă varietatea, în timp ce zonele din amonte, unde variază mai degrabă volumul decât configuraţia, sunt candidatele naturale pentru scalarea modulară.

Tabelul 4.2 – Tipuri de flexibilitate, mijloace de obținere și indicatori de verificare

Tipul de flexibilitate	Întrebarea la care răspunde	Mijlocul principal de obținere	Indicatorul care o face verificabilă
A mașinii	Câte operații diferite execută un utilaj fără intervenție majoră?	Control programabil, magazie și schimbare automată a sculelor	Numărul de operații distincte executate și durata schimbării sculei
A procesului	Câte produse pot fi realizate fără schimbarea sculelor?	Familii de produse, dispozitive de fixare universale	Numărul de variante prelucrate între două schimbări de fabricație
A produsului	Cât costă introducerea unei variante noi?	Interfețe mecanice și model de date pregătite pentru extindere	Durata de la aprobarea variantei până la prima piesă conformă
De rutare	Există trasee alternative utilizabile efectiv?	Stații redundante și nivel de coordonare capabil să realoce	Proporția pieselor deviate și timpul de reacție la indisponibilitatea unei stații
De volum	Funcționează sistemul economic la încărcări diferite?	Automatizare gradată, decuplare prin zone tampon	Costul unitar la 50 %, 75 % și 100 % din capacitate
De expansiune	Poate fi mărită capacitatea fără reproiectare?	Modularitate, spațiu și interfețe rezervate din proiectare	Mărimea, costul și durata treptei de capacitate

4.1.4. Dimensionarea capacității și costul treptei de scalare

Flexibilitatea de expansiune este singurul tip din Tabelul 4.2 care poate fi transformat direct într-un calcul, iar acest calcul este cel care decide dacă reconfigurarea este o soluţie sau doar o opţiune tehnică atrăgătoare. Exemplul care urmează este un scenariu didactic: ipotezele sunt declarate integral, iar valorile sunt alese pentru claritatea raţionamentului, nu preluate dintr-o instalaţie documentată.

Date de intrare. O staţie critică dintr-o linie de fabricaţie funcţionează 250 de zile pe an, în două schimburi de 8 ore. Disponibilitatea planificată, care exclude mentenanţa programată, schimbările de fabricaţie şi pauzele tehnologice, este de 85 %. Timpul de ciclu al staţiei este de 95 s/buc. Cererea anuală actuală este de 120 000 de bucăţi, iar prognoza indică o creştere la 210 000 de bucăţi.

Timpul de producţie disponibil:

$$T = 250 \times 2 \times 8 \times 3.600 \times 0{,}85 = 12.240.000 \text{ s/an, echivalent cu } 3.400 \text{ h/an}$$

Capacitatea unei staţii:

$$C_1 = T / t_c = 12.240.000 / 95 = 128.842 \text{ buc/an}$$

Timpul de tact la cererea actuală:

$$t_tact = T / Q = 12.240.000 / 120.000 = 102 \text{ s/buc}$$

Timpul de ciclu (95 s) fiind mai mic decât timpul de tact (102 s), o singură staţie acoperă cererea actuală, cu un grad de utilizare U = t_c / t_tact = 95 / 102 = 0,931, adică 93,1 %. Valoarea merită reţinută: ea arată că sistemul funcţionează deja peste pragul de la care variabilitatea timpului de ciclu şi opririle scurte încep să erodeze debitul real, iar capacitatea teoretică nu mai este atinsă [76].

Timpul de tact la cererea prognozată:

$$t_tact = 12.240.000 / 210.000 = 58,3 \text{ s/buc}$$

Numărul de staţii identice necesare:

$$n = \lceil t_c / t_tact \rceil = \lceil 95 / 58,3 \rceil = \lceil 1,63 \rceil = 2$$

Rezultatul fracţionar este esenţa problemei de scalare: cererea impune 1,63 staţii, iar sistemul admite numai valori întregi. Consecinţele acestei granularităţi se văd comparând variantele din Tabelul 4.3, calculate pornind de la aceleaşi date de intrare.

Tabelul 4.3 – Variante de acoperire a cererii

Variantă	Timp disponibil (s/an)	Staţii	Capacitate (buc/an)	Grad de utilizare	Observaţie
A. Situaţia actuală: 2 schimburi, 1 staţie	12.240.000	1	128.842	—	Acoperă 61 % din cerere; insuficientă
B. Modul suplimentar: 2 schimburi, 2 staţii	12.240.000	2	257.684	81,5 %	Rezervă de 47 700 buc/an; investiţie într-un modul
C. Extindere a regimului: 3 schimburi, 300 de zile, 1 staţie	22.032.000	1	231.916	90,6 %	Fără investiţie în echipament; utilizare peste pragul de siguranţă
D. Intervenţie tehnologică: ciclu redus la 58 s, 1 staţie	12.240.000	1	211.034	99,5 %	Fără rezervă; presupune reproiectarea operaţiei

Cazul-limită al staţiei dominante. Calculul presupune că numai staţia analizată limitează debitul, ipoteză care necesită verificare: dublarea acesteia transferă restricţia. Dacă următoarea staţie are ciclul de 55 s, faţă de 47,5 s pentru staţia dublată, capacitatea liniei devine 12.240.000 / 55 ≈ 222.545 buc./an. Cererea de 210.000 buc./an rămâne acoperită, dar rezerva scade de la 47 700 la 12 545 de bucăţi, de aproape patru ori. Un ciclu de 60 s al celei de-a doua staţii ar limita producţia la 204 000 buc./an, investiţia devenind insuficientă. După fiecare treaptă de scalare, capacitatea liniei trebuie recalculată folosind noua staţie dominantă.

Interpretare. Varianta A este exclusă prin calcul: raportul ciclu/tact depăşeşte unitatea, fără posibilitatea compensării prin reglaje. D, aparent economică, necesită reducerea ciclului cu 39 %, implicând reproiectarea operaţiei, şi oferă o rezervă

neglijabilă de 0,5 %. C transferă investiția în echipament către costurile cu personalul, atingând o utilizare de 90,6 %, peste pragul acumulării întârzierilor. B asigură singura o rezervă utilizabilă și o utilizare sub 85 %, ilustrând avantajul reconfigurării: treapta adecvată de capacitate. Cele 47.700 de bucăți neutilizate reprezintă costul granularității, care trebuie justificat economic împreună cu posibilitatea acoperirii unei cereri viitoare mai mari.

Limitele calculului. Modelul tratează stația critică izolat și presupune, în varianta de bază, că restul liniei poate susține noul ritm – ipoteză corectată prin verificarea stației dominante. Nu include timpul de rampă după reconfigurare, capacitatea zonelor tampon dinaintea și de după stație, timpul suplimentar de transport și de deviere introdus de a doua stație, variabilitatea timpului de ciclu, rebuturile, reechilibrarea celorlalte posturi și disponibilitatea efectivă, care diferă de cea planificată. Peste o utilizare de aproximativ 85 %, efectul variabilității asupra cozilor de așteptare devine dominant, iar capacitatea calculată nu mai este realizabilă [76]. Calculul este util pentru stabilirea ordinului de mărime și pentru delimitarea deciziei – o stație sau două, nu pentru dimensionarea finală, care se face prin simulare sau prin măsurare pe sistemul existent.

Datele pe care le presupune acest calcul – timpii de ciclu reali, disponibilitatea efectivă, cauzele și duratele opririlor – sunt exact cele pe care le furnizează infrastructura descrisă în secțiunea 4.3. În absența lor, dimensionarea se face pe valori nominale din catalog, care supraestimează sistematic capacitatea, iar diferența apare abia după punerea în funcțiune. Eficiența unei arhitecturi flexibile depinde însă nu doar de dimensionarea corectă a capacității, ci și de trei proprietăți care condiționează posibilitatea însăși a modificării: modularitatea, interoperabilitatea și adaptabilitatea, analizate în secțiunea următoare.

4.2. Modularitate, interoperabilitate și adaptabilitate

Funcționarea eficientă a FMS și RMS depinde de trei proprietăți complementare. Modularitatea face posibilă modificarea structurii, interoperabilitatea asigură colaborarea dintre componentele modificate, iar adaptabilitatea transformă informația despre proces într-un răspuns operațional. Ordinea nu este întâmplătoare: fiecare proprietate o presupune pe cea anterioară fără să o garanteze, iar absența oricăreia anulează, în practică, beneficiul celorlalte două.

Cele trei proprietăți trebuie prevăzute în etapa de proiectare, întrucât adăugarea lor ulterioară costă, de regulă, mai mult decât ar fi costat includerea lor inițială. Simplificarea unei modificări fizice nu este suficientă dacă integrarea software necesită dezvoltări ample, iar schimbul de date nu produce valoare dacă sistemul nu poate utiliza informațiile pentru monitorizare, coordonare sau decizie. Secțiunea 4.2.4 arată cantitativ cât valorează această anticipare, prin descompunerea efortului unei reconfigurări.

4.2.1. Modularitatea

Modularitatea reprezintă organizarea sistemului de fabricaţie în unităţi funcţionale cu roluri clar definite şi cu interfeţe controlate. Un modul poate fi o staţie de prelucrare, un robot, o unitate de inspecţie, un segment de transport, un dispozitiv de identificare sau o componentă software. Definiţia utilă în practică nu se referă la aspectul fizic al unităţii, ci la raportul dintre funcţiile pe care le îndeplineşte şi interfeţele prin care le expune: un modul este cu atât mai bine delimitat cu cât realizează o funcţie identificabilă şi o expune printr-un număr mic de interfeţe stabile. Formularea provine din teoria arhitecturii produsului, unde arhitectura modulară este definită prin corespondenţa univocă dintre funcţii şi componente şi prin interfeţe decuplate, în opoziţie cu arhitectura integrată, în care o funcţie este distribuită pe mai multe componente [122]. Consecinţa este aceeaşi pentru un produs şi pentru un sistem de producţie: gradul de modularitate se măsoară prin cât de local rămâne efectul unei modificări.

Pentru a putea fi adăugat, înlocuit sau reorganizat fără reconstruirea întregului sistem, un modul trebuie să dispună de şase categorii de interfeţe compatibile: *mecanice*, pentru poziţionare, fixare şi transferul produselor; *electrice şi pneumatice*, pentru alimentare şi acţionare; *de comunicaţie*, pentru schimbul de date şi comenzi; *software*, pentru configurare şi integrarea funcţiilor; *informaţionale*, pentru descrierea identităţii, a capabilităţilor şi a stării proprii; şi *de siguranţă*, pentru integrarea în mecanismele de protecţie ale sistemului. Un modul devine cu adevărat reconfigurabil doar atunci când este integrabil fizic, logic şi informaţional. Figura 4.4 prezintă aceste interfeţe, grupate pe cele trei planuri ale modularităţii.

Practica arată că primele trei categorii de interfeţe sunt aproape întotdeauna prevăzute, iar ultimele trei aproape întotdeauna neglijate. Un modul cu conector mecanic standardizat, dar fără o descriere formală a capabilităţilor sale şi fără o interfaţă de siguranţă proiectată pentru integrare, se montează în câteva ore şi se integrează în câteva săptămâni.

Practica arată că primele trei categorii de interfeţe sunt aproape întotdeauna prevăzute, iar ultimele trei aproape întotdeauna neglijate. Un modul cu conector mecanic standardizat, dar fără o descriere formală a capabilităţilor sale şi fără o interfaţă de siguranţă proiectată pentru integrare, se montează în câteva ore şi se integrează în câteva săptămâni.

Modularitatea se manifestă pe trei planuri, care nu decurg unul din altul şi trebuie tratate separat în specificaţie.

Modularitatea fizică: amplasarea, fixarea, racordarea şi reorganizarea echipamentelor şi a traseelor de producţie. Se obţine prin interfeţe mecanice, electrice şi pneumatice standardizate, spaţiu rezervat şi transport segmentat. Este planul cel mai vizibil şi cel mai des inclus în caietele de sarcini.

Modularitatea logică modificarea programelor, serviciilor și regulilor de coordonare fără rescrierea integrală a aplicațiilor. Suport normativ: standardul de programare a PLC-urilor definește unități de organizare cu interfețe explicite (funcții, blocuri funcționale, programe). Logica unei stații se izolează, se testează separat și se instanțiază repetat [123]. Instanțierea este operația-cheie: o stație identică nouă înseamnă o nouă instanță a aceluiași bloc funcțional, cu alte adrese I/O, nu copiere și editare manuală de cod. DCS: blocurile funcționale cu execuție declanșată de evenimente separă aplicația de dispozitive. Funcțiile se redistribuie la reconfigurare fără rescrierea aplicației [124].

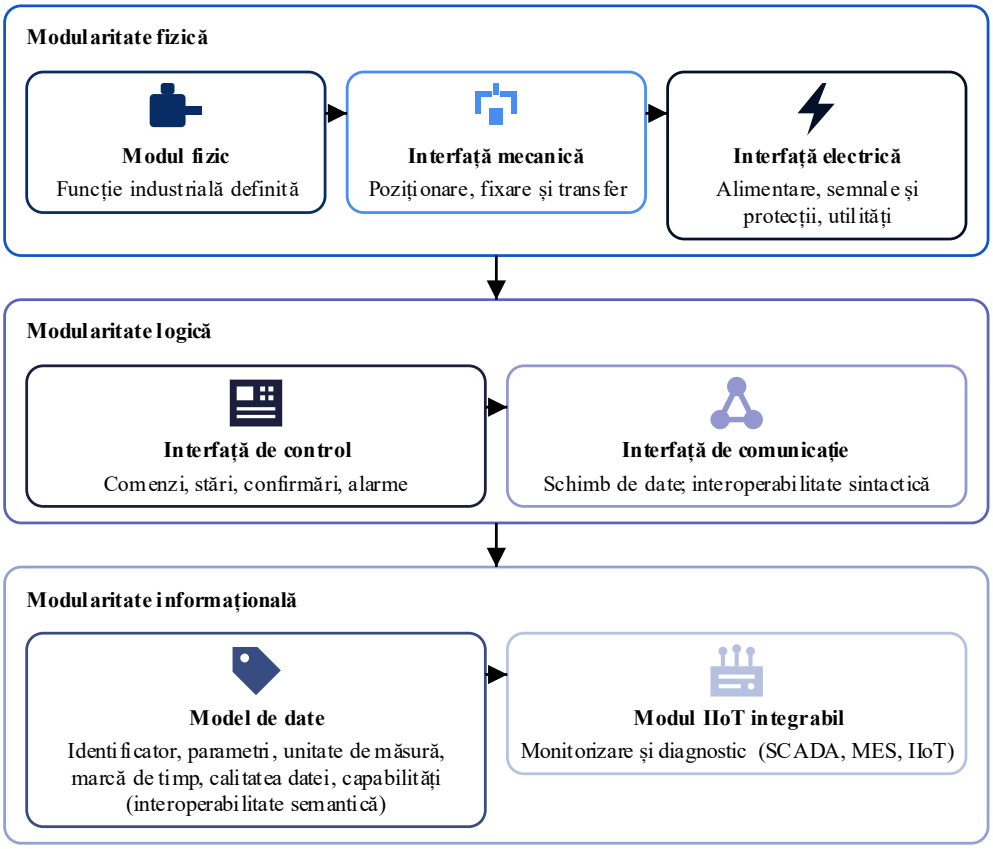
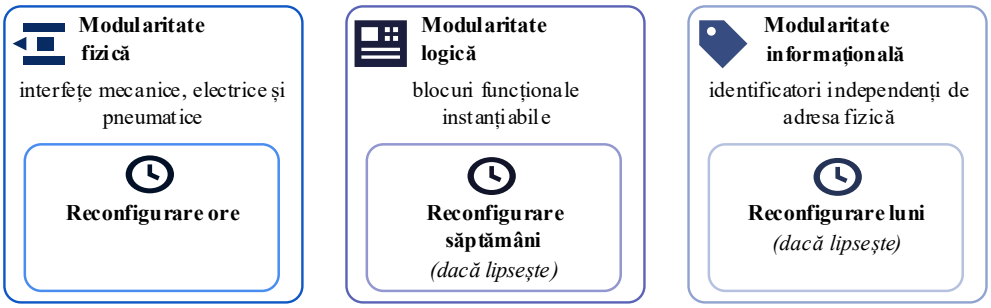


Figura 4.4 – Planurile modularității

Modularitatea informațională privește posibilitatea de a descrie un modul, capabilitățile și starea sa într-o formă independentă de amplasarea și de adresarea fizică. Ea se obține prin identificatori stabili, prin modele de date în care variabilele sunt legate de resursa logică, nu de adresa hardware și prin descrieri standardizate ale activului [120]. Este planul cel mai des omis și cel care determină, în cea mai mare măsură, durata reintegrării unui modul mutat: dacă variabilele sunt adresate

fizic, mutarea unui modul dintr-o poziție în alta impune redenumirea manuală a fiecărei variabile și actualizarea tuturor aplicațiilor care le consumă.

Cele trei planuri se pot afla în stadii diferite de maturitate în același sistem, iar durata totală a unei reconfigurări este dictată de cel mai puțin dezvoltat dintre ele (Figura 4.5). Un sistem cu module mecanice interschimbabile, dar cu un program monolit și cu variabile adresate fizic, se reconfigurează fizic în ore, logic în săptămâni și informațional în luni. Distincția corespunde separării dintre reconfigurarea materială și cea imaterială, tratată explicit în literatura dedicată sistemelor adaptabile [112], [119], iar cuantificarea ei face obiectul secțiunii 4.2.4.



** Durata totală a unei reconfigurări este dictată de planul cel mai puțin dezvoltat .*

Figura 4.5 – Modularitate fizică, logică și informațională

Într-un FMS, modulele susțin utilizarea aceloraşi resurse pentru mai multe produse și trasee tehnologice. Într-un RMS, ele permit modificarea structurii și a capacității sistemului. Adăugarea unei stații identice – situația calculată în secțiunea 4.1.4 – reprezintă scalarea capacității, conectarea unui modul nou de prelucrare sau de control reprezintă extinderea funcționalității, iar a treia operație elementară este înlocuirea unui modul cu altul, echivalent funcțional, dar cu alte caracteristici.

Infrastructura IIoT susține modularitatea prin identificarea componentelor, colectarea datelor locale și comunicarea capabilităților. Plug-and-produce („conectare și producție”): un modul nou este detectat, configurat și înregistrat cu intervenții manuale minime [125]. Condiții: descrieri standardizate ale capabilităților, versiuni software compatibile, reguli clare de acces la date și comenzi. Reprezentarea digitală uniformă a activului industrial asigură descrierea independentă de furnizor [120]. Decalaj laborator–industrie: integrarea necesită aproape întotdeauna o validare neautomatizabilă integral. Presupunerea unei conectări complet automate duce la subestimarea duratei proiectelor.

Modularitatea reduce timpul necesar extinderii și mentenanței, dar nu elimină validarea tehnică [115]. După înlocuirea sau rearanjarea unui modul, trebuie verificate geometria sistemului, precizia, timpul de ciclu, funcțiile de siguranță, comunicațiile și calitatea produsului. Ceea ce modularitatea poate reduce este întinderea acestei validări: dacă efectul modificării rămâne local, verificarea se limitează la

modulul afectat şi la interfeţele sale; dacă efectul se propagă, verificarea trebuie reluată pentru întregul sistem. Aceasta este, în termeni operaţionali, întreaga miză a proprietăţii.

4.2.2. Interoperabilitatea

Interoperabilitatea înseamnă că echipamentele şi aplicaţiile pot schimba date, le înţeleg la fel şi le folosesc împreună pentru o funcţie comună [126]. Ea contează mult în sistemele flexibile şi reconfigurabile, unde componentele vin de la furnizori diferiţi şi sunt instalate la momente diferite. Cu cât sistemul se modifică mai des, cu atât interoperabilitatea devine mai importantă: un sistem care se schimbă rar se poate descurca cu integrări punctuale, unul care se schimbă frecvent nu.

Simpla conectare la aceeaşi reţea nu garantează interoperabilitatea; colaborarea efectivă presupune patru niveluri succesive, definite în cadrele de referinţă pentru integrarea întreprinderii şi în analiza standardelor pentru fabricaţia inteligentă [126], [30].

Nivelul tehnic asigură transmiterea fizică a datelor: medii, conectică, viteze, protocoale de transport compatibile. Absenţa lui se observă imediat, la punerea în funcţiune, şi se remediază la fel de repede.

Nivelul sintactic asigură recunoaşterea structurii: formate, tipuri de date, gramatica mesajelor. Absenţa lui apare la prima integrare software şi impune, de regulă, un convertor.

Nivelul semantic asigură interpretarea unitară a semnificaţiei: ce mărime reprezintă valoarea, în ce unitate, cu ce referinţă temporală, în ce stare de validitate. Absenţa lui este cea mai costisitoare, tocmai pentru că sistemul funcţionează aparent corect: o valoare de temperatură raportată în grade Fahrenheit şi tratată ca grade Celsius circulă fără eroare prin toate nivelurile arhitecturii, este stocată, afişată şi utilizată în decizii, iar diferenţa devine vizibilă abia când cineva o compară cu o măsurătoare independentă.

Nivelul operaţional fixează comportamentul: iniţiator, confirmare, timp de răspuns, tratarea lipsei răspunsului, responsabilitatea acţiunii. Lipsa lui apare în exploatare: două componente corect conectate au aşteptări diferite privind desfăşurarea operaţiei.

Nivelurile se acumulează: fiecare îl presupune pe cel anterior şi niciunul nu îl substituie. Figura 4.6 sintetizează ierarhia împreună cu momentul în care fiecare lipsă devine vizibilă.

Să luăm valoarea „75" transmisă între două sisteme. Ea ajunge la destinaţie (nivel tehnic) şi este recunoscută ca număr întreg într-o structură validă (nivel sintactic). Totuşi, receptorul nu o poate folosi dacă nu ştie ce parametru s-a măsurat, în ce unitate, când, în ce stare era semnalul şi de la ce echipament edge vine. Aici se văd limitele nivelurilor inferioare. Modelele informaţionale industriale rezolvă problema: în OPC UA, spaţiul de adrese însoţeşte valoarea de tipul nodului, atribute, un

cod de calitate şi referinţe către contextul ei [127]. Aşa un şir de numere devine informaţie utilizabilă, temă dezvoltată în secţiunea 6.2.

Standardele şi protocoalele industriale deschise reduc dependenţa de interfeţe proprietare şi facilitează integrarea dintre controlere, roboţi, sisteme SCADA, MES şi platforme IIoT. Alegerea protocolului depinde însă de nivelul arhitectural, de timpul de răspuns, de volumul datelor şi de cerinţele de securitate; criteriile de selecţie sunt analizate în capitolul 6, iar corespondenţa dintre nivelurile funcţionale ale întreprinderii este stabilită normativ şi tratată în capitolul 7 [75], [49].

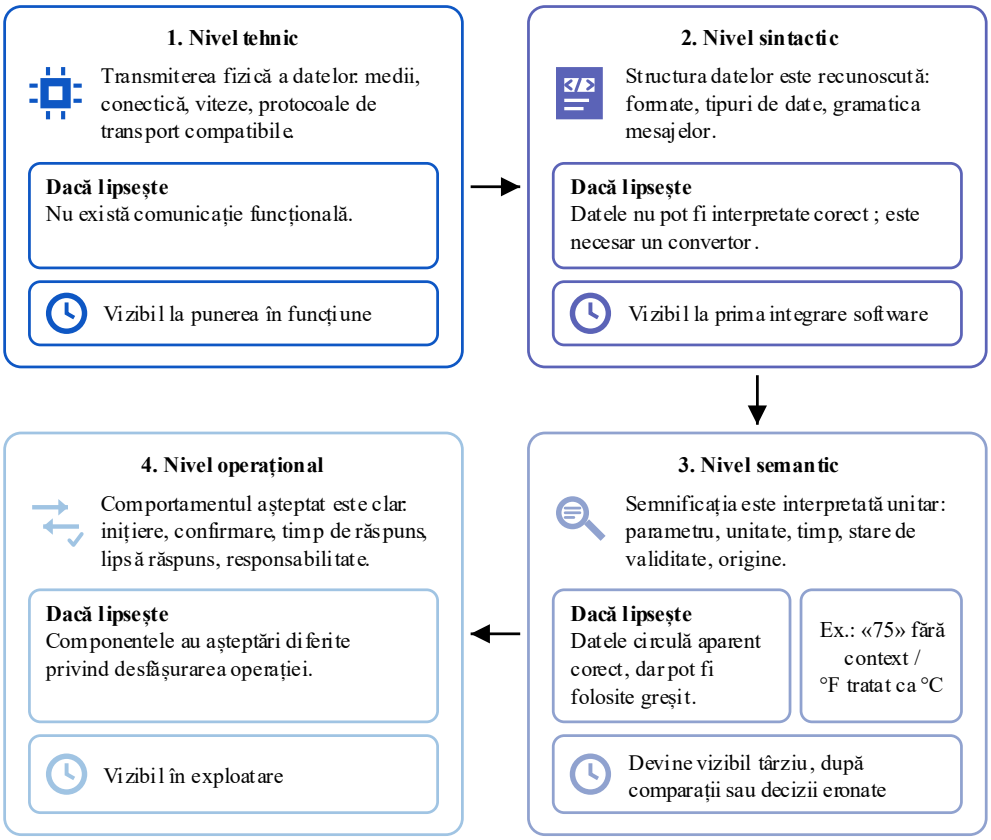


Figura 4.6 – Nivelurile interoperabilității și consecințele absenței fiecăruia

Echipamentele moştenite tehnologic pot fi integrate prin gateway-uri industriale, convertoare şi servere de comunicaţie. Aceste componente transformă datele şi le expun într-o formă utilizabilă de sistemele moderne, fără a modifica funcţiile locale de control. Conversia protocolului nu rezolvă însă automat diferenţele de denumire, de unitate de măsură, de structură sau de semnificaţie. Formulat pe nivelurile de mai sus: un gateway rezolvă nivelurile tehnic şi sintactic, dar nu îl rezolvă pe cel semantic, care rămâne o decizie de proiectare, luată explicit şi documentată într-un model de date comun (Figura 4.7). Aşteptarea contrară – că un echipament

de conversie produce și interoperabilitate semantică – este una dintre erorile frecvente în proiectele de integrare a instalațiilor existente.

Interoperabilitatea trebuie însoțită de mecanisme de autentificare, autorizare și validare. Capacitatea tehnică a unui modul de a transmite o comandă nu înseamnă că acesta trebuie să primească dreptul de a modifica procesul. Accesul se acordă în funcție de rolul componentei, de configurația aprobată și de impactul posibil asupra funcționării, iar delimitarea se realizează prin segmentarea în zone și conducte de comunicație, tratată în capitolul 8 [85], [25]. Într-un sistem reconfigurabil, cerința capătă o dimensiune suplimentară: drepturile de acces trebuie recalculate la fiecare schimbare de configurație, întrucât un modul mutat într-o altă zonă nu păstrează automat justificarea drepturilor pe care le avea.

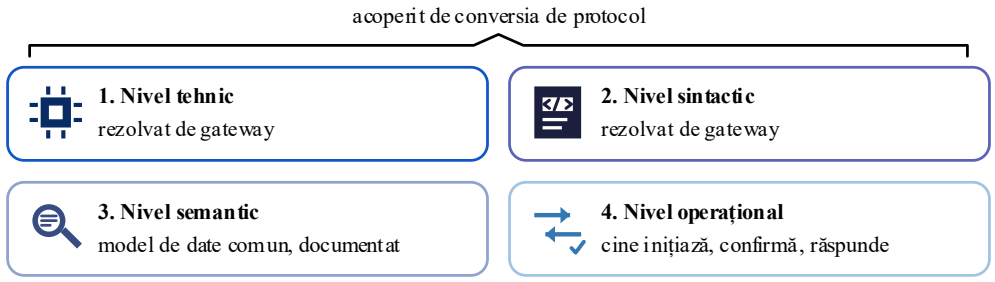


Figura 4.7 – Nivelurile interoperabilității acoperite și neacoperite de conversia de protocol

4.2.3. Adaptabilitatea

Adaptabilitatea reprezintă capacitatea sistemului de fabricație de a-și modifica funcționarea în raport cu schimbarea produsului, a cererii, a resurselor sau a stării echipamentelor. Modificarea poate fi inițiată manual, asistată de sistem sau executată automat, în limitele unei configurații validate. Deosebirea față de reconfigurare este de scară și de reversibilitate: reconfigurarea schimbă structura și presupune revalidare, adaptarea schimbă comportamentul în interiorul unei structuri deja validate – delimitare care corespunde nivelurilor de adaptabilitate descrise în literatura dedicată fabricației transformabile [119].

Formele uzuale de adaptare includ selectarea parametrilor corespunzători produsului identificat, redistribuirea operațiilor către resurse disponibile, ajustarea planului în funcție de progresul real, utilizarea unui traseu alternativ în cazul indisponibilității unei stații, modificarea controlată a vitezei sau a timpilor de proces, programarea unei intervenții pe baza degradării observate și trecerea între modurile de producție, mentenanță și verificare. Toate presupun aceleași două condiții: detectarea fiabilă a schimbării și existența unui domeniu aprobat în interiorul căruia răspunsul este permis.

Infrastructura IIoT furnizează datele necesare identificării schimbării și evaluării răspunsului. Senzorii și controlerele raportează starea procesului, procesarea

edge detectează evenimentele relevante suficient de aproape de sursă pentru ca reacţia să rămână utilă [111], iar MES corelează informaţiile cu produsul, ordinul de producţie şi resursele disponibile. Această colaborare între un nivel fizic care execută şi un nivel informaţional care observă şi corelează este definitorie pentru sistemele ciberfizice de producţie [9]. Relaţia dintre cele trei proprietăţi este sintetizată în Tabelul 4.4.

Un exemplu tipic îl constituie degradarea unei scule: creşterea vibraţiilor unei maşini-unelte poate indica uzura, iar sistemul poate reduce temporar regimul de prelucrare, poate semnala necesitatea înlocuirii şi poate actualiza estimarea duratei operaţiei. Dacă există o resursă echivalentă, comenzile următoare pot fi redistribuite fără oprirea fluxului. Exemplul este instructiv prin lanţul de condiţii pe care îl presupune: o măsurare relevantă, un prag validat, o regulă de decizie, o resursă alternativă declarată echivalentă şi un mecanism de înregistrare a deciziei. Absenţa oricăreia transformă adaptarea într-o alarmă suplimentară, netratată de nimeni.

Adaptarea automată trebuie limitată la un domeniu de funcţionare aprobat. Modificările care afectează siguranţa, calitatea sau parametrii tehnologici critici necesită reguli de validare, înregistrarea deciziei şi, după caz, confirmarea personalului autorizat. Sistemul trebuie să păstreze configuraţia anterioară şi să permită revenirea controlată atunci când rezultatul modificării nu este cel aşteptat. Cerinţa aceasta – existenţa unei căi de întoarcere verificate – este cea mai frecvent omisă în proiectele de digitalizare, deşi este singura care face acceptabilă operaţional o adaptare automată: fără ea, orice modificare automată devine un experiment ireversibil executat în producţie.

Delimitarea faţă de funcţiile de comandă critică rămâne, şi aici, obligatorie. Adaptarea poate modifica parametri de regim, alocări de resurse şi priorităţi, dar nu poate prelua interblocările, oprirea de urgenţă, limitarea mişcărilor şi celelalte funcţii de siguranţă, care se execută local şi independent de disponibilitatea reţelei sau a platformelor de analiză.

Tabelul 4.4 – Relația dintre modularitate, interoperabilitate și adaptabilitate

Proprietate	**Întrebarea principală**	**Cerințe de proiectare**	**Contribuția IIoT**
Modularitate	Cum poate fi modificată structura sistemului?	Module funcționale, interfețe standardizate și gestionarea configurației	Identificarea modulelor, monitorizarea individuală și configurarea controlată
Interoperabilitate	Cum colaborează componentele și aplicațiile?	Compatibilitate tehnică, sintactică, semantică și operațională	Schimb de date contextualizate și integrarea echipamentelor eterogene
Adaptabilitate	Cum răspunde sistemul la schimbare?	Detectarea stării, reguli de decizie, limite validate și posibilitatea revenirii	Monitorizare în timp real, analiză locală și coordonarea răspunsului

Cele trei proprietăţi se aplică împreună. Modular fără interoperabilitate: reorganizare fizică posibilă, dar integrare informaţională refăcută de la zero la fiecare schimbare. Interoperabil fără modularitate: schimb corect de date, dar sistem neextensibil. Modular şi interoperabil fără adaptabilitate: informaţia necesară există, reacţia nu se execută. Adaptabilitatea foloseşte primele două proprietăţi pentru a converti posibilitatea modificării şi disponibilitatea informaţiei într-un răspuns operaţional controlat.

4.2.4. Bugetul de reconfigurare

Justificările economice ale sistemelor reconfigurabile compară, de regulă, costul echipamentelor cu beneficiul flexibilităţii obţinute şi tratează efortul reconfigurării ca pe o mărime secundară. Descompunerea acestui efort arată de ce presupunerea este greşită şi unde trebuie făcută investiţia pentru ca reconfigurarea să rămână o operaţie de rutină. Exemplul care urmează este un scenariu didactic construit pe varianta B din Tabelul 4.3 – adăugarea unei staţii identice la o linie existentă – cu ipotezele declarate integral.

Tabelul 4.5 – Bugetul de reconfigurare pentru adăugarea unei staţii identice

Nr.	Componentă a efortului	Activităţi incluse	Durată (h)	Producţie oprită
1	Pregătire și documentare	Actualizarea planului de amplasare, a schemelor electrice și a listei de semnale; reluarea analizei de risc pentru noua configurație	24	Nu
2	Intervenție mecanică	Amplasarea, alinierea și fixarea modulului, racordarea la sistemul de transport	16	Da
3	Racordare electrică și pneumatică	Alimentare, cablaj de semnal, aer comprimat	10	Da
4	Integrare de comunicație	Adresare în rețea, configurarea nodului, expunerea variabilelor	6	Parțial
5	Modificarea logicii de control	Instanțierea blocului funcțional al stației, extinderea regulii de alocare a traseului	20	Nu
6	Actualizarea modelului de date și a configurației MES	Denumirea variabilelor, declararea resursei noi, actualizarea rutei tehnologice	12	Nu
7	Validare funcțională și de siguranță	Verificarea semnalelor, a interblocărilor, a funcțiilor de oprire, a preciziei și a timpului de ciclu	28	Da
8	Rampă de pornire	Reglaje, stabilizarea calității, atingerea timpului de ciclu proiectat	40	Parțial
	Total		**156**	**54 h cu oprire completă**

Ipoteze. Staţia adăugată este identică din punct de vedere funcţional cu cea existentă. Sistemul a fost proiectat modular pe toate cele trei planuri: interfeţele mecanice, electrice şi de comunicaţie sunt prevăzute, logica staţiei este organizată ca bloc

funcţional care poate fi instanţiat, iar modelul de date declară resursele prin identificatori independenţi de adresa fizică. Producţia funcţionează în două schimburi, cu un ritm nominal de 37,9 buc./h, rezultat din timpul de ciclu de 95 s. Duratele din Tabelul 4.5 sunt estimări de proiect, nu valori măsurate.

Structura efortului. Intervenţia mecanică şi racordarea utilităţilor – componentele 2 şi 3, cele la care se rezumă de obicei discuţia despre modularitate – însumează 26 h, adică 16,7 % din efortul total. Componentele informaţionale şi de validare – 1, 4, 5, 6 şi 7 – însumează 90 h, adică 57,7 %. Rampa de pornire reprezintă 25,6 % (Figura 4.8). Concluzia practică este directă: efortul unei reconfigurări este determinat în proporţie de peste 80 % de elemente care nu au natură mecanică, iar o investiţie în interfeţe mecanice mai bune, neînsoţită de modularitate logică şi informaţională, acţionează asupra celei mai mici componente a bugetului.

Pierderea de producţie. Oprirea completă durează 54 h, ceea ce, la ritmul nominal de 37,9 buc/h, înseamnă 2 046 de bucăţi nerealizate. În timpul rampei de 40 h se presupune un randament mediu de 60 % din cel nominal, ceea ce adaugă 40 × 37,9 × 0,4 ≈ 606 bucăţi. Pierderea totală este de aproximativ 2 650 de bucăţi, adică echivalentul a 70 h de producţie nominală, faţă de 54 h de oprire efectivă. Diferenţa de 16 h este contribuţia rampei, care nu apare în niciun grafic de intervenţie, dar apare integral în rezultatul lunii respective [118].

Efectul lipsei de pregătire. Dacă aceeaşi staţie este adăugată unui sistem neproiectat modular pe planurile logic şi informaţional (program de control monolitic, variabile adresate fizic, absenţa descrierii capabilităţilor şi a autodiagnosticării), patru componente se modifică substanţial: componenta 5 creşte de la 20 h la aproximativ 80 h, deoarece logica se rescrie în loc să fie instanţiată; componenta 6, de la 12 h la 40 h, prin renumirea manuală a variabilelor şi actualizarea rutelor; componenta 7, de la 28 h la 56 h, verificarea configuraţiei făcându-se manual, semnal cu semnal; componenta 8, de la 40 h la 90 h, prin prelungirea rampei. Totalul devine 322 h, de 2,06 ori mai mare, iar pierderea de producţie atinge aproximativ 4 471 de bucăţi, cu 69 % peste cazul pregătit.

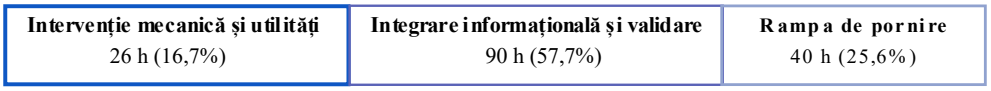


Figura 4.8 – Bugetul de timp al reconfigurării

Interpretare. Raportul dintre cele două scenarii este măsura economică a modularităţii logice şi informaţionale şi a diagnosticabilităţii, caracteristici de proiectare enumerate în secţiunea 4.1.2 şi cel mai des omise din specificaţii. Diferenţa de 166 h şi de aproximativ 1800 de bucăţi se produce la fiecare reconfigurare; dacă sistemul este reconfigurat de două ori pe an, investiţia iniţială în structurarea programului şi a modelului de date se amortizează, de regulă, în interiorul primului an.

Bugetul de reconfigurare oferă astfel criteriul care lipsește din majoritatea justificărilor: nu „*este sistemul modular*?“, ci „*cât durează și cât costă o schimbare, descompus pe componente*”.

Limitele calculului. Duratele sunt estimări pentru cazul de adăugare a unui modul identic, cea mai simplă operație de reconfigurare; înlocuirea unui modul cu altul, neechivalent funcțional, și conversia liniei către o funcționalitate nouă au bugete substanțial mai mari, dominate de componentele 1, 7 și 8. Modelul nu include achiziția și livrarea echipamentului, care se desfășoară în paralel cu producția, nici costul personalului, care depinde de organizarea internă. Randamentul de 60 % în timpul rampei este o ipoteză de lucru derivată din modelele de învățare aplicate rampelor de producție [118]: valoarea reală depinde de complexitatea operației și de experiența anterioară cu module similare, iar în absența unor date istorice proprii ea trebuie considerată optimistă. Bugetul are rolul de a arăta unde se concentrează efortul și unde merită făcută măsurarea, nu de a înlocui măsurarea pe instalația proprie.

Cele trei proprietăți discutate în această secțiune și bugetul care le cuantifică descriu condițiile în care un sistem poate fi modificat. Realizarea lor efectivă presupune însă conectarea echipamentelor, a controlerelor și a sistemelor informatice într-o infrastructură IIoT coerentă, cu date selectate, contextualizate și repartizate pe niveluri – subiectul secțiunii următoare.

4.3. Integrarea echipamentelor în rețele IIoT

Un sistem flexibil sau reconfigurabil își valorifică pe deplin capabilitățile atunci când echipamentele sale sunt integrate în fluxurile informaționale ale fabricii. O celulă robotizată, o mașină-unealtă cu comandă numerică, o stație de inspecție sau un transportor modular pot executa local operații complexe, dar devin noduri IIoT abia atunci când furnizează date interpretabile și pot primi controlat informațiile necesare producției. Această dublă calitate – entitate care execută un proces fizic și, simultan, entitate care participă la un flux informațional – definește sistemele ciber-fizice de producție, în care legătura dintre lumea fizică și serviciile de prelucrare a datelor este permanentă, nu ocazională [9].

Integrarea nu se reduce la conectarea echipamentului la o rețea Ethernet. Ea presupune selectarea datelor relevante, contextualizarea lor, definirea protocoalelor și a modelelor informaționale, protejarea comunicațiilor și delimitarea clară dintre controlul local și funcțiile de monitorizare sau analiză. Dificultățile practice ale acestei etape – cerințele de timp real, coexistența tehnologiilor de comunicație, interoperabilitatea și securitatea – sunt recunoscute în literatura de sinteză drept obstacolele principale ale adoptării industriale, nu detalii de implementare [22].

Într-un FMS, integrarea permite urmărirea pieselor, monitorizarea stațiilor și sincronizarea cu sistemul MES. Într-un RMS, ea susține suplimentar identificarea

modulelor, verificarea compatibilității și validarea configurației active, aspecte tratate în secțiunea 4.1.2. Cu alte cuvinte, într-un sistem care se modifică, infrastructura de date trebuie să descrie nu numai ce face echipamentul, ci și ce echipament este și în ce configurație se află.

4.3.1. Datele furnizate de echipamente

Un echipament integrat trebuie să ofere informații despre starea, activitatea și rezultatul său. Ele se împart în opt categorii: disponibilitate, mod de funcționare și alarme; produs, lot, comandă și operație executată; program, rețetă și parametri folosiți; timp de ciclu și cantități realizate; rezultate ale verificărilor de calitate; ore de funcționare și indicatori de degradare; consum de energie și utilități; configurație și versiuni ale componentelor active. Ultima categorie ține de RMS și lipsește de obicei din specificațiile pentru liniile fixe. Tabelul 4.6 grupează aceste date după utilizatorul principal și decizia pe care o susțin.

Tabelul 4.6 – Date furnizate de o celulă flexibilă într-o rețea IIoT

Categorie	Exemple	Utilizator principal	Decizie susținută
Stare	Disponibilă, ocupată, oprită sau în alarmă	Operator, SCADA	Intervenția operațională imediată
Producție	Comandă, lot, operație, cantitate, timp de ciclu	MES, planificare	Urmărirea execuției și identificarea stației limitative
Calitate	Măsurători, rezultat, codul neconformității	Responsabilul cu asigurarea calității	Analiza și tratarea neconformității
Mentenanță	Ore de funcționare, cicluri, vibrații, erori repetitive	Echipa de mentenanță	Planificarea intervenției
Energie	Consum electric, aer comprimat, vid	Responsabilul cu managementul energetic	Optimizarea consumurilor și identificarea pierderilor
Configurație	Modul, program, rețetă, parametri, versiuni	Inginerul de automatizări, MES	Validarea schimbării produsului sau a configurației
Siguranță	Oprire de urgență, acces nepermis, zonă ocupată	Operator, responsabilul cu siguranța	Oprirea și controlul accesului

O valoare izolată nu este utilizabilă industrial; ea trebuie asociată cel puțin sursei, mărcii temporale, unității de măsură, stării semnalului și contextului operațional. O temperatură devine relevantă numai dacă sunt cunoscute echipamentul și zona măsurată, momentul înregistrării, produsul procesat și limitele admise. Modelele informaționale industriale tratează explicit această cerință, așa cum s-a arătat în secțiunea 4.2.2 [127]; ceea ce interesează aici este consecința ei asupra proiectării: contextul se decide odată cu punctul de măsurare, nu ulterior, în platforma de analiză.

Nu toate semnalele disponibile în controler trebuie transmise către nivelurile superioare. Datele utilizate exclusiv pentru executarea secvențelor locale – stările intermediare ale unei secvențe, bistabilii interni, temporizatoarele de proces –

rămân la nivelul echipamentului. Stările agregate, alarmele, contoarele, rezultatele și indicatorii necesari unei decizii pot fi transmiși către SCADA, MES sau către platformele de analiză. Transmiterea nediferențiată a întregii memorii a automatului programabil produce volume mari de date fără destinatar, îngreunează identificarea informației utile, mărește costul stocării și extinde inutil suprafața de expunere a sistemului [111].

Selecția pornește de la utilizarea informației, nu de la disponibilitatea ei. Operator: stări și alarme imediate. MES: comenzi, operații, rezultate. Asigurarea calității: măsurători și neconformități. Mentenanță: indicatori de degradare. Pentru indicatorii de performanță, definițiile se preiau dintr-o referință comună, care fixează setul de indicatori și modul de compunere, evitând calculul diferit al aceleiași mărimi în două aplicații [51]. Eficacitatea globală a echipamentelor (cel mai utilizat indicator) este tratată în secțiunea 7.2.3. Date necesare: timp planificat, opriri clasificate, cantități conforme, timp de ciclu de referință, toate din categoriile enumerate. Lipsa oricăreia face indicatorul necalculabil.

4.3.2. Integrarea unei celule robotizate

O celulă robotizată poate include robotul și controlerul acestuia, un PLC, dispozitivul de prindere, senzorii, sistemul de siguranță, transportorul, dispozitivele de fixare, interfața om–mașină și, după caz, un sistem de vedere artificială. La nivel local, aceste componente execută și verifică operația; prin integrare, celula devine o resursă vizibilă și gestionabilă în fluxul informațional al fabricii.

Datele pe care o celulă integrată le poate furniza acoperă starea generală (*disponibilă*, *ocupată*, *oprită* sau *în alarmă*), modul de funcționare și programul activ, produsul sau comanda aflată în lucru, starea dispozitivului de prindere și confirmarea prezenței piesei, numărul ciclurilor și timpul de execuție, alarmele, opririle și erorile repetitive, rezultatele inspecției și ale operației, precum și orele de funcționare și indicatorii necesari mentenanței.

Starea coerentă a celulei este o decizie de proiectare, nu un efect al conectării. Dacă robotul, sistemul de vedere și transportorul raportează separat, aplicația receptoare reconstituie starea, iar rezultatul depinde de ordinea mesajelor (absența nivelului operațional al interoperabilității [30]). Aceleași mesaje pot da concluzii diferite despre disponibilitate în două aplicații. Soluție: PLC-ul agregă semnalele și expune o stare unică, definită explicit, alături de stările componentelor. SCADA: stări, alarme, tendințe. MES: corelare operație – ordin de producție – produs – rezultat. Date istorice: grad de utilizare, timpi de ciclu, cauze ale opririlor.

Schimbul de informații este bidirecțional; în sens descendent pot fi transmise ordinul de producție, identificatorul produsului, programul aprobat, parametrii și criteriile de verificare. În sens ascendent sunt raportate starea operației, cantitățile, timpul de ciclu, rezultatul, alarmele și consumurile. Asimetria dintre cele două sensuri, reprezentate în Figura 4.9, este esențială: fluxul ascendent poate fi întrerupt

fără consecinţe imediate asupra procesului, în timp ce fluxul descendent modifică comportamentul celulei şi trebuie tratat cu regulile aplicabile comenzilor.

Comenzile primite din exterior se validează, prin urmare, înaintea aplicării. Identificarea produsului nu trebuie să determine automat selectarea unui program dacă versiunea programului, dispozitivul de prindere montat, materialul sau configuraţia celulei nu sunt confirmate. Regula practică este că o comandă externă poate selecta dintre alternative deja validate, dar nu poate crea o alternativă nouă. Modificările cu impact asupra siguranţei sau asupra parametrilor tehnologici critici necesită mecanisme suplimentare de autorizare şi de înregistrare a deciziei.

Funcţiile de siguranţă nu depind de infrastructura IIoT. Oprirea de urgenţă, monitorizarea accesului, limitarea vitezei şi a spaţiului de lucru sunt asigurate de sisteme locale dedicate, proiectate şi validate ca funcţii de siguranţă. Integrarea lor la nivelul celulei este responsabilitatea integratorului de sistem, conform cerinţelor pentru aplicaţiile robotizate şi celulele de lucru [128]. Ediţia actuală a cerinţelor include şi securitatea cibernetică, deci siguranţa şi securitatea se tratează împreună în celulele conectate. Dacă se pierde conexiunea cu SCADA, MES sau platforma externă, celula trebuie să poată trece într-o stare sigură, iar pierderea conexiunii nu trebuie să fie ea însăşi un eveniment de siguranţă.

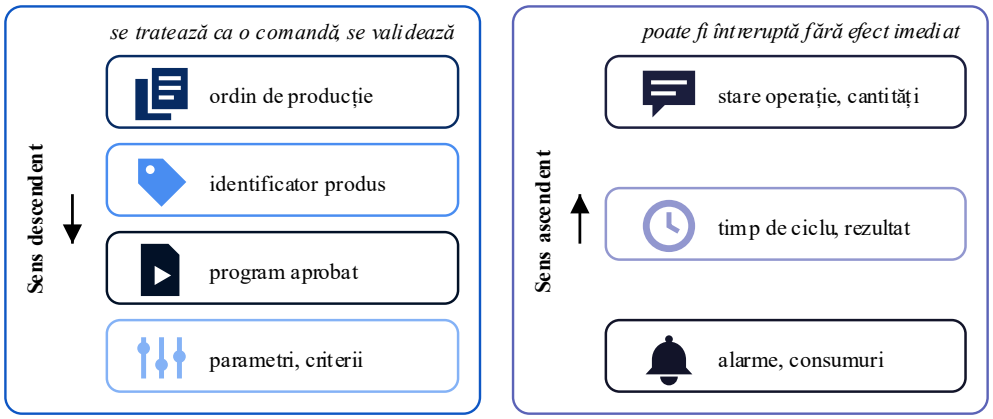


Figura 4.9 – Fluxul bidirecțional de date

Într-un sistem reconfigurabil, integrarea celulei include o obligaţie suplimentară: raportarea configuraţiei proprii. Dispozitivul de prindere montat, versiunea programului, sculele active şi parametrii încărcaţi trebuie să fie citibili din exterior, întrucât ei condiţionează validitatea oricărei comenzi primite. O celulă care raportează stări şi cantităţi, dar nu raportează configuraţia, poate executa corect un program greşit fără ca sistemul să dispună de vreun mijloc de a observa acest lucru.

4.3.3. Distribuirea funcțiilor în arhitectură

Integrarea trebuie să distribuie funcţiile în raport cu trei criterii: timpul de răspuns admis, volumul datelor şi consecinţele unei întreruperi. Cele trei nu conduc întotdeauna la aceeaşi soluţie, iar arbitrajul dintre ele constituie decizia arhitecturală centrală a oricărui proiect IIoT. Criteriile sunt reprezentate în Figura 4.10, iar repartizarea rezultată a funcţiilor, în Figura 4.11.

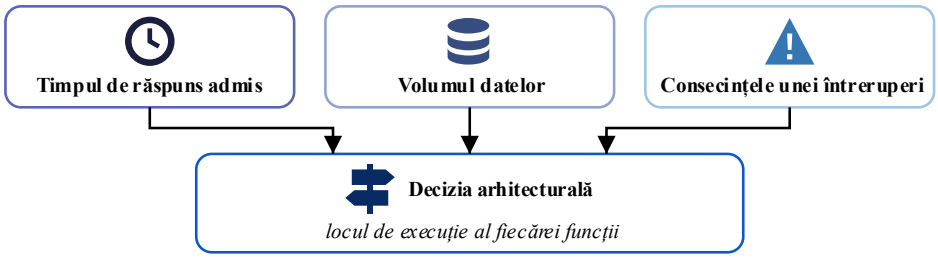


Figura 4.10 – Criteriile deciziei arhitecturale

La nivelul echipamentului se realizează achiziţia semnalelor, execuţia comenzilor, interblocările şi controlul procesului. PLC-ul, controlerul robotului sau controlerul maşinii-unelte trebuie să poată menţine funcţionarea locală şi trecerea în stare sigură chiar dacă legătura cu sistemele superioare este indisponibilă. Criteriul de repartizare este aici lipsit de ambiguitate: orice funcţie a cărei întârziere sau indisponibilitate poate produce daune se execută local.

La nivelul edge se realizează conversia protocoalelor, filtrarea, agregarea, detectarea evenimentelor şi stocarea temporară. Argumentele pentru prelucrarea aproape de sursă sunt aceleaşi în industrie ca în alte domenii (timpul de răspuns, reducerea volumului transmis, păstrarea datelor în perimetrul controlat) [111], dar au aici o consecinţă specifică: gateway-ul industrial poate păstra datele pe durata întreruperii conexiunii şi le poate transmite ulterior fără pierderea ordinii temporale, condiţie a validităţii oricărei analize ulterioare a succesiunii evenimentelor. Amplasarea la nivel edge nu conferă însă comportament determinist: sistemele de operare de uz general şi mediile de execuţie interpretate introduc o variabilitate fără limită superioară, de aceea funcţiile cu cerinţe temporale stricte rămân în controlere, aspect dezvoltat în secţiunea 5.4.

Sistemul SCADA asigură supravegherea procesului, gestionarea alarmelor şi păstrarea istoricului operaţional. MES adaugă contextul producţiei prin asocierea datelor cu ordinul, lotul, operaţia, resursa şi rezultatul. ERP utilizează informaţii agregate privind progresul, consumurile şi disponibilitatea resurselor. Delimitarea responsabilităţilor dintre aceste niveluri nu este arbitrară: modelul funcţional stabilit normativ defineşte ce categorii de informaţii circulă între managementul operaţiunilor de producţie şi sistemele de planificare a întreprinderii [75], [49], iar respectarea acestei delimitări previne situaţia frecventă în care aceeaşi funcţie este implementată de două ori, cu rezultate care diferă.

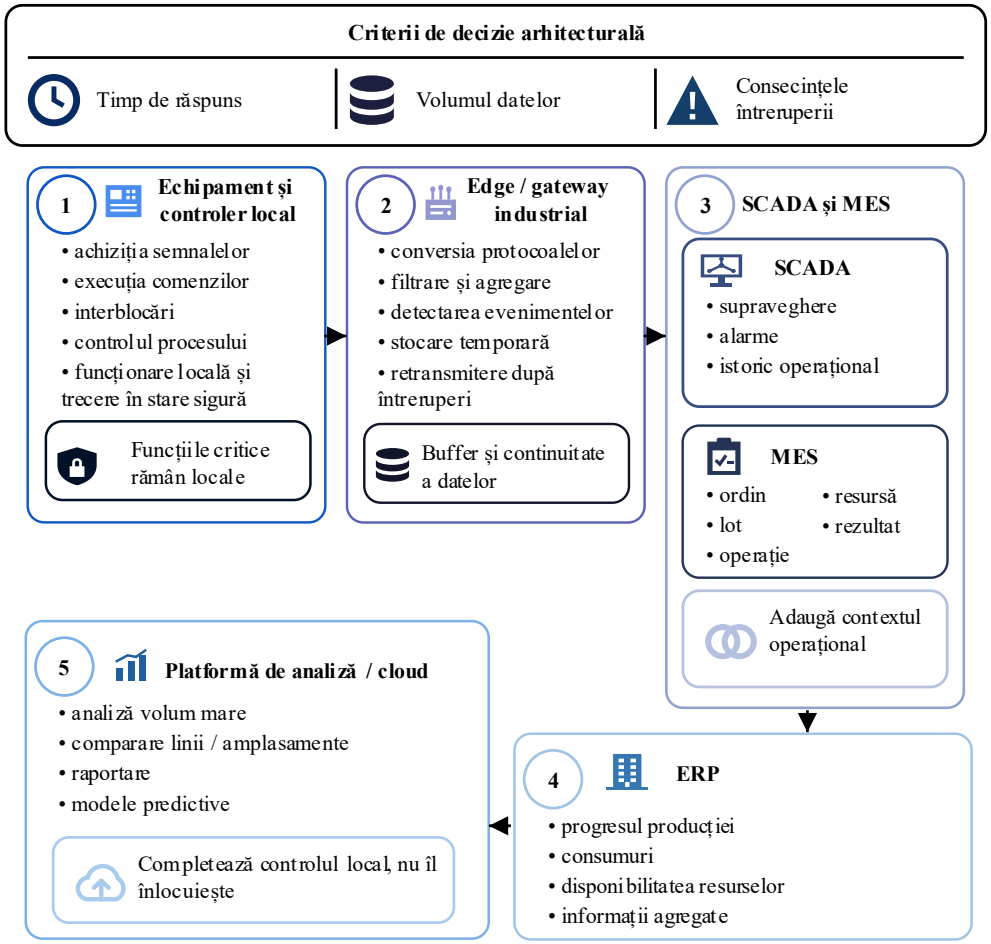


Figura 4.11 – Distribuirea funcțiilor în arhitectura IIoT

Platformele centralizate şi serviciile cloud pot fi utilizate pentru analiza unor volume mari de date, compararea mai multor linii sau amplasamente, raportare şi dezvoltarea modelelor predictive. Aceste funcţii completează controlul local, fără să îl înlocuiască. Formularea nu este o precauţie retorică: ghidurile de securitate pentru tehnologia operaţională tratează disponibilitatea locală a controlului ca pe o cerinţă de proiectare, nu ca pe o măsură de rezervă [25].

Traseul trebuie adaptat aplicaţiei. Unele echipamente pot comunica direct cu SCADA, iar datele altora pot fi preluate printr-un server OPC UA sau printr-un convertor de protocol. Esenţială este menţinerea originii şi a semnificaţiei datelor pe întregul flux: fiecare transformare intermediară – agregare, conversie de unităţi, schimbare de denumire, rotunjire – trebuie documentată, altfel valoarea care ajunge în platforma de analiză nu mai poate fi raportată la măsurarea iniţială, iar o eventuală neconcordanţă devine imposibil de localizat.

Traseul tipic al datelor este ilustrat în Figura 4.12.

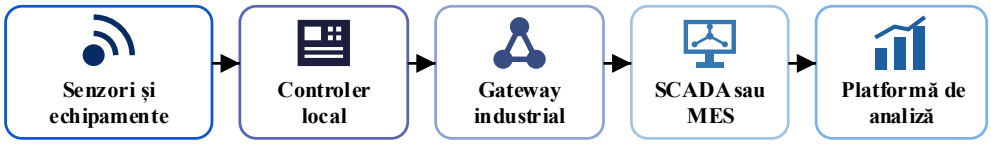


Figura 4.12 – Traseul tipic al datelor

4.3.4. Proiectarea şi validarea integrării

Integrarea trebuie începută prin definirea problemei operaţionale, nu prin conectarea nediferenţiată a tuturor echipamentelor. Pentru fiecare categorie de date se completează o fişă de specificaţie cu elementele din Tabelul 4.7, înainte de orice intervenţie tehnică.

Tabelul 4.7 – Fișa de specificație a unei categorii de date

Element	**Întrebarea la care răspunde**	**Exemplu pentru „timp de ciclu al stației”**
Sursa și semnificația	De unde provine valoarea și ce reprezintă exact?	PLC-ul stației; durata dintre confirmarea prezenței piesei și confirmarea evacuării
Frecvența și declanșarea	Cât de des se transmite și la ce eveniment?	O valoare la fiecare ciclu încheiat, nu la interval fix
Destinatarul	Cine utilizează informația?	MES și responsabilul de linie
Decizia susținută	Ce decizie se ia altfel dacă valoarea lipsește?	Identificarea stației care limitează debitul liniei
Perioada de păstrare	Cât timp rămâne utilă?	24 de luni, pentru comparații între configurații
Comportamentul la pierderea comunicației	Ce se întâmplă dacă legătura cade?	Memorare locală și retransmitere în ordine, fără pierderea mărcii temporale
Drepturile de acces	Cine citește și cine scrie?	Citire pentru MES și SCADA; fără drept de scriere
Cerințele de securitate și jurnalizare	Ce se protejează și ce se înregistrează?	Canal autentificat; jurnalizarea modificărilor de configurație a punctului

Dintre aceste elemente, „decizia susţinută” este criteriul care elimină cel mai mult efort inutil. O categorie de date pentru care nu poate fi numită decizia pe care o influenţează nu justifică infrastructura necesară colectării, transmiterii şi păstrării ei. Aplicarea consecventă a acestui criteriu reduce, în proiectele reale, numărul punctelor de colectare propuse iniţial, fără pierdere de informaţie utilă.

Implementarea graduală poate începe cu o singură celulă şi cu un număr restrâns de stări, alarme şi indicatori. Se verifică achiziţia, interpretarea, marca temporală, stocarea şi utilizarea informaţiei într-o decizie concretă. Extinderea către alte echipamente se realizează după validarea modelului de date şi a beneficiului operaţional, nu în paralel cu ea.

Integrarea poate fi afectată de transmiterea unor volume inutile de date, de denumirea neuniformă a variabilelor, de unităţi de măsură incompatibile, de lipsa sincronizării temporale între surse şi de propagarea unor valori incorecte. Într-un RMS se adaugă o categorie proprie de riscuri: identitatea modulelor, versiunile

programelor, parametrii încărcați și configurația activă. Abaterea dintre configurația fizică și cea înregistrată este una dintre cauzele frecvente ale rezultatelor neexplicabile după o reconfigurare, iar detectarea ei presupune ca sistemul să compare periodic configurația raportată de module cu cea aprobată – funcție care corespunde caracteristicii de diagnosticabilitate discutate în secțiunea 4.1.2 și care este cuantificată, prin efectele sale, în Tabelul 4.5.

Conectarea echipamentelor mărește suprafața de atac a sistemului de producție. Rețelele trebuie segmentate în zone și conducte de comunicație, accesul se acordă în funcție de rol, comunicațiile se monitorizează, iar comenzile cu impact asupra procesului se jurnalizează și se validează. Abordarea este formalizată de seria de standarde dedicate securității sistemelor de automatizare și control industrial, iar recomandările specifice tehnologiilor operaționale sunt detaliate în ghidul dedicat [25], [68]. Măsurile sunt dezvoltate în capitolul 8. Într-un sistem reconfigurabil, cerința are din nou o formă particulară: fiecare modificare de configurație schimbă topologia rețelei și repartizarea pe zone, iar analiza de risc trebuie reluată odată cu reconfigurarea, nu doar la punerea inițială în funcțiune.

Prin integrarea IIoT, flexibilitatea locală este extinsă către coordonarea digitală a fabricii: echipamentele devin resurse monitorizabile și gestionabile, iar datele lor susțin planificarea, calitatea, mentenanța și reconfigurarea. Aplicarea concretă a acestor principii, de la selecția semnalelor până la validarea comportamentului la abateri, este ilustrată în secțiunea următoare prin simularea unui sistem flexibil controlat prin automat programabil.

4.4. Exercițiu aplicativ – Simularea unui sistem flexibil de fabricație într-un mediu tridimensional cu control prin PLC

Exercițiul aplică principiile capitolului prin simularea unei linii flexibile de fabricație. Se utilizează un simulator tridimensional al procesului și un mediu de inginerie pentru programarea automatului programabil, legate printr-un canal de schimb de semnale. Exercițiul este declarat agnostic față de produs: poate fi realizat cu orice combinație de simulator și mediu de programare care permite maparea semnalelor modelului virtual pe intrările și ieșirile controlerului, iar rezultatele așteptate nu depind de furnizor. Concretizarea integrală pe o stivă tehnologică nominalizată face obiectul exercițiilor din secțiunile 5.7 și 7.5.

Scopul nu este reproducerea unei instalații industriale, ci proiectarea, programarea și verificarea unei logici de control capabile să gestioneze mai multe variante de produs, să modifice traseul pieselor și să reacționeze controlat la abateri. Valorile numerice de mai jos sunt propuse pentru ca exercițiul să fie reproductibil și verificabil; ele pot fi modificate, cu condiția recalculării temporizărilor și a criteriilor de reușită.

4.4.1. Scenariul de fabricație și dimensionarea modelului

Sistemul simulat realizează transportul, identificarea, procesarea și sortarea a două variante de produs. Configurația minimă cuprinde o stație pentru introducerea pieselor, un transportor principal, senzori pentru detectarea poziției și pentru identificarea tipului de produs, o stație simulată de prelucrare sau verificare, un mecanism de deviere acționat electric ori pneumatic, două zone de evacuare, dispozitive pentru pornire, oprire și resetare, precum și semnalizarea stării și a alarmelor. Produsele de tip A urmează traseul principal, iar produsele de tip B sunt direcționate către traseul alternativ.

Geometria și regimul propuse pentru model sunt următoarele: viteza transportorului principal 0,15 m/s; distanța de la punctul de introducere la senzorul de identificare 0,45 m; de la senzorul de identificare la stația de procesare 0,90 m; de la stație la deviator 0,60 m; de la deviator la zonele de evacuare 0,50 m; timpul de comutare a deviatorului 0,8 s; intervalul minim de introducere a pieselor, adică tactul impus, 12 s.

Durate nominale de deplasare: 3,0 s, 6,0 s, 4,0 s, respectiv 3,3 s. Ele stau la baza pragurilor de supraveghere a timpului. Regulă: timp maxim admis per tranziție = 2 × durata nominală, minimum 3 s. Evită alarmele false la funcționare normală (prag prea strâns) și blocajele nedetectate un ciclu întreg (prag prea larg).Două verificări de dimensionare trebuie efectuate înaintea programării, întrucât ele pot invalida scenariul.

Verificarea stației limitative. Ocuparea stației este egală cu timpul de procesare plus 1,0 s pentru oprirea și repornirea transportorului, adică 5,0 s pentru produsul A și 8,0 s pentru produsul B. Ambele valori sunt inferioare tactului de 12 s, iar cazul cel mai defavorabil – o succesiune de produse B – lasă o rezervă de 4,0 s, adică 33 %. Stația nu limitează, prin urmare, debitul liniei, iar identificarea resursei limitative precedă orice dimensionare a fluxului [76]; dacă timpul de procesare al produsului B ar fi fost de 12 s, tactul impus nu ar mai fi putut fi respectat, iar exercițiul ar fi trebuit reconstruit.

Verificarea numărului de piese aflate simultan pe linie. Durata totală de tranzit este de 3,0 + 6,0 + 4,0 + 4,0 + 3,3 = 20,3 s pentru produsul A și de 23,3 s pentru produsul B. Cum tranzitul depășește tactul, pe transportor se află simultan până la două piese, valoare obținută din tranzitul fără oprire; oprirea periodică a transportorului comun (secțiunea 4.4.3) poate permite local și o a treia piesă, motiv pentru care numărul maxim de piese se confirmă prin simulare. Consecința asupra programului este directă și frecvent omisă: logica nu poate fi scrisă ca o secvență liniară care tratează o singură piesă de la intrare până la evacuare, ci trebuie să urmărească fiecare piesă separat, prin asocierea rețetei cu poziția ei în flux. Este exact deosebirea dintre un program de laborator și unul utilizabil.

Debitul teoretic. La tactul de 12 s rezultă 300 buc/h. Într-un schimb de 8 h cu 30 de minute de pauze planificate, adică 7,5 h de producție planificată, debitul teoretic

este de 2 250 de bucăți. Valoarea servește ca referință pentru evaluarea rezultatelor în secțiunea 4.4.5. Rețetele celor două produse sunt prezentate în Tabelul 4.8.

Tabelul 4.8 – Rețetele de produs utilizate în model

Parametru	**Rețeta A**	**Rețeta B**
Cod produs	P-A	P-B
Criteriu de identificare	Senzor de identificare inactiv	Senzor de identificare activ
Timp de procesare în stație	4,0 s	7,0 s
Poziția deviatorului	Retras	Extins
Destinație	Zona de evacuare 1 (traseu principal)	Zona de evacuare 2 (traseu deviat)
Timp maxim admis în stație	8,0 s	14,0 s
Contor asociat	Contor_tip_A	Contor_tip_B

Un sistem este flexibil atunci când poate prelucra pe rând produse diferite, își alege singur traseul și își schimbă parametrii dintr-o configurație. Mai trebuie să urmărească separat cantitățile realizate, să izoleze o zonă blocată și să reia controlat funcționarea după remedierea erorii.

Rețeta este structura care face sistemul flexibil în sens propriu. Dacă timpii de procesare, destinațiile și pragurile sunt înscrise direct în logica secvenței, introducerea unei a treia variante impune modificarea programului. Dacă sunt păstrate într-o structură de date indexată după codul produsului, aceeași secvență deservește oricâte variante, iar modificarea se reduce la completarea unui rând. Aceasta este, la scara unui exercițiu, aplicarea directă a modularității logice și informaționale discutate în secțiunea 4.2.1: efectul unei schimbări rămâne local, în date, în loc să se propage în logică.

4.4.2. Configurarea modelului și a semnalelor

În simulator se amplasează componentele și se verifică individual comportamentul senzorilor și al elementelor de execuție. Fiecărui semnal îi este asociată o variabilă simbolică în programul automatului programabil. Adresele fizice sau virtuale trebuie separate de logica funcțională, astfel încât modificarea unei conexiuni să nu impună restructurarea programului – cerință care corespunde, la nivelul aplicației, principiului de decuplare a interfețelor formulat în secțiunea 4.2.1 și organizării programelor pe unități cu interfețe declarate explicit [123].

Categoria „Confirmare” merită o observație separată, întrucât lipsa ei este cauza celor mai multe erori din exercițiile de acest tip. Comanda deviatorului și poziția efectivă a acestuia sunt mărimi distincte: prima exprimă intenția programului, a doua exprimă starea procesului. Un program care presupune că deviatorul se află în poziția comandată, fără să o confirme, funcționează corect în simulare și eșuează la prima situație de blocaj mecanic. Aceeași distincție se aplică între comanda stației și confirmarea încheierii ciclului.

După configurarea variabilelor se stabileşte comunicaţia dintre simulator şi controler. Înaintea programării ciclului automat se verifică separat transmiterea fiecărei intrări şi aplicarea fiecărei ieşiri. Inversarea unui semnal, asocierea greşită a unei adrese sau menţinerea necontrolată a unei comenzi produc un comportament dificil de diagnosticat după integrarea întregii secvenţe, iar timpul economisit prin omiterea acestei verificări se pierde, de regulă, înmulţit. Semnalele utilizate sunt grupate în Tabelul 4.9.

Tabelul 4.9 – Semnalele utilizate în simularea sistemului flexibil

Categorie	Variabile	Tip	Rol
Comenzi	Pornire, Oprire, Resetare	Boolean	Controlul general al sistemului
Detectare	Senzor_intrare, Senzor_identificare, Senzor_statie, Senzor_evacuare_1, Senzor_evacuare_2	Boolean	Urmărirea poziției și identificarea produsului
Acționare	Transportor_principal, Statie_procesare, Deviator	Boolean	Transportul, procesarea și direcționarea pieselor
Confirmare	Deviator_pozitie_retras, Deviator_pozitie_extins, Statie_ciclu_incheiat	Boolean	Confirmarea execuției, distinctă de comandă
Stare	Sistem_pregatit, Sistem_activ, Ciclu_finalizat	Boolean	Monitorizarea desfășurării procesului
Diagnosticare	Blocaj, Timp_depasit, Eroare_senzor, Zona_afectata, Cod_cauza	Boolean, întreg	Detectarea abaterilor și inițierea reacției
Producție	Contor_tip_A, Contor_tip_B, Contor_neconforme, Durata_ciclu	Întreg, timp	Evidența rezultatelor procesului
Configurație	Reteta_activa, Timp_procesare, Destinatie_produs	Întreg, timp	Adaptarea comportamentului la varianta fabricată

4.4.3. Programarea secvenţei de control şi interblocările

Logica se organizează sub forma unor stări ale echipamentului; fiecare stare are o condiţie de intrare confirmată, o acţiune, o condiţie de ieşire şi un timp maxim admis, la depăşirea căruia sistemul trece în starea de eroare. Trecerea dintre stări se realizează pe baza unor condiţii confirmate, nu prin temporizare: comanda transportorului se opreşte atunci când piesa ajunge la staţie, iar operaţia începe numai după confirmarea poziţiei acesteia. Temporizatoarele simulează durata procesului şi detectează depăşirea timpului admis; ele nu înlocuiesc confirmarea.

Peste stările maşinii se suprapun patru interblocări care trebuie implementate independent de secvenţă şi verificate în orice stare. Prima interzice comanda transportorului atunci când staţia de procesare este activă, împiedicând deplasarea piesei în timpul operaţiei. A doua interzice comutarea deviatorului atâta timp cât o piesă se află în dreptul lui, condiţie dedusă din senzorul de poziţie şi din temporizarea tranzitului. A treia interzice introducerea unei piese noi dacă zona de intrare nu este liberă sau dacă sistemul se află în starea 9. A patra interzice pornirea din starea 0 dacă vreun senzor de evacuare este activ, situaţie care indică o piesă rămasă din ciclul anterior.

Interblocările nu sunt condiții de tranziție, ci condiții permanente de validare a ieşirilor; confuzia dintre cele două este cauza obişnuită a comportamentelor imprevizibile în modurile manual şi de reglaj.

Programul se împarte în blocuri funcţionale pentru comanda transportorului, identificarea produsului, controlul staţiei, sortare, diagnosticare şi numărare. Organizarea permite verificarea separată a modulelor şi facilitează introducerea ulterioară a unei staţii sau a unei variante suplimentare. Blocul de diagnosticare merită tratat ca funcţie de sine stătătoare, nu ca o colecţie de condiţii dispersate în secvenţă: el primeşte starea curentă, temporizatorul asociat şi pragul din reţetă şi returnează indicatorul de eroare împreună cu zona şi codul cauzei. Această separare este ceea ce permite ulterior transmiterea unei alarme interpretabile către nivelurile superioare, în locul unui simplu bit de defect.

Tabelul 4.10 – Structura mașinii de stări a ciclului automat

Nr.	Stare	Condiție de intrare	Acțiune	Condiție de ieșire	Timp maxim admis
0	Inițializare	Pornire activă, fără alarme, senzori în stare coerentă	Se șterg comenzile, se validează rețeta activă	Sistem_pregatit	5 s
1	Așteptare piesă	Sistem_pregatit	Transportor pornit, alimentare permisă	Senzor_intrare activ	—
2	Identificare	Senzor_intrare a trecut din activ în inactiv	Se citește senzorul de identificare, se încarcă rețeta	Reteta_activa validată	6 s
3	Transport la stație	Rețetă validată	Transportor pornit	Senzor_statie activ	12 s
4	Procesare	Senzor_statie activ și piesă oprită	Transportor oprit, stație activă, temporizator încărcat din rețetă	Statie_ciclu_incheiat	8 s (A) / 14 s (B)
5	Selectare traseu	Operație confirmată	Se comandă deviatorul conform rețetei	Confirmarea poziției corespunzătoare	3 s
6	Evacuare	Deviator confirmat în poziție	Transportor pornit	Senzorul zonei de evacuare corecte activ	15 s
7	Actualizare contoare	Evacuare confirmată	Incrementarea contorului asociat rețetei, înregistrarea duratei de ciclu	Contor actualizat	—
8	Pregătire ciclu următor	Contor actualizat	Se eliberează zona, se resetează temporizatoarele	Zonă liberă	3 s
9	Eroare	Depășirea timpului maxim admis sau semnale incoerente, în oricare dintre stările 0–8	Se oprește zona afectată, se blochează alimentarea, se generează alarma cu zona și codul cauzei	Cauza îndepărtată, semnale coerente și confirmarea operatorului	— (ieșire numai prin confirmare)

Secvența din Tabelul 4.10 descrie parcursul unei singure piese. Deoarece pe linie se pot afla simultan două piese, blocul de control păstrează câte o instanță a stării și a rețetei pentru fiecare piesă aflată între intrare și evacuare. Transportorul fiind comun, oprirea lui pe durata procesării prelungește tranzitul celeilalte piese; temporizatoarele de tranzit se suspendă, prin urmare, cât timp transportorul este oprit, altfel timpii maximi din tabel ar fi depășiți fără să existe un blocaj.

Starea 9 nu are condiție de ieșire prin temporizare, ci exclusiv prin confirmarea condițiilor de repornire. Distincția este esențială: o alarmă care se stinge singură după un interval ascunde cauza în loc să o semnaleze, iar sistemul revine în producție într-o stare nevalidată. Regula corespunzătoare, formulată în secțiunea 4.2.3, este că orice adaptare automată presupune o cale de revenire verificată; aici, revenirea este condiționată de îndepărtarea piesei blocate și de coerența semnalelor.

Când se detectează un blocaj, controlerul oprește zona afectată, nu mai lasă să intre piese noi și dă o alarmă cu zona și cauza probabilă. Piesele rămase pe transportor trebuie tratate clar: ori sunt scoase controlat, iar contoarele se actualizează, ori sunt marcate ca neprocesate. Dacă acest pas lipsește, apare cea mai frecventă greșeală din astfel de exerciții: piese numărate de două ori sau pierdute din evidență după fiecare alarmă.

4.4.4. Testarea, criteriile de reușită și limitele transferului

Validarea se realizează progresiv: mai întâi fiecare senzor și element de execuție, apoi modulele funcționale și, în final, ciclul complet. Setul minim de cazuri de testare cuprinde: prelucrarea unui produs de tip A; prelucrarea unui produs de tip B; succesiunea alternantă a celor două variante; succesiunea de produse B, care solicită cel mai mult stația; introducerea mai multor produse la intervale sub tactul de 12 s; absența confirmării la stație; blocarea unei piese pe transportor; menținerea activă a unui senzor; comanda deviatorului fără confirmarea poziției; oprirea și reluarea ciclului cu piese aflate pe linie; modificarea rețetei active între două piese; resetarea după apariția unei alarme; și verificarea fiecăreia dintre cele patru interblocări prin forțarea condiției corespunzătoare.

Exercițiul este considerat realizat corect dacă sunt îndeplinite simultan opt criterii: fiecare produs ajunge la destinația stabilită prin rețetă; operațiile incompatibile nu sunt comandate simultan, în niciun mod de funcționare; piesele nu sunt pierdute și nu sunt numărate de mai multe ori, inclusiv după o alarmă; schimbarea variantei nu necesită modificarea structurii programului, ci numai a datelor din rețetă; blocajele sunt detectate în intervalul stabilit prin timpii maximi din Tabelul 4.10; alarma identifică zona și codul cauzei; resetarea și reluarea funcționării se realizează controlat; iar programul păstrează o structură modulară verificabilă.

Ultimul criteriu trebuie verificat în practică, nu doar afirmat. Testul este simplu: adaugi în structura de rețete un rând pentru un produs C, cu timp de procesare de 5,5 s și aceeași destinație ca produsul A, apoi rulezi din nou testele. Dacă pentru

asta trebuie să schimbi maşina de stări, logica şi configuraţia nu au fost separate, iar programul trebuie refăcut înainte de a încheia exerciţiul. Este, la scară mică, testul măsurat de bugetul de reconfigurare din secţiunea 4.2.4: ce trebuie modificat pentru o variantă nouă, nu ce trebuie adăugat.

Trebuie spus clar ce nu s-a verificat la trecerea spre o instalaţie reală, pentru că aşa se vede ce a fost validat de fapt. Simularea verifică logica de comandă, succesiunea stărilor, interblocările şi tratarea abaterilor pe care le poate genera modelul. Nu include uzura, jocurile mecanice, variabilitatea materialului, alunecarea pieselor pe transportor, comportamentul senzorilor la praf, vibraţii sau variaţii de temperatură, întârzierile reale ale elementelor de execuţie şi defectele de cablare. Nici funcţiile de siguranţă nu pot fi validate prin simulare: ele se verifică pe instalaţie, în condiţii reale, împreună cu circuitele şi dispozitivele lor dedicate. Un program corect în simulator este deci doar începutul punerii în funcţiune. Înainte de transfer se validează separat echipamentele, timpii reali, interblocările fizice şi funcţiile de siguranţă.

4.4.5. Extinderea către integrarea IIoT şi indicatorii locali

După validarea controlului local, sistemul poate fi extins prin adăugarea unei interfeţe om–maşină şi prin expunerea controlată a datelor către o aplicaţie de supraveghere. Pot fi transmise starea sistemului, reţeta activă, cantităţile pe variantă, durata fiecărui ciclu, blocajele cu zona şi codul cauzei, precum şi istoricul alarmelor. Selecţia urmează criteriul enunţat în secţiunea 4.3.4 şi fişa de specificaţie din Tabelul 4.7: se transmite ceea ce susţine o decizie identificabilă. Stările intermediare ale maşinii de stări, temporizatoarele şi bistabilii interni rămân în controler.

O extensie utilă calculează local, pe durata unui schimb, timpul mediu de ciclu, numărul de opriri, durata cumulată a opririlor şi repartizarea acestora pe cauze. Aceste valori pot fi publicate printr-un gateway industrial către un sistem SCADA, MES sau către o platformă de analiză, în timp ce comenzile şi reacţiile necesare funcţionării rămân la nivelul PLC-ului.

Evaluarea rezultatului unui schimb – scenariu didactic. Se presupun următoarele valori măsurate pe modelul simulat, într-un schimb de 8 h cu 30 de minute de pauze planificate: 2 040 de piese evacuate, dintre care 37 neconforme; trei opriri neplanificate, cu o durată cumulată de 25 de minute. Debitul teoretic calculat în secţiunea 4.4.1 este de 2 250 de bucăţi pentru 7,5 h de producţie planificată.

Raportul dintre producţia realizată şi cea teoretică este 2 040 / 2 250 = 0,907, adică 90,7 %. Timpul de funcţionare efectiv este de 450 − 25 = 425 min, iar producţia teoretică pentru acest interval ar fi fost de 425 × 60 / 12 = 2 125 de bucăţi. Rezultă că opririle explică 2 250 − 2 125 = 125 de bucăţi din diferenţă, iar restul de 85 de bucăţi provine din micro-opriri şi din alimentare neuniformă, sub pragul de înregistrare. Concluzia operaţională este că intervenţia asupra celor trei opriri

înregistrate recuperează cel mult 5,6 puncte procentuale, în timp ce regularizarea alimentării are un potenţial comparabil, deşi nu apare în niciun jurnal de alarme.

Cele patru mărimi utilizate mai sus – timpul planificat, opririle clasificate, cantitatea conformă şi timpul de ciclu de referinţă – sunt exact datele din care se compune eficacitatea globală a echipamentelor. Indicatorul, formula sa, exemplul numeric complet şi discuţia limitelor sunt prezentate în secţiunea 7.2.3, împreună cu convenţiile de care depinde valabilitatea comparaţiilor între linii [51]; aici interesează numai faptul că modelul simulat produce, prin construcţie, toate mărimile necesare, iar acesta este criteriul practic după care se evaluează dacă un sistem este instrumentat suficient. Un sistem din care indicatorul nu poate fi reconstituit din date brute nu poate fi nici verificat, nici comparat cu o configuraţie anterioară.

Modelul poate fi dezvoltat ulterior prin introducerea unui robot industrial, a unei staţii suplimentare, a unor trasee alternative sau a unei strategii de redistribuire a operaţiilor. Adăugarea unei a doua staţii de procesare este extinderea cea mai instructivă, întrucât transformă exerciţiul dintr-un caz de flexibilitate de produs într-unul de flexibilitate de rutare, cu tot ce presupune aceasta: o regulă de alocare, tratarea situaţiei în care ambele staţii sunt ocupate şi verificarea faptului că piesele nu îşi pierd identitatea la deviere.

Exerciţiul evidenţiază că flexibilitatea nu rezultă din utilizarea unor echipamente programabile. Ea depinde de organizarea modulară a controlului, de separarea dintre logică şi configuraţia produsului, de urmărirea stării procesului şi de gestionarea controlată a abaterilor – aceleaşi proprietăţi care, la scara unei linii întregi, au fost analizate în secţiunile 4.2 şi 4.3.

4.5. Concluzii

FMS şi RMS răspund aceleiaşi presiuni – variaţia produselor, a volumelor şi a resurselor – prin mecanisme diferite, iar alegerea dintre ele nu este o chestiune de modernitate, ci de natura incertitudinii pe care fabrica trebuie să o suporte. FMS valorifică versatilitatea unor echipamente programabile într-un domeniu stabilit la proiectare şi transferă costul în investiţia iniţială. RMS modifică structura, capacitatea şi funcţionalitatea în trepte discrete şi plăteşte fiecare extindere separat. Cele două paradigme nu se exclud: aceeaşi fabrică poate exploata o linie flexibilă acolo unde se manifestă varietatea şi poate proiecta după principii reconfigurabile zonele în care variază volumul.

Distincţia dintre tipurile de flexibilitate – de maşină, de proces, de produs, de rutare, de volum şi de expansiune – transformă o cerinţă calitativă într-o decizie de proiectare cu indicatori proprii. Fiecare tip se obţine prin alte mijloace şi se verifică prin altă măsurătoare, iar o cerinţă de „*mai multă flexibilitate*” formulată fără această precizare conduce, aproape întotdeauna, la un sistem capabil de altceva decât ceea ce i se cere. Ultima coloană a Tabelului 4.2 are o consecinţă directă asupra

infrastructurii de date: o proprietate al cărei indicator nu poate fi calculat din datele colectate nu poate fi nici demonstrată, nici îmbunătățită.

Calculele din secțiunile 4.1.4 și 4.2.4 arată de ce reconfigurarea trebuie tratată ca problemă de dimensionare, nu ca opțiune tehnică. Când raportul dintre timpul de ciclu și timpul de tact depășește unitatea, cererea nu mai poate fi acoperită prin reglaje, iar variantele reale se reduc la un număr mic, comparabile prin capacitate, grad de utilizare și rezervă. Adăugarea unui modul rămâne, în exemplul analizat, singura variantă care lasă rezervă utilizabilă și menține utilizarea sub pragul de la care variabilitatea erodează debitul; capacitatea neutilizată care rezultă nu este o eroare de dimensionare, ci prețul granularității. Verificarea stației dominante adaugă o corecție esențială: capacitatea liniei se recalculează după fiecare treaptă de scalare, întrucât dublarea unei stații deplasează limitarea în loc să o elimine. Bugetul de reconfigurare completează imaginea cu observația cea mai contraintuitivă a capitolului: intervenția mecanică reprezintă mai puțin de o cincime din efortul unei schimbări, în timp ce integrarea informațională, validarea și rampa de pornire însumează peste patru cincimi.

Modularitatea, interoperabilitatea și adaptabilitatea condiționează împreună funcționarea acestor sisteme și niciuna nu compensează absența celorlalte. Modularitatea trebuie tratată pe trei planuri – fizic, logic și informațional, iar durata unei reconfigurări este dictată de cel mai puțin dezvoltat dintre ele. Interoperabilitatea se construiește pe patru niveluri succesive, dintre care cel semantic este cel mai costisitor atunci când lipsește, tocmai pentru că erorile lui nu se manifestă la punerea în funcțiune, ci mult mai târziu, prin comparație cu o măsurătoare independentă; un echipament de conversie rezolvă primele două niveluri și nu îl rezolvă pe al treilea. Adaptabilitatea devine acceptabilă operațional numai dacă domeniul de variație este aprobat și dacă există o cale de revenire verificată – cerința cel mai frecvent omisă din proiectele de digitalizare, deși fără ea orice modificare automată este un experiment ireversibil executat în producție.

Integrarea IIoT extinde flexibilitatea locală: monitorizarea echipamentelor, urmărirea produselor, contextualizarea datelor, corelarea producției cu SCADA, MES și ERP. Repartizarea funcțiilor (echipament, controler local, edge, niveluri superioare) depinde de timpul de răspuns admis, volumul datelor și consecințele unei întreruperi. Criteriu principal: decizia susținută de fiecare categorie de date. Comanda critică, interblocările și funcțiile de siguranță rulează local, independent de platforme și comunicații externe. În sistemele reconfigurabile, echipamentul raportează și configurația activă: o celulă care execută corect un program greșit nu generează eroare.

Exercițiul aplicativ confirmă, la scară redusă, aceleași principii. Separarea dintre logica de control și rețeta produsului este ceea ce face un program efectiv extensibil, iar testul acestei separări nu este o declarație, ci adăugarea unei variante noi urmată de reluarea setului de verificări. Dimensionarea prealabilă a modelului –

verificarea stației limitative și a numărului de piese aflate simultan pe linie – arată că structura programului decurge din proces, nu invers: un tranzit mai lung decât tactul impune urmărirea individuală a pieselor, oricât de simplă ar părea instalația. Limitele simulării rămân, totodată, explicite: ea validează logica, nu procesul, iar funcțiile de siguranță nu pot fi validate decât pe instalația reală.

Toate rezultatele din acest capitol depind, în ultimă instanță, de calitatea semnalelor care intră în sistem. Un buget de reconfigurare, un grad de utilizare sau o alarmă interpretabilă nu valorează mai mult decât măsurarea din care provin. Senzorii care detectează, elementele de execuție care acționează, controlerele care decid în timp determinist și sistemele de supraveghere care prezintă informația operatorului constituie stratul pe care se sprijină întreaga construcție discutată până aici. Capitolul 5 tratează aceste dispozitive: principiile lor de funcționare, caracteristicile metrologice, modul de integrare în bucle de control și criteriile după care se aleg pentru o aplicație dată.

4.6. Întrebări de verificare

1. *Care dintre situații favorizează alegerea unui sistem reconfigurabil de fabricație (RMS) în locul unui FMS?*

a) volumul este stabil, iar varietatea este mare și anticipată în interiorul unei familii de produse;
b) varietatea de produse este cunoscută, dar volumul cererii este incert;
c) gama de produse este restrânsă și nu se va modifica pe durata de viață a liniei;
d) investiția inițială trebuie maximizată pentru a reduce costul marginal al schimbării.

2. *O stație are timpul de ciclu de 95 s/buc și un timp de producție disponibil de 12.240.000 s/an. Câte stații identice sunt necesare pentru o cerere anuală de 210.000 de bucăți?*

a) 3 stații, deoarece fiecare stație trebuie să aibă o rezervă de 100 %;
b) 1,63 stații, deoarece numărul de stații poate fi fracționar;
c) 1 stație, deoarece 1,63 se rotunjește în jos;
d) 2 stații, deoarece timpul de tact este 58,3 s, iar 95 / 58,3 = 1,63, care se rotunjește în sus.

3. *După dublarea stației critice (ciclu efectiv 47,5 s), următoarea stație din linie are ciclul de 55 s. Cu T = 12.240.000 s/an, care este capacitatea liniei?*

a) aproximativ 222.500 buc/an, deoarece restricția s-a transferat la stația cu ciclul de 55 s
b) aproximativ 128.800 buc/an, deoarece capacitatea rămâne cea inițială
c) aproximativ 257.700 buc/an, deoarece capacitatea se dublează odată cu stația
d) aproximativ 210.000 buc/an, deoarece linia produce exact cererea

4. *Care este indicatorul prin care poate fi verificată flexibilitatea de rutare a unui sistem?*

a) proporția pieselor deviate pe trasee alternative și timpul de reacție la indisponibilitatea unei stații;
b) costul unitar la 50 %, 75 % și 100 % din capacitate;
c) durata de la aprobarea unei variante noi până la prima piesă conformă;
d) numărul de operații distincte executate de un utilaj fără intervenție majoră.

5. *De ce depinde durata totală a unei reconfigurări, atunci când modularitatea fizică, logică și informațională au grade diferite de maturitate?*

a) depinde exclusiv de modularitatea fizică, deoarece este cea mai vizibilă
b) nu depinde de modularitate, ci numai de numărul de operatori;
c) este dictată de planul cel mai puțin dezvoltat dintre cele trei;
d) este dictată de planul cel mai avansat dintre cele trei.

6. *O valoare de temperatură raportată în grade Fahrenheit este tratată drept grade Celsius de aplicația receptoare, fără nicio eroare de transmisie sau de format. Care nivel de interoperabilitate lipsește?*

a) nivelul semantic, a cărui absență este cea mai costisitoare tocmai pentru că sistemul pare să funcționeze corect;
b) nivelul operațional, deoarece nu există confirmare a mesajului;
c) nivelul sintactic, deoarece structura mesajului este invalidă;
d) nivelul tehnic, deoarece datele nu ajung la destinație.

7. *Ce înseamnă plug-and-produce într-un sistem reconfigurabil?*

a) un modul nou poate fi conectat fără nicio validare tehnică ulterioară;
b) un modul nou este detectat, configurat și înregistrat cu intervenții manuale minime;
c) funcțiile de siguranță ale modulului sunt configurate de platforma cloud;
d) producția pornește automat la conectarea oricărui echipament la rețea.

8. *În bugetul de reconfigurare al unei stații adăugate, ce pondere au componentele informaționale și de validare comparativ cu intervenția mecanică și racordarea utilităților?*

a) cele două grupe au ponderi aproximativ egale, de câte 50 %;
b) componentele informaționale sunt neglijabile, sub 5 % din efort;
c) intervenția mecanică și racordarea utilităților domină, cu peste 80 % din efort;
d) componentele informaționale și de validare însumează circa 57,7 % din efort, iar intervenția mecanică și racordarea utilităților circa 16,7 %.

9. *Ce nu poate prelua adaptarea automată a funcționării unui sistem flexibil, chiar dacă poate modifica parametri de regim, alocări de resurse și priorități?*

a) utilizarea unui traseu alternativ când o stație este indisponibilă;
b) interblocările, oprirea de urgență, limitarea mișcărilor și celelalte funcții de siguranță, care se execută local și independent de rețea;

c) alocarea operaţiilor către resurse echivalente disponibile;
d) selectarea parametrilor corespunzători produsului identificat.

10. Care dintre următoarele date ale unui controler rămân, de regulă, la nivelul echipamentului şi nu se transmit către nivelurile superioare?

a) indicatorii de degradare utili mentenanţei;
b) alarmele şi stările agregate ale echipamentului;
c) stările intermediare ale secvenţelor, bistabilii interni şi temporizatoarele de proces;
d) rezultatele inspecţiei şi cantităţile realizate.

5. DISPOZITIVE INTELIGENTE INDUSTRIALE ȘI AUTOMATIZAREA PROCESELOR

Capitolul 4 s-a încheiat cu observaţia că un buget de reconfigurare, un grad de utilizare sau o alarmă interpretabilă nu valorează mai mult decât măsurarea din care provin. Capitolul de faţă tratează stratul care produce acea măsurare şi care aplică asupra procesului deciziile luate pe baza ei. Un sistem IIoT nu începe la nivelul platformei de analiză, ci la nivelul echipamentelor care transformă starea fizică a procesului în date şi deciziile în acţiune: senzorii convertesc mărimi precum temperatura, presiunea, poziţia, nivelul sau debitul în semnale prelucrabile; PLC-urile execută logica de comandă în ritmul impus de proces; actuatoarele aplică rezultatul acestei logici asupra instalaţiei; gateway-urile industriale şi nivelul de procesare la edge pregătesc datele pentru utilizarea lor în afara zonei de control; sistemele HMI şi SCADA fac procesul vizibil şi operabil. Fără acest strat, nivelurile superioare ale unei arhitecturi IIoT nu au nici date de prelucrat, nici efect asupra producţiei.

Datele parcurg un traseu care începe la nivelul procesului şi continuă prin condiţionarea şi conversia semnalelor, achiziţia în PLC, procesarea la nivel edge şi transmiterea către sistemele SCADA, MES sau platformele de analiză. În sens invers, comenzile, valorile de referinţă şi reţetele aprobate coboară către nivelul de control, unde sunt validate şi aplicate în limitele configuraţiei tehnologice şi ale condiţiilor de siguranţă. Cele două sensuri nu sunt simetrice: fluxul ascendent tolerează întârzieri şi agregări, în timp ce fluxul descendent modifică starea unui proces fizic şi trebuie tratat cu reguli de autorizare, validare şi confirmare.

Această asimetrie explică de ce echipamentele descrise în capitol nu pot fi tratate ca simple surse de date. Ele funcţionează sub restricţii simultane de timp, de mediu şi de consecinţă: un ciclu de scanare depăşit, o valoare nevalidată sau o alarmă interpretată greşit produc efecte imediate asupra disponibilităţii instalaţiei şi a siguranţei personalului. Din acest motiv, criteriul de selecţie nu este conectivitatea, ci comportamentul întregului lanţ de măsurare şi acţionare, inclusiv atunci când o componentă se defectează sau comunicaţia cu nivelurile superioare devine indisponibilă. Conectivitatea nu înlocuieşte funcţiile locale de control: procesele critice trebuie să poată continua ori să treacă într-o stare sigură independent de disponibilitatea reţelei sau a platformelor externe.

Capitolul urmează traseul semnalului. Secţiunile 5.1 şi 5.2 tratează senzorii şi actuatoarele ca extremităţi ale buclei de măsurare şi acţionare. Secţiunea 5.3 analizează automatul programabil ca nivel de decizie deterministă, iar secţiunea 5.4 prezintă gateway-ul industrial şi procesarea la edge ca nivel de pregătire, filtrare şi

separare a fluxurilor, incluzând dimensionarea cantitativă a latenței și a lățimii de bandă. Secțiunea 5.5 tratează sistemele SCADA și interfețele HMI ca nivel de supraveghere. Secțiunile 5.6 și 5.7 aplică aceste principii prin proiectarea unei interfețe de monitorizare și prin integrarea verticală locală a unui senzor cu un automat programabil și un sistem SCADA.

Rezultatul capitolului pregătește Capitolul 6, dedicat protocoalelor prin care aceste echipamente schimbă efectiv date, și Capitolul 7, în care componentele sunt integrate într-o arhitectură IIoT completă. Ca și în capitolul precedent, valorile numerice din exemplele de calcul sunt ipoteze de lucru declarate, iar exercițiile din secțiunile 5.6 și 5.7 sunt scenarii didactice executabile în laborator, nu instalații documentate.

Obiectivele capitolului

La finalul acestui capitol, cititorul va fi capabil:

- să diferențieze senzorul, traductorul și lanțul de măsurare și să interpreteze corect caracteristicile metrologice relevante pentru IIoT: acuratețea, precizia, rezoluția, liniaritatea, histerezisul și deriva;
- să selecteze un senzor pe baza criteriilor metrologice, constructive și de mediu și să argumenteze compromisurile acceptate, inclusiv relația dintre clasa de toleranță și modul de conectare;
- să explice rolul actuatoarelor și al elementelor finale de control în transformarea comenzilor în acțiune fizică și să selecteze categoria de acționare potrivită unei aplicații, inclusiv comportamentul la pierderea energiei;
- să descrie arhitectura, ciclul de scanare și organizarea programului unui automat programabil și să argumenteze de ce timpul de reacție al unei funcții nu se reduce la timpul de scanare declarat;
- să diferențieze automatul programabil de sistemul de control distribuit pe baza unor criterii explicite de aplicație, structură și inginerie;
- să explice rolul gateway-ului industrial și al procesării la edge în integrarea și, simultan, în separarea domeniilor OT și IT;
- să calculeze un buget de latență și necesarul de lățime de bandă pentru un lanț senzor–PLC–gateway–broker–bază de date și să interpreteze limitele rezultatului;
- să descrie funcțiile unui sistem SCADA și principiile de proiectare a interfețelor HMI, inclusiv tratarea alarmelor, a drepturilor de acces și a calității datelor;
- să proiecteze și să valideze integrarea verticală locală a unui senzor cu un automat programabil și un sistem SCADA, incluzând comportamentul la defectarea senzorului și la pierderea comunicației.

5.1. Senzori industriali

Senzorii realizează legătura dintre procesul fizic şi sistemul de control, transformând mărimi precum temperatura, presiunea, poziţia, distanţa, nivelul sau debitul în semnale electrice utilizabile. Informaţiile furnizate permit monitorizarea procesului, executarea secvenţelor automate, detectarea abaterilor, controlul calităţii şi planificarea mentenanţei.

Într-o buclă de control, punctul de referinţă (SP) reprezintă valoarea dorită, iar valoarea procesului (PV) este determinată prin măsurare. Controlerul compară cele două valori şi calculează mărimea de comandă (CV), transmisă prin lanţul de acţionare pentru reducerea abaterii. Calitatea controlului depinde astfel atât de algoritmul utilizat, cât şi de corectitudinea măsurării: o buclă bine reglată care primeşte o valoare eronată reglează corect un proces greşit. Bucla de control a procesului este reprezentată în Figura 5.1.

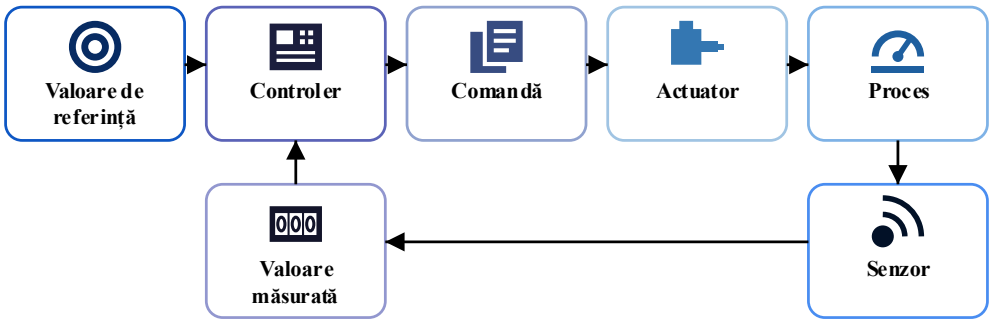


Figura 5.1 – Bucla de control a procesului

Elementul sensibil reacţionează la variaţia mărimii măsurate, iar traductorul transformă această reacţie într-un semnal electric [129]. Condiţionarea poate include amplificarea, filtrarea, izolarea galvanică, compensarea şi liniarizarea. Dacă semnalul este analogic, convertorul analog–digital îl transformă într-o valoare numerică, preluată de PLC sau de modulul de achiziţie. Fiecare etapă a lanţului adaugă propria contribuţie la incertitudinea rezultatului, motiv pentru care performanţa sistemului de măsurare nu poate fi dedusă din specificaţia unui singur element [36]. Lanţul rezultat şi tipurile de semnal pe care le poate furniza sunt reprezentate în Figura 5.2.

După forma semnalului furnizat, senzorii pot fi:

- *analogici*, cu ieşiri precum 4–20 mA sau 0–10 V;
- *digitali*, care transmit valori şi informaţii de diagnostic printr-o interfaţă de comunicaţie;
- *binari*, care indică două stări, precum prezenţă–absenţă sau activ–inactiv.

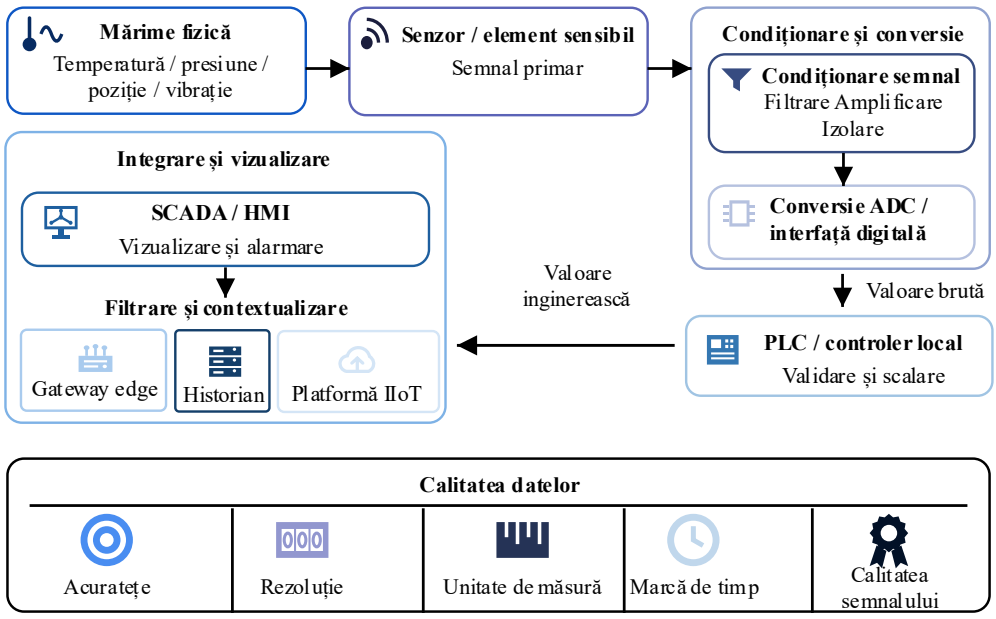


Figura 5.2 – Lanțul de măsurare industrial

Bucla de curent 4–20 mA rămâne semnalul analogic dominant în măsurările industriale, fiind standardizată ca semnal de curent continuu pentru sistemele de control al proceselor [130]. Avantajul său nu este doar rezistența la perturbații: deoarece limita inferioară a domeniului util este 4 mA, nu zero, întreruperea circuitului produce 0 mA și devine astfel distinctă de o valoare de proces validă.

Pe această proprietate se sprijină convenția de semnalizare a defectelor, care rezervă intervalul 3,8–20,5 mA informației de măsurare și indică defectarea aparatului prin valori de cel mult 3,6 mA sau de cel puțin 21,0 mA. Intervalele 3,6–3,8 mA și 20,5–21,0 mA sunt zone de diferențiere pe care transmițătorul nu trebuie să le utilizeze, tocmai pentru ca sistemul de control să poată fixa praguri de detecție intermediare fără risc de alarme false produse de deriva semnalului [131]. Consecința pentru proiectarea aplicației este directă: modulul de intrare trebuie configurat pentru un domeniu care acoperă întreaga plajă 0–22 mA, iar programul trebuie să trateze separat depășirea domeniului de proces și defectarea transmițătorului – mecanism aplicat efectiv în secțiunea 5.7.2.

Ieșirile binare PNP și NPN sunt întâlnite la senzorii de proximitate, iar interfețele digitale punct-la-punct de tip IO-Link permit transmiterea simultană a valorii, a parametrilor de configurare și a informațiilor de diagnostic pe același cablu cu care se realizează conexiunea binară clasică. Interfața este standardizată ca SDCI și definită normativ ca extensie a intrărilor și ieșirilor digitale către o legătură bidirecțională punct-la-punct [132]. Avantajul operațional nu constă în viteză, ci în parametrizarea de la distanță și în înlocuirea unui senzor fără reconfigurare manuală

– funcție relevantă atunci când instalația conține zeci de dispozitive identice cu reglaje diferite.

Performanța unui senzor este descrisă prin mai multe caracteristici:

- *domeniul de măsurare*, delimitat de valorile minimă și maximă;
- *sensibilitatea*, care exprimă variația ieșirii în raport cu variația intrării;
- *rezoluția*, reprezentând cea mai mică variație care poate fi diferențiată;
- *acuratețea*, denumită exactitate de măsurare în vocabularul internațional de metrologie, care indică apropierea rezultatului de valoarea de referință;
- *precizia*, asociată dispersiei rezultatelor obținute prin măsurări repetate;
- *liniaritatea*, care descrie abaterea față de relația ideală dintre intrare și ieșire;
- *histerezisul*, determinat de diferența dintre valorile obținute la creșterea și la descreșterea mărimii;
- *eroarea de deplasare a originii*, denumită și offset;
- *deriva*, reprezentând modificarea lentă a rezultatului în timp;
- *timpul de răspuns și lățimea de bandă*, care caracterizează comportamentul dinamic;
- *repetabilitatea* și *stabilitatea* în condiții constante.

Definiții conform vocabularului internațional de metrologie: exactitate = apropierea de valoarea adevărată; precizie = concordanța indicațiilor obținute în condiții specificate [133]. Sinteza celor trei noțiuni: Tabelul 5.1.

Un senzor poate fi precis, dar insuficient de exact, dacă rezultatele sunt apropiate între ele și prezintă aceeași eroare sistematică. Rezoluția ridicată nu garantează acuratețea, deoarece un sistem poate afișa variații foarte mici fără ca acestea să corespundă corect valorii reale. Confuzia dintre cele trei mărimi este frecventă în specificațiile comerciale și conduce la supradimensionarea inutilă a lanțului de achiziție sau, invers, la încrederea nejustificată într-o valoare afișată cu multe zecimale. Numărul de zecimale prezentate operatorului trebuie stabilit în raport cu incertitudinea reală a lanțului, nu cu rezoluția convertorului – decizie cuantificată în secțiunea 5.7.2.

Tabelul 5.1 – Diferența dintre acuratețe, precizie și rezoluție

Caracteristică	Semnificație	Exemplu
Acuratețe	Apropierea valorii măsurate de valoarea de referință	Senzorul indică 100,1 °C pentru o temperatură de referință de 100 °C
Precizie	Gradul de apropiere dintre rezultatele măsurărilor repetate	Senzorul furnizează valori foarte apropiate la repetarea măsurării
Rezoluție	Cea mai mică variație care poate fi diferențiată	Sistemul poate evidenția modificări de 0,1 °C

Selecția senzorului trebuie să ia în considerare mărimea măsurată, domeniul și acuratețea necesare, timpul de răspuns, condițiile de mediu, materialul țintei, modul de montare, semnalul de ieșire și compatibilitatea cu sistemul de control [134]. Trebuie analizate suplimentar gradul de protecție al carcasei, definit prin codul IP [86], rezistența la vibrații, imunitatea electromagnetică cerută mediilor industriale

[67], necesitatea calibrării şi posibilitatea înlocuirii fără modificarea instalaţiei. Un senzor corect ales metrologic, dar cu un grad de protecţie insuficient pentru zona în care este montat, devine sursa principală de opriri neplanificate.

5.1.1. Pt100 – senzor de temperatură cu rezistenţă

Pt100 este un termometru cu rezistenţă de platină cu o rezistenţă nominală de $100\ \Omega$ la $0\ °C$. Creşterea temperaturii determină creşterea rezistenţei electrice, iar relaţia cunoscută dintre cele două mărimi permite calcularea temperaturii. Caracteristica este definită normativ prin coeficientul de temperatură convenţional $\alpha = 3{,}851 \cdot 10^{-3}\ °C^{-1}$ şi acoperă domeniul $-200…+850\ °C$ [135].

Senzorul este utilizat în aplicaţii în care sunt importante acurateţea, stabilitatea şi repetabilitatea, precum procesele alimentare, instalaţiile chimice, sistemele termice şi echipamentele pentru tratarea materialelor. Elementul sensibil poate fi introdus într-o teacă de protecţie adaptată presiunii, temperaturii şi compatibilităţii chimice a mediului; teaca ameliorează durabilitatea, dar măreşte constanta de timp a măsurării, ceea ce trebuie luat în considerare la reglarea buclelor termice.

Standardul defineşte patru clase de toleranţă, exprimate ca funcţii de temperatura măsurată |t|, în grade Celsius: clasa AA, ±(0,1 + 0,0017 · |t|); clasa A, ±(0,15 + 0,002 · |t|); clasa B, ±(0,3 + 0,005 · |t|); clasa C, ±(0,6 + 0,01 · |t|). La 100 °C, un senzor de clasă B admite o abatere de ±0,8 °C, iar unul de clasă AA, de ±0,27 °C. Diferenţa devine determinantă când pragul de alarmare este apropiat de valoarea normală de funcţionare: o limită fixată la 80 °C şi verificată cu un senzor de clasă B implică, numai din partea elementului sensibil, o incertitudine de aproximativ ±0,7 °C, la care se adaugă erorile transmiţătorului, ale modulului de intrare şi ale scalării. Ediţia în vigoare elimină o ambiguitate frecventă din specificaţiile de achiziţie: toleranţa se aplică termometrului complet, nu doar elementului rezistiv [135].

Conectarea poate fi realizată prin două, trei sau patru conductoare. Configuraţia cu două conductoare este simplă, dar include în rezultat rezistenţa cablurilor. Conectarea cu trei conductoare permite compensarea acesteia în aplicaţiile industriale uzuale, iar configuraţia cu patru conductoare este utilizată atunci când se urmăreşte reducerea suplimentară a erorii, prin eliminarea influenţei rezistenţei de linie [129]. Alegerea nu este liberă: pentru clasele A şi AA, standardul impune conectarea cu trei sau patru conductoare, deoarece rezistenţa conductoarelor ar consuma singură toleranţa clasei declarate [135]. Din acest motiv, o specificaţie de tipul „Pt100, două conductoare, clasa A” este contradictorie şi nu poate fi verificată metrologic.

Semnalul rezistiv poate fi preluat direct de un modul compatibil al PLC-ului sau convertit local într-un semnal standardizat, precum 4–20 mA. Transmiţătorul poate realiza liniarizarea, compensarea şi diagnosticarea circuitului înaintea transmiterii valorii către sistemul de control, iar semnalizarea defectului prin ieşirea în afara domeniului util permite PLC-ului să diferenţieze o măsurare nevalidă de o temperatură scăzută [131].

Într-o arhitectură IIoT, valoarea temperaturii trebuie însoțită de unitatea de măsură, marca temporală, identificatorul senzorului și starea semnalului. Depășirea limitelor poate genera o reacție locală a PLC-ului, în timp ce istoricul valorilor poate fi utilizat pentru analiza procesului și identificarea degradării echipamentului. Modul concret în care această valoare este achiziționată, scalată și transmisă mai departe este dezvoltat în secțiunea 5.7.

5.1.2. Senzori de presiune

Senzorii de presiune măsoară presiunea gazelor și lichidelor din instalațiile hidraulice, pneumatice, termice sau tehnologice. În funcție de referința utilizată, măsurarea poate fi absolută, raportată la vid, relativă, raportată la presiunea atmosferică, sau diferențială, între două puncte ale instalației. Confuzia dintre cele trei referințe este o sursă frecventă de erori de interpretare la punerea în funcțiune, deoarece diferența dintre presiunea absolută și cea relativă – aproximativ 1 bar – poate fi comparabilă cu întregul domeniu de măsurare al aplicației.

Elementul sensibil poate utiliza un principiu tensometric, capacitiv sau piezoelectric [136]. Senzorii tensometrici măsoară deformarea unei membrane și sunt utilizați într-o gamă largă de aplicații. Cei capacitivi sunt potriviți inclusiv pentru variații reduse de presiune. Senzorii piezoelectrici generează sarcină electrică numai la variația solicitării, motiv pentru care nu pot menține o măsurare statică; utilizarea lor este limitată la fenomene dinamice, precum pulsațiile, șocurile hidraulice și vârfurile de presiune din ciclurile rapide.

Alegerea trebuie să țină seama de domeniul de presiune, temperatura fluidului, compatibilitatea chimică, tipul conexiunii mecanice, suprapresiunea admisă și comportamentul dinamic. În aplicațiile cu fluide agresive sau temperaturi ridicate pot fi necesare membrane de separare și materiale speciale [1].

Semnalul poate fi transmis către PLC sub forma unei valori analogice sau printr-o interfață digitală. PLC-ul utilizează măsurarea pentru reglarea pompelor, supapelor și compresoarelor, pentru confirmarea forței de acționare sau pentru detectarea unor pierderi și blocaje.

Analiza simultană a presiunii în mai multe puncte permite determinarea căderilor de presiune și identificarea unei funcționări anormale. Datele istorice trebuie interpretate împreună cu regimul de lucru, temperatura și starea actuatoarelor, deoarece o valoare izolată nu indică întotdeauna cauza abaterii. Contextualizarea măsurării cu regimul de funcționare al instalației este condiția care transformă o serie temporală într-o informație de mentenanță utilizabilă [22].

5.1.3. Senzori fotoelectrici

Senzorii fotoelectrici detectează obiecte fără contact, prin emiterea și recepționarea unui fascicul luminos, și sunt utilizați pentru confirmarea prezenței, numărare, poziționare, sortare și sincronizarea operațiilor automate. Ca aparatură de

comandă, aparţin comutatoarelor de proximitate, ale căror caracteristici electrice, distanţe de comutare şi condiţii de încercare sunt normate [137].

Principalele configuraţii sunt:

- barieră, cu emiţătorul şi receptorul amplasate separat;
- retroreflexivă, cu emiţătorul şi receptorul în aceeaşi carcasă şi un reflector amplasat opus;
- reflexie difuză, în care lumina este reflectată direct de obiectul detectat;
- reflexie difuză cu suprimarea fundalului, la care detecţia este condiţionată de distanţa până la obiect, nu numai de intensitatea luminii reflectate.

Configuraţia de tip barieră oferă, în general, o detecţie stabilă pe distanţe mai mari, dar necesită instalarea şi alinierea a două componente. Soluţia retroreflexivă simplifică partea electrică a montajului, iar senzorul cu reflexie difuză este compact, însă comportamentul său poate fi influenţat de culoarea, textura, forma şi înclinarea obiectului. Varianta cu suprimarea fundalului, introdusă ca tip distinct în ediţia în vigoare a standardului, răspunde tocmai acestei limitări şi permite detecţia unei piese închise la culoare în faţa unui fundal reflectorizant apropiat [137].

Praful, depunerile, lumina ambientală, obiectele transparente sau suprafeţele foarte reflectorizante pot afecta detecţia. Selectarea şi testarea trebuie realizate cu piesele reale, în condiţiile de iluminare şi contaminare specifice instalaţiei; o rezervă de semnal insuficientă la punerea în funcţiune se transformă, după câteva săptămâni de exploatare, în opriri intermitente greu de diagnosticat.

Ieşirea binară este preluată de PLC pentru confirmarea poziţiei sau declanşarea unei secvenţe. Unele modele furnizează suplimentar intensitatea semnalului recepţionat, gradul de contaminare sau avertizări privind pierderea alinierii – informaţii care nu au valoare de control, dar care sunt exact tipul de date pe care nivelul de procesare la edge le poate transforma în indicatori de mentenanţă, conform secţiunii 5.4.2.

5.1.4. Senzori inductivi

Senzorii inductivi detectează obiecte metalice fără contact fizic. Bobina din interiorul senzorului generează un câmp electromagnetic, iar apropierea unui obiect metalic modifică acest câmp. Circuitul electronic identifică variaţia şi comută ieşirea [136].

Aceşti senzori sunt utilizaţi pentru confirmarea poziţiei componentelor metalice, detectarea prezenţei pieselor, numărarea elementelor şi stabilirea poziţiilor de capăt. Absenţa contactului mecanic reduce uzura şi permite utilizarea în cicluri repetitive.

Cât de departe detectează un senzor depinde de dimensiunea lui, de forma ţintei şi de materialul ei. Standardul defineşte distanţa nominală de comutare sn pe o ţintă de referinţă din oţel, cu dimensiuni şi grosime precizate, iar distanţa asigurată

sa este o fracțiune din ea. Metalele neferoase reduc distanța, prin factori de corecție dați de producător [137]. Practic, valoarea din catalog nu se aplică direct pieselor din aluminiu, alamă sau oțel inoxidabil austenitic, iar distanța de montare se alege în funcție de sa, nu de sn. Senzorii se montează la distanțe suficiente de alte piese metalice și de senzorii vecini, ca să nu se influențeze reciproc.

Avantajele principale sunt robustețea, repetabilitatea și rezistența la praf, ulei sau vibrații. Limitările sunt asociate detectării exclusive a obiectelor metalice și distanței relativ reduse. Într-un sistem IIoT, numărul comutărilor și modificarea comportamentului semnalului pot completa informațiile utilizate pentru diagnosticarea mecanismului monitorizat.

5.1.5. Senzori ultrasonici

Senzorii ultrasonici determină prezența sau distanța unui obiect prin măsurarea timpului necesar unei unde acustice pentru a ajunge la țintă și a reveni la receptor. Cunoscând viteza de propagare a sunetului, sistemul calculează distanța până la obiect.

Tehnologia poate fi utilizată pentru măsurarea nivelului, detectarea obiectelor transparente, monitorizarea distanței și poziționarea fără contact. Spre deosebire de senzorii optici, funcționarea nu depinde direct de culoarea sau transparența obiectului.

Rezultatul poate fi influențat de temperatura aerului, curenții puternici, turbulențe, spumă, forma țintei și unghiul de incidență. Dependența de temperatură nu este neglijabilă și este cuantificată normativ: deoarece viteza sunetului variază cu temperatura aerului, distanța de comutare se modifică cu aproximativ 0,17 % pentru fiecare kelvin [137]. Pentru o măsurare la 2 m într-o hală în care temperatura variază cu 20 °C între schimburi, abaterea rezultată depășește 6 cm – inacceptabilă pentru o poziționare, dar tolerabilă pentru o detecție de prezență. Senzorii destinați măsurării nivelului includ, din acest motiv, compensare de temperatură. În apropierea senzorului există o zonă în care măsurarea nu poate fi realizată corect, iar obiectele cu suprafețe înclinate pot devia unda în afara receptorului.

Pentru aplicațiile de nivel trebuie verificate forma rezervorului, obstacolele interne și caracteristicile suprafeței măsurate. În aplicațiile de poziționare trebuie analizate timpul de răspuns și variația măsurării în raport cu viteza obiectului.

Senzorul poate furniza o ieșire binară, o valoare analogică proporțională cu distanța sau date digitale. PLC-ul utilizează informația pentru comandă și interblocare, iar sistemele de supraveghere pot păstra evoluția nivelului, frecvența depășirii pragurilor și calitatea semnalului. Principiile de detecție prezentate în secțiunile 5.1.3–5.1.5 sunt sintetizate comparativ în Figura 5.3.

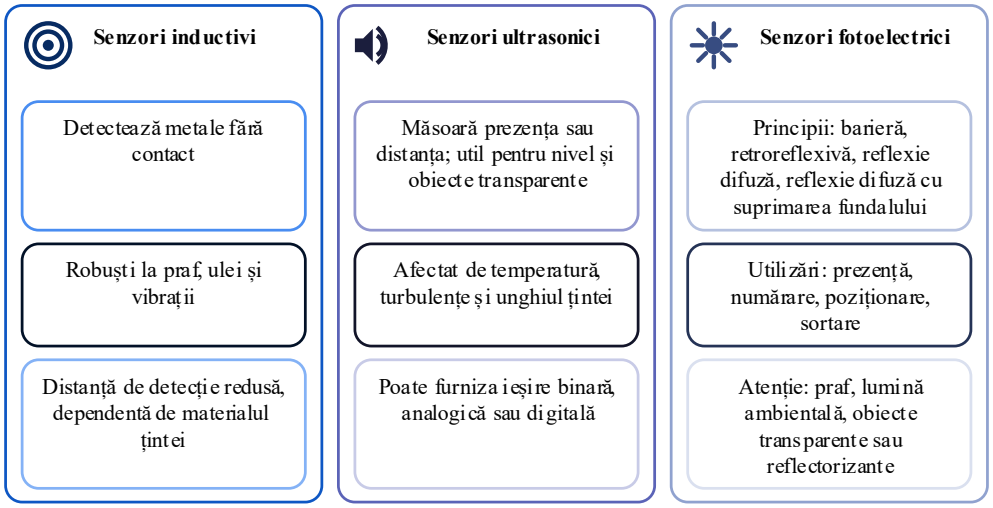


Figura 5.3 – Principii de detecție fără contact

5.1.6. Senzorii inteligenți și integrarea în IIoT

Senzorii industriali inteligenţi integrează conversia, compensarea, filtrarea, parametrizarea şi funcţiile de diagnostic în dispozitivul de măsurare; pe lângă valoarea măsurată, aceştia pot furniza identitatea dispozitivului, versiunea, limitele configurate, calitatea semnalului, temperatura internă şi avertizări privind contaminarea sau degradarea. Interfeţele digitale *punct-la-punct* permit, suplimentar, parametrizarea de la distanţă şi înlocuirea unui senzor fără reconfigurare manuală, prin transferul automat al parametrilor din controler către dispozitivul nou [132].

Existenţa unei interfeţe digitale nu transformă însă automat senzorul într-o sursă utilă pentru IIoT. Datele trebuie contextualizate, asociate echipamentului şi operaţiei şi transmise cu frecvenţa necesară aplicaţiei; în lipsa acestor elemente, o valoare corectă din punct de vedere metrologic rămâne neinterpretabilă la nivelul aplicaţiei receptoare [22]. Reacţiile critice rămân la nivelul controlerului local, iar sistemele SCADA, MES şi platformele de analiză utilizează valorile pentru monitorizare, trasabilitate şi optimizare. Structura minimală a unui mesaj contextualizat – identificator, valoare, unitate, marcă temporală, calitate – este detaliată în secţiunea 5.4.4.

Frecvenţa de achiziţie trebuie stabilită în raport cu dinamica mărimii măsurate, nu cu performanţa maximă a echipamentului. Achiziţia unei temperaturi de proces la 10 ms nu adaugă informaţie, deoarece constanta termică a instalaţiei este de ordinul secundelor sau minutelor, dar încarcă inutil controlerul, reţeaua şi spaţiul de stocare; consecinţele cantitative ale acestei alegeri sunt calculate în secţiunea 5.4.5.

Înainte de conectarea unui senzor fizic, semnalul acestuia poate fi simulat pentru verificarea scalării, a limitelor, a alarmelor şi a comportamentului programului

PLC. Simularea validează logica lanţului de măsurare, dar nu reproduce integral zgomotul, deriva, defectele de montaj şi influenţele mediului. Validarea finală se realizează cu senzorul şi procesul reale, conform secţiunii 5.7.5.

Datele obţinute prin măsurare sunt transformate în acţiuni fizice prin intermediul actuatoarelor industriale, analizate în secţiunea următoare.

5.2. Actuatoare industriale

Actuatoarele transformă semnalele generate de sistemul de control în acţiuni fizice asupra procesului. Acestea pot produce deplasare liniară sau rotativă, pot modifica poziţia unei valve, pot acţiona un mecanism de prindere ori pot controla viteza şi cuplul unei axe. Împreună cu senzorii şi controlerul, actuatoarele închid bucla dintre măsurare, decizie şi acţiune: fără ele, un sistem IIoT observă procesul, dar nu îl influenţează.

Senzorii măsoară rezultatul acţiunii şi transmit către controler poziţia, viteza, presiunea, forţa sau starea procesului. Controlerul compară rezultatul cu valoarea stabilită şi corectează comanda atunci când abaterea depăşeşte limitele admise.

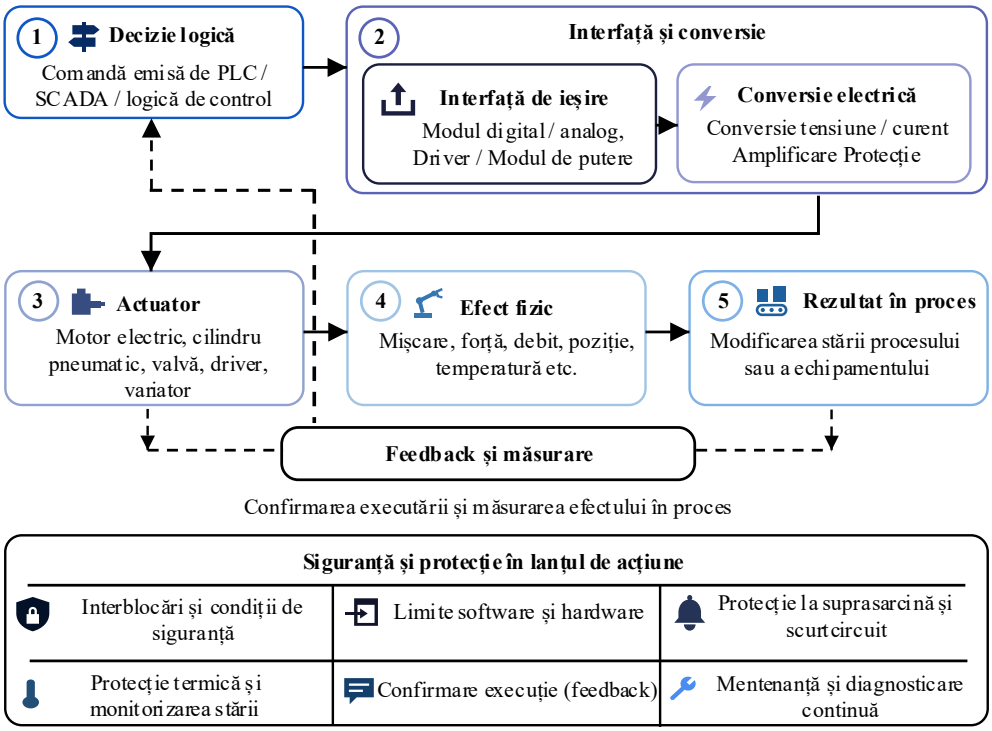


Figura 5.4 – Lanțul de acționare

Actuatorul trebuie diferențiat de elementul final de control. Actuatorul transformă energia electrică, pneumatică sau hidraulică în mișcare, iar elementul final aplică această mișcare asupra procesului [138]. De exemplu, într-un ansamblu de reglare a debitului, actuatorul deplasează tija, iar corpul valvei modifică secțiunea de curgere. Distincția nu este formală: performanța de reglare a buclei depinde de caracteristica elementului final, în timp ce disponibilitatea și diagnosticarea depind în principal de actuator, iar cele două componente se dimensionează, se achiziționează și se înlocuiesc separat. Lanțul de acționare și această delimitare sunt reprezentate în Figura 5.4.

În funcție de energia utilizată, actuatoarele industriale pot fi:

- *electrice*, precum motoarele, servomotoarele și actuatoarele liniare;
- *pneumatice*, precum cilindrii și motoarele pneumatice;
- *hidraulice*, utilizate pentru obținerea unor forțe și cupluri ridicate.

Compararea celor trei categorii este prezentată în Tabelul 5.2.

Selecția actuatorului trebuie să țină seama de tipul mișcării, cursă, viteză, forță sau cuplu, precizie, frecvența ciclurilor, condițiile de mediu și comportamentul necesar la pierderea energiei [1]. Trebuie analizate și compatibilitatea cu sistemul de control, posibilitatea diagnosticării, consumul energetic, mentenanța și modul în care actuatorul ajunge într-o stare sigură în cazul unei defecțiuni.

Tabelul 5.2 – Compararea principalelor categorii de actuatoare industriale

Categorie	Avantaje principale	Limitări	Aplicații tipice
Electrici	Control precis, eficiență ridicată și integrare digitală facilă	Cost mai ridicat pentru sistemele servo și necesitatea protecției la suprasarcină	Roboți, mașini-unelte, transportoare și sisteme de poziționare
Pneumatici	Mișcare rapidă, construcție simplă și utilizare sigură în numeroase medii industriale	Precizie și rigiditate reduse, consum de aer și posibilitatea apariției pierderilor	Manipulare, fixare, sortare și ambalare
Hidraulici	Forțe și cupluri mari, construcție compactă și comportament bun la sarcini ridicate	Instalație auxiliară complexă, pierderi de fluid și cerințe de mentenanță	Prese, echipamente mobile, sisteme de ridicare și utilaje grele

Comportamentul la oprire nu poate fi tratat ca o consecință implicită a întreruperii comenzii. Standardul privind echipamentul electric al mașinilor definește trei categorii de oprire: oprirea necontrolată prin întreruperea imediată a alimentării actuatoarelor, oprirea controlată în care alimentarea este menținută până la atingerea opririi și apoi întreruptă, respectiv oprirea controlată cu menținerea alimentării [139]. Alegerea categoriei este o decizie de proiectare bazată pe analiza de risc a instalației, nu o preferință de programare: pentru o axă verticală, întreruperea imediată a alimentării poate produce căderea sarcinii, în timp ce pentru un mecanism de tăiere menținerea alimentării poate prelungi expunerea la pericol. Aceeași

cerință este formulată explicit și pentru sistemele de acționare cu fluid, unde proiectantul trebuie să stabilească comportamentul instalației atât la întreruperea, cât și la restabilirea alimentării, astfel încât niciunul dintre cele două evenimente să nu producă o mișcare neașteptată [140], [141]. Cerințele privind părțile sistemelor de comandă cu rol de siguranță sunt tratate separat de logica de proces [45], [142].

5.2.1. Valve de control

Valvele de control reglează debitul, presiunea, nivelul sau temperatura, modificând cât de mult curge un lichid, un gaz sau un vapor. Ele se compun din corp, obturator, actuator, poziționer și dispozitive care confirmă poziția [138].

În funcție de aplicație, pot fi utilizate:

- *valve cu bilă*, potrivite în special pentru închidere și deschidere rapidă;
- *valve cu clapetă*, utilizate pentru debite mari și construcții compacte;
- *valve cu diafragmă*, adecvate mediilor corozive sau proceselor cu cerințe ridicate de igienă;
- *valve cu ventil*, care permit reglarea progresivă și precisă a debitului.

Acționarea poate fi pneumatică, electrică sau hidraulică. Acționarea pneumatică oferă viteză și robustețe, cea electrică permite poziționarea controlată fără o instalație de aer comprimat, iar acționarea hidraulică este utilizată atunci când sunt necesare forțe mari.

Valvele cu funcționare binară ocupă pozițiile deschis sau închis. Valvele modulante pot adopta poziții intermediare, stabilite printr-un semnal analogic sau prin comunicație digitală. Poziționerul compară poziția comandată cu poziția măsurată și corectează alimentarea actuatorului până la reducerea abaterii.

Dimensionarea nu se reduce la alegerea diametrului nominal al conductei. Capacitatea de curgere a valvei se exprimă printr-un coeficient determinat experimental, iar ecuațiile de dimensionare corelează acest coeficient cu debitul, căderea de presiune și proprietățile fluidului în condițiile reale de instalare, incluzând corecțiile pentru reducții, curgere neturbulentă și comportamentul fluidelor compresibile [143]. O valvă supradimensionată lucrează permanent în apropierea poziției închise, unde caracteristica de reglare este cea mai neliniară, ceea ce degradează stabilitatea buclei chiar dacă regulatorul este corect acordat [144]. Practica uzuală este alegerea unei valve care, la debitul nominal, lucrează într-o zonă intermediară a cursei, astfel încât să existe rezervă de reglare în ambele sensuri.

Pentru alegerea unei valve, trebuie analizate tipul fluidului, temperatura și presiunea acestuia, debitul necesar și căderea de presiune. Materialele valvei trebuie să fie compatibile cu mediul de lucru, iar modul în care aceasta reglează debitul, etanșeitatea și rapiditatea răspunsului trebuie să corespundă cerințelor aplicației. De asemenea, trebuie stabilită poziția sigură pe care valva o adoptă la pierderea alimentării cu energie și trebuie luate în considerare cerințele de curățare și mentenanță.

Poziția sigură poate fi închisă, deschisă sau menținută, în funcție de consecințele defectării [144]. De exemplu, alimentarea cu combustibil trebuie întreruptă în anumite situații, în timp ce circuitul de răcire poate necesita menținerea curgerii. La acționările pneumatice, această poziție este obținută constructiv, prin arc, și nu depinde de programul controlerului – o proprietate care trebuie păstrată explicit în documentația instalației, deoarece este ușor de anulat printr-o modificare aparent nesemnificativă a circuitului de comandă. Poziția declarată trebuie și verificată prin încercare: o valvă specificată drept „normal închisă" poate rămâne blocată într-o poziție intermediară dacă frecarea acumulată depășește forța arcului.

Într-un sistem IIoT, ansamblul poate transmite poziția comandată și cea reală, timpul de deplasare, numărul acționărilor, presiunea de alimentare și codurile de diagnosticare. Creșterea progresivă a timpului de deplasare sau apariția unei diferențe persistente între poziția comandată și cea măsurată poate indica depuneri, frecare, uzură ori o alimentare insuficientă. Aceste mărimi nu au valoare de control, dar constituie exact tipul de date pe care nivelul de procesare la edge le convertește în indicatori de mentenanță, conform secțiunii 5.4.2.

Reglarea procesului și reacțiile de protecție: execuție locală, în PLC sau controler. Platformele de supraveghere: analiză și mentenanță, fără a înlocui funcțiile locale de menținere a procesului în limite sigure.

5.2.2. Servomotoare

Servomotoarele sunt actuatoare electromecanice utilizate pentru controlul precis al poziției, vitezei și cuplului. Sistemul servo cuprinde motorul, amplificatorul de acționare (*servo drive*), traductorul de poziție și controlerul de mișcare, care poate fi integrat în PLC sau într-un controler specializat.

Controlerul generează valoarea de referință, iar amplificatorul reglează energia furnizată motorului. Un encoder incremental sau absolut ori un resolver măsoară poziția axului și furnizează semnalul de reacție. Diferența dintre valoarea comandată și cea măsurată este utilizată pentru corectarea continuă a mișcării.

Controlul este organizat, de regulă, prin bucle succesive pentru curent sau cuplu, viteză și poziție. Bucla de curent are răspunsul cel mai rapid, iar bucla de poziție stabilește deplasarea finală. Ordinea nu este arbitrară: fiecare buclă exterioară poate fi acordată stabil numai dacă bucla interioară îi răspunde cu un ordin de mărime mai repede [145]. Această structură permite executarea unor profile controlate de accelerație și decelerație și sincronizarea mai multor axe.

Servomotoarele sunt utilizate în:

- axele roboților industriali;
- mașini-unelte cu comandă numerică;
- instalații de ambalare și etichetare;
- sisteme de tăiere și dozare sincronizată;

– mecanisme de poziţionare şi manipulare;
– sisteme de inspecţie şi asamblare automată.

La dimensionare trebuie luate în calcul cuplul necesar, inerţia sarcinii, viteza maximă, acceleraţia, regimul de funcţionare şi transmisia mecanică. Dacă alegi doar după cuplul nominal, poţi obţine un sistem care nu face faţă acceleraţiilor sau unul supradimensionat şi costisitor. Contează în primul rând raportul dintre inerţia sarcinii (raportată la ax) şi inerţia rotorului, plus cuplul efectiv din întregul ciclu de mişcare, nu vârful dintr-un singur punct. Un raport de inerţie mare limitează banda de acord a buclei de poziţie chiar dacă cuplul este suficient [145]. Efectul este oscilaţia la oprire, nu lipsa de forţă, iar soluţia se caută în transmisia mecanică, nu în reglaj.

Amplificatorul poate furniza către PLC şi sistemul de supraveghere informaţii despre poziţie, viteză, cuplu estimat, curent, temperatură, eroarea de urmărire şi starea alarmelor. Evoluţia acestor valori poate indica apariţia frecărilor, dezechilibrelor, suprasarcinilor sau degradării transmisiei mecanice. Eroarea de urmărire este, în acest context, cel mai sensibil indicator timpuriu: ea creşte înaintea oricărei alarme de suprasarcină, iar tendinţa sa pe durata mai multor săptămâni descrie starea mecanică a axei mai bine decât valoarea instantanee a curentului.

Parametrii de reglare şi limitele de mişcare trebuie modificaţi numai prin proceduri autorizate. O valoare transmisă de la un sistem extern nu trebuie aplicată direct dacă depăşeşte limitele validate sau nu corespunde configuraţiei mecanice active.

Funcţiile de protecţie nu se realizează prin logica standard de automatizare, ci prin subfuncţii de siguranţă implementate în amplificator şi validate pentru nivelul de integritate cerut de analiza de risc. Standardul aplicabil le grupează în funcţii de oprire, funcţii de monitorizare şi funcţii de ieşire, printre care cuplul dezactivat în siguranţă (STO), oprirea sigură (SS1), viteza limitată în siguranţă (SLS) şi comanda sigură a frânei (SBC) [146]. Delimitarea are consecinţe practice imediate: o comandă de oprire transmisă prin program opreşte mişcarea, dar nu garantează absenţa cuplului la ax, în timp ce STO garantează acest lucru fără a garanta imobilizarea unei sarcini suspendate – pentru care este necesară comanda frânei.

5.2.3. Cilindri pneumatici

Cilindrii pneumatici transformă energia aerului comprimat în mişcare liniară. Aceştia sunt utilizaţi frecvent pentru împingerea, ridicarea, fixarea, separarea sau poziţionarea pieselor în operaţii repetitive. Dimensiunile de montare şi de racordare ale seriei uzuale de 10 bar, cu alezaje între 32 mm şi 320 mm, sunt standardizate, ceea ce asigură interschimbabilitatea între producători şi permite înlocuirea unui cilindru fără modificarea mecanismului [147].

La cilindrul cu simplu efect, aerul comprimat produce mişcarea într-un singur sens, iar revenirea este realizată printr-un arc sau printr-o forţă externă. La cilindrul cu dublu efect, aerul este introdus alternativ în cele două camere, ceea ce permite controlul ambelor sensuri de deplasare.

Forţa teoretică este determinată de presiunea de lucru şi suprafaţa activă a pistonului:

$$F = p \cdot A$$

Exemplu de calcul: se consideră un cilindru cu dublu efect cu diametrul pistonului D = 63 mm şi diametrul tijei d = 20 mm, alimentat la presiunea relativă p = 6 bar. Se admite că presiunea de alimentare este constantă, iar randamentul mecanic al ansamblului, care include frecările interne şi contrapresiunea de evacuare, este $\eta \approx 0{,}85$.

Suprafaţa activă la extindere:

$$A_{ext} = \pi D^2 / 4 = \pi \cdot 63^2 / 4 = 3\,117 \text{ mm}^2$$

Suprafaţa activă la retragere, diminuată de secţiunea tijei:

$$A_{ret} = \pi(D^2 - d^2) / 4 = \pi(63^2 - 20^2) / 4 = 2\,803 \text{ mm}^2$$

Cu p = 6 bar = 0,6 N/mm^2, rezultă forţele teoretice:

$$F_{ext} = 0{,}6 \cdot 3\,117 = 1\,870 \text{ N} \quad F_{ret} = 0{,}6 \cdot 2\,803 = 1\,682 \text{ N}$$

iar forţele disponibile în instalaţie:

$$F_{ext,util} = 0{,}85 \cdot 1\,870 \approx 1\,590 \text{ N} \quad F_{ret,util} = 0{,}85 \cdot 1\,682 \approx 1\,430 \text{ N}$$

Interpretare. Forţa la retragere reprezintă aproximativ 90 % din cea de la extindere, exclusiv din cauza secţiunii tijei. Diferenţa este relevantă atunci când mişcarea de retragere este cea care execută lucrul util – de exemplu la un mecanism de tragere sau la o prindere care se închide prin retragere. O sarcină care necesită 1 500 N în ambele sensuri este acoperită la extindere, dar nu şi la retragere. Pierderea de aproximativ 15 % prin frecări şi contrapresiune arată de ce dimensionarea la limită conduce la mecanisme care funcţionează în stand şi se blochează în producţie.

Limite. Randamentul de 0,85 este o valoare orientativă; valoarea reală depinde de garnituri, lubrifiere, dimensiunea racordurilor şi reglajul regulatoarelor de debit. Calculul este static şi nu descrie comportamentul dinamic: la viteze mari, presiunea din camera activă nu atinge valoarea de alimentare, iar forţa efectivă este mai mică. Pentru sarcini care nu sunt pur axiale trebuie verificate suplimentar solicitările laterale admise ale tijei.

Consumul de aer: Pentru aceeaşi configuraţie, cu cursa s = 200 mm şi o cadenţă de 20 de cicluri pe minut, volumul consumat pe ciclu complet, măsurat la presiunea de lucru, este:

$$V_p = (A_{ext} + A_{ret}) \cdot s = (3\,117 + 2\,803) \cdot 200 = 1{,}18 \text{ dm}^3$$

Raportarea la condiţiile atmosferice se face prin raportul de compresie, calculat cu presiunile absolute:

$$r = (p + p_{atm}) / p_{atm} = (6 + 1{,}013) / 1{,}013 \approx 6{,}9$$

$$V_{liber} = 1{,}18 \cdot 6{,}9 \approx 8{,}2\ dm^3/ciclu \Rightarrow Q \approx 8{,}2 \cdot 20 = 164\ dm^3/min \approx 9{,}8\ m^3/h$$

Interpretare. Un singur cilindru de dimensiune medie solicită aproape 10 m^3/h de aer liber. Rezultatul explică de ce o linie cu câteva zeci de actuatoare pneumatice devine rapid principalul consumator energetic al halei și de ce o pierdere permanentă echivalentă cu funcționarea continuă a unui astfel de cilindru trece neobservată în producție, dar este vizibilă în factura de energie.

Limite. Calculul nu include volumul conductelor și al racordurilor, care se umple și se golește la fiecare ciclu, și nu ține seama de pierderile din instalație; consumul real este, în practică, mai mare [148].

Comanda este realizată prin electrovalve conectate la ieșirile PLC-ului sau la module distribuite. Regulatoarele de debit permit modificarea vitezei, iar senzorii magnetici montați pe cilindru confirmă pozițiile retras și extins. Pentru poziții intermediare sau control continuu sunt necesare soluții constructive și senzori suplimentari.

Cilindrii pneumatici sunt potriviți pentru:

- mecanisme de prindere și fixare;
- sisteme de sortare și evacuare;
- dispozitive de ridicare și împingere;
- operații de ambalare;
- acționarea clapetelor și mecanismelor auxiliare.

Limitările sunt asociate compresibilității aerului, care reduce rigiditatea și precizia poziționării, precum și eficienței energetice a producerii aerului comprimat. Pierderile din conducte și racorduri pot crește consumul fără a produce o modificare evidentă a ciclului.

Integrarea digitală poate furniza numărul de cicluri, timpii de extindere și retragere, confirmarea pozițiilor, presiunea și consumul de aer. Creșterea timpului de acționare, lipsa confirmării poziției sau consumul anormal pot indica scurgeri, uzura garniturilor, modificarea sarcinii ori blocarea mecanismului.

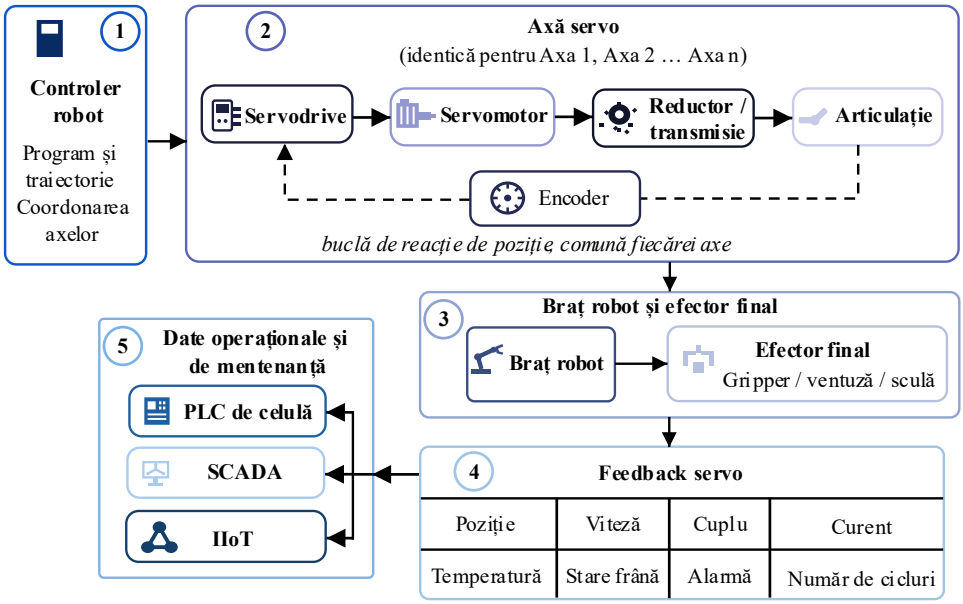
În cazul pierderii aerului comprimat trebuie analizat comportamentul sarcinii. O piesă ridicată sau fixată nu trebuie să se deplaseze necontrolat. Pot fi necesare supape de blocare, dispozitive mecanice de reținere sau circuite pneumatice proiectate pentru menținerea stării sigure, conform regulilor generale aplicabile sistemelor pneumatice și hidraulice [140], [141].

5.2.4. Robotul industrial ca sistem integrat de acționare

Robotul industrial reunește mai multe lanțuri servo coordonate de un controler comun. Fiecare axă cuprinde un motor, un amplificator de acționare, un traductor de poziție, o transmisie mecanică și o articulație. Controlerul utilizează modelul cinematic pentru transformarea traiectoriei efectorului final în mișcările individuale ale axelor [149], [145].

Pozițiile axelor trebuie coordonate astfel încât efectorul final să urmeze traiectoria programată cu viteza și orientarea stabilite. Controlerul gestionează suplimentar accelerațiile, limitele mecanice, singularitățile, sarcina utilă și interacțiunea cu echipamentele celulei.

Robotul include și senzori pentru poziția axelor, temperatura motoarelor, starea frânelor și funcțiile de siguranță. Dispozitivul de prindere adaugă propriile actuatoare și confirmări privind deschiderea, închiderea, presiunea ori prezența piesei. Robotul trebuie tratat astfel ca un sistem integrat de actuatoare, senzori, control și comunicație, nu ca un actuator individual (Figura 5.5).



** Robotul este un ansamblu de lanțuri servo coordonate.*

Figura 5.5 – Robotul industrial

Această interpretare corespunde și cadrului normativ. Standardul aplicabil tratează robotul ca mașină incompletă, ale cărei cerințe se completează la nivelul aplicației, iar ediția în vigoare explicitează cerințele de siguranță funcțională, introduce cerințe de securitate cibernetică în măsura în care aceasta afectează siguranța și integrează în serie conținutul referitor la aplicațiile colaborative [150]. Consecința practică este dublă. În primul rând, cerințele de limitare a spațiului și a vitezei, oprirea de protecție și funcționarea în mod de învățare sunt stabilite pentru robot ca ansamblu, iar respectarea lor nu poate fi asigurată prin logica standard a PLC-ului din celulă. În al doilea rând, expresia „robot colaborativ” nu descrie o proprietate a echipamentului: numai aplicația poate fi proiectată, verificată și validată drept colaborativă.

Către infrastructura IIoT pot fi transmise modul de funcționare, programul activ, durata ciclului, numărul operațiilor, pozițiile axelor, curenții sau cuplurile

estimate, temperaturile și alarmele. Aceste date permit analiza productivității, identificarea opririlor și observarea unor tendințe de degradare.

Controlul traiectoriei și sincronizarea axelor rămân în controlerul robotului. Comenzile provenite din MES, SCADA sau dintr-o platformă externă trebuie limitate la funcții validate, precum selectarea unei comenzi de producție ori a unui program aprobat. Acestea nu trebuie să ocolească interblocările celulei sau funcțiile locale de siguranță, iar canalul prin care sunt transmise trebuie tratat ca parte a analizei de securitate, nu doar ca o interfață de date. Regula este generală și revine în secțiunea 5.5.7 pentru comenzile de supraveghere și în secțiunea 5.4.4 pentru fluxul descendent printr-un gateway industrial.

Actuatoarele aplică asupra procesului deciziile sistemului de automatizare, însă coordonarea lor necesită un controler capabil să achiziționeze intrările, să execute logica și să actualizeze ieșirile într-un mod determinist. Structura și funcționarea automatelor programabile sunt analizate în secțiunea următoare.

5.3. Automate programabile

Automatul programabil (*PLC*) este un echipament industrial destinat achiziției semnalelor, executării logicii de control și comandării actuatoarelor. Acesta coordonează funcționarea procesului pe baza unui program memorat și a condițiilor primite de la senzori, echipamente și sisteme auxiliare. Definiția normativă îl delimitează ca sistem electronic digital destinat utilizării în mediu industrial, care folosește o memorie programabilă pentru stocarea internă a instrucțiunilor orientate către utilizator și controlează, prin intrări și ieșiri numerice sau analogice, diverse tipuri de mașini și procese [151].

PLC-urile au fost dezvoltate pentru înlocuirea circuitelor de comandă realizate cu relee, temporizatoare și contoare electromecanice. Evoluția procesoarelor, a modulelor de intrare–ieșire și a comunicațiilor industriale a extins funcțiile acestora către reglare, controlul mișcării, diagnosticare, siguranță funcțională și integrare IIoT [26].

Spre deosebire de calculatoarele de uz general, PLC-urile sunt proiectate pentru funcționarea continuă în medii industriale caracterizate prin variații de temperatură, vibrații, perturbații electromagnetice, praf și umiditate; cerințele de mediu, alimentare, imunitate și încercările corespunzătoare sunt stabilite normativ [152]. Comportamentul lor trebuie să fie predictibil, iar defectarea unui modul, pierderea comunicației sau apariția unei valori nevalide trebuie identificată și gestionată controlat.

5.3.1. Arhitectura unui automat programabil

Un sistem PLC poate avea o structură compactă, în care procesorul, alimentarea, intrările și ieșirile sunt integrate în aceeași carcasă, sau una modulară, în care funcțiile sunt distribuite între module montate pe un suport comun. Pentru instalațiile

extinse pot fi utilizate module de intrare–ieşire amplasate la distanţă şi conectate printr-o reţea industrială. Structura unui sistem modular şi fluxul semnalelor între module sunt reprezentate în Figura 5.6, iar rolul fiecărei componente este sintetizat în Tabelul 5.3.

Intrările binare preiau stări precum activarea unui buton, prezenţa unei piese sau confirmarea poziţiei unui cilindru. Intrările analogice convertesc semnale precum 4–20 mA sau 0–10 V în valori numerice, cu o rezoluţie şi un timp de conversie declarate de producător pentru fiecare canal. Modulele specializate pot conecta direct senzori rezistivi de temperatură, termocupluri, encodere sau alte dispozitive care necesită condiţionare şi conversie dedicate; pentru termorezistenţe, modulul preia inclusiv liniarizarea conform relaţiei normate a senzorului [135].

Ieşirile binare comandă funcţii cu două stări, precum pornit–oprit sau deschis–închis. Ieşirile analogice transmit valori continue către regulatoare, valve proporţionale ori amplificatoare de acţionare. Comanda sarcinilor de putere nu este realizată, de regulă, direct de PLC, ci prin contactoare, relee, convertoare de frecvenţă, amplificatoare servo sau distribuitoare electropneumatice – element care revine în bugetul de timp analizat în secţiunea 5.3.2, deoarece fiecare dintre aceste componente adaugă propria întârziere de comutare.

Unitatea centrală include procesorul, memoria, ceasul intern şi circuitele de supraveghere. Un temporizator de supraveghere verifică executarea programului şi trece controlerul într-o stare prestabilită dacă timpul maxim admis este depăşit, comportament impus ca funcţie de bază a echipamentului [152]. Funcţiile de diagnostic urmăresc starea modulelor, alimentarea, comunicaţiile, erorile de program şi validitatea configuraţiei.

Tabelul 5.3 – Componentele principale ale unui sistem PLC

Componentă	Rol principal
Sursa de alimentare	Furnizează tensiunile necesare procesorului și modulelor; poate include monitorizarea tensiunii și soluții de redundanță
Unitatea centrală de procesare	Execută programul, gestionează memoria, comunicațiile și funcțiile de diagnosticare
Memoria	Păstrează programul, configurația, valorile procesului, rețetele și datele care trebuie menținute după întreruperea alimentării
Modulele de intrare	Preiau semnale binare, analogice sau provenite de la senzori și traductoare specializate
Modulele de ieșire	Comandă relee, contactoare, electrovalve, amplificatoare de acționare și alte elemente finale
Modulele specializate	Realizează funcții precum măsurarea temperaturii, numărarea rapidă, poziționarea, reglarea sau controlul mișcării
Interfețele de comunicație	Permit conectarea la echipamente de câmp, alte controlere, interfețe HMI, sisteme SCADA și gateway-uri industriale
Magistrala internă	Asigură transferul datelor și alimentarea între procesor și module
Sistemul de programare	Permite configurarea echipamentului, dezvoltarea programului, diagnosticarea, simularea și gestionarea versiunilor

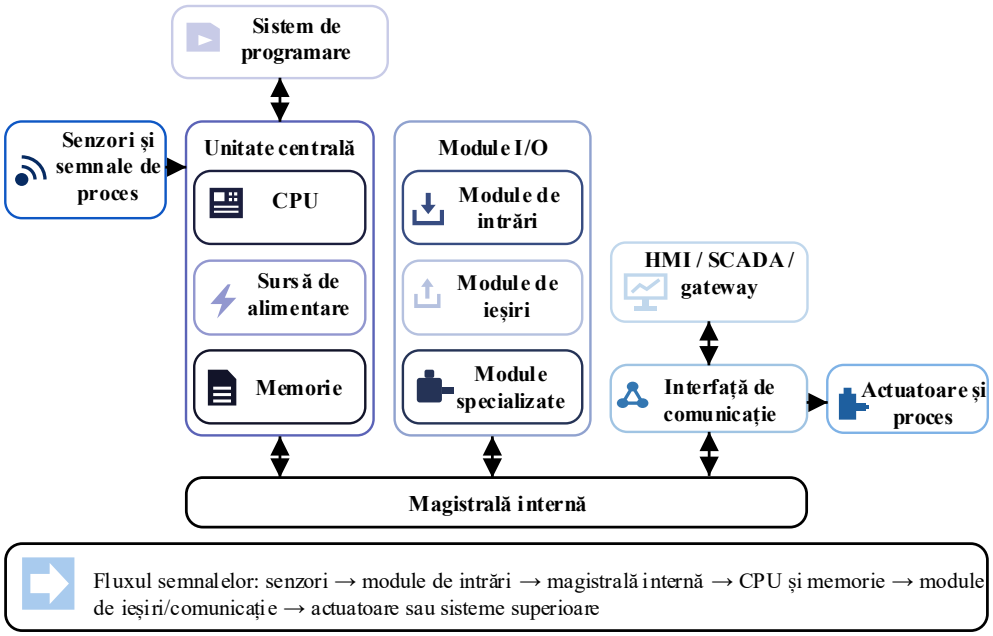


Figura 5.6 – Structura unui sistem PLC modular și fluxul semnalelor între module

Un sistem modular se poate extinde adăugând module. Intrările şi ieşirile distribuite scurtează cablurile dintre dispozitivele de câmp şi dulapul de automatizare, dar fac sistemul dependent de reţea [153]. Dacă se întrerupe comunicaţia, fiecare modul trebuie să treacă în starea configurată, iar PLC-ul trebuie să observe că a pierdut datele şi să nu mai folosească valori vechi. Comportamentul la defect nu vine de la sine: se configurează explicit, pentru fiecare modul şi, la unele familii, pentru fiecare canal. Valoarea din fabrică nu este mereu cea sigură pentru aplicaţia ta.

5.3.2. Ciclul de scanare

Majoritatea PLC-urilor execută programul într-o succesiune repetitivă denumită ciclu de scanare, una dintre caracteristicile funcţionale de bază ale acestei categorii de echipamente [151]. Forma simplificată a acestuia cuprinde: citirea intrărilor, executarea programului, actualizarea ieşirilor, realizarea funcţiilor de comunicaţie şi diagnosticare şi reluarea ciclului.

La începutul ciclului, stările intrărilor sunt copiate într-o zonă de memorie denumită imaginea procesului pentru intrări. Programul utilizează aceste valori pe durata execuţiei, ceea ce asigură o imagine coerentă a procesului în interiorul ciclului curent. Rezultatele sunt păstrate în imaginea procesului pentru ieşiri şi sunt transferate către module după finalizarea execuţiei [2].

O modificare produsă la o intrare după citirea imaginii procesului este preluată, în mod obişnuit, în ciclul următor. În aplicaţiile care necesită reacţii mai rapide pot fi utilizate întreruperi, module rapide, acces direct la periferie sau sarcini executate periodic, cu priorităţi diferite.

Timpul de scanare este influenţat de:

- dimensiunea şi complexitatea programului;
- numărul modulelor de intrare–ieşire;
- operaţiile matematice şi prelucrarea datelor;
- frecvenţa comunicaţiilor;
- numărul sarcinilor şi al întreruperilor;
- funcţiile de diagnosticare şi jurnalizare;
- performanţa procesorului.

Bugetul timpului de reacţie: exemplu numeric

Timpul total de reacţie nu este determinat numai de scanarea programului. Confuzia dintre timpul de scanare declarat şi timpul de reacţie al unei funcţii este una dintre cele mai costisitoare erori de dimensionare din automatizări, deoarece conduce la specificarea unui procesor rapid pentru o problemă care nu este generată de procesor.

Se consideră o aplicaţie de sortare pe transportor: un senzor inductiv detectează piesa, iar PLC-ul comandă un cilindru pneumatic de evacuare printr-o electrovalvă. Se cunosc: timpul de răspuns al senzorului 2 ms; filtrul de intrare configurat 3 ms; timpul de conversie al modulului de intrare 1 ms; timpul de scanare al PLC-ului 10 ms; întârzierea modulului de ieşire cu relee 10 ms; timpul de reacţie al electrovalvei şi al cilindrului până la începerea mişcării 15 ms.

Ipoteza determinantă este că evenimentul de proces este asincron faţă de ciclul de scanare. În cazul cel mai defavorabil, tranziţia intrării apare imediat după citirea imaginii procesului, deci se pierde un ciclu până când este observată şi încă un ciclu până când rezultatul logicii ajunge la ieşirea fizică. Rezultă bordul superior uzual de două cicluri de scanare:

$$t_{\text{reacţie}} = t_{\text{senzor}} + t_{\text{filtru}} + t_{\text{conversie}} + 2 \cdot t_{\text{scanare}} + t_{\text{ieşire}} + t_{\text{actuator}}$$

$$t_{\text{reacţie}} = 2 + 3 + 1 + 2 \cdot 10 + 10 + 15 = 51 \text{ ms}$$

Componentele acestui buget sunt reprezentate în Figura 5.7.

Interpretare. Timpul de scanare contribuie cu 20 ms, adică aproximativ 39 % din total; restul de 31 ms provine din elemente asupra cărora programul nu are nicio influenţă. Dacă transportorul se deplasează cu 1 m/s, cele 51 ms corespund unei deplasări de 51 mm a piesei între detecţie şi începerea evacuării – valoare care trebuie compensată prin poziţionarea senzorului sau prin întârziere calculată, nu prin achiziţionarea unui procesor mai rapid. Înjumătăţirea timpului de scanare, de la 10 la 5 ms, reduce totalul doar la 41 ms, adică o îmbunătăţire de 20 %, în timp ce

înlocuirea modulului de ieşire cu relee printr-unul cu tranzistoare, cu întârziere sub 1 ms, produce o reducere comparabilă la un cost mult mai mic.

Limite. Valorile sunt orientative şi trebuie înlocuite cu cele din documentaţia echipamentelor utilizate. Modelul presupune intrări şi ieşiri locale; intrările şi ieşirile distribuite adaugă timpul de actualizare al reţelei de câmp, care poate depăşi singur timpul de scanare. Calculul descrie cazul cel mai defavorabil, nu valoarea medie observată la testare – motiv pentru care o funcţie validată prin câteva încercări reuşite poate eşua ulterior în producţie. Pentru funcţiile cu cerinţe temporale stricte trebuie utilizate întreruperi de proces sau acces direct la periferie, care elimină componenta de două cicluri, dar mută problema în domeniul priorităţilor dintre sarcini. Un buget analog, construit pentru traseul datelor către nivelurile superioare, este dezvoltat în secţiunea 5.4.5.

Un program care funcţionează corect la un timp de scanare redus poate deveni instabil dacă sunt adăugate comunicaţii, funcţii de diagnosticare sau calcule complexe. De aceea, timpul de execuţie trebuie monitorizat, iar depăşirea limitei configurate trebuie tratată ca o abatere. Funcţiile cu cerinţe temporale stricte trebuie separate de operaţiile de raportare, arhivare sau schimb masiv de date.

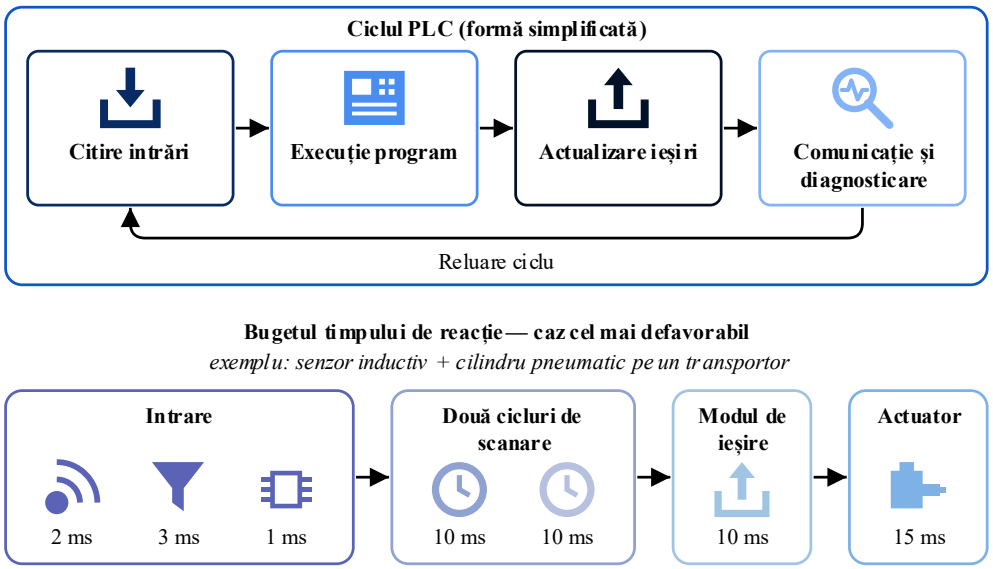


Figura 5.7 – Ciclul de scanare şi componentele timpului total de reacţie

5.3.3. Organizarea şi programarea aplicaţiei

Programul PLC trebuie structurat în module care corespund funcţiilor instalaţiei, precum transport, dozare, poziţionare, reglare, diagnosticare sau gestionarea modurilor de lucru. Separarea logicii pe echipamente şi funcţii permite testarea independentă, reutilizarea şi localizarea mai rapidă a erorilor.

Organizarea se bazează, în mod uzual, pe programe care coordonează funcționarea generală, blocuri funcționale care păstrează starea internă și permit reutilizarea pentru echipamente similare și funcții care execută prelucrări și returnează rezultate. Acestora li se adaugă structurile de date, utilizate pentru reprezentarea stărilor, parametrilor, rețetelor și informațiilor de diagnosticare, precum și sarcinile, care stabilesc momentul, periodicitatea și prioritatea execuției.

Aceste elemente nu sunt convenții ale unui producător, ci componente ale modelului software definit normativ, împreună cu regulile de declarare a variabilelor și cu tipurile de date elementare și derivate [123].

Adresele fizice trebuie separate de logica funcțională prin utilizarea unor variabile simbolice. De exemplu, programul utilizează variabila *Senzor_piesa_statie*, iar asocierea acesteia cu un canal fizic este realizată în configurația intrărilor. Astfel, înlocuirea modulului sau modificarea conexiunii nu impune rescrierea logicii procesului.

Ediția în vigoare a standardului de programare definește textul structurat (ST), diagrama cu contacte (LD) și diagrama blocurilor funcționale (FBD). Standardul include și elementele diagramei funcționale secvențiale (SFC), utilizate pentru structurarea programelor și blocurilor funcționale. Limbajul listă de instrucțiuni (IL), întâlnit în instalațiile mai vechi și inclus în edițiile anterioare, nu mai face parte din suita ediției actuale [123]. Consecința practică depășește nomenclatorul: programele existente scrise în IL rămân funcționale prin instrumentele producătorilor, dar nu mai pot fi invocate ca fiind conforme cu suita standardizată, ceea ce este relevant la specificarea unei migrări sau a unei preluări de aplicație. Domeniile de utilizare adecvate ale fiecărei reprezentări sunt sintetizate în Tabelul 5.4.

Limbajul trebuie ales în funcție de natura funcției și de competențele echipei de mentenanță. Utilizarea unui singur limbaj pentru întreaga aplicație nu este obligatorie. O secvență poate fi structurată prin SFC, interblocările pot fi realizate în LD, iar prelucrările numerice în ST.

Tabelul 5.4 – Utilizarea limbajelor și elementelor de programare pentru PLC

Limbaj sau reprezentare	**Caracteristici**	**Utilizare adecvată**
Diagramă cu contacte (LD)	Reprezentare grafică inspirată de circuitele cu relee	Interblocări, comenzi binare și secvențe simple
Diagramă a blocurilor funcționale (FBD)	Funcțiile sunt conectate prin semnale și fluxuri de date	Reglare, prelucrarea semnalelor și interconectarea blocurilor reutilizabile
Text structurat (ST)	Limbaj textual potrivit pentru expresii și algoritmi	Calcule, prelucrarea structurilor de date, bucle și condiții complexe
Diagramă funcțională secvențială (SFC)	Organizează procesul în etape, tranziții și acțiuni	Secvențe tehnologice și mașini de stări
Listă de instrucțiuni (IL)	Limbaj textual de nivel redus, eliminat din ediția actuală a standardului	Întreținerea programelor moștenite tehnologic

Indiferent de limbaj, programul trebuie să includă explicit:

- condiţiile de pornire şi oprire;
- modurile automat, manual şi mentenanţă;
- interblocările dintre comenzi incompatibile;
- confirmarea executării acţiunilor;
- supravegherea timpilor de răspuns;
- identificarea şi memorarea alarmelor;
- condiţiile de resetare şi reluare;
- starea adoptată la pierderea unui semnal sau a comunicaţiei.

Modul manual nu trebuie să elimine interblocările necesare protejării instalaţiei şi personalului. Comenzile manuale trebuie limitate la funcţiile autorizate şi aplicate numai în condiţiile permise de starea echipamentului.

Programul, configuraţia hardware şi parametrii trebuie gestionate împreună. O copie a programului fără configuraţia modulelor, versiunile *firmware*-ului şi valorile parametrilor poate fi insuficientă pentru refacerea sistemului. Modificările trebuie documentate, testate şi transferate controlat, iar versiunea existentă trebuie salvată înaintea actualizării – cerinţă tratată în ghidurile de securitate a sistemelor de control ca element de bază al gestionării configuraţiei, nu ca bună practică opţională [25].

5.3.4. Funcţii de control şi diagnosticare

PLC-ul poate executa mai multe categorii de funcţii:

- control logic, pentru comenzi, interblocări şi selectarea modurilor;
- control secvenţial, pentru coordonarea etapelor unui proces;
- reglare, prin algoritmi precum regulatorul proporţional–integral–derivativ;
- controlul mişcării, pentru poziţionarea şi sincronizarea axelor;
- diagnosticare, pentru detectarea abaterilor şi identificarea cauzelor probabile.

Într-o linie de producţie, PLC-ul coordonează transportoare, senzori, mecanisme de sortare şi staţii de lucru. Într-un proces tehnologic, acesta poate regla temperatura, presiunea, debitul sau nivelul. Într-o celulă robotizată, PLC-ul gestionează schimbul de semnale dintre robot, dispozitivele de prindere, echipamentele auxiliare şi sistemul de siguranţă, fără a prelua controlul intern al traiectoriei robotului, conform secţiunii 5.2.4.

Diagnosticarea trebuie proiectată odată cu logica de control. O alarmă generică de tip „*defecţiune sistem*" nu permite localizarea eficientă a problemei. Mesajul trebuie să indice echipamentul, funcţia afectată, condiţia care nu a fost confirmată şi momentul apariţiei. Cerinţele privind conţinutul, prioritizarea şi ciclul de viaţă al unei alarme sunt tratate detaliat în secţiunea 5.5.5.

Pentru fiecare acţiune importantă, trebuie precizat ce comandă se transmite, ce confirmare se aşteaptă şi în cât timp trebuie primită aceasta. Totodată, trebuie

stabilit cum reacţionează sistemul dacă nu primeşte confirmarea, în ce condiţii se poate face resetarea şi care este starea sigură sau controlată a echipamentului.

De exemplu, după comandarea extinderii unui cilindru, PLC-ul aşteaptă confirmarea senzorului de capăt. Dacă aceasta nu apare în intervalul stabilit, comanda este retrasă sau menţinută conform analizei de risc, alimentarea cu piese este oprită, iar alarma identifică actuatorul şi confirmarea absentă. Intervalul de supraveghere trebuie stabilit pornind de la timpul de deplasare măsurat, majorat cu o rezervă; un interval prea strâns generează alarme false la variaţii normale de presiune sau temperatură, iar unul prea larg întârzie detectarea blocajului până când piesa următoare a intrat deja în staţie.

PLC-urile de siguranţă folosesc arhitecturi şi module certificate, cu logică distinctă de automatizarea standard. Oprirea de urgenţă, monitorizarea uşilor, limitarea sigură a vitezei şi celelalte protecţii necesită proiectare şi validare conform riscului, cadrului siguranţei funcţionale [44] şi standardelor pentru maşini [45], [142] sau procese continue [154]. Implementarea corectă în programul standard nu demonstrează nivelul de performanţă cerut: lipsesc justificările privind diagnosticarea, arhitectura şi rata de defectare presupuse de analiza de risc.

5.3.5. Automatul programabil şi sistemul de control distribuit

Sistemul de control distribuit (DCS) coordonează funcţiile de control prin mai multe controlere integrate într-o arhitectură comună. PLC-ul şi DCS-ul pot executa reglare, logică secvenţială, achiziţie de date şi comunicaţii, iar diferenţele tradiţionale dintre cele două categorii s-au redus semnificativ în ultimele două decenii [153]. Criteriile care le delimitează în continuare sunt prezentate în Tabelul 5.5.

Alegerea nu trebuie realizată numai pe baza tipului de echipament. Trebuie analizate numărul buclelor de reglare, viteza secvenţelor, întinderea instalaţiei, disponibilitatea necesară, redundanţa, integrarea alarmelor, competenţele echipei şi costul întregului ciclu de viaţă. Pentru producţia pe loturi, criteriul suplimentar este capacitatea de a implementa modelele de control procedural – reţetă, procedură, operaţie, fază – definite normativ, pe care mediile DCS le oferă de regulă nativ, iar aplicaţiile PLC le construiesc explicit [95].

Deosebirea cu efect economic cel mai mare nu apare la punerea în funcţiune, ci pe durata exploatării. Într-un DCS, baza de date a variabilelor, ecranele de operare, alarmele şi arhiva provin dintr-o singură definiţie a echipamentului, astfel încât adăugarea unei bucle propagă automat modificarea în toate componentele. Într-o arhitectură construită din PLC, HMI şi SCADA de la furnizori diferiţi, aceeaşi modificare trebuie realizată separat în fiecare instrument, iar consecvenţa dintre ele depinde de disciplina echipei de inginerie. Costul suplimentar al mediului unificat se recuperează, în general, acolo unde numărul buclelor este mare şi modificările sunt frecvente. În aplicaţiile moderne pot fi utilizate arhitecturi hibride, în care PLC-urile controlează maşinile, iar DCS-ul coordonează procesul tehnologic.

Tabelul 5.5 – Compararea automatului programabil cu sistemul de control distribuit

Criteriu	PLC	DCS
Domeniu tradițional	Mașini, celule și procese discrete	Procese continue sau pe loturi
Structură	Controler compact ori modular, integrat cu echipamente diverse	Controlere distribuite într-un sistem unificat
Comportament dominant	Secvențe rapide, interblocări și controlul echipamentelor	Reglarea simultană a unui număr mare de bucle
Extindere	Prin module locale, intrări–ieșiri la distanță și controlere suplimentare	Prin adăugarea controlerelor și stațiilor în arhitectura sistemului
Interfață și istoric	Necesită integrarea cu HMI, SCADA sau un sistem de arhivare	Funcțiile de operare, alarmare și arhivare sunt, de regulă, integrate
Inginerie	Poate combina echipamente și aplicații de la furnizori diferiți	Utilizează un mediu de inginerie unificat pentru întregul sistem

5.3.6. Rolul automatului programabil în IIoT

Într-o arhitectură IIoT, PLC-ul reprezintă sursa principală a datelor asociate direct procesului şi, în acelaşi timp, nivelul la care sunt aplicate deciziile de control. Rolul său poate fi sintetizat prin cinci funcţii:

- achiziţia şi validarea datelor provenite de la senzori;
- prelucrarea locală, inclusiv scalarea, filtrarea şi calcularea unor indicatori;
- executarea deterministă a comenzilor, reglajelor şi interblocărilor;
- transmiterea stărilor, valorilor şi alarmelor către sistemele superioare;
- furnizarea informaţiilor de diagnosticare privind procesul, modulele şi comunicaţiile.

Datele pot fi expuse către HMI, SCADA, MES sau către un gateway industrial prin protocoale industriale. Un PLC poate furniza valori prin OPC UA, ale cărui concepte de spaţiu de adrese şi model informaţional sunt definite de specificaţia de bază [127], prin Modbus TCP [155] ori prin protocoale specifice producătorului. Publicarea directă prin MQTT este disponibilă pentru anumite controlere, dar nu trebuie considerată o funcţie universală; comparaţia detaliată a acestor protocoale este realizată în Capitolul 6.

Transmiterea datelor trebuie separată de controlul local. O întârziere în actualizarea tabloului de bord sau întreruperea conexiunii cu platforma externă nu trebuie să împiedice executarea interblocărilor şi reacţiilor critice. Dacă funcţionarea autonomă nu este posibilă, PLC-ul trebuie să treacă procesul într-o stare definită.

Pentru a putea fi interpretate corect, datele transmise trebuie să arate de la ce echipament provin, ce variabilă descriu, care este valoarea acesteia, în ce unitate este exprimată şi ce marcă temporală îi este asociată. De asemenea, trebuie precizate starea de funcţionare, calitatea sau validitatea semnalului, reţeta ori varianta de produs şi, dacă este cazul, codul alarmei.

Conectarea PLC-ului la rețelele informatice extinde suprafața de atac. Accesul la program, modificarea parametrilor și comenzile de la distanță trebuie limitate prin autentificare, autorizare, segmentarea rețelei și jurnalizarea intervențiilor [25]. Cerințele tehnice aplicabile unui controler ca element component al unui sistem de automatizare – identificarea și autentificarea, integritatea software-ului, jurnalizarea evenimentelor, actualizarea controlată – sunt formulate explicit în seria de standarde de securitate pentru automatizări industriale [156], iar aplicarea lor la nivel de arhitectură este tratată în Capitolul 8. Interfețele neutilizate trebuie dezactivate, iar actualizarea programului sau firmware-ului trebuie realizată numai printr-o procedură controlată.

PLC-ul nu este destinat stocării unor volume mari de date sau executării analizelor complexe. Resursele sale trebuie rezervate prioritar controlului și diagnosticării locale. Agregarea datelor, conversia protocoalelor, păstrarea temporară și transmiterea securizată către platformele externe pot fi transferate unui gateway industrial sau unui sistem de procesare la edge, analizate în secțiunea următoare.

5.4. Gateway-urile industriale și prelucrarea edge

Gateway-urile industriale și sistemele de procesare la edge asigură legătura dintre echipamentele operaționale și aplicațiile de supraveghere, stocare și analiză. Acestea preiau date din PLC-uri, controlere, senzori inteligenți și sisteme existente, le validează și le transmit către SCADA, MES, baze de date sau servicii cloud.

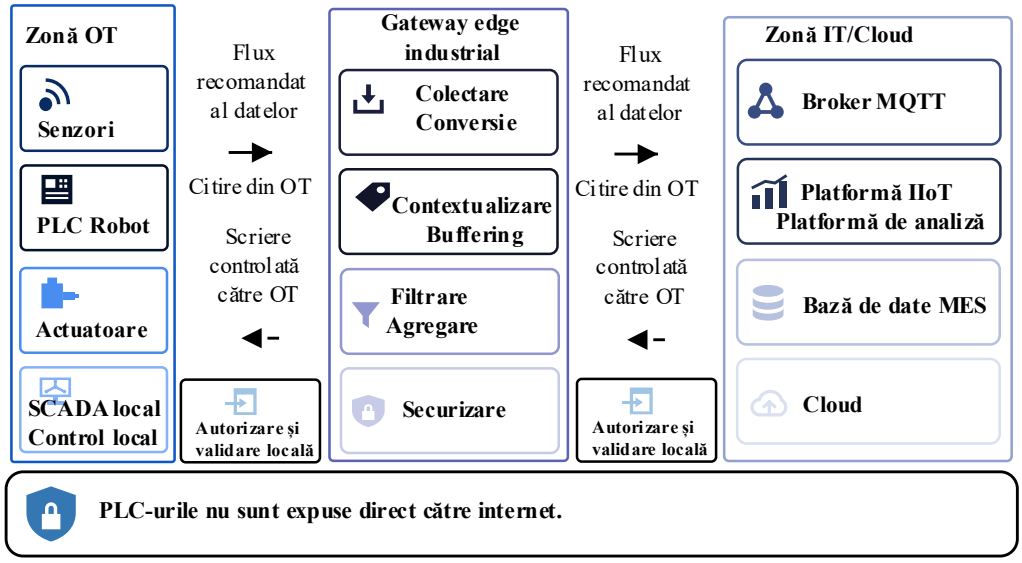


Figura 5.8 – Poziția Gateway-ului între OT și IT

Gateway-ul industrial asigură în principal conectivitatea şi transformarea fluxurilor de date. Procesarea edge adaugă resurse pentru filtrare, stocare temporară, analiză şi executarea unor aplicaţii în apropierea procesului, cu obiectivul declarat de a reduce latenţa şi volumul transferat către infrastructurile centrale [111]. Cele două funcţii pot fi implementate pe echipamente separate sau integrate în acelaşi calculator industrial. Poziţia lor în lanţul de date este reprezentată în Figura 5.8.

Aceste sisteme nu înlocuiesc PLC-ul. Controlul determinist, interblocările şi reacţiile critice trebuie să rămână la nivelul controlerului local. Gateway-ul şi sistemul de procesare la edge pregătesc datele pentru utilizare la nivelurile superioare şi pot genera recomandări ori evenimente, fără a prelua necontrolat funcţiile de automatizare.

5.4.1. Rolul gateway-urilor industriale

Un gateway industrial intermediază schimbul de date dintre echipamente care utilizează protocoale, interfeţe şi modele informaţionale diferite. Acesta poate conecta dispozitive seriale, reţele Ethernet industriale şi servicii informatice, evitând expunerea directă a PLC-urilor către reţele externe [26].

Funcţiile principale ale unui gateway industrial sunt:

- achiziţia datelor din una sau mai multe surse;
- conversia protocoalelor şi a formatelor;
- validarea şi contextualizarea valorilor;
- filtrarea şi agregarea datelor;
- etichetarea şi aplicarea mărcilor temporale;
- stocarea temporară în cazul pierderii conexiunii;
- rutarea şi retransmiterea către aplicaţiile autorizate;
- monitorizarea comunicaţiilor şi raportarea erorilor;
- separarea controlată a reţelelor operaţionale de cele informatice.

Conversia protocoalelor permite integrarea echipamentelor care nu pot comunica direct. De exemplu, un gateway poate citi registre prin Modbus RTU şi le poate expune prin Modbus TCP sau OPC UA. Într-un alt scenariu, poate prelua variabile de la un server OPC UA şi le poate publica prin MQTT către un broker.

Conversia tehnică nu asigură automat şi interoperabilitatea semantică. Un registru numeric trebuie asociat cu denumirea variabilei, echipamentul, unitatea de măsură, domeniul valid, marca temporală şi calitatea semnalului. Fără aceste informaţii, valoarea poate fi transmisă corect, dar interpretată greşit de aplicaţia care o primeşte. Distincţia este esenţială pentru arhitecturile IIoT: un protocol rezolvă transportul, în timp ce modelul informaţional rezolvă înţelegerea, iar cele două nu se substituie [127], [22]. Este exact nivelul semantic al interoperabilităţii, identificat în secţiunea 4.2.2 drept cel mai costisitor atunci când lipseşte, tocmai pentru că erorile lui nu se manifestă la punerea în funcţiune.

Filtrarea opreşte transmiterea datelor care nu ajută la nimic în exploatare. Se pot elimina valorile repetate, variaţiile mici, încadrate într-o bandă stabilită, şi mesajele trimise mai des decât are nevoie aplicaţia. Agregarea calculează valori medii, minime sau maxime, numere de evenimente ori durate de funcţionare.

De exemplu, PLC-ul poate actualiza temperatura unui proces la fiecare 100 ms, în timp ce platforma de analiză primeşte la fiecare zece secunde media, valoarea minimă şi valoarea maximă. Depăşirea unei limite este transmisă imediat ca eveniment, fără a aştepta următorul interval de agregare. Valorile şi perioadele trebuie stabilite în funcţie de dinamica procesului, nu aplicate identic tuturor variabilelor; efectul cantitativ al acestei decizii este calculat în secţiunea 5.4.5.

Etichetarea datelor trebuie să păstreze, atunci când este disponibilă, marca temporală generată la sursă. Dacă aceasta lipseşte, gateway-ul poate adăuga momentul achiziţiei, dar cele două situaţii nu sunt echivalente. Sincronizarea ceasurilor este necesară pentru corelarea alarmelor, comenzilor şi valorilor provenite din echipamente diferite; ea se realizează prin protocolul de timp în reţea, suficient pentru corelarea la nivel de sute de milisecunde [157], sau prin protocolul de timp de precizie, atunci când sunt necesare exactităţi sub o milisecundă [35].

Întreruperea conexiunii cu sistemul superior nu trebuie să conducă automat la pierderea datelor. Prin mecanismul de stocare şi retransmitere (engl. *store-and-forward*), mesajele sunt păstrate local şi expediate după restabilirea comunicaţiei. Fiecare înregistrare trebuie să-şi menţină marca temporală iniţială, iar sistemul receptor trebuie să poată diferenţia datele curente de cele transmise cu întârziere.

Gateway-ul poate contribui la securizarea arhitecturii prin limitarea conexiunilor, autentificarea entităţilor, criptarea comunicaţiilor şi jurnalizarea transferurilor. Acesta nu trebuie însă considerat implicit un echipament de securitate complet. Rolul său corect este cel de punct de trecere controlat între zone cu cerinţe de securitate diferite, definite prin analiza de risc a instalaţiei, nu cel de substitut al segmentării [85]. Funcţiile disponibile, actualizarea software-ului, configurarea serviciilor şi amplasarea în reţea trebuie verificate pentru fiecare implementare.

Un gateway industrial trebuie diferenţiat de un convertor simplu. Convertorul adaptează o interfaţă sau un protocol, în timp ce gateway-ul poate gestiona simultan mai multe surse, poate contextualiza datele, aplica reguli de rutare, păstra temporar mesajele şi comunica securizat cu aplicaţii externe.

5.4.2. Prelucrarea edge

Procesarea edge presupune executarea unor funcţii de calcul şi analiză în apropierea sursei datelor. Echipamentul poate fi amplasat într-un dulap de automatizare, într-o celulă de producţie sau într-o cameră tehnică din fabrică.

La acest nivel pot fi realizate:

- filtrarea şi normalizarea semnalelor;

- calcularea indicatorilor locali;
- detectarea abaterilor şi generarea evenimentelor;
- analiza vibraţiilor şi a consumului energetic;
- prelucrarea imaginilor provenite de la camere industriale;
- stocarea temporară sau păstrarea unui istoric local;
- executarea unor reguli de rutare;
- rularea unor modele de analiză sau învăţare automată;
- gestionarea comunicaţiei cu platformele externe.

Principalul avantaj este reducerea latenţei dintre achiziţia datelor şi obţinerea rezultatului. O aplicaţie locală poate identifica o abatere şi transmite imediat un eveniment către PLC sau către operator, fără a aştepta transferul către o platformă externă. Totuşi, amplasarea unei aplicaţii la edge nu garantează un comportament determinist: sistemele de operare de uz general, containerele şi mediile interpretate introduc variabilitate care nu poate fi limitată superior. Funcţiile cu cerinţe temporale stricte şi cele de siguranţă trebuie executate de controlere proiectate şi validate pentru aceste scopuri [111].

Procesarea locală reduce şi volumul transmis. În cazul monitorizării vibraţiilor, semnalul brut poate avea o frecvenţă de eşantionare de ordinul kilohertzilor şi poate genera un volum imposibil de transmis continuu. Sistemul local poate calcula indicatori, extrage componentele spectrale şi transmite doar rezultatele, alertele sau intervalele de semnal relevante. Datele brute pot fi păstrate temporar pentru analiza detaliată a unui eveniment.

Un alt avantaj este continuitatea operaţională. Aplicaţiile locale pot continua achiziţia şi prelucrarea datelor în timpul întreruperii conexiunii cu platforma centrală. După restabilirea legăturii, rezultatele sunt sincronizate, fără ca funcţionarea procesului să fi depins permanent de disponibilitatea unei conexiuni externe.

Păstrarea locală a datelor poate limita expunerea informaţiilor sensibile şi traficul dintre reţele. Aceasta nu elimină însă riscurile de securitate. Echipamentul aflat la edge trebuie administrat, actualizat şi monitorizat. Accesul fizic, conturile implicite, serviciile neutilizate, aplicaţiile instalate şi certificatele expirate pot transforma sistemul într-un punct vulnerabil [25]. Suprafaţa de atac a acestui nivel este, în practică, mai mare decât a PLC-ului pe care îl deserveşte, deoarece rulează software de uz general, are conectivitate în ambele direcţii şi este adesea administrat de o echipă diferită de cea care răspunde de automatizare.

Aplicaţiile pot fi instalate direct în sistemul de operare sau pot rula în containere izolate. Utilizarea containerelor simplifică distribuirea şi actualizarea aplicaţiilor, dar necesită controlul imaginilor software, al resurselor alocate şi al comunicaţiilor permise. Actualizarea unei aplicaţii nu trebuie să afecteze funcţiile locale necesare menţinerii fluxului de date.

Instrumentele de compunere vizuală a fluxurilor pot fi utilizate pentru construirea lanțurilor de achiziție, transformare și transmitere. Acestea sunt potrivite pentru integrare, prototipare și aplicații de monitorizare, dar nu trebuie utilizate pentru înlocuirea nejustificată a logicii deterministe din PLC.

5.4.3. Delimitarea dintre prelucrarea edge, fog și cloud

Procesarea edge, procesarea distribuită în proximitatea instalației (*fog computing*) și serviciile *cloud* reprezintă niveluri complementare. Modelul fog a fost formulat tocmai pentru aplicațiile care nu tolerează latența și dependența unei arhitecturi exclusiv centralizate, dar care depășesc resursele disponibile lângă echipament [158]. Delimitarea dintre edge și fog nu este uniformă în toate arhitecturile, însă termenul edge indică, de regulă, procesarea foarte apropiată de echipament, iar fog descrie resurse distribuite la nivelul unei zone, al unei linii sau al întregii fabrici. Cloud desemnează, în accepțiunea consacrată, un model de acces la resurse de calcul partajate, configurabile la cerere și eliberate rapid, indiferent dacă infrastructura este publică sau proprie [159]. Compararea celor trei niveluri este prezentată în Tabelul 5.6.

Distribuirea funcțiilor trebuie realizată în funcție de latența admisă, volumul datelor, necesitatea funcționării autonome, resursele disponibile și consecințele pierderii comunicației. Procesarea nu trebuie transferată către cloud doar pentru că există conectivitate și nici păstrată integral la edge dacă resursele locale nu permit administrarea și analiza necesare.

Tabelul 5.6 – Compararea nivelurilor edge, fog și cloud

Criteriu	Edge	Fog	Cloud
Amplasare	În apropierea echipamentului sau celulei	La nivelul unei zone, linii ori fabrici	Într-un centru de date local sau extern
Funcții dominante	Achiziție, filtrare, reacție locală și analiză rapidă	Corelarea datelor din mai multe sisteme și coordonarea serviciilor locale	Stocare extinsă, analiză complexă și integrarea mai multor amplasamente
Volumul datelor	Date detaliate și evenimente locale	Date agregate provenite de la mai multe surse	Volume mari și istorice pe perioade îndelungate
Dependența de comunicații	Poate funcționa temporar fără conexiune externă	Necesită conectivitate în interiorul amplasamentului	Depinde de legătura cu centrul de date
Orizont temporal	Milisecunde, secunde sau minute, în funcție de aplicație	Minute, ore și coordonare operațională	Analize istorice, tendințe și planificare
Exemple	Filtrarea semnalelor, analiza vibrațiilor și inspecția vizuală	Agregarea datelor unei linii și servicii comune pentru mai multe celule	Analiza comparativă între fabrici și antrenarea modelelor complexe

Un model echilibrat integrează nivelurile într-un ansamblu funcţional, în care controlul local este realizat în PLC, filtrarea şi analiza rapidă au loc la edge, corelarea datelor se desfăşoară la nivelul fabricii, iar stocarea şi analiza extinsă sunt realizate în cloud.

Această distribuire permite păstrarea reacţiilor critice aproape de proces şi transferarea analizelor complexe către infrastructuri cu resurse mai mari.

5.4.4. Proiectarea unui flux de date printr-un gateway industrial

Un flux minimal poate utiliza un server OPC UA ca sursă de date şi protocolul MQTT pentru transmiterea acestora către sistemele superioare. Datele provenite de la PLC sau de la serverul OPC UA sunt preluate de un gateway industrial şi transmise printr-un broker MQTT către o aplicaţie de stocare, analiză ori vizualizare; vezi Figura 5.9.

În acest flux, gateway-ul execută succesiv:

1. conectarea autorizată la serverul OPC UA;
2. selectarea variabilelor necesare;
3. citirea prin interogare periodică sau abonare;
4. verificarea valorii, tipului şi calităţii semnalului;
5. asocierea identificatorului echipamentului, unităţii şi mărcii temporale;
6. filtrarea, agregarea sau transformarea valorii;
7. construirea mesajului şi asocierea subiectului MQTT;
8. păstrarea temporară în cazul indisponibilităţii conexiunii;
9. publicarea securizată şi confirmarea transmiterii;
10. jurnalizarea erorilor şi a stării fluxului.

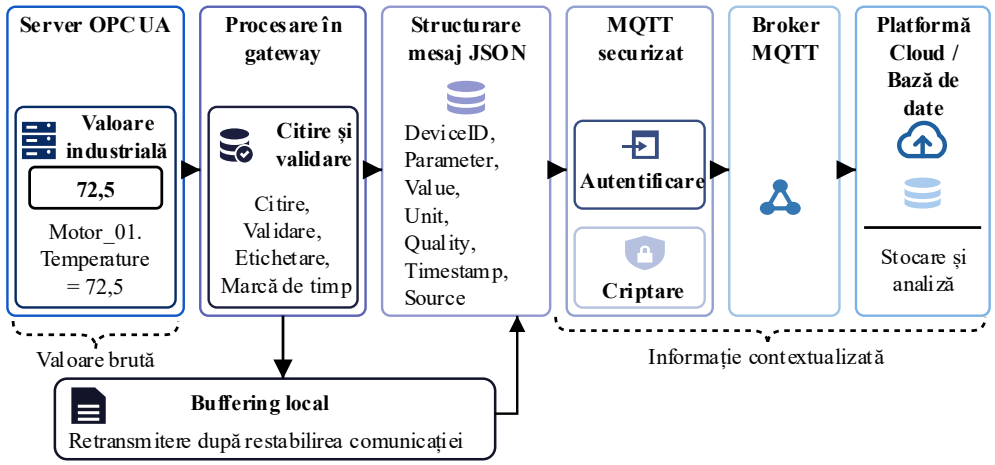


Figura 5.9 – Flux minimal OPC UA - Gateway edge - MQTT – Cloud

Selectarea variabilelor trebuie realizată explicit. Preluarea tuturor nodurilor disponibile poate încărca PLC-ul, rețeaua și sistemul receptor fără a produce informații utile. Pentru fiecare variabilă trebuie stabilite frecvența de achiziție, condiția de transmitere, perioada de păstrare și aplicația care o utilizează.

Mesajul construit la pasul 7 trebuie să fie autosuficient: aplicația receptoare nu are acces la configurația PLC-ului și nu poate deduce unitatea, domeniul sau starea semnalului. Un payload minimal contextualizat, în format JSON, are forma:

```
{
  "deviceId": "L1-MOT-01",
  "metric": "temperatura_stator",
  "value": 72.4,
  "unit": "degC",
  "ts": "2026-03-17T09:41:22.350Z",
  "tsSource": "plc",
  "quality": "good",
  "seq": 48213
}
```

Câmpul *ts* păstrează marca temporală a măsurării, iar *tsSource* arată dacă aceasta provine de la sursă sau a fost adăugată de gateway – distincția necesară pentru interpretarea corectă a datelor retransmise după o întrerupere. Câmpul quality transportă starea de validitate a semnalului, iar seq permite receptorului să identifice ordinea și să elimine duplicatele produse prin retransmitere. Denumirile câmpurilor din acest exemplu sunt proprii exercițiului; convenția de referință pentru subiectele MQTT și pentru structura mesajului este stabilită în secțiunea 6.2.8, iar mecanismele protocolului sunt tratate în secțiunea 6.2.

Fluxul trebuie să diferențieze valorile periodice de evenimente. Temperatura sau consumul pot fi transmise periodic, în timp ce o alarmă, schimbarea modului de funcționare ori oprirea unui echipament trebuie publicate imediat.

Pentru comenzile transmise în sens invers trebuie utilizat un traseu separat și controlat. Gateway-ul trebuie să accepte numai comenzile autorizate și să le transmită către PLC împreună cu informațiile necesare validării. PLC-ul verifică starea procesului, limitele și interblocările înainte de aplicare și transmite confirmarea rezultatului. O comandă provenită dintr-o aplicație externă nu trebuie să modifice direct o ieșire fizică și nu trebuie să ocolească logica locală.

Selectarea echipamentului de tip gateway sau edge trebuie să țină seama de:

- interfețele și protocoalele necesare;
- volumul și frecvența datelor;
- puterea de procesare și memoria disponibile;
- capacitatea de stocare temporară;
- condițiile de temperatură, vibrații și alimentare;
- posibilitatea sincronizării timpului;
- mecanismele de autentificare și criptare;
- administrarea certificatelor și actualizărilor;

- monitorizarea de la distanță și păstrarea jurnalelor;
- comportamentul la pierderea comunicației sau alimentării;
- durata de viață și disponibilitatea suportului tehnic.

5.4.5. Dimensionarea cantitativă a fluxului de date

Deciziile descrise în secțiunile anterioare – intervalul de publicare, gruparea mesajelor, banda moartă, frecvența de scriere în baza de date – sunt de obicei luate implicit, prin acceptarea valorilor implicite ale instrumentelor. Cele două calcule de mai jos arată ce anume determină aceste valori și de ce o alegere aparent tehnică decide, în fapt, atât reactivitatea tabloului de bord, cât și costul de stocare al instalației.

Bugetul de latență. Se consideră lanțul senzor, PLC, gateway industrial, broker MQTT, bază de date de serii temporale, cu ipotezele: PLC cu timp de scanare 10 ms; expunerea variabilelor prin OPC UA cu abonare și interval de publicare 100 ms; gateway și broker amplasate în aceeași rețea locală comutată de 1 Gbit/s; publicare MQTT cu calitatea serviciului 1; scriere în baza de date în loturi acumulate la 100 ms. Rezultatele sunt prezentate în Tabelul 5.7.

Interpretare. Latența tipică de la modificarea mărimii fizice până la disponibilitatea valorii pentru interogare este de aproximativ 0,13 s, iar în cazul cel mai defavorabil 0,30 s. Contribuția dominantă nu provine din rețea sau din procesor, ci din două decizii de configurare: intervalul de publicare al abonării OPC UA și acumularea în loturi la scriere, care împreună reprezintă 100 ms din 131 ms în regim tipic. Reducerea intervalului de publicare la 20 ms coboară totalul tipic la aproximativ 91 ms, cu prețul creșterii proporționale a numărului de mesaje – compromis cuantificat în calculul următor. Bugetul confirmă totodată delimitarea din secțiunea 5.4.2: un lanț de această structură este adecvat pentru supraveghere, raportare și mentenanță, dar nu poate susține o funcție de control cu cerință de reacție sub 100 ms, care rămâne în PLC.

Tabelul 5.7 – Bugetul de latență pe lanțul senzor–PLC–gateway–broker–bază de date

Segment	Ipoteza dominantă	Tipic (ms)	Maxim (ms)
Senzor și condiționarea semnalului	Transmițător 4–20 mA, constantă de timp 5 ms	5	15
Achiziție în PLC	Filtru 3 ms, conversie 1 ms, un ciclu de scanare	14	24
Expunere OPC UA și preluare de gateway	Abonare, interval de publicare 100 ms	50	100
Prelucrare în gateway	Validare, contextualizare, serializare	5	15
Transport gateway – broker	LAN comutat 1 Gbit/s, o treaptă, TLS	2	10
Broker MQTT	Recepție, rutare, livrare cu confirmare	5	20
Consumator și scriere în baza de date	Acumulare în loturi la 100 ms	50	120
Total		131	304

Limite. Însumarea valorilor maxime este conservatoare: probabilitatea ca toate segmentele să atingă simultan cazul cel mai defavorabil este redusă, dar dimensionarea unei cerințe contractuale se face pe acest bord superior, nu pe medie. Bugetul nu include legătura către servicii cloud, care adaugă latența rețelei de arie largă și variația acesteia, și nu modelează comportamentul în saturație: la depășirea capacității brokerului sau a bazei de date, întârzierea nu crește proporțional, ci prin acumulare în cozi, cu creșteri de ordinul secundelor. Valorile trebuie înlocuite cu cele măsurate în instalația reală; bugetul are rolul de a arăta unde merită făcută măsurarea, nu de a o înlocui.

Necesarul de lățime de bandă

Se consideră o linie cu 250 de variabile monitorizate: 200 lente, transmise la 1 Hz, și 50 rapide, transmise la 10 Hz. Se utilizează payloadul JSON prezentat în secțiunea 5.4.4, cu lungimea de aproximativ 130 de octeți, publicat prin MQTT cu subiect de circa 45 de caractere. Se estimează suplimentar 51 de octeți antet MQTT (inclusiv subiectul), 29 de octeți supraîncărcare TLS și 58 de octeți antete TCP/IP și Ethernet, deci aproximativ 270 de octeți transmiși efectiv pentru fiecare mesaj individual.

Scenariul A – un mesaj pentru fiecare variabilă:

$$nA = 200 \cdot 1 + 50 \cdot 10 = 700 \text{ mesaje/s}$$

$$DA = 700 \cdot 270 = 189.000 \text{ octeți/s} \approx 1{,}51 \text{ Mbit/s} \approx 16{,}3 \text{ GB/zi}$$

Scenariul B – grupare: cele 200 de variabile lente într-un singur mesaj pe secundă, cele 50 rapide în câte un mesaj la 100 ms. Într-un mesaj grupat, identificatorul echipamentului, marca temporală și antetele nu se repetă, iar fiecărei variabile îi revin aproximativ 55 de octeți:

$$DB = (200 \cdot 55 + 140) \cdot 1 + (50 \cdot 55 + 140) \cdot 10 = 11.140 + 28.900 \approx 40.000 \text{ octeți/s}$$

$$DB \approx 0{,}32 \text{ Mbit/s} \approx 3{,}5 \text{ GB/zi}$$

Scenariul C – grupare și transmitere la excepție, cu bandă moartă aplicată variabilelor lente, dintre care în medie 10 % se modifică semnificativ într-un interval, și cu păstrarea transmiterii periodice pentru cele rapide:

$$DC \approx (20 \cdot 55 + 140) + 28.900 \approx 30.140 \text{ octeți/s} \approx 0{,}24 \text{ Mbit/s} \approx 2{,}6 \text{ GB/zi}$$

Interpretare. Într-o rețea locală de 1 Gbit/s, niciunul dintre cele trei scenarii nu constituie o problemă de lățime de bandă – sub 0,2 % din capacitate în cazul cel mai încărcat. Constrângerea reală este în altă parte: volumul stocat, numărul de mesaje pe secundă pe care brokerul și baza de date trebuie să le proceseze și, mai ales, legătura către exterior. Pe o conexiune de arie largă de 10 Mbit/s cu 50 % capacitate utilizabilă, scenariul A ocupă permanent circa 30 % din bandă pentru o singură linie de producție, în timp ce scenariul B ocupă 6 %. Gruparea mesajelor reduce volumul de aproximativ 4,7 ori fără nicio pierdere de informație, iar transmiterea la excepție adaugă o reducere suplimentară cu preț informațional real: valorile stabile nu mai sunt confirmate periodic, iar receptorul nu poate distinge o variabilă neschimbată de o sursă oprită dacă nu se păstrează un mesaj periodic de viață. Diferența dintre A și B nu este de tehnologie, ci de configurare, și explică de ce două instalații identice pot avea costuri de stocare care diferă cu un ordin de mărime.

Limite. Estimarea nu include retransmisiile, mesajele de menţinere a conexiunii, renegocierile TLS şi traficul de administrare. Lungimea antetului depinde direct de convenţia de denumire a subiectelor: o ierarhie prea detaliată poate depăşi singură dimensiunea payloadului. Formatul JSON a fost ales pentru lizibilitate; codificările binare reduc substanţial volumul la acelaşi conţinut informaţional, iar compararea lor este realizată în secţiunea 6.2. Cifrele nu descriu volumul stocat efectiv, deoarece bazele de date de serii temporale aplică propria compresie.

Gateway-urile industriale şi procesarea la edge transformă datele generate de automatizare într-un flux contextualizat, controlat şi dimensionat conştient. Valorile astfel pregătite sunt preluate de sistemele HMI şi SCADA pentru reprezentarea procesului, gestionarea alarmelor şi sprijinirea operatorilor, funcţii analizate în secţiunea următoare.

5.5. Sisteme SCADA și interfețe om–mașină

Sistemele de control de supraveghere şi achiziţie de date (*SCADA*) permit monitorizarea centralizată şi coordonarea operaţională a proceselor industriale. Acestea colectează date de la PLC-uri, unităţi terminale la distanţă, echipamente electronice inteligente şi alte surse, le contextualizează şi le prezintă operatorilor prin interfeţe om–maşină [25].

Interfaţa om–maşină (*HMI*) reprezintă componenta prin care operatorul urmăreşte starea instalaţiei, analizează alarmele, introduce parametri şi transmite comenzile permise. Aceasta poate fi implementată sub forma unui panou local, a unei staţii de operare, a unei aplicaţii pentru calculator sau a unei interfeţe web.

Un panou HMI poate comunica direct cu un PLC şi poate funcţiona fără o infrastructură SCADA. Sistemul SCADA are un domeniu mai extins: agregă date provenite de la mai multe controlere, gestionează utilizatori şi alarme, păstrează istoricul procesului şi poate furniza informaţii către MES, aplicaţii de mentenanţă şi platforme IIoT. În modelul ierarhic al integrării întreprinderii, aceste funcţii aparţin nivelului de supraveghere, distinct atât de controlul de proces, cât şi de sistemele de gestiune a operaţiunilor de producţie [75].

Poziţia sa în arhitectura de automatizare poate fi descrisă printr-un lanţ funcţional care porneşte de la proces, continuă cu senzorii şi actuatoarele, PLC-ul sau unitatea terminală la distanţă şi reţeaua industrială şi ajunge la serverul SCADA. Acesta asigură legătura cu interfeţele HMI, funcţiile de alarmare şi de păstrare a istoricului, precum şi cu sistemele superioare.

Arhitectura rezultată este reprezentată în Figura 5.10.

SCADA realizează controlul de supraveghere, nu controlul determinist al procesului. Interblocările, reglajele rapide şi funcţiile de siguranţă trebuie să rămână în PLC sau în controlerele locale. Pierderea serverului SCADA ori a unei staţii HMI nu trebuie să determine pierderea necontrolată a funcţiilor esenţiale ale instalaţiei.

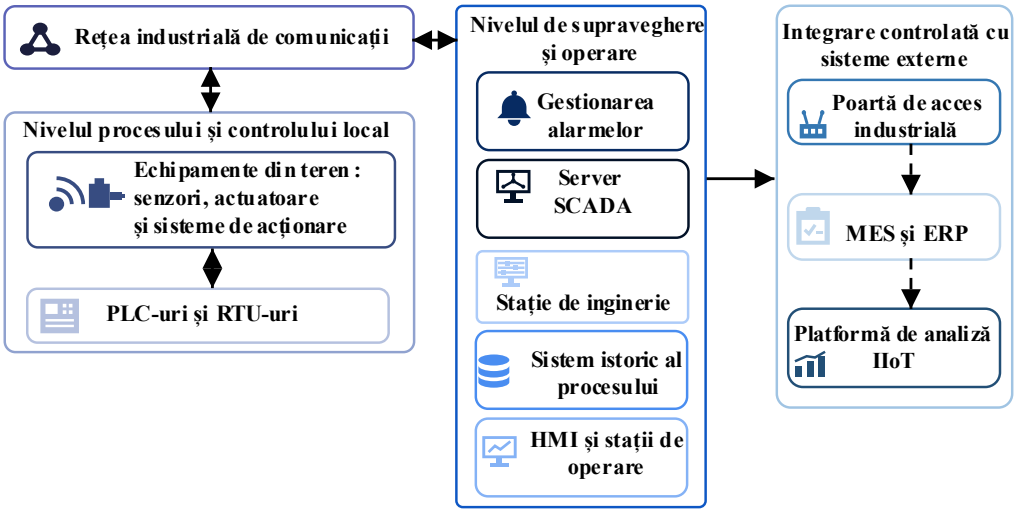


Figura 5.10 – Arhitectura generală a unui sistem SCADA

5.5.1. Funcțiile unui sistem SCADA

Funcţionarea unui sistem SCADA poate fi organizată în patru categorii principale: achiziţia datelor, reprezentarea procesului, gestionarea alarmelor şi controlul de supraveghere, sintetizate în Tabelul 5.8.

Achiziţia datelor presupune stabilirea unei conexiuni cu sursa, identificarea variabilelor şi actualizarea valorilor acestora. Datele pot fi citite periodic, preluate la schimbarea valorii sau primite sub forma unor evenimente. Metoda trebuie aleasă în funcţie de dinamica procesului şi de importanţa variabilei, iar consecinţele cantitative ale acestei alegeri au fost calculate în secţiunea 5.4.5.

Citirea periodică este potrivită pentru valori care evoluează continuu, precum temperatura sau presiunea. Transmiterea la schimbare reduce traficul pentru stări binare şi variabile relativ stabile. Alarmele şi modificările importante ale modului de funcţionare trebuie transmise imediat, fără a depinde exclusiv de următorul ciclu de citire [25].

Tabelul 5.8 – Funcțiile principale ale unui sistem SCADA

Funcție	Conținut	Rezultat operațional
Achiziția datelor	Preluarea valorilor, stărilor, alarmelor și informațiilor de diagnosticare de la PLC-uri și echipamentele din câmp	Imagine actualizată și contextualizată a procesului
Reprezentarea procesului	Afișarea valorilor, stărilor, tendințelor și relațiilor tehnologice prin interfețe HMI	Înțelegerea rapidă a situației operaționale
Gestionarea alarmelor	Detectarea, prioritizarea, afișarea, confirmarea și păstrarea condițiilor anormale	Identificarea abaterilor și sprijinirea intervenției operatorului
Controlul de supraveghere	Transmiterea comenzilor, valorilor de referință, rețetelor și modurilor de funcționare către controlere	Coordonarea procesului în limitele validate local

Pentru fiecare variabilă, sistemul SCADA trebuie să păstreze cel puțin:

- identificatorul și denumirea;
- sursa și adresa de comunicație;
- tipul de date;
- politica de arhivare;
- valoarea și unitatea de măsură;
- marca temporală;
- starea de calitate sau validitate; limitele de alarmare;
- drepturile de citire și scriere.

O valoare fără informații privind calitatea nu trebuie prezentată operatorului ca fiind certă. Protocoalele industriale moderne transportă explicit această informație: OPC UA asociază fiecărei valori un cod de stare care distinge valorile bune de cele incerte și de cele nevalide, iar aplicația receptoare este obligată să îl interpreteze, nu să îl ignore [127]. La pierderea comunicației, interfața trebuie să diferențieze explicit valoarea neactualizată de una validă. Păstrarea ultimei valori fără indicarea întreruperii este una dintre cele mai periculoase erori de configurare a unui sistem de supraveghere, deoarece produce o imagine falsă asupra procesului fără niciun semn vizibil pentru operator.

Reprezentarea datelor transformă variabilele tehnice în informații utilizabile. Operatorul nu trebuie să urmărească numai valori izolate, ci și relațiile dintre echipamente, sensul fluxului tehnologic, modul de funcționare, comenzile active și condițiile care împiedică executarea unei acțiuni. Obiectivul nu este afișarea datelor, ci construirea conștientizării situației: perceperea elementelor relevante, înțelegerea semnificației lor în contextul curent și anticiparea evoluției imediate [160].

Controlul de supraveghere poate include pornirea sau oprirea unei instalații, selectarea unei rețete, modificarea unei valori de referință ori schimbarea modului de lucru. Comanda este transmisă către PLC, iar acesta verifică interblocările și condițiile locale înainte de aplicare. Sistemul SCADA nu trebuie să scrie direct în ieșirile fizice și nu trebuie să ocolească logica validată a controlerului.

În contextul SCADA, expresia „*în timp real*" indică actualizarea suficient de rapidă pentru supravegherea procesului. Aceasta nu presupune automat un timp de răspuns determinist. Viteza efectivă depinde de PLC, rețea, frecvența achiziției, încărcarea serverului și modul de actualizare a interfețelor; bugetul din Tabelul 5.7 arată ordinul de mărime rezultat dintr-un lanț tipic.

5.5.2. Arhitectura unui sistem SCADA

Un sistem SCADA cuprinde trei componente funcționale majore:

- echipamentele de control și achiziție din câmp;
- rețeaua de comunicații;
- centrul de control.

Echipamentele din câmp includ PLC-uri, unități terminale la distanță, controlere dedicate și dispozitive electronice inteligente. Acestea achiziționează semnalele,

execută controlul local și furnizează către SCADA valorile, stările, alarmele și informațiile de diagnosticare.

Unitățile terminale la distanță sunt utilizate frecvent în instalații distribuite geografic, precum rețelele de alimentare cu apă, transportul și distribuția energiei sau infrastructurile de conducte [161]. Acestea trebuie să poată continua funcționarea locală și în perioadele în care legătura cu centrul de control este indisponibilă.

Rețeaua de comunicații asigură transferul datelor dintre echipamentele distribuite și centrul de control. În funcție de instalație, aceasta poate include rețele Ethernet industriale, legături seriale, fibră optică, comunicații radio și conexiuni prin infrastructuri de telecomunicații. Arhitectura trebuie să ia în considerare lățimea de bandă, latența, redundanța, distanța, condițiile de mediu și securitatea [153].

Centrul de control poate include:

- unul sau mai multe servere SCADA;
- stații HMI pentru operatori;
- stații de inginerie;
- servere de comunicație;
- servere de date istorice;
- servicii de alarmare și raportare;
- sisteme pentru autentificare și administrarea utilizatorilor;
- interfețe către MES și alte aplicații.

Serverul SCADA gestionează conexiunile cu sursele, baza de variabile, stările de comunicație, alarmele și distribuirea datelor către clienți. Într-o arhitectură redusă, toate funcțiile pot fi instalate pe același calculator. În sistemele extinse, funcțiile sunt distribuite între mai multe servere.

Stația de inginerie este utilizată pentru configurarea variabilelor, proiectarea ecranelor, definirea alarmelor, elaborarea rapoartelor și gestionarea aplicației. Accesul acesteia trebuie separat de operarea curentă, deoarece modificările de configurare pot afecta întregul sistem. Separarea nu este doar organizatorică: ea constituie o cerință explicită de securitate privind limitarea funcțiilor la cele necesare rolului și restricționarea utilizării interfețelor de programare [68].

Pentru instalațiile la care indisponibilitatea SCADA ar afecta semnificativ operarea pot fi utilizate servere redundante. Un server activ gestionează funcțiile curente, iar unul de rezervă menține datele și configurația sincronizate. Trecerea la serverul de rezervă trebuie testată periodic, deoarece existența fizică a două servere nu garantează recuperarea corectă a conexiunilor, alarmelor și arhivelor.

Redundanța trebuie analizată pentru întregul traseu. Două servere conectate printr-un singur comutator, alimentate din aceeași sursă sau dependente de aceeași bază de date păstrează puncte comune de defectare. Pot fi necesare rețele, surse de alimentare și căi de comunicație redundante – iar dacă redundanța nu poate fi extinsă la întregul traseu, comportamentul instalației la pierderea supravegherii trebuie definit explicit, nu presupus.

5.5.3. Delimitarea dintre PLC, SCADA şi Historian

PLC-ul, sistemul SCADA şi serverul de date istorice (*historian*) utilizează aceleaşi variabile ale procesului, dar îndeplinesc funcţii diferite. Confuzia dintre ele este frecventă în specificaţiile de achiziţie şi conduce fie la sisteme SCADA solicitate să garanteze determinism, fie la arhive construite pe un server de operare. Delimitarea funcţională este prezentată în Tabelul 5.9.

Serverul de date istorice este optimizat pentru stocarea seriilor temporale industriale. Acesta poate păstra valori cu frecvenţe diferite, evenimente, alarme şi informaţii privind calitatea datelor. În funcţie de arhitectură, funcţia poate fi integrată în SCADA sau furnizată de un sistem separat.

SCADA utilizează istoricul pentru afişarea tendinţelor şi generarea rapoartelor, dar nu trebuie confundat cu acesta. Serverul de date istorice poate deservi mai multe sisteme şi poate furniza date către aplicaţii de analiză fără a participa la operarea directă a procesului.

Dacă achiziţia către serverul de date istorice este întreruptă, valorile pot fi păstrate temporar în serverul SCADA, în gateway-ul industrial sau în echipamentul sursă. După restabilirea conexiunii, datele trebuie retransmise cu marca temporală originală, fără a fi confundate cu valorile curente – mecanismul de stocare şi retransmitere descris în secţiunea 5.4.1 şi câmpurile de mesaj care îl fac posibil, prezentate în secţiunea 5.4.4.

Tabelul 5.9 – Delimitarea dintre PLC, SCADA și serverul de date istorice

Criteriu	**PLC**	**SCADA**	**Server de date istorice**
Rol principal	Controlul local al procesului	Supravegherea și coordonarea operațională	Păstrarea și interogarea datelor în timp
Orizont temporal	Milisecunde și secunde	Secunde, minute și durata schimbului de lucru	Zile, luni sau ani
Funcții dominante	Logică, reglare, secvențe și interblocări	Vizualizare, alarme, comenzi și raportare	Arhivare, compresie, tendințe și analiză
Tipul datelor	Valori curente și stări interne	Valori curente, alarme și context operațional	Serii temporale, evenimente și metadate
Dependența procesului	Poate fi esențial pentru funcționare	Procesul trebuie să poată adopta o stare definită dacă SCADA devine indisponibil	Pierderea temporară nu trebuie să afecteze controlul local
Utilizatori principali	Ingineri de automatizare și personal de mentenanță	Operatori, supervizori și ingineri de proces	Ingineri de proces, mentenanță, calitate și analiză
Comenzi către proces	Direct, prin ieșiri și rețele de câmp	Indirect, prin cereri validate de PLC	În mod obișnuit, nu transmite comenzi

Un aspect frecvent trecut cu vederea este compresia. Serverele de date istorice aplică, de regulă, algoritmi cu pierdere care păstrează numai punctele necesare reconstruirii curbei într-o bandă de toleranţă configurată. Banda respectivă trebuie

stabilită per variabilă, în raport cu utilizarea ulterioară a datelor: o toleranță potrivită pentru raportarea consumului poate elimina exact vârfurile scurte care ar fi permis analiza unui incident.

5.5.4. Interfețele HMI

Interfața HMI trebuie să sprijine operatorul în identificarea stării procesului, a abaterilor și a acțiunilor permise. Calitatea acesteia nu este determinată de numărul animațiilor sau de complexitatea graficii, ci de rapiditatea și corectitudinea cu care informația poate fi interpretată. Proiectarea interfețelor de operare a devenit obiectul unui standard dedicat, care tratează ciclul de viață complet – filozofia de proiectare, stilul, implementarea, exploatarea și modificarea [162].

Interfețele HMI pot fi clasificate în:

- panouri locale montate pe utilaje sau dulapuri;
- stații de operare pentru linii și zone de producție;
- console pentru camere de control;
- interfețe web pentru supraveghere autorizată;
- aplicații mobile destinate unor activități limitate de monitorizare sau mentenanță.

Panoul local este utilizat pentru operarea unui echipament sau a unei celule. Stația SCADA oferă o vedere mai largă și poate coordona mai multe instalații. Interfața web facilitează accesul de la distanță, dar trebuie să respecte aceleași reguli de autorizare și validare a comenzilor.

Ecranele trebuie organizate într-o structură ierarhică, de la imaginea generală a fabricii sau a instalației la ecranul zonei ori al liniei și, ulterior, la ecranul echipamentului. Această structură este completată de ecrane dedicate detaliilor, diagnosticării, alarmelor și tendințelor.

Imaginea generală trebuie să permită identificarea rapidă a zonei cu abatere. Ecranul de proces prezintă fluxul tehnologic și relațiile dintre echipamente. Ecranul de diagnosticare oferă informații suplimentare privind senzori, actuatoare, comunicații și condițiile care împiedică funcționarea. O aplicare concretă a acestei ierarhii, la nivelul ecranului de echipament, este realizată în secțiunea 5.6.2 și reprezentată în Figura 5.11.

Proiectarea trebuie să respecte principii de vizibilitate, consecvență și claritate a informațiilor. Informațiile importante trebuie amplasate în zone vizibile și menținute în aceeași poziție pe ecrane similare, iar denumirile, simbolurile și unitățile de măsură trebuie utilizate consecvent. Culorile intense trebuie rezervate abaterilor, alarmelor și selecțiilor, în timp ce starea normală trebuie reprezentată discret, pentru a evidenția situațiile anormale. Semnalarea stărilor critice trebuie să asocieze culorii un text, un simbol sau o formă. Valorile trebuie afișate împreună cu unitățile de măsură și, unde este util, cu domeniul normal, iar animațiile trebuie

utilizate exclusiv pentru transmiterea informaţiilor necesare. Navigarea între imaginea generală şi detaliul echipamentului trebuie să fie directă. Comenzile incompatibile trebuie blocate, cu posibilitatea identificării cauzei blocării, iar acţiunile cu efect important trebuie să necesite confirmare şi să fie jurnalizate.

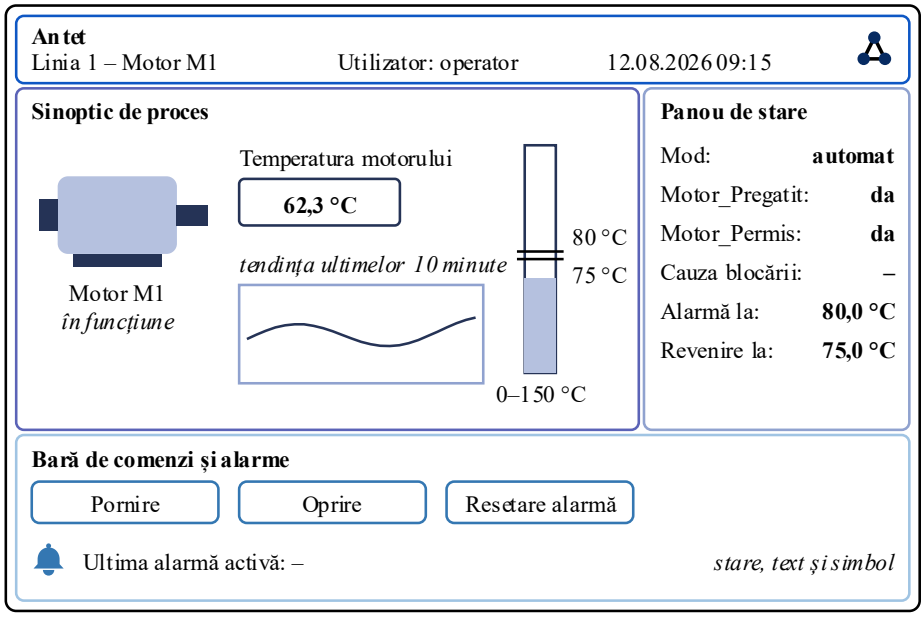


Figura 5.11 – Structura ecranului de operare pentru monitorizarea unui motor (exemplu)

Primele patru principii formează împreună ceea ce literatura de specialitate numeşte interfaţă cu contrast redus: fondul ecranului este neutru, echipamentele în stare normală sunt desenate în tonuri de gri, iar culoarea saturată apare exclusiv acolo unde există o abatere care necesită atenţie [47]. Rezultatul contrazice aşteptarea intuitivă a unui ecran „bogat”, dar reduce semnificativ timpul necesar identificării unei anomalii. Regula de a nu semnala o stare critică numai prin culoare nu este o preferinţă stilistică: codificarea informaţiei trebuie să folosească cel puţin două atribute distincte, atât pentru accesibilitate, cât şi pentru condiţiile reale de iluminare din hală [163].

Afişarea unui echipament în culoarea verde nu trebuie interpretată automat ca dovadă a funcţionării. Interfaţa trebuie să diferenţieze între comanda emisă, confirmarea primită şi starea reală. Pentru un motor pot fi prezentate separat cererea de pornire, contactorul activ, viteza măsurată şi existenţa unei alarme.

Introducerea parametrilor trebuie limitată prin domenii validate. Dacă operatorul încearcă să introducă o valoare în afara limitelor permise, interfaţa trebuie să refuze transmiterea şi să indice intervalul acceptat. Limitele finale sunt verificate şi în PLC, deoarece HMI nu reprezintă singurul nivel de protecţie.

Drepturile trebuie stabilite în funcție de rol. Un operator poate porni și opri instalația în condițiile permise, un supervizor poate valida anumite modificări, iar un inginer poate modifica parametri tehnologici autorizați. Configurarea aplicației și administrarea conturilor necesită drepturi distincte, iar acțiunile cu efect asupra procesului trebuie jurnalizate cu identificarea utilizatorului și a momentului [68].

5.5.5. Alarme, evenimente și date istorice

O alarmă semnalează o condiție care necesită atenția sau intervenția operatorului. Un eveniment consemnează apariția unei modificări, fără ca aceasta să impună neapărat o reacție. Pornirea unui motor este un eveniment, în timp ce declanșarea protecției sale reprezintă o alarmă. Definiția normativă adaugă un criteriu care elimină majoritatea alarmelor inutile dintr-un sistem: o alarmă presupune existența unei acțiuni pe care operatorul o poate întreprinde și a unui interval în care aceasta trebuie întreprinsă [46].

Pentru fiecare alarmă trebuie definite:

- sursa și condiția de activare;
- mesajul afișat;
- prioritatea;
- momentul apariției;
- acțiunea așteptată;
- condiția de revenire;
- dreptul de confirmare;
- informațiile necesare diagnosticării.

Mesajul trebuie să descrie concret problema. Formularea „*Eroare motor transportor 2 – protecție declanșată*" este mai utilă decât „*Avarie sistem*". Dacă sunt cunoscute, interfața poate indica verificările recomandate, fără a substitui procedurile de mentenanță și siguranță.

Confirmarea unei alarme arată că operatorul a observat-o; nu înseamnă că problema a fost eliminată. Interfața trebuie să diferențieze între alarmă activă neconfirmată, alarmă activă confirmată și alarmă revenită la normal. Aceste stări fac parte dintr-un ciclu de viață definit al alarmei, care include suplimentar stările de suprimare și de scoatere din serviciu, ambele necesare pentru mentenanță și ambele obligatoriu jurnalizate [46].

Prioritățile trebuie asociate cu impactul asupra siguranței, mediului, producției și echipamentului. Utilizarea aceleiași priorități pentru un număr mare de alarme împiedică operatorul să distingă situațiile critice de notificările secundare. Distribuția recomandată în practică este puternic asimetrică – majoritatea alarmelor de prioritate redusă, o proporție mică de prioritate ridicată – iar o distribuție uniformă este un semn sigur că prioritizarea nu a fost făcută.

O singură defecțiune poate genera mai multe alarme consecutive. De exemplu, pierderea unui senzor poate determina alarma de comunicație, depășirea unei limite calculate și oprirea unei secvențe. Fenomenul de inundare cu alarme, definit ca depășirea capacității operatorului de a le procesa, apare tocmai în momentele în care atenția acestuia este cea mai necesară [46]. Proiectarea trebuie să ajute la identificarea cauzei inițiale, prin gruparea alarmelor dependente, prin condiționarea lor de starea echipamentului și prin evitarea repetării aceluiași mesaj.

Datele istorice ajută la înțelegerea modului în care s-a desfășurat un incident, prin reconstituirea ordinii evenimentelor. Ele permit urmărirea tendințelor, compararea loturilor și a schimburilor de lucru, identificarea opririlor, calcularea indicatorilor și analiza consumurilor, oferind totodată informații utile pentru mentenanță.

Frecvența de arhivare nu trebuie să fie identică pentru toate variabilele. O stare care se modifică rar poate fi păstrată la schimbare, în timp ce o variabilă dinamică poate necesita eșantionare periodică. Arhivarea excesivă crește volumul fără a îmbunătăți analiza, iar o frecvență prea redusă poate ascunde evenimente importante; ordinele de mărime rezultate din aceste decizii au fost calculate în secțiunea 5.4.5.

Sincronizarea ceasurilor este esențială. PLC-urile, serverele SCADA, gateway-urile și sistemele de date istorice trebuie să utilizeze o referință temporală coerentă, obținută prin protocolul de timp în rețea sau, pentru exactități sub o milisecundă, prin protocolul de timp de precizie [157], [35]. Altfel, ordinea aparentă a alarmelor și comenzilor poate fi diferită de succesiunea reală, iar analiza unui incident conduce la o cauză greșită.

5.5.6. Evoluția sistemelor SCADA

Tabelul 5.10 – Cele patru generații ale sistemelor SCADA

Generație	Arhitectură dominantă	Caracteristici	Limitări principale
Prima generație – monolitică	Calculator central și terminale dedicate	Funcțiile sunt concentrate într-un singur sistem; comunicațiile și formatele sunt proprietare	Punct unic de defectare, extindere dificilă și interoperabilitate redusă
A doua generație – distribuită	Mai multe calculatoare conectate într-o rețea locală	Funcțiile de achiziție, operare și stocare sunt distribuite	Integrarea între furnizori și administrarea sistemelor rămân dificile
A treia generație – în rețea	Arhitectură client–server și rețele standardizate	Servere specializate, clienți multipli, conectare extinsă și redundanță	Creșterea complexității și a expunerii la amenințări cibernetice
A patra generație – conectată IIoT și web	Servicii distribuite, interfețe web și integrare edge–cloud	Acces controlat de la distanță, schimb de date cu platforme externe și analiză avansată	Dependență crescută de administrarea identităților, actualizări și securizarea comunicațiilor

Evoluția sistemelor SCADA poate fi descrisă prin patru generații, sintetizate în Tabelul 5.10 și în Figura 5.12. Delimitarea este orientativă, deoarece instalațiile industriale pot utiliza simultan componente provenite din generații diferite; o instalație cu durata de viață de douăzeci de ani conține aproape întotdeauna straturi tehnologice succesive.

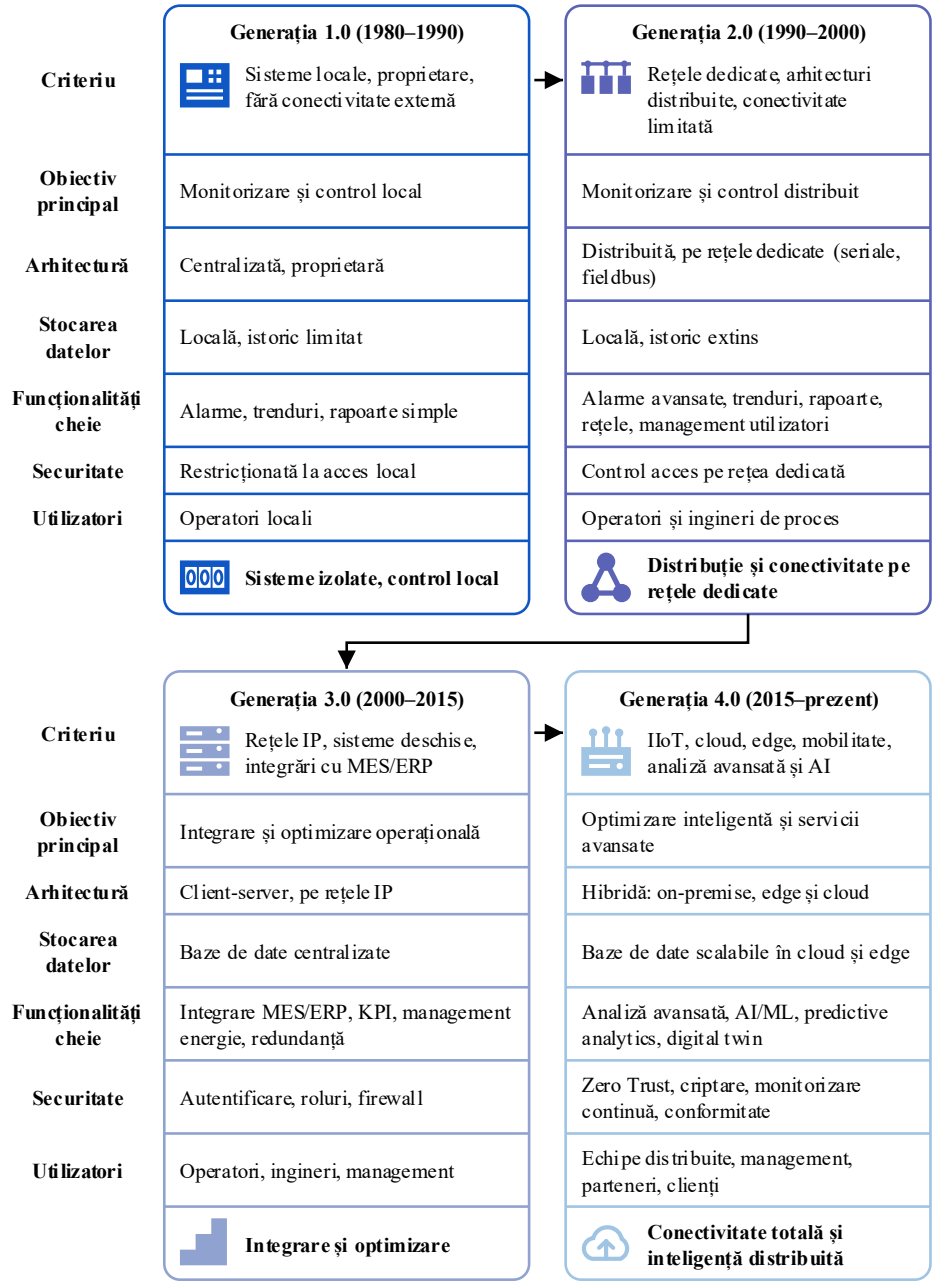


Figura 5.12 – Evoluția sistemelor SCADA

Prima generaţie utiliza sisteme centrale izolate şi protocoale specifice. A doua generaţie a distribuit funcţiile între mai multe calculatoare aflate în aceeaşi reţea. A treia generaţie a adoptat arhitecturi client–server şi tehnologii de comunicaţie standardizate, permiţând conectarea unui număr mai mare de staţii şi servere [161].

A patra generaţie extinde sistemul SCADA prin interfeţe web, procesare la edge, servicii distribuite şi conectare la platforme IIoT. Această evoluţie nu transferă automat controlul procesului în cloud. Funcţiile critice rămân locale, iar serviciile externe sunt utilizate pentru analiză, raportare, coordonare şi acces controlat. Câştigul de interoperabilitate al acestei generaţii este însoţit de o creştere a suprafeţei de atac, motiv pentru care adoptarea sa fără o arhitectură de securitate corespunzătoare transformă un avantaj funcţional într-un risc operaţional [25].

Modernizarea unui sistem existent nu impune înlocuirea integrală a infrastructurii. Serverele, reţelele şi interfeţele pot fi actualizate gradual, cu condiţia păstrării compatibilităţii, testării comunicaţiilor şi definirii comportamentului la pierderea conexiunilor.

5.5.7. Integrarea SCADA în arhitectura IIoT

Într-o arhitectură IIoT, SCADA poate furniza date contextualizate despre proces fără a expune direct fiecare PLC către sistemele externe. Variabilele, alarmele şi evenimentele pot fi preluate prin OPC UA, interfeţe de programare sau gateway-uri industriale care le transformă în mesaje adecvate platformei receptoare.

Fluxul informaţional porneşte de la PLC şi echipamentele de câmp, continuă prin sistemul SCADA şi serverul de date istorice şi ajunge, prin intermediul unui gateway industrial, la sistemul MES, aplicaţiile de analiză şi platforma IIoT. O arhitectură mai complexă este ilustrată în Figura 5.13.

SCADA poate primi de la MES informaţii precum ordinul de producţie, reţeta autorizată sau varianta de produs. În sens invers, furnizează starea echipamentelor, cantităţile realizate, alarmele şi timpii de funcţionare. Această delimitare a responsabilităţilor între niveluri urmează modelele de integrare a întreprinderii [75] şi este analizată tehnic în Cap.7.

Comenzile provenite din exterior trebuie tratate separat de fluxurile de monitorizare. Acestea trebuie autentificate, autorizate şi validate înainte de transmiterea către PLC. Accesul de la distanţă la ecranele HMI nu trebuie publicat direct în internet; sesiunile trebuie iniţiate prin puncte de trecere controlate, limitate în durată, protejate criptografic şi jurnalizate [68], [25]. Arhitectura de segmentare care susţine aceste cerinţe, inclusiv DMZ industrial, este tratată în Capitolul 8.

Alegerea unei platforme SCADA/HMI trebuie să ţină seama de:

- numărul variabilelor şi frecvenţa actualizării;
- protocoalele şi controlerele existente;

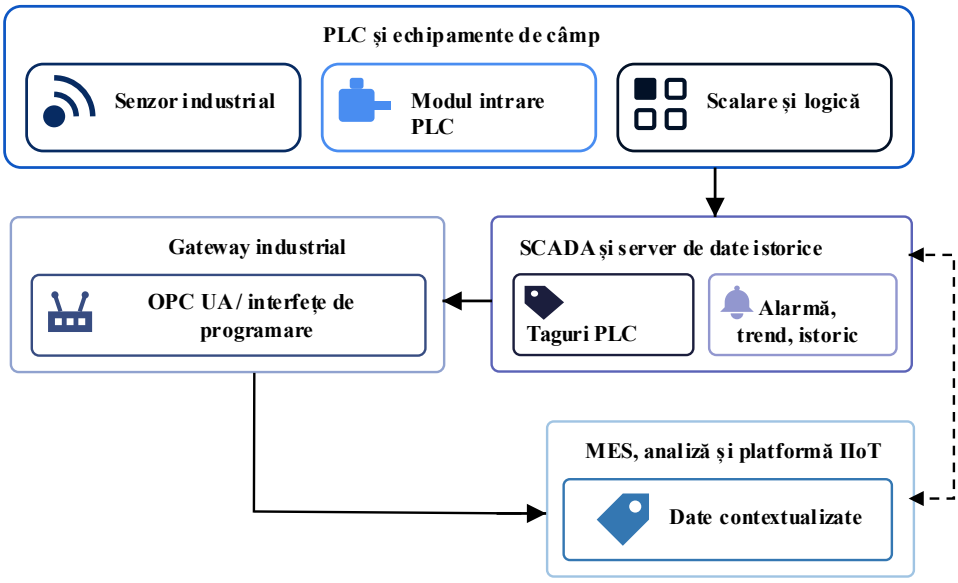


Figura 5.13 – Lanțul complet senzor–PLC–SCADA–IIoT

- arhitectura locală, distribuită sau redundantă;
- numărul şi rolurile utilizatorilor;
- funcţiile de alarmare, arhivare şi raportare;
- integrarea cu servere de date istorice, MES şi platforme IIoT;
- posibilitatea administrării centralizate;
- securizarea comunicaţiilor şi gestionarea drepturilor;
- instrumentele de diagnosticare;
- licenţierea, mentenanţa şi disponibilitatea suportului;
- posibilitatea migrării proiectului şi durata de viaţă estimată.

Platformele comerciale trebuie prezentate ca exemple de implementare, nu ca definiţii ale arhitecturii. Exemple utilizate frecvent în industrie sunt portofoliul SIMATIC WinCC al Siemens, Proficy iFIX al GE Vernova şi AVEVA Plant SCADA, denumit Citect SCADA în versiunile anterioare. Selectarea trebuie realizată pe baza cerinţelor aplicaţiei şi a infrastructurii existente, nu exclusiv pe baza producătorului PLC-ului.

Principiile prezentate sunt aplicate în secţiunea următoare prin proiectarea unei interfeţe HMI pentru monitorizarea şi operarea unui proces industrial.

5.6. Exercițiu aplicativ – Configurarea unei interfețe HMI pentru monitorizare

Exercițiul urmărește proiectarea și configurarea unei interfețe HMI pentru monitorizarea unui proces industrial simplu. Scopul nu este învățarea comenzilor specifice unei platforme, ci aplicarea principiilor prezentate în secțiunea 5.5 pentru transformarea datelor PLC-ului în informații utile operatorului.

Stiva (stack) tehnologică declarată. Pentru ca exercițiul să fie reproductibil, toate valorile de mai jos se raportează la o configurație concretă: automat programabil SIMATIC S7-1214C DC/DC/DC, modul de intrări analogice SM 1231 AI 4 × 13 biți configurat pentru 4–20 mA, panou de operare SIMATIC HMI KTP700 Basic cu rezoluția de 800 × 480 pixeli, mediu de inginerie TIA Portal V19 sau versiune ulterioară, cu WinCC Basic integrat, comunicație PROFINET printr-o conexiune S7 [164]. Modulul analogic este utilizat efectiv în secțiunea 5.7; în secțiunea de față temperatura poate fi generată intern.

Această stivă este un vehicul didactic, nu o recomandare de produs. Echivalentele funcționale ale altor producători permit realizarea aceluiași exercițiu; se modifică denumirile obiectelor, adresarea și valorile numerice ale conversiei analog–digitale, nu logica aplicației. Exercițiile 5.6 și 5.7, exercițiul din secțiunea 7.5 și miniproiectele din Capitolul 9 sunt concretizate pe platforme declarate; celelalte exerciții rămân, în mod deliberat, independente de producător, pentru a putea fi executate cu echipamentele disponibile în laboratorul cititorului.

Scenariul consideră un motor electric a cărui temperatură este măsurată sau simulată. Operatorul poate solicita pornirea și oprirea motorului, iar interfața afișează temperatura, starea echipamentului, condițiile care permit funcționarea și eventualele alarme. Dacă temperatura depășește limita admisă, PLC-ul generează alarma și blochează pornirea sau comandă oprirea controlată, în funcție de cerințele aplicației.

Interfața trebuie să permită:

- monitorizarea temperaturii;
- afișarea stării motorului;
- semnalizarea alarmei de supratemperatură;
- transmiterea comenzilor operaționale;
- indicarea condițiilor care permit pornirea;
- reinițializarea controlată a alarmei;
- identificarea pierderii comunicației dintre HMI și PLC.

5.6.1. Definirea etichetelor și a schimbului de date

Primul pas constă în definirea etichetelor care realizează legătura dintre variabilele PLC-ului și obiectele interfeței. Fiecare etichetă trebuie să aibă o denumire clară, un tip de date compatibil și un singur rol funcțional. Tipurile utilizate sunt

cele elementare definite normativ – BOOL, INT, REAL – şi nu depind de platformă [123].

Variabilele se grupează într-un bloc de date dedicat echipamentului, DB10 DB_Motor, astfel încât interfaţa să acceseze o zonă delimitată, iar nu memoria generală a controlerului. Lista completă este prezentată în Tabelul 5.11.

Adresele absolute au rol documentar şi presupun un bloc de date în format standard. Dacă blocul este creat în format optimizat, adresarea absolută nu mai este disponibilă, iar accesul se realizează exclusiv simbolic; coloana rămâne utilă atunci când aceleaşi variabile sunt expuse ulterior către un sistem SCADA extern sau prin OPC UA, situaţie tratată în secţiunea 5.7.4.

Tabelul 5.11 – Etichetele utilizate în exercițiul HMI

Etichetă	Tip	Adresă	Sens	Ciclu de achiziție	Rol în HMI
Temperatura_PV	Real	DB10.DBD0	PLC – HMI	100 ms	Afișaj numeric, bargraf și tendință
Temperatura_SP_Max	Real	DB10.DBD4	bidirecțional	1 s	Afișarea și configurarea autorizată a pragului
Temperatura_SP_Reset	Real	DB10.DBD8	PLC – HMI	1 s	Afișarea pragului de revenire
Alarma_Supratemperatura	Bool	DB10.DBX12.0	PLC – HMI	100 ms	Indicator și mesaj de alarmă
Motor_Pornit	Bool	DB10.DBX12.2	PLC – HMI	100 ms	Confirmarea funcționării
Motor_Pregatit	Bool	DB10.DBX12.3	PLC – HMI	500 ms	Disponibilitatea echipamentului
Motor_Permis	Bool	DB10.DBX12.4	PLC – HMI	100 ms	Activarea sau blocarea comenzii de pornire
Cauza_Blocare	Int	DB10.DBW20	PLC – HMI	500 ms	Text indirect cu motivul blocării
Comanda_Pornire_Motor	Bool	DB10.DBX14.0	HMI – PLC	la eveniment	Buton de pornire
Comanda_Oprire_Motor	Bool	DB10.DBX14.1	HMI – PLC	la eveniment	Buton de oprire
Resetare_Alarma	Bool	DB10.DBX14.2	HMI – PLC	la eveniment	Buton de reinițializare
Mod_Sistem	Int	DB10.DBW16	PLC – HMI	500 ms	Afișarea modului: 0 oprit, 1 manual, 2 automat, 3 simulare
Comunicatie_OK	Bool	variabilă internă HMI	intern	500 ms	Indicator de comunicație

Ciclul de achiziție se stabilește pentru fiecare etichetă, nu global. O valoare de proces dinamică se citește la 100 ms, o stare care se modifică rar la 500 ms sau 1 s, iar un parametru de configurare doar la deschiderea ecranului. Configurarea tuturor etichetelor la cel mai scurt ciclu este cea mai frecventă cauză a interfețelor lente și încarcă inutil conexiunea, fără niciun câștig de informație – efect cuantificat în secțiunea 5.4.5.

Comenzile de pornire, oprire și reinițializare trebuie tratate ca solicitări transmise PLC-ului, nu ca variabile care comandă direct ieșirile fizice. Butoanele se configurează cu funcțiile SetBit la apăsare și ResetBit la eliberare, astfel încât rezultatul să fie un impuls de durată limitată; menținerea accidentală a unei variabile la valoarea adevărat nu trebuie să conducă la repetarea necontrolată a comenzii. Programul PLC evaluează, la rândul său, frontul crescător al solicitării, nu nivelul acesteia [164].Denumirile trebuie să indice echipamentul, parametrul și funcția. Identificatorii generici, precum Bit_03 sau Valoare_1, îngreunează diagnosticarea și întreținerea aplicației. Etichetele expuse către HMI trebuie limitate la informațiile necesare operării și monitorizării; expunerea integrală a memoriei controlerului contravine principiului limitării funcțiilor la strictul necesar rolului [68].

Starea comunicației trebuie obținută din mecanismele de diagnosticare ale platformei, nu dintr-o variabilă citită prin aceeași legătură întreruptă, a cărei ultimă valoare poate rămâne afișată ca validă. Se utilizează două mecanisme complementare:

- în sensul PLC – HMI, comportamentul nativ al panoului: la pierderea conexiunii, câmpurile de valoare sunt marcate ca nevalide, iar sistemul generează o alarmă proprie;
- în sensul HMI – PLC, indicatorul de viață din zona de coordonare, comutat ciclic de panou. PLC-ul supraveghează comutarea și, dacă aceasta lipsește mai mult de 3 s, invalidează solicitările provenite de la interfață și continuă procesul conform logicii locale.

Cele două mecanisme nu sunt redundante, ci acoperă defecte diferite: primul detectează pierderea legăturii din perspectiva panoului, al doilea detectează un panou blocat care menține conexiunea, dar nu mai actualizează. Un sistem care implementează numai primul mecanism nu poate distinge o interfață funcțională de una înghețată.

5.6.2. Proiectarea ecranului și gestionarea alarmei

Ecranul principal trebuie să permită identificarea rapidă a stării procesului. Conform principiilor prezentate în secțiunea 5.5.4, elementele grafice transmit informație, fără aglomerarea interfeței.

Pentru o suprafață de 800 × 480 pixeli se propune o împărțire fixă în patru zone, păstrată identic pe toate ecranele aplicației și prezentată în Tabelul 5.12.

Tabelul 5.12 – Structura ecranului de operare

Zonă	Suprafață	Conținut
Antet	800 × 50 px	Denumirea instalației, utilizatorul conectat, data și ora, indicatorul de comunicație
Sinoptic de proces	560 × 280 px	Simbolul motorului, temperatura numerică cu unitatea °C, bargraf cu marcaje la 75 °C și 80 °C, tendința ultimelor 10 minute
Panou de stare	240 × 280 px	Modul de funcționare, Motor_Pregatit, Motor_Permis, cauza blocării, pragurile configurate
Bară de comenzi și alarme	800 × 150 px	Butoanele Pornire, Oprire, Resetare alarmă și linia ultimei alarme active

Fondul ecranului este neutru, iar echipamentul în stare normală este reprezentat în tonuri de gri. Culoarea saturată este rezervată exclusiv abaterilor: roşu pentru alarma activă neconfirmată, galben pentru condiţia care blochează pornirea, albastru pentru selecţia curentă [47], [162]. Starea de alarmă nu este semnalată numai cromatic: indicatorul are simbol propriu şi text asociat, conform principiului codificării prin cel puţin două atribute distincte [163].

Operatorul trebuie să poată răspunde imediat la trei întrebări:

- procesul funcţionează normal?
- există o condiţie care împiedică funcţionarea?
- ce acţiune este permisă sau necesară?

Interfaţa trebuie să diferenţieze solicitarea de pornire de confirmarea funcţionării. Acţionarea butonului nu înseamnă că motorul a pornit. Starea reală este indicată numai după confirmarea primită de la PLC, stabilită pe baza semnalelor disponibile în proces.

Configurarea alarmei: condiţia este evaluată exclusiv în PLC, iar interfaţa afişează bitul rezultat, ca alarmă discretă asociată etichetei Alarma_Supratemperatura. Parametrii sunt:

- prag de activare: 80,0 °C;
- durata de confirmare: 3 s de depăşire continuă;
- prag de revenire: 75,0 °C, deci un histerezis de 5 K;
- prioritate: ridicată, cu confirmare obligatorie;
- clasa de alarmă: „Avarii”, cu memorare până la reiniţializare.

Histerezisul şi temporizarea au roluri distincte şi nu se substituie: temporizarea elimină alarmele produse de vârfuri scurte, iar histerezisul elimină comutarea repetată în apropierea pragului. O aplicaţie care implementează doar unul dintre cele două mecanisme va prezenta, în exploatare, fie alarme false la fiecare perturbaţie, fie o succesiune rapidă de activări şi reveniri.

Reiniţializarea este permisă doar atunci când toate condiţiile sunt îndeplinite: temperatura a coborât sub 75 °C, pragul stabilit pentru revenire, valoarea furnizată

de senzor este validă, iar cauza alarmei a fost eliminată. În plus, operatorul trebuie să fi confirmat alarma, iar celelalte condiţii locale trebuie să fie îndeplinite.

Mesajul afişat trebuie să identifice problema şi să sprijine intervenţia. O formulare adecvată este: „Temperatura motorului a depăşit limita admisă. Verificaţi sistemul de răcire, sarcina motorului şi starea senzorului înainte de repornire."

Formularea aceasta ajută mai mult decât un cod generic, pentru că spune ce condiţie a fost detectată şi ce trebuie verificat. Confirmarea mesajului arată doar că alarma a fost observată; eliminarea şi reiniţializarea ei le decide logica PLC-ului. Stările „activă neconfirmată", „activă confirmată" şi „revenită" fac parte din ciclul de viaţă normat al alarmei şi trebuie afişate în interfaţă [46].

Modificarea pragului Temperatura_SP_Max este permisă exclusiv utilizatorilor din grupul cu drepturi de supervizor. Câmpul de introducere este limitat la intervalul 40–110 °C, iar PLC-ul reverifică valoarea primită înainte de a o prelua în logica de alarmare; limitarea din interfaţă este o măsură de ergonomie, nu de siguranţă.

5.6.3. Comenzile, interblocările şi simularea

HMI transmite intenţia operatorului, iar PLC-ul stabileşte dacă acţiunea poate fi executată. Motorul poate porni numai dacă:

- nu există o alarmă activă de supratemperatură;
- sistemul se află într-un mod care permite pornirea;
- motorul este disponibil;
- interblocările tehnologice sunt îndeplinite;
- oprirea de urgenţă nu este activă;
- funcţiile locale de siguranţă permit funcţionarea.

Rezultatul acestor condiţii este Motor_Permis. Dacă una dintre ele nu este îndeplinită, comanda este respinsă, iar butonul de pornire se afişează inactiv. Simpla dezactivare a butonului nu este însă suficientă: interfaţa trebuie să indice **care** condiţie blochează acţiunea. În acest scop, PLC-ul scrie în Cauza_Blocare un cod corespunzător primei condiţii neîndeplinite (1 – alarmă activă; 2 – măsurare nevalidă; 3 – mod necorespunzător; 4 – motor indisponibil; 5 – interblocare tehnologică; 6 – oprire de urgenţă activă), iar interfaţa afişează textul asociat printr-o listă de texte indirecte. Ordinea de evaluare este fixă, astfel încât operatorul să primească întotdeauna cauza cea mai apropiată de sursă, nu ultima condiţie verificată.

Oprirea de urgenţă şi celelalte funcţii dedicate siguranţei nu depind de HMI şi nu pot fi ocolite prin interfaţă.

Modul de simulare: în lipsa unui senzor fizic, temperatura poate fi generată în PLC. Se utilizează Mod_Sistem = 3 şi o variabilă Temperatura_Simulata, introdusă de pe un ecran separat, accesibil numai cu drepturi de inginer. Când modul de simulare este activ, ecranul afişează permanent o bandă distinctă cu textul „Date simulate – valorile nu provin din proces", iar valoarea numerică este marcată vizual.

Trecerea în modul normal invalidează sursa simulată şi impune revalidarea măsurării reale înainte de utilizarea ei în logica de control.

Secvenţa de testare cuprinde zece paşi:

1. Se stabileşte comunicaţia dintre HMI şi PLC;
2. Se verifică actualizarea temperaturii şi a stărilor motorului;
3. Motorul este pornit în condiţii normale, la o temperatură simulată de 60 °C;
4. Temperatura este crescută progresiv până la 80 °C;
5. Valoarea este menţinută peste prag mai puţin de 3 s şi se verifică faptul că alarma nu se activează;
6. Valoarea este menţinută peste prag mai mult de 3 s: alarma se activează, iar comanda de pornire este blocată;
7. Temperatura este redusă la 78 °C şi se verifică faptul că alarma rămâne memorată;
8. Temperatura este redusă sub 75 °C, alarma este confirmată şi reiniţializată;
9. Motorul este repornit după îndeplinirea tuturor interblocărilor;
10. Comunicaţia HMI–PLC este întreruptă prin deconectarea cablului şi ulterior restabilită.

Paşii 5 şi 7 sunt cei care verifică efectiv temporizarea şi memorarea; ei sunt şi cei omişi cel mai frecvent la punerea în funcţiune, deoarece o testare care creşte temperatura direct şi rapid peste prag produce un rezultat aparent corect fără a valida niciunul dintre cele două mecanisme.

Pierderea comunicaţiei trebuie semnalată explicit. Valorile rămase pe ecran nu trebuie prezentate ca fiind actuale, ci marcate drept neactualizate sau incerte. Comenzile care depind de legătura cu PLC-ul trebuie dezactivate, iar controlerul local trebuie să continue procesul sau să îl aducă într-o stare definită, conform logicii implementate.

5.6.4. Validarea interfeței

Validarea urmăreşte relaţia dintre date, reprezentarea vizuală, comenzile operatorului şi logica PLC-ului. Aspectul grafic este acceptabil numai dacă interfaţa prezintă corect starea reală şi împiedică acţiunile nepermise. Criteriile aplicabile sunt prezentate în Tabelul 5.13.

Criteriul de claritate este singurul care nu poate fi verificat de proiectantul aplicaţiei: acesta cunoaşte ecranul şi îl citeşte corect indiferent cât de aglomerat este. Verificarea trebuie făcută cu o persoană care nu a participat la proiectare, iar rezultatul se consemnează. Este cea mai ieftină formă de validare ergonomică şi, în practică, cea mai des omisă.

După verificarea şi validarea funcţiilor de bază, aplicaţiei i se pot adăuga funcţii noi: urmărirea evoluţiei temperaturii pe intervale care pot fi configurate, păstrarea unui jurnal cu alarme şi evenimente şi definirea rolurilor de operator, mentenanţă şi administrator. De asemenea, se poate introduce un ecran separat pentru

configurare şi se pot adăuga valori de vibraţie sau curent. Datele pot fi arhivate într-o bază de date, iar valorile pot fi transmise către un sistem SCADA sau un gateway industrial.

Rezultatul exerciţiului este o interfaţă care afişează temperatura şi starea motorului, transmite solicitările operatorului, semnalizează condiţiile anormale şi indică pierderea comunicaţiei. Validarea comenzilor şi a interblocărilor rămâne la nivelul PLC-ului.

Secţiunea următoare extinde aplicaţia de la proiectarea interfeţei la integrarea verticală a unui senzor industrial cu PLC-ul şi sistemul SCADA, urmărind traseul valorii de la achiziţie şi scalare până la vizualizare, alarmare şi arhivare.

Tabelul 5.13 – Criteriile de validare a interfeței HMI

Criteriu	Verificare	Rezultat acceptat
Comunicație	HMI primește și actualizează valorile PLC-ului?	Valorile se actualizează la ciclul configurat; Temperatura_PV urmărește sursa cu întârziere sub 0,5 s
Afișare	Temperatura este prezentată împreună cu unitatea de măsură?	Valoarea este afișată cu o zecimală și unitatea °C
Starea motorului	Este diferențiată comanda de confirmarea funcționării?	Indicatorul se modifică numai după Motor_Pornit, nu la apăsarea butonului
Alarmă	Alarma apare după depășirea confirmată a pragului?	Se activează după 3 s peste 80 °C și nu se activează la depășiri mai scurte
Interblocare	Pornirea este blocată în timpul alarmei?	Solicitarea este respinsă de PLC, iar Cauza_Blocare indică motivul corect
Reinițializare	Alarma poate fi reinițializată numai după eliminarea condiției?	Reinițializarea este refuzată peste 75 °C și acceptată sub acest prag
Pierderea comunicației	HMI indică întreruperea conexiunii?	Valorile sunt marcate ca nevalide în cel mult 3 s, iar comenzile devin inactive
Simulare	Modul de simulare este identificabil?	Banda de avertizare este permanent vizibilă cât timp Mod_Sistem = 3
Claritate	Poate fi identificată rapid starea procesului?	O persoană neinstruită pe această aplicație răspunde la cele trei întrebări din 5.6.2 în sub 5 s
Protejarea comenzilor	Sunt limitate acțiunile cu efect important?	Modificarea pragului este posibilă numai cu drepturi de supervizor și este jurnalizată

5.7. Exercițiu aplicativ – Integrarea unui senzor industrial cu PLC și SCADA

Exerciţiul urmăreşte integrarea verticală locală a unui senzor industrial într-un lanţ complet de achiziţie, control şi supraveghere. Valoarea măsurată este preluată de PLC, transformată într-o mărime tehnică, verificată şi utilizată în logica procesului, apoi transmisă sistemului SCADA pentru vizualizare, alarmare şi arhivare.

Aplicaţia continuă scenariul prezentat în secţiunea 5.6, foloseşte aceeaşi stivă tehnologică declarată acolo şi utilizează temperatura unui motor drept variabilă de proces. Se adaugă modulului de intrări analogice SM 1231 AI 4 × 13 biţi, configurat

pentru domeniul 4–20 mA, și un transmițător de temperatură cu ieșire în buclă de curent [164].

Temperatura este măsurată de senzor, iar semnalul este transmis prin transmițător și modulul de intrare către PLC. Informația ajunge apoi în sistemul SCADA, unde este afișată operatorului.

PLC-ul rămâne responsabil pentru validarea măsurării, interblocări și controlul motorului. Sistemul SCADA afișează informațiile și transmite solicitările operatorului, fără a prelua funcțiile deterministe ale controlerului.

5.7.1. Scenariul și cerințele funcționale

Senzorul măsoară temperatura statorului unui motor și furnizează un semnal către modulul de intrare al PLC-ului. Se utilizează un senzor Pt100 în conexiune cu trei conductoare, clasa A [135], conectat la un transmițător cu ieșire 4–20 mA configurat pentru domeniul 0–150 °C. Conexiunea cu trei conductoare nu este o opțiune de montaj, ci o cerință a clasei de toleranță alese, conform secțiunii 5.1.1. Conectarea directă a unui Pt100 la PLC este posibilă numai printr-un modul destinat termorezistențelor; varianta cu transmițător a fost aleasă aici pentru că permite tratarea explicită a diagnosticării prin nivelul semnalului, mecanism prezentat în secțiunea 5.1.

Aplicația trebuie să îndeplinească următoarele cerințe:

- achiziția semnalului furnizat de senzor;
- conversia valorii brute în grade Celsius;
- verificarea stării canalului și a validității măsurării;
- afișarea temperaturii și a calității valorii;
- generarea alarmei de supratemperatură;
- blocarea pornirii motorului în condiții nepermise;
- oprirea controlată a motorului dacă temperatura depășește limita stabilită;
- afișarea stării motorului și a interblocărilor;
- păstrarea alarmei și a evoluției temperaturii;
- semnalizarea pierderii comunicației dintre PLC și SCADA.

Parametrii aplicației sunt cei stabiliți în secțiunea 5.6: limită de alarmare 80 °C, prag de revenire 75 °C, durată de confirmare 3 s. Valorile au rol demonstrativ. Într-o aplicație reală, ele se stabilesc în funcție de clasa de izolație a motorului, de condițiile procesului și de cerințele producătorului; pentru un motor cu izolație de clasă F, de exemplu, limitele admise sunt substanțial mai ridicate decât valoarea folosită aici, aleasă pentru a permite testarea comodă a mecanismelor.

Sistemul trebuie să deosebească situația în care temperatura este normală și valoarea senzorului este validă de cea în care temperatura depășește limita admisă. Separat, trebuie să indice situația în care măsurarea lipsește sau valoarea obținută nu poate fi considerată validă.

Defectarea senzorului nu trebuie interpretată ca o temperatură normală. În această situaţie se generează o alarmă distinctă, iar motorul adoptă comportamentul definit prin analiza procesului. Confuzia dintre a doua şi a treia situaţie este cea mai frecventă eroare de proiectare a acestui tip de aplicaţie: un circuit întrerupt produce o valoare brută mică, care, scalată fără verificare prealabilă, apare ca o temperatură scăzută, deci ca o stare aparent sigură.

5.7.2. Configurarea achiziției și scalarea valorii

Configurarea începe cu documentarea lanţului de măsurare. Pentru fiecare element trebuie cunoscute domeniul fizic, tipul semnalului, modul de conectare, precizia, alimentarea şi comportamentul la defectare. Parametrii utilizaţi sunt prezentaţi în Tabelul 5.14.

Tabelul 5.14 – Parametrii lanțului de măsurare

Element	Parametru	Valoare
Senzor	Tip, conexiune, toleranță	Pt100, 3 conductoare, clasa A
Transmițător	Domeniu configurat, ieșire, alimentare	0–150 °C, 4–20 mA, 24 V c.c., 2 fire
Transmițător	Semnalizarea defectului	≤ 3,6 mA sau ≥ 21 mA [131]
Modul de intrare	Tip și cod de comandă	SM 1231 AI 4 × 13 biți; 6ES7231-4HD32-0XB0
Modul de intrare	Domeniu configurat și rezoluție	4–20 mA; 12 biți + semn
Modul de intrare	Valoare brută pentru domeniul nominal	0 … 27648
Modul de intrare	Domeniu de depășire admis	−4864 … 32511
Modul de intrare	Rejecția perturbațiilor; timpul de integrare	50 Hz; 20 ms
Modul de intrare	Timp de eșantionare și actualizare pentru toate canalele	5 ms, pentru configurația la 50 Hz
Aplicație	Ciclu de citire, filtrare	100 ms, filtru de ordinul întâi cu τ = 2 s

Valorile numerice ale domeniului şi ale zonei de depăşire provin din documentaţia modulului utilizat [164]. Modulul de intrare trebuie configurat pentru tipul de semnal utilizat. Selectarea greşită a domeniului – de exemplu configurarea unei intrări pentru tensiune atunci când transmiţătorul furnizează curent – conduce la valori incorecte sau la imposibilitatea diagnosticării canalului.

Timpul de integrare, timpul de actualizare al modulului și ciclul de citire al aplicației reprezintă parametri diferiți. Pentru configurația aleasă, integrarea asociată rejecției la 50 Hz este de 20 ms, iar modulul actualizează valorile la 5 ms [164]. Aplicația le preia la 100 ms și aplică filtrul software cu constanta de timp de 2 s. Actualizarea unei valori la 5 ms nu înseamnă că întregul lanț de măsurare răspunde în acest interval la o variație a temperaturii.

Scalarea. Valoarea furnizată de modulul de intrare este transformată în grade Celsius prin relaţia generală:

$$T = T_{min} + (V_{brut} - V_{brut,min}) / (V_{brut,max} - V_{brut,min}) \cdot (T_{max} - T_{min})$$

unde *T*min şi *T*max sunt limitele domeniului configurat al transmiţătorului, iar *V*brut,min şi *V*brut,max sunt limitele numerice corespunzătoare modulului de intrare. Cu valorile din Tabelul 5.14

$$T = 0 + (Vbrut - 0) / (27648 - 0) \cdot (150 - 0) = Vbrut \cdot 5{,}4253 \cdot 10^{-3}$$

Puncte de verificare. Trei perechi valoare–temperatură, prezentate în Tabelul 5.15, permit identificarea imediată a unei erori de scalare.

Tabelul 5.15 – Puncte de verificare a scalării

Curent	Valoare brută	Temperatură calculată
4 mA	0	0,0 °C
12 mA	13824	75,0 °C
20 mA	27648	150,0 °C

Punctul median este cel mai util: o inversare a limitelor, o configurare pe 0–20 mA în loc de 4–20 mA sau o confuzie între domeniul senzorului şi cel al modulului produc la 12 mA o valoare diferită de 75 °C, în timp ce capetele de domeniu pot părea corecte în mai multe configuraţii greşite.

Rezoluţia reprezentării şi eroarea de măsurare. În relaţia de scalare, o unitate a valorii brute corespunde unei variaţii de 150 / 27648 ≈ 0,00543 °C. Acesta este pasul numeric al reprezentării scalate, nu dovada că lanţul poate distinge sau măsura temperatura cu această exactitate. Rezoluţia convertorului şi codificarea valorii în domeniul 0…27648 trebuie diferenţiate de toleranţele componentelor.

Pentru temperatura de 80 °C, toleranţa senzorului Pt100 de clasă A este ±(0,15 + 0,002 × 80) = ±0,31 °C [135]. În exemplul didactic se presupune pentru transmiţător o limită de eroare de ±0,1% din domeniul configurat de 150 °C, adică ±0,15 °C; această ipoteză trebuie verificată în documentaţia transmiţătorului ales. Pentru modulul SM 1231 AI 4 × 13 biţi, limita de ±0,2% din domeniu, specificată pentru temperatura ambiantă de −20…60 °C, corespunde unei contribuţii de ±0,30 °C [164]. Temperatura ambiantă a modulului nu trebuie confundată cu temperatura măsurată de senzor.

Prin însumarea valorilor absolute ale acestor trei contribuţii se obţine o estimare conservatoare pentru cazul cel mai defavorabil:

$$E = 0{,}31 + 0{,}15 + 0{,}30 = 0{,}76\ °C$$

Rezultatul reprezintă limita estimată pentru contribuţiile considerate, nu o incertitudine extinsă a întregului lanţ. Evaluarea incertitudinii necesită ipoteze privind distribuţiile, dependenţa contribuţiilor şi condiţiile efective de măsurare [36]. Pot interveni suplimentar efectele montajului, ale conductoarelor, ale autoîncălzirii şi ale etalonării.

Pentru afişarea operatorului, o zecimală este o alegere adecvată acestui exemplu, fără a implica o exactitate de ±0,1 °C. Calculele interne pot păstra mai multe zecimale pentru a evita rotunjirile premature. Distincţia dintre rezoluţie şi acurateţe, tratată în secţiunea 5.1 şi în Tabelul 5.1, are astfel o consecinţă directă asupra

proiectării interfeței. Etichetele suplimentare față de Tabelul 5.11 sunt prezentate în Tabelul 5.16.

Tabelul 5.16 – Etichete suplimentare pentru integrarea senzorului

Etichetă	Tip	Adresă	Rol
Temperatura_Bruta	Int	IW64	Valoarea furnizată de modulul de intrare
Temperatura_Filtrata	Real	DB10.DBD24	Valoarea scalată și filtrată
Temperatura_Valida	Bool	DB10.DBX12.5	Confirmarea validității măsurării
Defect_Senzor_Temperatura	Bool	DB10.DBX12.6	Diagnosticarea senzorului sau a canalului
Mod_Simulare_Temperatura	Bool	DB10.DBX14.3	Activarea controlată a sursei simulate
Temperatura_Simulata	Real	DB10.DBD28	Valoarea utilizată în timpul testării

Validarea măsurării se execută înainte ca valoarea să fie utilizată în control. PLC-ul verifică, în această ordine:

- starea canalului, prin diagnosticul modulului: întrerupere de circuit, depășire de domeniu, canal neconfigurat;
- domeniul numeric: Temperatura_Bruta sub −500 (echivalent aproximativ 3,7 mA, între nivelul de defect de 3,6 mA și limita inferioară a domeniului util, de 3,8 mA) indică circuit întrerupt sau transmițător în defect, iar peste 28800 (aproximativ 20,7 mA) indică depășire de domeniu sau scurtcircuit;
- plauzibilitatea dinamică: o variație mai mare de 20 K între două citiri succesive la 100 ms este fizic imposibilă pentru masa termică a unui stator și indică o problemă a lanțului de măsurare, nu a procesului.

Dacă oricare verificare eșuează, Temperatura_Valida devine falsă, iar *Defect_Senzor_Temperatura* se activează după o temporizare de 1 s, pentru evitarea reacției la perturbații tranzitorii. Pragurile numerice de la punctul 2 corespund domeniilor rezervate semnalizării defectului [131] și sunt exact mecanismul care permite diferențierea celei de-a treia situații de prima, definite în secțiunea 5.7.1.

Filtrarea reduce zgomotul, dar nu trebuie să ascundă schimbările importante. Un filtru de ordinul întâi cu $\tau = 2$ s, la un ciclu de eșantionare de 100 ms, atenuează perturbațiile rapide, dar întârzie semnalul: răspunsul ajunge la 63 % după 2 s și la aproximativ 98 % după 8 s. Pentru o mărime termică, care variază în ordinul minutelor, întârzierea e acceptabilă, însă se adaugă la durata de confirmare a alarmei. Valoarea brută se păstrează separat, pentru diagnosticare, iar cea filtrată se folosește la afișare și alarmare.

În modul de simulare, Temperatura_Simulata înlocuiește controlat sursa fizică, iar interfața indică permanent acest lucru, conform secțiunii 5.6.3. La revenirea în modul normal, sursa reală parcurge integral validarea înainte de a fi utilizată în logica de control.

5.7.3. Implementarea logicii în PLC

Programul se organizează într-un bloc funcţional FB_Motor_Temperatura, apelat ciclic din blocul de organizare principal, cu structura internă în opt paşi:

1. citeşte valoarea şi diagnosticul modulului de intrare;
2. stabileşte dacă măsurarea este validă;
3. scalează valoarea brută în grade Celsius;
4. aplică filtrarea;
5. evaluează pragurile şi temporizarea alarmei;
6. verifică interblocările motorului;
7. procesează solicitările operatorului;
8. actualizează comenzile şi stările transmise sistemului SCADA.

Ordinea nu este arbitrară: validarea precedă scalarea, iar scalarea precedă evaluarea pragurilor. Inversarea paşilor 2 şi 3 – frecventă în aplicaţiile realizate rapid – produce exact eroarea descrisă în secţiunea 5.7.1, deoarece o valoare de defect scalată devine o temperatură plauzibilă.

Nucleul logicii de alarmare, exprimat în text structurat [123]:

```
   // Pasul 5 — evaluarea pragurilor
IF Temperatura_Valida AND (Temperatura_Filtrata > Temperatura_SP_Max) THEN
    Timp_Depasire(IN := TRUE, PT := T#3S);
ELSE
    Timp_Depasire(IN := FALSE, PT := T#3S);
END_IF;

// activare memorată
IF Timp_Depasire.Q THEN
    Alarma_Supratemperatura := TRUE;
END_IF;

// reinițializare condiționată
IF Alarma_Supratemperatura
   AND Temperatura_Valida
   AND (Temperatura_Filtrata < Temperatura_SP_Reset)
   AND Resetare_Alarma_Front THEN
    Alarma_Supratemperatura := FALSE;
END_IF;
```

Alarma este, aşadar, activată dacă temperatura validă depăşeşte 80 °C timp de cel puţin 3 s continuu şi rămâne memorată până când sunt îndeplinite simultan trei condiţii: temperatura sub 75 °C, măsurare validă şi front crescător al unei solicitări autorizate de reiniţializare. Evaluarea pe front, nu pe nivel, împiedică reiniţializarea automată la fiecare ciclu de scanare dacă butonul rămâne activ.

Motorul poate porni numai dacă sunt îndeplinite simultan condiţiile:

- temperatura este validă şi se află sub limita admisă;
- nu există alarmă de supratemperatură;
- senzorul şi modulul de intrare nu semnalează defecte;

- motorul este disponibil;
- modul de funcţionare permite pornirea;
- interblocările tehnologice sunt îndeplinite;
- funcţiile de siguranţă permit funcţionarea.

Rezultatul acestor condiţii este transmis prin eticheta Motor_Permis, iar prima condiţie neîndeplinită este codificată în Cauza_Blocare, conform secţiunii 5.6.3. Solicitarea *Comanda_Pornire_Motor*, primită de la SCADA sau de la HMI, este acceptată numai dacă Motor_Permis este adevărată. PLC-ul comandă ieşirea corespunzătoare şi aşteaptă confirmarea stării reale a motorului într-un interval de 2 s; absenţa confirmării generează o alarmă distinctă de nepornire, care identifică explicit confirmarea lipsă, conform principiului din secţiunea 5.3.4.

Dacă temperatura depăşeşte limita în timpul funcţionării, PLC-ul execută comportamentul stabilit pentru proces: oprirea controlată a motorului, menţinerea temporară a ventilaţiei forţate timp de 120 s şi blocarea repornirii până la reiniţializare. Categoria de oprire trebuie declarată explicit în documentaţia aplicaţiei: aici se utilizează oprirea controlată cu întreruperea alimentării la atingerea repausului, iar pentru procesele în care oprirea imediată poate produce un risc suplimentar secvenţa trebuie definită prin analiza funcţională şi de siguranţă [139].

Defectarea senzorului trebuie deosebită de depăşirea limitei de temperatură. Dacă senzorul se defectează, PLC-ul indică faptul că valoarea nu este validă, activează alarma de defect al măsurării şi nu permite pornirea motorului. Dacă motorul funcţionează deja, iar oprirea lui ar produce un risc mai mare, PLC-ul îl menţine în funcţiune şi semnalează că acesta funcţionează fără supraveghere termică. Cauza blocării pornirii este transmisă sistemului SCADA.

Ultima decizie este cea mai delicată din întregul exerciţiu şi nu are un răspuns universal: oprirea la pierderea măsurării protejează motorul, dar poate produce o oprire de proces nejustificată; continuarea protejează producţia, dar elimină o funcţie de protecţie. Alegerea aparţine analizei de risc a instalaţiei, iar aplicaţia trebuie să facă vizibil faptul că funcţionează fără supraveghere termică, nu să ascundă acest lucru.

Funcţiile de siguranţă nu se implementează prin logica standard a PLC-ului sau prin sistemul SCADA. Dacă protejarea persoanelor ori a instalaţiei necesită funcţii de siguranţă, acestea se realizează prin echipamente şi programe corespunzătoare nivelului de performanţă cerut de analiza de risc [45], [142].

5.7.4. Integrarea cu sistemul SCADA

Conexiunea dintre PLC şi SCADA utilizează, în această configuraţie, serverul OPC UA integrat în controler, activat din configuraţia hardware. Fiecare variabilă expusă primeşte un identificator de nod în forma *ns=3;s="DB_Motor"."Temperatura_PV"*, iar aplicaţia SCADA se conectează în calitate de client, cu autentificare şi certificat acceptat reciproc [127]. Se preferă abonarea faţă de interogarea periodică: clientul

declară un interval de publicare şi o bandă moartă, iar serverul transmite numai modificările semnificative – mecanism care reduce substanţial traficul, conform calculului din secţiunea 5.4.5.

Pentru fiecare etichetă se verifică identificatorul de nod, tipul de date, drepturile de acces şi intervalul de publicare, conform Tabelului 5.17.

Sistemul SCADA preia temperatura brută şi cea scalată, starea de validitate, diagnosticul senzorului, limita de alarmare şi pragul de revenire, starea alarmei, permisiunea de pornire, solicitarea şi confirmarea funcţionării, modul normal sau de simulare şi starea comunicaţiei.

Interfaţa realizată în secţiunea 5.6 se completează cu informaţiile privind sursa şi calitatea valorii. Codul de stare transportat de OPC UA nu este o informaţie de diagnostic internă, ci un atribut al valorii, care trebuie reprezentat în interfaţă [127]: o valoare marcată drept incertă se afişează distinct, iar una nevalidă nu se afişează ca măsurare curentă. Afişarea numerică a temperaturii se face cu o zecimală, conform discuţiei despre rezoluţie din secţiunea 5.7.2, însoţită de unitate şi de indicatorul de validitate.

Tabelul 5.17 – Configurarea abonării OPC UA

Grup de variabile	Interval de publicare	Bandă moartă	Sens
Temperatură brută, scalată, filtrată	200 ms	0,2 °C	citire
Stări binare: alarmă, permisiune, motor pornit, validitate	100 ms	–	citire
Praguri și mod de funcționare	1 s	–	citire
Cauza blocării	500 ms	–	citire
Solicitări de pornire, oprire, reinițializare	la eveniment	–	scriere

Pentru această aplicaţie sunt utile trei zone de reprezentare:

- imaginea procesului, cu motorul, temperatura şi comenzile permise;
- tendinţa temperaturii, cu limita de alarmare, pragul de revenire şi momentele opririi;
- lista alarmelor şi a evenimentelor, cu apariţia, confirmarea şi revenirea acestora.

Arhivarea se configurează diferenţiat: temperatura filtrată se înregistrează la 1 s cu o bandă moartă de 0,2 °C; stările binare şi alarmele se înregistrează la fiecare modificare, fără bandă moartă. Se păstrează 30 de zile la rezoluţia completă şi 2 ani în formă agregată la 1 minut, cu valorile minimă, maximă şi medie. Agregarea trebuie configurată astfel încât vârfurile scurte să rămână vizibile în seria de valori maxime; păstrarea exclusivă a mediei ar elimina exact evenimentele care justifică arhivarea, conform observaţiei din secţiunea 5.5.3.

Pragul de supratemperatură şi logica de memorare sunt implementate în PLC. Sistemul SCADA primeşte starea rezultată şi gestionează prezentarea, prioritatea, confirmarea şi arhivarea alarmei [46]. Definirea independentă a aceleiaşi condiţii în PLC şi SCADA produce diferenţe între starea reală a controlului şi informaţia

afișată operatorului – o sursă de erori greu de diagnosticat, deoarece ambele sisteme funcționează corect separat.

Comanda transmisă din SCADA este o solicitare. PLC-ul o acceptă sau o respinge și returnează rezultatul. Dacă pornirea este blocată, interfața afișează motivul preluat din Cauza_Blocare.

Pierderea comunicației este indicată distinct de defectarea senzorului. În primul caz, SCADA nu mai poate actualiza informațiile, dar PLC-ul continuă să primească valoarea senzorului și să controleze local motorul. În al doilea caz, conexiunea cu SCADA funcționează, însă măsurarea temperaturii nu este validă. Cele două situații necesită intervenții diferite – una a echipei de rețea, cealaltă a echipei de mentenanță – iar interfața care le confundă trimite intervenția pe traseul greșit.

5.7.5. Testarea și validarea integrării

Validarea urmărește întregul traseu, de la semnalul aplicat la intrare până la reprezentarea și arhivarea sa în SCADA. Testarea exclusivă a ecranului nu confirmă funcționarea corectă a achiziției și a logicii PLC-ului.

Semnalul de intrare se aplică cu un calibrator de buclă conectat în locul transmițătorului, ceea ce permite parcurgerea controlată a întregului domeniu, inclusiv a zonelor de defect. Cazurile principale sunt prezentate în Tabelul 5.18.

Pentru fiecare caz se compară: valoarea aplicată sau simulată, valoarea brută citită de PLC, valoarea scalată, valoarea filtrată, starea de validitate, rezultatul logicii de alarmare, comanda transmisă către motor, confirmarea stării motorului, valoarea și starea afișate în SCADA, precum și înregistrările din istoricul de evenimente.

Mărcile temporale trebuie să permită reconstruirea succesiunii: depășirea temperaturii, activarea alarmei, oprirea motorului, intervenția operatorului și reinițializarea. Dacă ceasurile PLC-ului și serverului SCADA nu sunt sincronizate printr-o referință comună [157], ordinea aparentă poate fi diferită de cea reală, iar analiza incidentului conduce la o cauză greșită.

Criteriile de reușită ale exercițiului sunt: abaterea de scalare sub 0,5 °C în cele trei puncte de verificare; alarma activată exclusiv după 3 s de depășire continuă și niciodată la depășiri mai scurte; reinițializarea refuzată peste 75 °C și acceptată sub acest prag; cele trei cazuri de defect al lanțului de măsurare tratate distinct de supratemperatură; valorile marcate ca nevalide în cel mult 3 s de la întreruperea comunicației; succesiunea completă a unui incident reconstituibilă din jurnalul de evenimente, cu mărci temporale coerente.

Tabelul 5.18 – Cazurile principale de testare a integrării

Caz de testare	Semnal aplicat	Comportamentul PLC-ului	Comportamentul sistemului SCADA
Verificarea scalării	4 / 12 / 20 mA	Afișează 0,0 / 75,0 / 150,0 °C, cu abatere sub 0,5 °C	Aceleași valori, cu calitate „bună”
Funcționare normală	11,5 mA (≈ 70 °C)	Motorul poate fi pornit dacă celelalte interblocări sunt îndeplinite	Afișează valoarea validă și starea normală
Apropierea de limită	Variație în jurul a 12,5 mA (≈ 80 °C), sub 3 s	Nu activează alarma	Tendința prezintă variația, fără alarmări repetitive
Supratemperatură	12,6 mA menținut peste 3 s	Activează alarma, oprește motorul, menține ventilația 120 s	Afișează alarma, cauza și momentul apariției
Histerezis	Coborâre la 12,3 mA (≈ 78 °C)	Menține alarma memorată	Indică alarmă activă, reinițializare refuzată
Revenire controlată	Coborâre sub 12,0 mA (< 75 °C)	Acceptă reinițializarea la front autorizat	Permite solicitarea și consemnează revenirea
Circuit întrerupt	0 mA	Invalidează măsurarea, alarmă de defect după 1 s, blochează pornirea	Afișează alarma de senzor; ultima valoare nu apare ca actuală
Depășire de domeniu	21,5 mA	Invalidează măsurarea, alarmă de defect	Idem, cu mesaj distinct de circuit întrerupt
Salt neplauzibil	Trecere bruscă 4 – 20 mA	Detectează variația imposibilă și invalidează măsurarea	Semnalează măsurare incertă
Comandă nepermisă	Pornire solicitată în timpul alarmei	Respinge solicitarea, menține ieșirea în starea sigură	Indică motivul din Cauza_Blocare
Pierderea comunicației	Deconectare PLC–SCADA	Continuă controlul local conform programului	Semnalează întreruperea; valorile devin nevalide în ≤ 3 s
Restabilirea comunicației	Reconectare	Furnizează stările și valorile curente	Resincronizează afișarea fără a confunda valorile istorice cu cele curente
Repornirea echipamentelor	Repornire PLC și server SCADA	Inițializează ieșirile și alarmele în stările definite	Reface conexiunile și prezintă corect stările memorate

5.7.6. Rezultatul exercițiului și posibilitățile de extindere

Rezultatul este un sistem local integrat în care senzorul furnizează o valoare verificată PLC-ului, controlerul aplică logica şi interblocările, iar sistemul SCADA prezintă procesul, gestionează alarmele şi păstrează istoricul. Aplicaţia demonstrează traseul informației între nivelul de câmp, nivelul de control şi nivelul de supraveghere.

Documentarea exerciţiului trebuie să includă:

- configuraţia senzorului, a transmiţătorului şi a modulului de intrare;
- domeniul, relaţia de scalare şi punctele de verificare;
- lista etichetelor schimbate între PLC şi SCADA, cu identificatorii de nod;

- condiţiile de alarmare şi reiniţializare;
- interblocările motorului şi codurile de blocare;
- cazurile de testare şi rezultatele obţinute;
- comportamentul la defectarea senzorului şi la pierderea comunicaţiei.

Aplicaţia poate fi extinsă prin adăugarea măsurării vibraţiilor, curentului sau consumului de energie, prin calcularea indicatorilor de funcţionare şi prin transmiterea datelor către un server de date istorice ori către un gateway industrial.

Lanţul realizat reprezintă o integrare verticală locală, nu o arhitectură IIoT completă. Deosebirea este esenţială: aici, un client SCADA citeşte direct de la un controler, în aceeaşi reţea şi sub acelaşi administrator. Extinderea către sisteme externe presupune protocoale, modele de date şi mecanisme de securitate adecvate: publicarea prin broker MQTT, convenţia de subiecte, contextualizarea payloadului şi separarea zonelor de reţea. Acestea sunt analizate în capitolul următor, dedicat comunicaţiilor industriale şi IIoT, şi aplicate în exerciţiul din secţiunea 7.5.

5.8. Concluzii

Stratul de dispozitive analizat în acest capitol este cel care transformă un proces fizic într-un obiect observabil şi comandabil. Senzorii, actuatoarele, automatele programabile, gateway-urile industriale şi sistemele de supraveghere nu formează o listă de componente, ci un lanţ în care performanţa rezultată este dată de veriga cea mai slabă, nu de cea mai performantă. Un senzor exact conectat la un modul greşit configurat, o logică corectă executată cu o valoare nevalidată sau o interfaţă impecabilă grafic care afişează o valoare neactualizată produc, toate, acelaşi rezultat: o decizie luată pe o informaţie falsă.

Din această perspectivă, capitolul a insistat asupra a trei delimitări pe care practica le confundă frecvent. Prima separă mărimea măsurată de calitatea măsurării: o valoare fără informaţie de validitate nu este o valoare, iar mecanismele care permit diferenţierea unui defect de o stare normală – domeniile rezervate semnalizării defectului, codurile de stare, verificările de plauzibilitate – trebuie proiectate explicit, nu presupuse. A doua separă comanda de confirmare şi de starea reală, atât în programul controlerului, cât şi în reprezentarea oferită operatorului. A treia separă controlul de supraveghere: interblocările, reglajele rapide şi funcţiile de protecţie rămân la nivelul local, iar sistemele superioare colectează, prezintă şi solicită, fără să preia răspunderea deterministă.

Aceleaşi delimitări explică de ce criteriile de selecţie prezentate în capitol nu se reduc la specificaţia de catalog. Un senzor se alege pe baza întregului lanţ de măsurare, nu a toleranţei elementului sensibil; clasa de toleranţă impune modul de conectare, iar rezoluţia afişată nu poate depăşi acurateţea demonstrabilă. Un actuator se alege împreună cu elementul final de control şi cu starea pe care o adoptă la pierderea energiei, stare care se obţine constructiv şi se verifică prin încercare, nu

se presupune din denumirea componentei. Un controler se alege pe baza comportamentului la defectarea unui modul sau la pierderea comunicației, nu doar a timpului de scanare declarat. În fiecare dintre cazuri, criteriul decisiv este comportamentul la abatere, nu performanța în regim nominal.

Tratarea cantitativă introdusă în capitol arată că aceste delimitări au consecințe măsurabile. Bugetul timpului de reacție demonstrează că întârzierea unei funcții de automatizare provine, în cea mai mare parte, din elemente asupra cărora programul nu are influență, ceea ce reorientează efortul de optimizare dinspre procesor către lanțul fizic. Bugetul de latență pe traseul către baza de date arată că întârzierea dominantă nu provine din rețea, ci din două decizii de configurare, și că un asemenea lanț este adecvat supravegherii, nu controlului. Calculul lățimii de bandă indică faptul că gruparea mesajelor reduce volumul de aproape cinci ori fără pierdere de informație, în timp ce transmiterea la excepție aduce un câștig suplimentar cu un cost informațional real. Calculul forței și al consumului unui cilindru pneumatic arată că diferența dintre extindere și retragere și volumul de aer liber consumat pe ciclu determină dimensionarea și factura de energie, nu catalogul. În toate cazurile, diferența dintre o instalație bine dimensionată și una risipitoare ține de decizii luate conștient în locul valorilor implicite, nu de tehnologie.

Exercițiile aplicative au parcurs traseul complet al unei valori de proces: achiziția semnalului, validarea și scalarea în automatul programabil, utilizarea în logica de control, afișarea în interfața de operare, alarmarea și arhivarea. Ele au arătat de asemenea că validarea unei aplicații nu se confundă cu demonstrarea funcționării ei: cazurile care contează sunt cele în care ceva nu merge – depășirea mai scurtă decât temporizarea, valoarea aflată între pragul de activare și cel de revenire, circuitul întrerupt, comanda respinsă, comunicația pierdută. O aplicație testată exclusiv pe traiectoria nominală pare corectă și eșuează în exploatare.

O fabrică conectată se sprijină tehnic pe senzori, actuatoare, automate programabile, interfețe de operare, sisteme de supraveghere și gateway-uri integrate, dar prezența acestor componente nu constituie, prin ea însăși, o arhitectură IIoT completă. Exercițiul din secțiunea 5.7 s-a oprit deliberat la o integrare verticală locală: un client citește direct de la un controler, în aceeași rețea și sub aceeași administrare. Circulația coerentă a datelor între câmp, control, supraveghere și sisteme externe presupune protocoale compatibile, modele de comunicație adecvate și securitate aplicată consecvent. Acestea sunt tratate în Capitolul 6, dedicat protocoalelor de comunicare industrială și IIoT, unde revin, ca proprietăți ale protocoalelor, cele trei cerințe de aici: transportul calității datelor, delimitarea dintre solicitare și confirmare și separarea controlului local de accesul extern.

5.9. Întrebări de verificare

1. *Care este avantajul semnalului de curent 4–20 mA legat de detectarea defectelor, în afara rezistenței la perturbații?*

a) semnalul nu poate fi afectat de defectarea transmițătorului;
b) semnalul de 0 mA indică întotdeauna valoarea minimă a mărimii măsurate;
c) limita inferioară a domeniului util este 4 mA, deci întreruperea circuitului (0 mA) se distinge de o valoare măsurată validă;
d) întreruperea circuitului produce automat valoarea maximă de 20 mA.

2. *Un senzor Pt100 de clasă A are toleranța ±(0,15 + 0,002·|t|) °C. Care este abaterea admisă la 100 °C?*

a) ±0,27 °C;
b) ±0,35 °C;
c) ±0,80 °C;
d) ±0,15 °C.

3. *Un senzor furnizează la măsurări repetate valori foarte apropiate între ele, dar toate afectate de aceeași eroare sistematică față de valoarea de referință. Cum se caracterizează?*

a) precis, dar insuficient de exact;
b) cu rezoluție nulă;
c) exact, dar imprecis;
d) exact și precis.

4. *Cum este obținută poziția sigură a unei valve cu acționare pneumatică la pierderea aerului comprimat?*

a) prin platforma de analiză din cloud, care detectează pierderea aerului;
b) prin sistemul SCADA, care transmite comanda de închidere;
c) constructiv, prin arc, și nu depinde de programul controlerului;
d) prin programul PLC, care comandă valva în poziția sigură.

5. *Un senzor are timpul de răspuns de 2 ms, filtrul de intrare 3 ms, conversia 1 ms, scanarea PLC 10 ms, ieșirea cu relee 10 ms și actuatorul 15 ms. Care este timpul de reacție în cazul cel mai defavorabil (două cicluri de scanare)?*

a) 31 ms, deoarece scanarea nu se include în bugetul de reacție;
b) 41 ms, deoarece se numără un singur ciclu de scanare;
c) 10 ms, deoarece reacția este determinată de timpul de scanare;
d) 51 ms.

6. *Ce face mecanismul de stocare și retransmitere (store-and-forward) al unui gateway industrial?*

a) convertește protocolul Modbus RTU în Modbus TCP fără a păstra mesajele;
b) reia la restabilire valorile curente și le marchează cu ora restabilirii;
c) păstrează local mesajele la pierderea conexiunii și le expediază după restabilire, fiecare cu marca temporală inițială;
d) șterge mesajele netransmise pentru a nu încărca sistemul receptor.

7. *În bugetul de latență al lanțului senzor–PLC–gateway–broker–bază de date, care sunt contribuțiile dominante?*

a) criptarea TLS și serializarea mesajului;
b) intervalul de publicare al abonării OPC UA și acumularea în loturi la scrierea în baza de date, ambele fiind decizii de configurare;
c) conversia analog–digital și filtrul de intrare;
d) rețeaua locală de 1 Gbit/s și procesorul PLC.

8. *Care este relația corectă dintre sistemul SCADA și automatul programabil în privința comenzilor?*

a) SCADA preia interblocările și reglajele rapide ale PLC pentru a le executa centralizat;
b) SCADA realizează controlul de supraveghere și transmite cereri către PLC, care verifică interblocările și condițiile locale înainte de aplicare; SCADA nu scrie direct în ieșirile fizice;
c) pierderea serverului SCADA oprește automat toate funcțiile esențiale ale instalației;
d) SCADA scrie direct în ieșirile fizice ale PLC pentru a obține un răspuns determinist.

9. *Care afirmație despre alarme și evenimente este corectă?*

a) o alarmă este utilă chiar dacă nu cere nicio reacție din partea operatorului;
b) orice modificare de stare este o alarmă, iar confirmarea ei elimină defecțiunea;
c) alarmele și evenimentele sunt sinonime și au aceeași prioritate în orice sistem;
d) pornirea unui motor este un eveniment, iar declanșarea protecției sale este o alarmă; confirmarea unei alarme arată că operatorul a observat-o, nu că problema a fost eliminată.

10. *Pentru 250 de variabile (200 la 1 Hz și 50 la 10 Hz), transmiterea fiecărei valori într-un mesaj separat generează circa 700 mesaje/s și aproximativ 1,5 Mbit/s. Care este concluzia corectă privind dimensionarea într-o rețea locală de 1 Gbit/s?*

a) lățimea de bandă locală nu este o problemă; constrângerile reale sunt volumul stocat, numărul de mesaje procesate de broker și baza de date și legătura către exterior;
b) transmiterea la excepție este interzisă, deoarece pierde informații esențiale;
c) lățimea de bandă locală este restricția dominantă și impune reducerea numărului de variabile;
d) gruparea mesajelor este inutilă, deoarece nu modifică volumul de date transmis.

6. PROTOCOALE DE COMUNICARE INDUSTRIALĂ ȘI IIOT

Comunicarea industrială asigură schimbul de date dintre senzori, actuatoare, automate programabile, interfețe HMI, sisteme SCADA, gateway-uri industriale și aplicații informatice. Capitolul anterior a prezentat componentele care produc și consumă aceste date; capitolul de față tratează regulile după care ele comunică. Alegerea protocoalelor influențează timpul de răspuns, disponibilitatea instalației, interoperabilitatea echipamentelor, posibilitatea diagnosticării și integrarea informației cu nivelurile superioare ale întreprinderii. Este o decizie de arhitectură, nu una de achiziție: ea determină ce se poate măsura, ce se poate corela și ce rămâne inaccesibil pe toată durata de viață a instalației.

Cerințele nu sunt identice pe întregul traseu al datelor. O buclă de control sau o aplicație de sincronizare a axelor necesită timpi de transmisie previzibili, în timp ce raportarea producției, analiza consumurilor și transmiterea datelor către o platformă externă tolerează întârzieri mai mari, dar solicită scalabilitate, securitate și integrare cu tehnologiile informatice. Din acest motiv, întrebarea utilă nu este care protocol este cel mai bun, ci care protocol este potrivit pentru fiecare segment și pentru fiecare categorie de date.

Trebuie diferențiate mediul fizic, tehnologia de rețea și protocolul aplicației. RS-485 definește caracteristici electrice ale comunicației seriale, iar Ethernet stabilește mecanisme de transmisie la nivelurile fizic și de legătură de date. Modbus, PROFIBUS, PROFINET, EtherNet/IP și EtherCAT adaugă reguli pentru schimbul de informații industriale, iar OPC UA și MQTT răspund cerințelor de integrare și de distribuire a datelor către aplicații, servicii de procesare edge și platforme externe. Confuzia dintre aceste niveluri este sursa celor mai multe comparații lipsite de sens între tehnologii care nu îndeplinesc aceeași funcție.

Niciun protocol nu este optim pentru toate nivelurile. O arhitectură IIoT utilizează, de regulă, mai multe tehnologii complementare: un protocol determinist pentru control, un mecanism standardizat de acces la date și un protocol scalabil pentru distribuirea mesajelor. Modernizarea unei instalații existente nu presupune înlocuirea comunicațiilor care funcționează, ci separarea funcțiilor și adăugarea controlată a conectivității.

Capitolul urmează acest parcurs. Primul subcapitol tratează protocoalele de câmp și de control, împreună cu noțiunile de determinism și comportament temporal fără de care compararea lor nu este posibilă. Al doilea prezintă protocoalele de integrare, cu accent pe OPC UA și MQTT, pe delimitarea rolurilor dintre ele și pe convențiile care fac o implementare administrabilă. Al treilea așază aceste

tehnologii în stiva de comunicaţie şi urmăreşte traseul unei valori de la traductor până la baza de date. Al patrulea transformă criteriile de selecţie în calcule de dimensionare, iar al cincilea propune exerciţii de validare etapizată.

O regulă traversează întregul capitol şi se enunţă de la început: funcţiile de control, interblocările şi funcţiile de siguranţă rămân locale. Fluxul către platformă este un flux de observare, iar indisponibilitatea lui nu are voie să afecteze conducerea procesului. Consecinţele arhitecturale ale acestei reguli sunt dezvoltate în capitolul 7, iar cele de securitate, în capitolul 8.

Obiectivele capitolului

La finalul acestui capitol, cititorul va fi capabil să:

- diferenţieze protocoalele industriale clasice de protocoalele de integrare IIoT, după rolul dominant, modelul de date şi comportamentul la întreruperea comunicaţiei;
- explice determinismul, latenţa şi variaţia latenţei şi să stabilească dacă o comunicaţie satisface cerinţele temporale ale unei funcţii date;
- compare modelele client–server, producător–consumator şi publicare–abonare din perspectiva cuplării, a numărului de conexiuni necesare şi a extinderii cu noi consumatori;
- descrie rolul Modbus, PROFIBUS, PROFINET, EtherNet/IP şi EtherCAT în zona OT, precum şi limitele lor în raport cu integrarea externă;
- explice contribuţia OPC UA la interoperabilitate, prin spaţiul de adrese, modelul informaţional, transportul calităţii datelor şi mecanismele de securitate;
- descrie rolurile MQTT, Sparkplug, AMQP şi CoAP şi să definească o convenţie de subiecte şi un contract de date pentru un echipament;
- calculeze bugetul de latenţă şi lăţimea de bandă ale unui flux de date, pornind de la parametrii de configurare declaraţi;
- selecteze protocoalele pentru fiecare segment al unei arhitecturi hibride şi să argumenteze alegerea prin cerinţele procesului.

6.1. Protocoale industriale clasice

Protocoalele industriale clasice au fost dezvoltate pentru schimbul fiabil de date între senzori, module de intrare–ieşire, automate programabile, sisteme de acţionare, roboţi, interfeţe HMI, sisteme SCADA şi controlere de proces. Înainte ca IIoT să devină o direcţie majoră de dezvoltare, ele au constituit infrastructura comunicaţiilor din fabrici, instalaţii energetice, procese chimice şi sisteme de transport. Poziţia lor în arhitectura OT–IIoT este reprezentată în Figura 6.1.

Proiectarea lor a urmărit cerinţele zonei OT: fiabilitatea, rezistenţa la perturbaţii electromagnetice, predictibilitatea comunicaţiei, compatibilitatea cu echipamentele industriale şi funcţionarea în condiţii de mediu dificile. Spre deosebire de

comunicațiile informatice obișnuite, comunicațiile industriale susțin procese fizice, în care pierderea unui mesaj, transmiterea întârziată a unei comenzi sau interpretarea greșită a unei stări poate determina oprirea producției, apariția rebuturilor sau apariția unor riscuri privind siguranța.

Aceste protocoale rămân relevante în arhitecturile IIoT. Modernizarea nu presupune înlocuirea automată a comunicațiilor existente. În numeroase aplicații, soluția adecvată este hibridă: protocoalele industriale rămân în zona de teren și de control, iar gateway-urile industriale și serviciile de procesare la edge transformă datele în formate potrivite pentru SCADA, MES, baze de date, aplicații de analiză sau servicii cloud. Subcapitolul prezintă mai întâi noțiunile fără de care compararea acestor tehnologii nu este posibilă, apoi principalele familii de protocoale și, în final, poziționarea lor în raport cu integrarea IIoT.

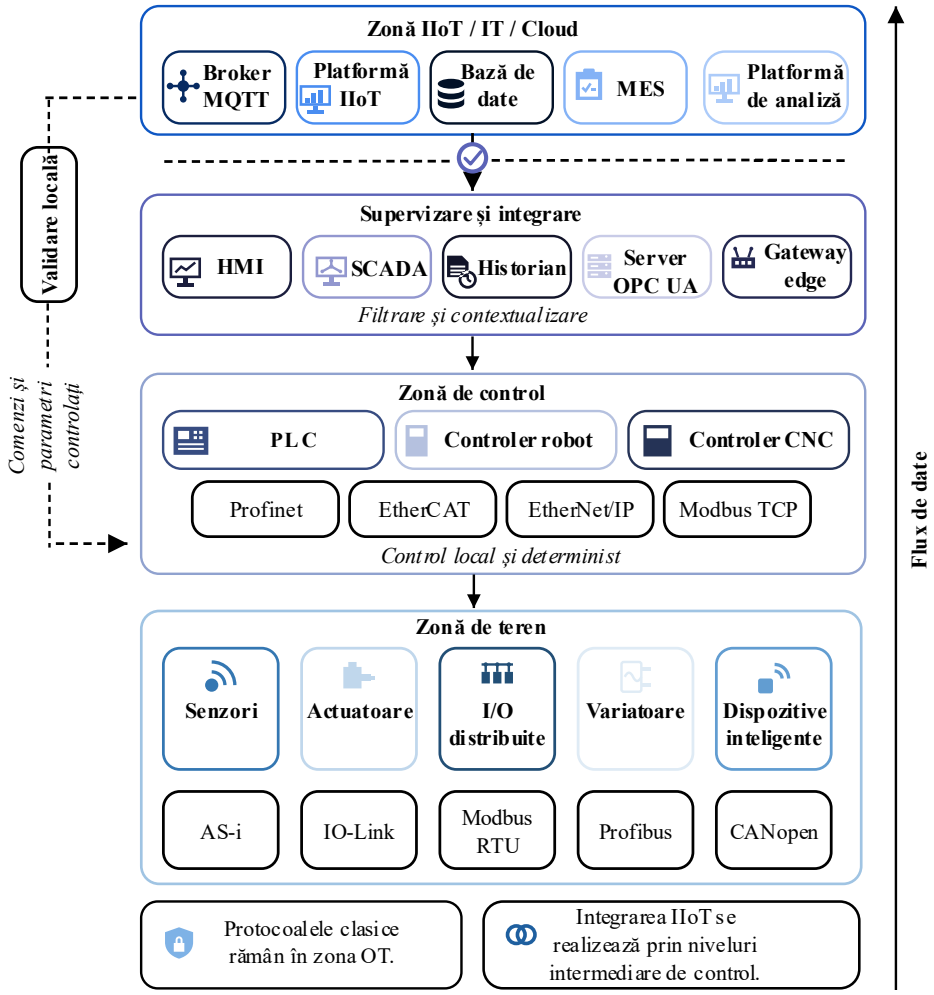


Figura 6.1 – Protocoalele industriale clasice în arhitectura OT–IIoT

6.1.1. Determinismul şi comunicarea în timp real

Într-un sistem industrial, viteza ridicată nu este echivalentă cu funcţionarea în timp real. O comunicaţie este adecvată unei funcţii de timp real dacă informaţia ajunge la destinaţie înaintea termenului impus de proces şi dacă variaţia timpului de transmisie se menţine în limite cunoscute. Determinismul nu înseamnă, prin urmare, rapiditate, ci existenţa unei limite superioare demonstrabile pentru întârziere şi pentru variaţia ei. O reţea care livrează mesajul în 2 ms în 99 % dintre cazuri şi în 40 ms în restul cazurilor este mai rapidă în medie, dar mai puţin deterministă decât una care livrează întotdeauna în 8 ms.

Evaluarea unei comunicaţii industriale trebuie să considere timpul de ciclu, latenţa dintre emitere şi recepţie, variaţia acestei latenţe, probabilitatea pierderii mesajelor, timpul necesar detectării unei întreruperi, comportamentul la supraîncărcarea reţelei, sincronizarea temporală dintre dispozitive şi timpul de revenire după o defecţiune. Standardul care formalizează această evaluare pentru reţelele Ethernet industriale defineşte un set de indicatori de performanţă comparabili între profiluri – între care timpul de livrare, numărul de staţii, debitul util, precizia sincronizării temporale şi timpul de restabilire după o redundanţă – tocmai pentru ca alegerea să nu se sprijine pe afirmaţii comerciale [24].

Cerinţele diferă considerabil în funcţie de aplicaţie. Controlul temperaturii unui proces lent tolerează actualizări la intervale de sute de milisecunde; automatizarea generală a unei maşini se încadrează uzual în cicluri de ordinul milisecundelor; sincronizarea mai multor servomotoare impune cicluri sub o milisecundă şi o variaţie a întârzierii de ordinul microsecundelor. Pentru monitorizare şi arhivare, completitudinea datelor, marcarea lor temporală şi retransmiterea după o întrerupere contează mai mult decât livrarea într-un interval scurt.

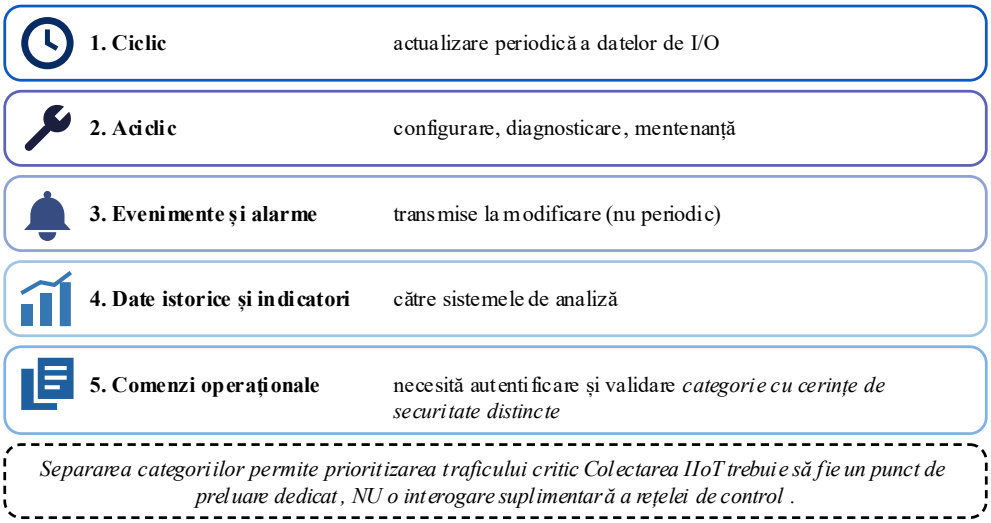


Figura 6.2 – Cele cinci categorii de trafic industrial

O regulă de dimensionare aplicabilă înaintea alegerii oricărei tehnologii provine din teoria reglării: perioada de eşantionare a buclei trebuie să fie de cinci până la zece ori mai mică decât constanta de timp dominantă a procesului condus. Pentru un proces termic cu o constantă de timp de 30 s, o perioadă de 3 s este suficientă, iar utilizarea unei reţele izocrone nu aduce niciun beneficiu funcţional. Pentru o axă de poziţionare cu o constantă de timp de 20 ms, perioada admisibilă coboară la 2–4 ms, iar tehnologia de comunicaţie devine un factor determinant. Supradimensionarea nu este neutră: perioade de actualizare foarte scurte, cerute pentru toate variabilele, cresc traficul şi încărcarea controlerelor fără să îmbunătăţească reglarea.

Traficul industrial se împarte în trafic ciclic, prin care sunt actualizate periodic intrările şi ieşirile; trafic aciclic, utilizat pentru configurare, diagnosticare şi mentenanţă; evenimente şi alarme, transmise la apariţia unei modificări; date istorice şi indicatori, transferate către aplicaţii de analiză; şi comenzi operaţionale, care necesită autentificare şi validare înainte de executare. Separarea acestor categorii (Figura 6.2) permite prioritizarea traficului critic şi împiedică transferurile secundare să afecteze controlul procesului. Este şi motivul pentru care colectarea datelor pentru o platformă IIoT nu se face prin interogarea suplimentară a reţelei de control, ci printr-un punct de preluare dedicat.

6.1.2. Magistralele de câmp şi CAN

Magistralele de câmp (*fieldbus*) au înlocuit o parte dintre conexiunile individuale dintre controler şi dispozitivele de teren cu o cale comună de comunicaţie. Prin aceeaşi reţea sunt transmise valori de proces, comenzi, parametri şi informaţii de diagnosticare. O magistrală de câmp cuprinde mediul fizic şi elementele de conectare, regulile de acces la reţea, structura cadrelor, adresarea dispozitivelor, detectarea erorilor, servicii pentru schimbul ciclic şi aciclic de date şi profiluri care uniformizează comportamentul anumitor categorii de echipamente.

Avantajele principale sunt reducerea cablării, diagnosticarea mai detaliată şi posibilitatea configurării de la distanţă a dispozitivelor. În schimb, proiectarea incorectă a magistralei, terminarea necorespunzătoare, depăşirea lungimilor admise sau utilizarea unor adrese duplicate afectează simultan mai multe echipamente – un mod de defectare pe care conexiunile individuale nu îl aveau.

CAN (*Controller Area Network*) defineşte mecanismele de comunicaţie la nivelul legăturii de date şi la subnivelul de codificare fizică. Mesajele sunt identificate printr-un identificator care stabileşte şi prioritatea accesului la magistrală; dacă mai multe noduri transmit simultan, arbitrarea este nedistructivă, iar mesajul cu prioritatea cea mai ridicată îşi continuă transmisia fără repetare. Mecanismele de detectare a erorilor, de retransmitere şi de izolare a nodurilor defecte contribuie la robusteţea comunicaţiei. Ediţia în vigoare a standardului este a treia şi înlocuieşte ediţia din 2015; pe lângă formatul clasic, cu câmpuri de date de cel mult 8 octeţi, şi formatul cu rată variabilă, ea specifică formatul extins, care admite câmpuri de date

de până la 2048 de octeți [165]. Distincția are consecințe practice: o instalație proiectată pe formatul clasic nu poate transporta structuri de date mari fără fragmentare la nivel superior.

Comportamentul temporal al unei magistrale CAN se poate estima direct. Un cadru standard cu opt octeți de date ocupă aproximativ 111 biți, iar inserția biților de umplere îl poate extinde la circa 135. La o rată de 500 kbit/s, transmisia durează, prin urmare, între 0,22 și 0,27 ms. Aceasta este însă durata proprie a cadrului, nu timpul de răspuns: un mesaj cu prioritate redusă poate fi întârziat de toate mesajele cu prioritate mai mare aflate în așteptare, astfel încât timpul său de răspuns în cel mai defavorabil caz este suma propriei transmisii și a blocajului produs de acestea. Determinismul unei rețele CAN nu rezultă din protocol, ci din proiectarea traficului: perioade de transmitere stabilite explicit, priorități alocate în funcție de criticitate și o încărcare maximă a magistralei menținută sub un prag verificat prin calcul.

CAN nu definește singur toate informațiile necesare unei aplicații industriale. Protocoale de nivel superior adaugă modele de dispozitiv, obiecte de comunicație, profiluri și reguli de configurare. CANopen structurează dispozitivul printr-un dicționar de obiecte, separă obiectele de date de proces de cele de serviciu, definește gestiunea stărilor rețelei și mesajele de urgență și admite rate cuprinse între 10 kbit/s și 1 Mbit/s [166]. Este utilizat în acționări, echipamente mobile, sisteme de transport și mașini cu arhitectură distribuită. DeviceNet aplică peste CAN un model de obiecte comun cu celelalte tehnologii din aceeași familie.

6.1.3. Modbus RTU și Modbus TCP

Modbus funcționează pe principiul cerere–răspuns: un echipament cere date, altul răspunde. Se folosește între controlere, module de intrare și ieșire, instrumente de măsurare, convertizoare de frecvență și alte echipamente industriale. Fiind simplu, a fost adoptat pe scară largă și a rezistat neobișnuit de mult.

Modelul de date cuprinde patru categorii: bobine, pentru valori booleene care pot fi citite și scrise; intrări discrete, pentru valori booleene numai în citire; registre de intrare, pentru valori numerice numai în citire; și registre de menținere, pentru valori numerice care pot fi citite și scrise. Operațiile sunt identificate prin coduri de funcție, iar protocolul transmite adresa și valoarea, fără să descrie semnificația tehnologică a registrului [155]. Unitatea de măsură, factorul de scalare, ordinea octeților și interpretarea grupurilor de registre trebuie obținute din documentația echipamentului.

Modbus RTU transmite cadre binare printr-o conexiune serială, de regulă RS-485. Clientul, denumit tradițional master, inițiază interogarea, iar serverul adresat, denumit tradițional slave, răspunde. Utilizarea unei magistrale comune reduce cablarea, dar comunicarea rămâne strict secvențială. Viteza de transmisie, paritatea și numărul biților de oprire trebuie configurate identic pe toate dispozitivele conectate la aceeași magistrală. În schimb, fiecare server trebuie să aibă o adresă unică

pe magistrală, astfel încât clientul să poată identifica fără ambiguitate dispozitivul căruia îi este destinată cererea. Parametrii de comunicaţie şi adresele atribuite trebuie documentate. Modbus TCP păstrează modelul de date şi codurile de funcţie, dar transportă mesajele prin TCP/IP, pe portul rezervat 502 [167].

Caracterul secvenţial al variantei seriale impune un calcul de dimensionare înaintea stabilirii perioadei de interogare. Se consideră o linie RS-485 la 19200 bit/s, cu formatul de caracter 8E1, adică 11 biţi transmişi pentru fiecare octet. O cerere de citire a 20 de registre de menţinere are 8 octeţi, iar răspunsul, 45: un octet de adresă, unul de cod de funcţie, unul de contor, 40 de octeţi de date şi doi de control. Cei 53 de octeţi însumează 583 de biţi, adică 30,4 ms de transmisie efectivă. La aceasta se adaugă cele două intervale de linişte de 3,5 caractere, circa 2,0 ms fiecare, şi timpul de prelucrare al dispozitivului, estimat la 10 ms. Rezultă aproximativ 44 ms pentru o tranzacţie şi circa 0,44 s pentru interogarea succesivă a zece dispozitive. O perioadă de achiziţie de o secundă este, prin urmare, realizabilă; una de 100 ms nu este. Creşterea vitezei la 115.200 bit/s reduce termenul de transmisie la 5,1 ms; peste 19.200 bit/s specificaţia Modbus serial fixează intervalul de linişte dintre cadre la 1,75 ms, astfel că totalul coboară doar la circa 18,6 ms pe tranzacţie (5,1 + 2 × 1,75 + 10), pentru că timpul de prelucrare al dispozitivului devine termenul dominant – o ilustrare a regulii enunţate în secţiunea 6.3.4, potrivit căreia intervenţia are efect numai asupra termenului dominant.

Modbus are mai multe avantaje: se implementează uşor, există pe multe categorii de echipamente, permite integrarea dispozitivelor de la furnizori diferiţi, are convertoare între variantele seriale şi Ethernet, iar datele se preiau simplu prin automate programabile, SCADA şi gateway-uri industriale. Limitările vin din modelul de date redus şi din lipsa contextului semantic: două echipamente pot folosi aceeaşi adresă de registru pentru mărimi complet diferite. De aceea ai nevoie de o hartă a registrelor, cu adresa, tipul de date, scalarea, unitatea de măsură, drepturile de acces şi frecvenţa recomandată de interogare. Harta face parte din proiect, nu din nota de punere în funcţiune, şi se păstrează cu documentaţia instalaţiei.

Protocolul de bază nu asigură autentificarea şi nici confidenţialitatea. Specificaţia distinctă de securitate încapsulează mesajele Modbus în TLS, utilizează certificate X.509v3 pentru autentificarea reciprocă a clientului şi a serverului şi foloseşte portul rezervat 802 [168]. Compatibilitatea trebuie verificată pentru fiecare echipament, deoarece adoptarea în produsele existente este parţială. În instalaţiile aflate în exploatare, dispozitivele Modbus se păstrează în reţele segmentate şi se conectează la sistemele superioare prin automate programabile sau prin gateway-uri industriale securizate, pe traseul: echipament Modbus RTU, convertor sau gateway industrial, Modbus TCP ori OPC UA, SCADA şi platformă IIoT.

Gateway-ul trebuie să păstreze corespondenţa dintre registre şi mărimile tehnologice, să limiteze explicit operaţiile de scriere permise şi să trateze pierderea

comunicației cu dispozitivul serial ca pe o stare distinctă, semnalată prin codul de calitate al valorii, nu prin repetarea ultimei valori citite.

6.1.4. PROFIBUS şi PROFINET

PROFIBUS şi PROFINET aparţin aceleiaşi familii tehnologice, dar se sprijină pe arhitecturi diferite: primul este o magistrală de câmp, al doilea o tehnologie Ethernet industrială. Distincţia nu este formală. PROFIBUS este standardizat ca tip 3 în seria de specificaţii de magistrală, în timp ce PROFINET constituie familia de profiluri CPF 3 din standardul dedicat reţelelor Ethernet în timp real, unde îi sunt asociate clase de conformitate şi indicatori de performanţă măsurabili [24]. Migrarea dintre ele se realizează gradual, prin controlere, legături de reţea şi gateway-uri industriale, nu prin înlocuirea simultană a instalaţiei.

PROFIBUS DP serveşte la schimbul rapid de date între controler şi periferia distribuită. De obicei foloseşte transmisie RS-485 şi comunicare ciclică între controler şi dispozitive, iar parametrii echipamentelor sunt descrişi în fişiere de configurare date de producător. Serviciile aciclice permit diagnosticarea şi parametrizarea în paralel cu schimbul ciclic. Viteza poate ajunge la 12 Mbit/s, dar cu cât creşte viteza, cu atât segmentul poate fi mai scurt: aproximativ 1.200 m la 9,6 kbit/s, în jur de 200 m la 1,5 Mbit/s şi circa 100 m la 12 Mbit/s. Sunt valori orientative, de verificat în documentaţia cablului şi a repetoarelor. Alegerea dintre viteză şi lungime se face la proiectare, nu la punerea în funcţiune.

PROFIBUS este întâlnit în instalaţii cu durată mare de exploatare, module de intrare şi ieşire, acţionări şi echipamente de proces. Menţinerea sa este justificată dacă reţeaua îndeplineşte cerinţele aplicaţiei şi există suport pentru componente. Extinderea către sistemele informatice se realizează prin controler sau printr-un gateway industrial, nu prin expunerea directă a magistralei.

PROFINET IO organizează comunicaţia în jurul a trei roluri: controlerul de intrări şi ieşiri, care gestionează schimbul de date; dispozitivele de intrări şi ieşiri, precum modulele distribuite şi acţionările; şi supervizorul, folosit pentru configurare şi diagnosticare. Modelul de schimb este de tip producător–consumator, iar dispozitivele sunt descrise prin fişiere în format XML [169]. Arhitectura separă comunicaţia standard bazată pe TCP/IP de transferul datelor de proces: canalul în timp real, PROFINET RT, acoperă automatizarea generală, cu timpi de ciclu de ordinul milisecundelor, iar PROFINET IRT asigură comunicaţie izocronă pentru aplicaţii cu cerinţe stricte de sincronizare, cu cicluri sub o milisecundă. Comunicaţia standard, traficul RT şi traficul IRT coexistă pe aceeaşi infrastructură, iar topologiile pot fi de tip linie, stea şi inel [169].

Clasele de conformitate definite în standardul de profiluri stabilesc ce anume este certificat: în cea mai permisivă, numai dispozitivele; în următoarea, şi infrastructura de reţea; în cea mai strictă, şi capacitatea de comunicaţie izocronă [24]. Precizarea clasei în caietul de sarcini este singurul mod prin care beneficiarul poate

impune un nivel de performanţă verificabil, în locul unei cerinţe generice de „compatibilitate PROFINET".

Profilurile complementare permit utilizarea aceleiaşi infrastructuri pentru funcţii specializate: PROFIsafe tratează comunicaţia asociată siguranţei funcţionale şi este standardizat ca IEC 61.784-3-3, PROFIdrive uniformizează integrarea acţionărilor, iar PROFIenergy sprijină gestionarea stărilor energetice. Utilizarea unui profil nu elimină necesitatea validării aplicaţiei şi a respectării standardelor specifice funcţiei implementate; un canal de comunicaţie certificat nu constituie, singur, o funcţie de siguranţă.

PROFINET facilitează integrarea dintre nivelurile operaţionale şi cele informatice, dar această capacitate nu justifică plasarea tuturor dispozitivelor în aceeaşi reţea. Traficul de control trebuie separat logic de accesul pentru configurare, diagnosticare şi colectarea datelor IIoT, iar preluarea datelor pentru platformă trebuie să se facă dintr-un punct dedicat, nu prin interogarea suplimentară a reţelei care susţine ciclul de proces.

6.1.5. EtherNet/IP

EtherNet/IP este o tehnologie Ethernet industrială care aplică protocolul industrial comun (CIP) peste Ethernet şi familia TCP/IP. CIP utilizează un model orientat pe obiecte şi defineşte servicii, profiluri de dispozitiv şi mecanisme pentru configurare, control, diagnosticare şi schimb de informaţii [170].

Caracteristica structurală a acestei familii este independenţa faţă de mediul de comunicaţie. Acelaşi nivel aplicaţie este utilizat peste Ethernet, în cazul EtherNet/IP, peste CAN, în cazul DeviceNet, şi peste alte medii, iar profilurile corespunzătoare sunt definite în seriile IEC 61.784-1 şi IEC 61.784-2 ca membri ai aceleiaşi familii de profiluri de comunicaţie. Consecinţa practică nu este de ordin teoretic: un profil de dispozitiv, o structură de parametri şi o procedură de punere în funcţiune învăţate pe una dintre reţele rămân valabile pe celelalte, ceea ce reduce efortul de inginerie într-o instalaţie cu tehnologii mixte.

Informaţia unui dispozitiv este organizată în obiecte. Obiectul de identitate expune producătorul, tipul, codul produsului şi versiunea, obiectele de tip ansamblu grupează datele de intrare şi de ieşire într-o structură transferabilă printr-o singură conexiune, obiectul de parametri descrie mărimile configurabile, iar managerul de conexiuni administrează stabilirea şi menţinerea conexiunilor. Această organizare explică de ce, într-o reţea EtherNet/IP, punerea în funcţiune constă în principal din alegerea ansamblurilor şi a intervalelor de actualizare, nu din construirea manuală a unei hărţi de adrese, cum se întâmplă în cazul Modbus.

EtherNet/IP utilizează două forme principale de mesagerie:

- mesaje explicite, utilizate pentru configurare, diagnosticare și operații de tip cerere–răspuns, în care fiecare mesaj conține descrierea completă a serviciului solicitat;
- mesaje implicite, utilizate pentru schimbul periodic al datelor de intrare și ieșire, în care semnificația conținutului este stabilită la deschiderea conexiunii, iar cadrele transportă exclusiv date.

Mesajele explicite sunt transportate în mod obișnuit prin TCP, iar datele ciclice de intrare și ieșire utilizează UDP. Modelul producător–consumator permite distribuirea acelorași date către mai mulți consumatori, fără repetarea nejustificată a informației.

Perioada solicitată de actualizare stabilește intervalul la care un echipament produce datele pentru o conexiune. Configurarea unor perioade foarte scurte pentru toate dispozitivele crește traficul și încărcarea controlerelor fără a îmbunătăți neapărat controlul, iar efectul se resimte în primul rând asupra procesorului de comunicație al controlerului, nu asupra lățimii de bandă. Intervalele trebuie stabilite în funcție de dinamica procesului și de rolul fiecărei variabile: un semnal de poziție și o temperatură de ulei nu au aceeași nevoie de actualizare.

Un aspect frecvent subestimat este distribuirea multicast a datelor produse. Într-o rețea în care comutatoarele nu gestionează apartenența la grupuri multicast, cadrele sunt difuzate către toate porturile, inclusiv către dispozitive care nu le consumă. Rezultatul este încărcarea inutilă a interfețelor și, la echipamentele cu resurse reduse, pierderi de cadre fără cauză aparentă. Configurarea comutatoarelor aparține proiectării rețelei, nu depanării ei.

EtherNet/IP poate utiliza infrastructură Ethernet standardizată, dar rețeaua industrială necesită proiectare controlată. Comutatoarele, segmentarea, prioritizarea traficului, gestionarea mesajelor multicast, sincronizarea timpului și redundanța trebuie configurate în raport cu cerințele aplicației. Pentru funcții precum controlul mișcării, sincronizarea și siguranța există extensii CIP dedicate, iar securizarea comunicației se realizează prin CIP Security, care aplică TLS pentru traficul bazat pe TCP și DTLS pentru traficul ciclic bazat pe UDP și definește profiluri distincte pentru confidențialitatea comunicației, autentificarea utilizatorilor și dispozitivele cu resurse limitate. Suportul efectiv diferă între echipamente și trebuie verificat înaintea proiectării; disponibilitatea unei extensii în specificație nu implică prezența ei în produsul achiziționat.

Într-o arhitectură IIoT, EtherNet/IP poate transporta datele între controlere și dispozitivele locale, iar informațiile selectate sunt furnizate sistemelor superioare printr-un server OPC UA, un gateway industrial sau o interfață controlată. Utilizarea aceleiași infrastructuri Ethernet nu înseamnă că dispozitivele de control trebuie să fie accesibile direct din rețeaua întreprinderii. Distincția dintre compatibilitatea tehnică și necesitatea funcțională este, în acest caz, decizia de arhitectură cu cel mai mare impact asupra securității instalației.

Secţiunea următoare tratează o tehnologie construită pe un principiu diferit de prelucrare a cadrelor, destinată aplicaţiilor cu cicluri foarte scurte şi sincronizare precisă: EtherCAT.

6.1.6. EtherCAT

EtherCAT este o tehnologie Ethernet industrială destinată aplicaţiilor cu cicluri scurte şi sincronizare precisă, standardizată ca tip 12 în seria de specificaţii de magistrală şi ca familie de profiluri CPF 12 în standardul reţelelor Ethernet în timp real [24]; specificaţia de referinţă este publicată de organizaţia care administrează tehnologia, sub denumirea ETG.1000 [171].

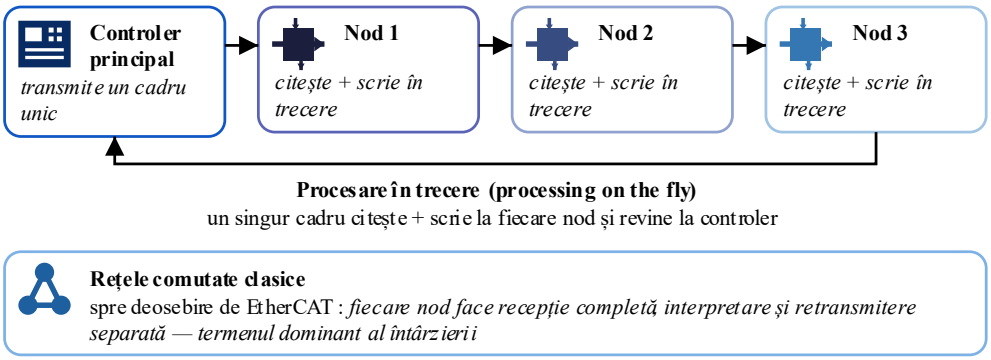


Figura 6.3 – Procesarea în EtherCAT

Principiul de funcţionare o separă de celelalte tehnologii Ethernet industriale. Controlerul principal transmite un cadru care parcurge succesiv dispozitivele, iar fiecare nod citeşte datele care îi sunt destinate şi îşi inserează propriile date în timp ce cadrul traversează echipamentul. Această prelucrare în trecere, reprezentată în Figura 6.3, elimină recepţionarea, interpretarea şi retransmiterea separată a cadrelor la fiecare nod, care în reţelele comutate reprezintă termenul dominant al întârzierii.

Ordinul de mărime se poate estima printr-un calcul simplu. Un cadru cu 100 de octeţi de date de proces conţine 14 octeţi de antet Ethernet, 2 de antet EtherCAT, 10 de antet de datagramă, cei 100 de date, 2 de contor de lucru şi 4 de control, în total 132 de octeţi. Cu preambulul şi intervalul dintre cadre, pe mediu se transmit 152 de octeţi, adică 1.216 biţi. La 100 Mbit/s asta înseamnă circa 12,2 µs, plus întârzierea de propagare a fiecărui nod, de ordinul zecilor până la sutelor de nanosecunde. Ciclurile ajung astfel la zeci de microsecunde pentru reţele cu zeci de noduri, de aceea tehnologia e folosită la controlul coordonat al mai multor axe.

Ceasurile distribuite permit sincronizarea dispozitivelor din reţea şi reduc diferenţele temporale dintre acţiunile executate de acestea, abaterile obţinute fiind uzual sub o microsecundă [171]. Aplicaţiile tipice sunt controlul mai multor axe, roboţii şi sistemele de manipulare, maşinile-unelte, instalaţiile de ambalare cu viteze ridicate, achiziţiile de date care necesită sincronizare şi modulele de intrare şi ieşire cu cicluri scurte.

Topologia poate fi adaptată structurii maşinii şi poate include linii, ramificaţii, stele sau inele, ultima variantă permiţând continuarea funcţionării la întreruperea unui cablu. Dispozitivele necesită controlere de comunicaţie compatibile, iar proiectarea trebuie să ţină seama de timpul total al ciclului, numărul nodurilor, cantitatea datelor şi sincronizarea necesară. Pentru siguranţa funcţională există un profil dedicat, standardizat ca IEC 61.784-3-12.

EtherCAT este optimizat pentru domeniul local al controlului, nu pentru transmiterea directă a datelor către platforme externe. Un controler sau un calculator industrial preia datele relevante şi le publică prin OPC UA ori MQTT, păstrând traficul de analiză separat de ciclul de control.

6.1.7. OPC Classic şi tranziţia către OPC UA

OPC Classic nu este o magistrală de câmp, ci o familie de specificaţii pentru schimbul de date între aplicaţii software industriale. Apariţia sa a permis sistemelor SCADA, serverelor de date istorice şi aplicaţiilor de raportare să acceseze informaţiile furnizate de echipamente printr-o interfaţă comună, reducând dependenţa de drivere dezvoltate separat pentru fiecare combinaţie de produse. Principalele specificaţii acoperă accesul la date, cu valori curente, mărci temporale şi informaţii privind calitatea; alarmele şi evenimentele; şi accesul la datele istorice [172].

Limitarea structurală provine din tehnologia pe care se sprijină. OPC Classic utilizează mecanismele de obiecte distribuite ale sistemului de operare Microsoft, iar comunicarea între calculatoare necesită configurarea drepturilor, conturilor, serviciilor şi regulilor de reţea. Traversarea paravanelor de protecţie şi administrarea conexiunilor devin dificile în sisteme distribuite, iar restrângerile de securitate impuse ulterior asupra acestor mecanisme au eliminat o parte dintre configuraţiile permisive utilizate în trecut. Consecinţa practică este că numeroase instalaţii funcţionale au ajuns să depindă de tuneluri şi adaptoare specializate pentru a menţine o legătură care, la proiectare, părea simplă.

Instalaţiile existente pot continua să utilizeze OPC Classic în interiorul zonelor controlate. Integrarea cu sisteme noi se realizează prin adaptoare, tuneluri sau gateway-uri industriale care convertesc datele către OPC UA. Modernizarea trebuie realizată gradual, după inventarierea serverelor, clienţilor, etichetelor, alarmelor şi dependenţelor dintre aplicaţii; un inventar incomplet transformă migrarea într-o succesiune de întreruperi neprevăzute, pentru că relaţiile dintre aplicaţii nu sunt documentate nicăieri altundeva.

OPC UA reuneşte funcţiile separate ale tehnologiilor OPC Classic într-o arhitectură independentă de platformă, cu mecanisme proprii de securitate şi de modelare a informaţiei. Structura şi utilizarea sa în IIoT sunt analizate în secţiunea 6.2.

6.1.8. Poziționarea protocoalelor în arhitectura IIoT

Tabelul 6.1 – Poziționarea comparativă a principalelor protocoale industriale și IIoT

Protocol	Rol dominant	Determinism	Topologie uzuală	Model de date	Securitate	Utilizare tipică
Modbus RTU/TCP	Achiziție și comenzi simple	Limitat; depinde de interogare, încărcare și transport	Magistrală serială sau Ethernet comutat	Bobine și registre	Protocolul de bază nu include protecție; există Modbus Security pentru implementările compatibile	Instrumente de măsurare, contoare, convertizoare, echipamente existente
PROFINET RT/IRT	Intrări și ieșiri distribuite, control și mișcare	Ridicat pentru RT; foarte ridicat și sincronizat pentru IRT	Linie, stea sau inel	Date ciclice, parametri, diagnostic și profiluri de dispozitiv	Mecanisme și profiluri specifice, completate prin segmentarea rețelei	Automatizarea mașinilor, liniilor și celulelor de producție
EtherNet/IP	Schimb ciclic și configurare într-un model de obiecte comun	Mediu spre ridicat; determinat de perioada solicitată de actualizare și de proiectarea rețelei	Stea comutată, inel	Obiecte CIP, profiluri de dispozitiv	CIP Security, completat prin segmentare și filtrarea traficului multicast	Celule de producție, acționări, roboți, module distribuite
EtherCAT	Control rapid și sincronizarea dispozitivelor	Ridicat, cu cicluri și sincronizare previzibile	Linie, arbore, stea sau inel	Date de proces și obiecte de configurare	Protecția se realizează în principal prin izolarea domeniului de control și controlul accesului	Servosisteme, robotică, mașini-unelte și achiziții sincronizate
OPC UA	Integrare interoperabilă și contextualizarea datelor	Depinde de profil și implementare; nu substituie protocolul de control	Client–server sau publicare–abonare	Spațiu de adrese și modele informaționale semantice	Autentificare, certificate, semnare, criptare și controlul accesului	Integrarea PLC–SCADA–MES–edge
MQTT	Distribuirea scalabilă a mesajelor	Fără determinism specific controlului în timp real	Clienți conectați la un broker	Subiecte și payload definite de aplicație	TLS, autentificare și politici de acces configurate la broker	Transmiterea datelor către servicii de edge, centre de date și platforme IIoT

Protocoalele de câmp și de control nu trebuie înlocuite automat pentru realizarea unei arhitecturi IIoT. Dacă o rețea funcționează stabil și îndeplinește cerințele procesului, datele sale pot fi preluate prin automatul programabil, prin sistemul SCADA sau printr-un gateway industrial. Modernizarea urmărește separarea funcțiilor și adăugarea controlată a conectivității, nu uniformizarea tehnologică. Un traseu uzual este: dispozitive de câmp, protocol industrial de control, automat programabil sau controler industrial, OPC UA ori gateway industrial, MQTT și platformă IIoT. Poziționarea comparativă a protocoalelor prezentate este sintetizată în Tabelul 6.1.

Tabelul nu stabilește un clasament. Un protocol cu timp de ciclu foarte scurt poate fi nepotrivit pentru transmiterea datelor către o platformă distribuită, iar un protocol scalabil de mesagerie nu trebuie utilizat pentru închiderea unei bucle critice de control. Selectarea se face pentru fiecare segment al arhitecturii, în funcție de rolul datelor și de comportamentul necesar la întreruperea comunicației – criteriu care, în practică, departajează mai bine decât performanța nominală.

Secțiunea următoare analizează protocoalele utilizate pentru integrarea IIoT, cu accent pe OPC UA și MQTT, pe modelele lor de comunicație, pe structura informației și pe delimitarea rolurilor dintre controlul industrial, procesarea la edge și platformele externe.

6.2. Protocoale IIoT

Protocoalele utilizate pentru integrarea IIoT răspund unor cerințe diferite de cele ale comunicației deterministe dintre controler și dispozitivele de teren. Rolul lor principal este accesarea, contextualizarea și distribuirea datelor către sisteme SCADA, aplicații de edge, baze de date, platforme de analiză și servicii cloud. În această categorie trebuie diferențiate protocoalele și standardele de integrare industrială, precum OPC UA; protocoalele de mesagerie, precum MQTT și AMQP; protocoalele orientate către dispozitive cu resurse limitate, precum CoAP; interfețele bazate pe HTTP și principiile REST; și tehnologiile de acces la rețea, precum LoRaWAN și 5G industrial.

Aceste tehnologii se utilizează împreună, nu alternativ. Un gateway industrial poate prelua date contextualizate prin OPC UA, le poate filtra și le poate publica prin MQTT către mai multe aplicații simultan. Alegerea ține seama de rolul fiecărui segment, de frecvența datelor, de calitatea necesară, de comportamentul la întreruperea conexiunii și de mecanismele de securitate disponibile.

6.2.1. OPC UA

OPC UA (*Open Platform Communications Unified Architecture*) este o arhitectură standardizată pentru schimbul interoperabil de informaţii industriale. Nu defineşte doar transportul valorilor, ci şi modul în care echipamentele, variabilele, proprietăţile, metodele, evenimentele şi relaţiile dintre ele sunt reprezentate şi accesate. Această deosebire explică de ce OPC UA nu poate fi comparat direct cu un protocol de mesagerie: el transportă, pe lângă valoare, semnificaţia ei.

Elementul central este spaţiul de adrese al serverului. Informaţiile sunt reprezentate prin noduri, fiecare nod aparţinând unei clase şi fiind descris prin atribute, iar relaţiile dintre noduri sunt exprimate prin referinţe [173]. O aplicaţie nu primeşte, astfel, doar valoarea numerică a unei temperaturi, ci poate identifica echipamentul căruia îi aparţine, tipul de date, unitatea de măsură, drepturile de acces şi relaţia cu celelalte componente ale instalaţiei. Clasele de noduri permit reprezentarea obiectelor fizice sau logice, a variabilelor şi proprietăţilor, a metodelor care pot fi apelate, a tipurilor de obiecte, de variabile şi de date, a evenimentelor, precum şi a relaţiilor şi vizualizărilor asupra spaţiului de adrese.

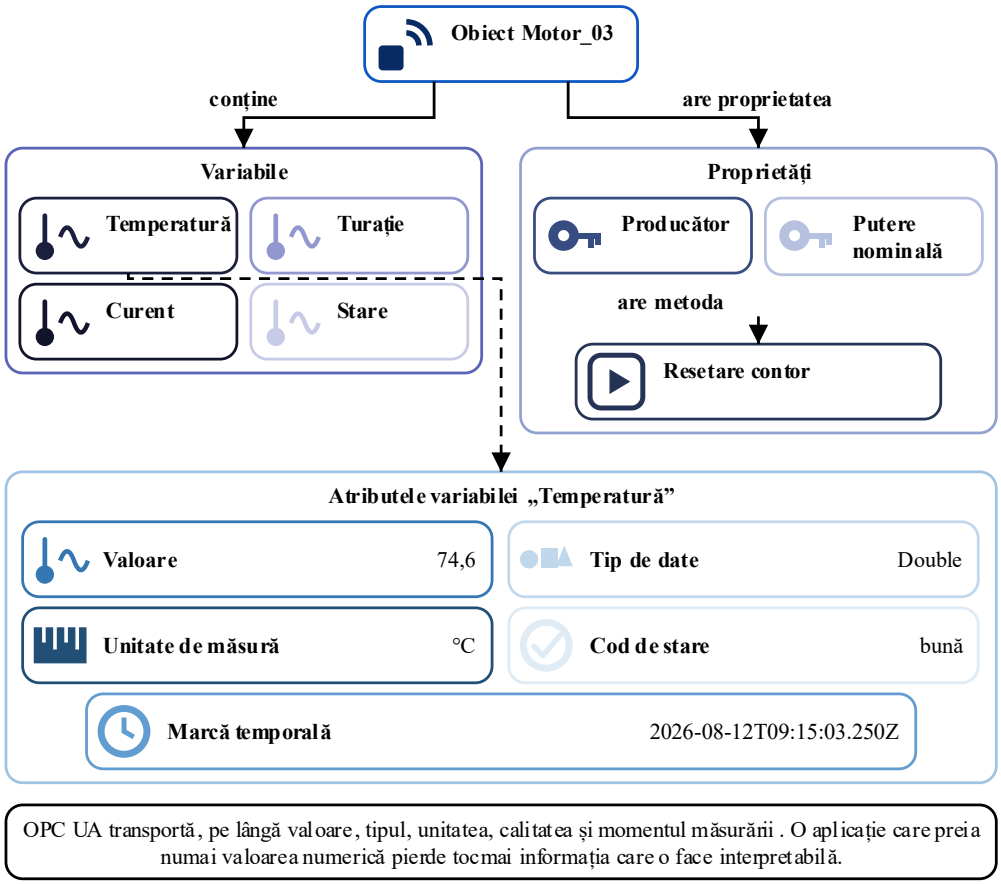


Figura 6.4 – Structura simplificată a spațiului de adrese OPC UA

Un motor poate fi reprezentat ca obiect care conţine variabile pentru turaţie, temperatură, curent şi stare de funcţionare, proprietăţi pentru producător şi putere nominală şi metode pentru operaţiile permise. Tipurile de obiecte sunt reutilizabile, ceea ce asigură reprezentarea uniformă a echipamentelor similare: cincizeci de motoare identice se descriu o singură dată ca tip şi se instanţiază de cincizeci de ori, iar o aplicaţie scrisă pentru tip funcţionează pentru toate instanţele. Figura 6.4 prezintă structura simplificată a unui astfel de spaţiu de adrese.

Fiecare nod este identificat printr-un NodeId, format dintr-un indice de spaţiu de nume şi un identificator propriu. Spaţiile de nume separă modelul standard OPC UA de modelele definite de producător, de organizaţie sau de o specificaţie complementară. Formele reale ale identificatorilor, regulile de rezolvare a indicelui de spaţiu de nume şi corespondenţa dintre nod şi mesajul publicat mai departe sunt tratate în secţiunea 6.2.8; aici este suficient de reţinut că utilizarea unor modele informaţionale consecvente reduce dependenţa aplicaţiilor de denumirile şi adresele interne ale unui anumit controler.

În modelul client–server, clientul iniţiază conexiunea şi utilizează serviciile puse la dispoziţie de server: descoperirea serverelor şi a punctelor de conectare, navigarea prin spaţiul de adrese, citirea şi scrierea atributelor, apelarea metodelor, crearea abonamentelor, monitorizarea modificării valorilor, recepţionarea evenimentelor şi accesarea informaţiilor istorice, dacă serverul oferă această funcţie [174].

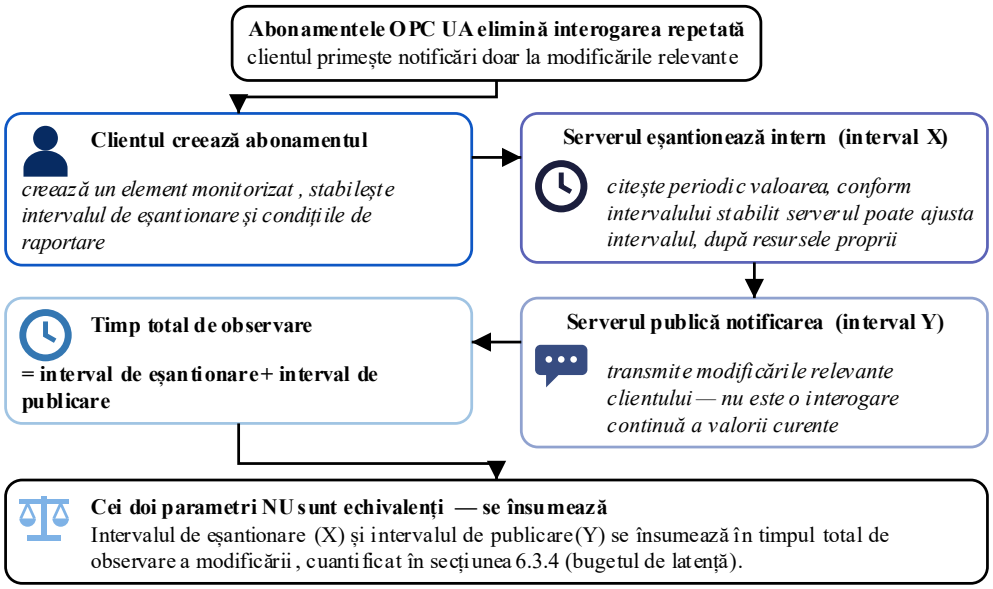


Figura 6.5 – Abonamentul OPC UA vs. interogarea repetată

Abonamentele elimină interogarea repetată (Figura 6.5). Clientul creează elemente monitorizate, stabilește intervalul de eșantionare și condițiile de raportare, iar serverul transmite notificări la apariția modificărilor relevante. Intervalele solicitate pot fi ajustate de server în funcție de resursele proprii, iar fiabilitatea recuperării după o întrerupere depinde de durata de viață a abonamentului, de dimensiunea cozilor și de strategia de reconectare [174]. Cei doi parametri – intervalul de eșantionare și intervalul de publicare – nu sunt echivalenți și se însumează în timpul total de observare, aspect cuantificat în secțiunea 6.3.4.

O valoare OPC UA este însoțită de codul care indică starea bună, incertă sau necorespunzătoare, de marca temporală a sursei, de marca temporală atribuită de server și, opțional, de informații de diagnosticare. Aplicația client nu trebuie să utilizeze numai valoarea numerică: o temperatură de 45 °C cu stare necorespunzătoare nu este echivalentă cu o măsurare validă de 45 °C. Calitatea și vechimea informației trebuie păstrate pe întregul traseu către sistemul SCADA, baza de date sau platforma IIoT – regulă care, încălcată la prima conversie, nu mai poate fi recuperată în aval.

Securitatea OPC UA cuprinde mecanisme pentru autentificarea aplicațiilor, semnarea și criptarea mesajelor, autentificarea utilizatorilor și controlul accesului. În modelul client–server, aplicațiile utilizează certificate pentru stabilirea unui canal securizat: serverul verifică certificatul clientului și lista de încredere, clientul verifică identitatea serverului, iar sesiunea stabilește ulterior identitatea utilizatorului și drepturile aplicabile [175]. O configurare corectă presupune puncte de conectare cu politici de securitate acceptate, certificate valabile și liste de încredere administrate, dezactivarea accesului anonim atunci când nu este justificat, drepturi diferențiate pentru citire, scriere și apelarea metodelor, limitarea variabilelor expuse, jurnalizarea operațiilor importante, sincronizarea ceasurilor și proceduri pentru reînnoirea și revocarea certificatelor.

Două erori frecvente merită enunțate explicit. Acceptarea automată a tuturor certificatelor necunoscute simplifică un experiment de laborator, dar transformă mecanismul de încredere într-o formalitate. Iar existența unui canal criptat nu corectează drepturile configurate excesiv: un client care poate scrie în orice variabilă printr-un canal securizat rămâne un risc de exploatare, nu de interceptare. Etapele stabilirii unei sesiuni securizate sunt reprezentate în Figura 6.6.

OPC UA include și un model de publicare–abonare, distinct de abonamentele client–server. În acest model, producătorii și consumatorii sunt separați logic și schimbă seturi de date printr-o infrastructură de comunicație, iar metadatele descriu structura și semnificația informației publicate; mecanismele de transport utilizabile sunt multiple [176]. Existența acestui model nu anulează rolul MQTT: alegerea dintre ele depinde de infrastructura disponibilă, de instrumentele de administrare și de compatibilitatea aplicațiilor consumatoare.

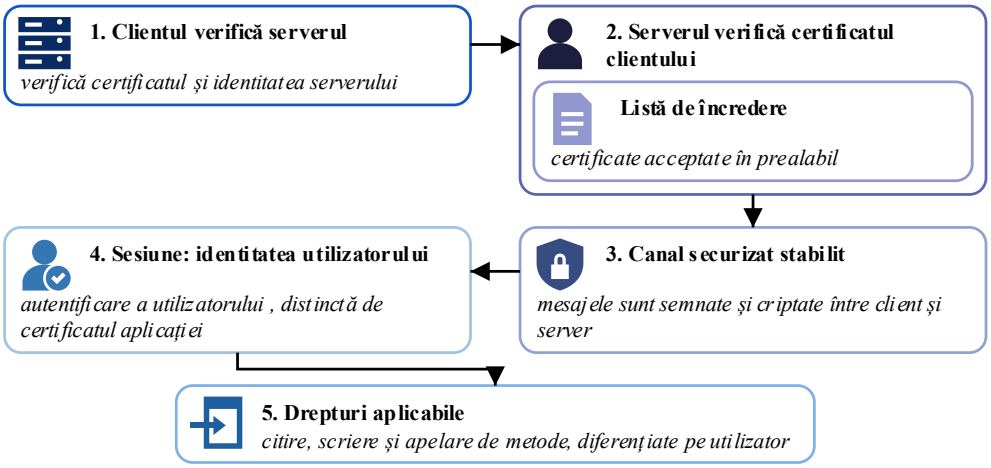


Figura 6.6 – Stabilirea sesiunii securizate OPC UA

OPC UA este potrivit în special pentru integrarea dintre automate programabile, servere de date, sisteme SCADA, aplicații MES și gateway-uri industriale. Utilizarea sa nu implică conectarea directă a fiecărui dispozitiv la sistemele externe. Serverul poate fi implementat în controler, în sistemul SCADA, într-un calculator industrial sau într-un gateway industrial, în funcție de resurse, de politica de securitate și de separarea zonelor de rețea.

6.2.2. MQTT

MQTT este un protocol de mesagerie bazat pe modelul publicare–abonare (Figura 6.7). Clienții nu comunică direct între ei, ci se conectează la un broker MQTT: un client publică un mesaj pe un subiect, iar brokerul îl distribuie clienților abonați la acel subiect [177]. Separarea produce trei forme de independență – producătorul nu trebuie să cunoască destinatarii, producătorul și consumatorul nu trebuie să prelucreze simultan mesajul, iar un mesaj poate ajunge la mai multe aplicații fără o conexiune distinctă pentru fiecare.

Subiectele sunt organizate ierarhic și separate prin caracterul „/". O structură posibilă este:

```
fabrica/hala_1/linia_2/motor_03/dat/temperatura
```

Ierarhia trebuie să permită identificarea locației, a echipamentului și a tipului informației, iar drepturile de acces trebuie corelate cu structura subiectelor. Regulile complete de construcție a arborelui, împreună cu clasele de trafic și cu exemplele de abonare, sunt stabilite în secțiunea 6.2.8.

MQTT nu stabilește semnificația payloadului. Acesta poate conține text, date binare, JSON sau o structură definită de aplicație. Pentru utilizarea industrială trebuie fixat un contract de date care precizează identificatorul echipamentului, marca temporală, valoarea și unitatea de măsură, calitatea informației, numărul versiunii

structurii, tipul evenimentului sau al măsurării şi modul de interpretare a valorilor absente. Structura adoptată în această carte şi corespondenţa ei cu sursa OPC UA sunt prezentate în secţiunea 6.2.8, iar consecinţele dimensionale ale alegerii dintre publicarea individuală şi cea grupată, în secţiunea 6.4.5.

Protocolul defineşte trei niveluri ale calităţii serviciului. La nivelul 0, mesajul este transmis cel mult o dată, fără confirmarea livrării. La nivelul 1, mesajul este transmis cel puţin o dată, astfel încât pot apărea duplicate. La nivelul 2, schimbul urmăreşte livrarea exact o dată. Alegerea depinde de importanţa şi de frecvenţa datelor: nivelul 0 este suficient pentru valori publicate des, când pierderea unei măsurări nu afectează analiza; nivelul 1 este potrivit atunci când pierderea mesajului este mai problematică decât apariţia unui duplicat; nivelul 2 introduce schimburi suplimentare şi trebuie rezervat situaţiilor care îl justifică. Costul nu este neglijabil: nivelul 1 dublează numărul de pachete transmise, prin confirmările asociate, ceea ce în exemplul din secţiunea 6.4.5 adaugă circa 200 kbit/s în sens invers pentru 240 de mesaje pe secundă.

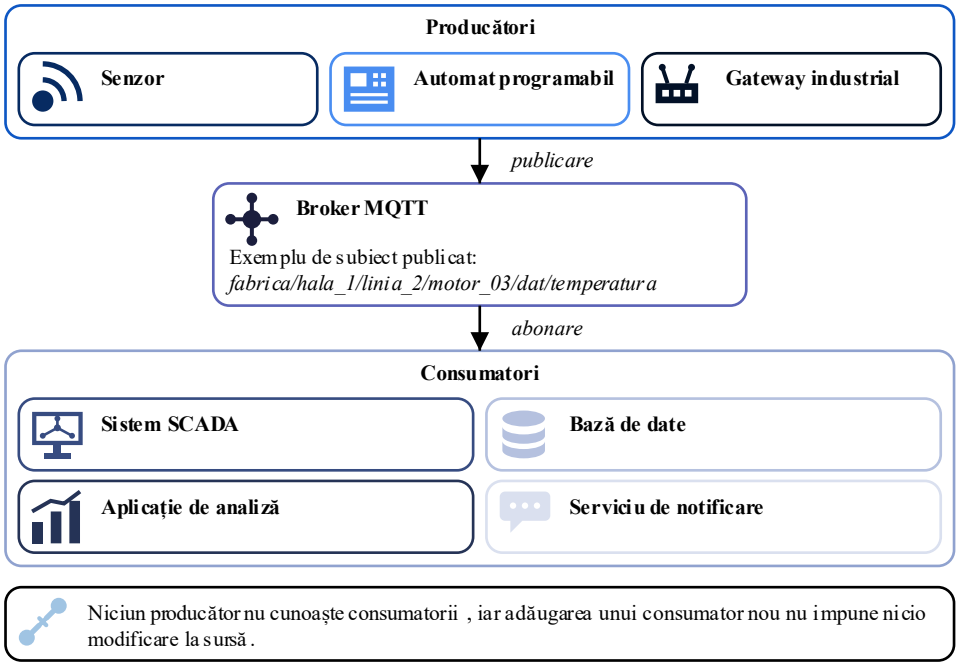


Figura 6.7 – Modelul publicare–abonare utilizat de MQTT

Nivelul 2 nu garantează că operaţia industrială sau tranzacţia aplicaţiei se execută o singură dată. Duplicarea poate apărea în alte segmente ale fluxului, la stocare sau la reluarea procesării. Consumatorii trebuie să utilizeze identificatori de mesaj, mărci temporale şi operaţii idempotente atunci când repetarea ar produce rezultate incorecte. Confuzia dintre garanţia de transport şi garanţia de efect este una dintre cele mai costisitoare erori de proiectare a unui flux IIoT.

Alte mecanisme importante sunt mesajul reţinut, prin care brokerul păstrează ultima valoare publicată pe un subiect; mesajul de testament, configurat la stabilirea conexiunii şi publicat automat la deconectarea necontrolată; păstrarea sesiunii şi a abonamentelor; intervalul de menţinere a conexiunii; expirarea mesajelor; şi abonamentele partajate, utilizabile pentru distribuirea sarcinii între consumatori [177]. Mesajul reţinut nu constituie un istoric. El păstrează ultima valoare publicată şi devine periculos dacă nu este însoţit de o marcă temporală şi de o stare de validitate: o aplicaţie care se conectează după o întrerupere de două ore trebuie să poată deosebi o valoare curentă de una reţinută înaintea întreruperii.

MQTT nu include implicit criptarea. Protecţia se obţine prin configurarea TLS, autentificarea clienţilor şi aplicarea politicilor de acces la nivelul brokerului. Într-o implementare industrială trebuie urmărite identitatea unică a fiecărui client, autentificarea prin credenţiale sau certificate X.509, autorizarea separată pentru conectare, publicare şi abonare, limitarea accesului la subiectele strict necesare, protejarea cheilor private, reînnoirea şi revocarea certificatelor, limitarea dimensiunii şi frecvenţei mesajelor, monitorizarea conexiunilor şi a tentativelor respinse, precum şi disponibilitatea brokerului.

Un broker unic devine un punct critic. Pentru aplicaţiile importante sunt necesare mecanisme de redundanţă, stocare controlată, monitorizare şi recuperare. Chiar şi într-o configuraţie redundantă, funcţiile de control esenţiale trebuie să continue local atunci când legătura MQTT este întreruptă; brokerul este o infrastructură de observare, nu o componentă a buclei de reglare.

6.2.3. Sparkplug B

MQTT defineşte transportul mesajelor, dar nu impune o structură industrială a subiectelor, o reprezentare comună a variabilelor sau un mecanism de gestionare a stării echipamentelor. Consecinţa practică este că două implementări MQTT corecte pot fi complet incompatibile între ele. Sparkplug adaugă exact elementele lipsă, păstrând MQTT ca transport [110].

Specificaţia defineşte o ierarhie standardizată a subiectelor, rolurile nodurilor de edge, ale dispozitivelor şi ale aplicaţiilor gazdă, tipurile mesajelor, structura payloadului, reprezentarea metricilor, mecanismele pentru indicarea conectării şi deconectării şi gestionarea stării sesiunii. Structura generală a unui subiect este:

```
spBv1.0/grup/tip_mesaj/nod_edge/dispozitiv
```

Tipurile de mesaje acoperă întregul ciclu de viaţă al unei surse. Mesajele de naştere descriu starea iniţială a nodului şi a dispozitivului, împreună cu lista completă a metricilor şi cu tipurile lor; mesajele de deces semnalează pierderea legăturii; mesajele de date transportă actualizările; iar mesajele de comandă transportă solicitările către nod sau către dispozitiv. Specificaţia impune, pentru fiecare tip, valori precise ale nivelului de calitate a serviciului şi ale indicatorului de reţinere, astfel încât comportamentul să fie identic indiferent de implementare [110].

Două mecanisme merită reținute pentru consecințele lor operaționale. Primul este numerotarea secvențială a mesajelor: fiecare mesaj poartă un număr de ordine, iar aplicația gazdă detectează astfel o discontinuitate și poate solicita retransmiterea stării complete, în locul unei reconstrucții aproximative. Al doilea este marcarea informațiilor drept neactualizate atunci când legătura cu un nod se pierde: fără acest mecanism, un tablou de bord alimentat prin MQTT continuă să afișeze ultima valoare recepționată, indistinct de o valoare curentă – exact eroarea pe care mesajul reținut o poate produce în implementările fără Sparkplug.

Payloadul este binar, bazat pe Protocol Buffers, și transmite metricile împreună cu tipurile și metadatele lor. Alegerea reduce substanțial dimensiunea mesajelor față de o structură JSON echivalentă, dar are un preț: mesajele nu mai pot fi citite direct cu un client MQTT obișnuit, iar diagnosticarea necesită instrumente care interpretează schema.

Sparkplug este util pentru sisteme SCADA distribuite, gateway-uri industriale și aplicații în care numeroase dispozitive trebuie descoperite și reprezentate coerent. Adoptarea sa presupune însă compatibilitate simultană la nivelul nodurilor de edge, al brokerului și al aplicațiilor consumatoare; nu toate sistemele MQTT interpretează automat aceste mesaje. Utilizarea specificației nu înlocuiește proiectarea politicilor de securitate și a drepturilor pentru comenzi: mesajele de comandă rămân solicitări, validate local înainte de executare, potrivit regulii enunțate în secțiunea 6.2.7.

6.2.4. CoAP și HTTP/REST

CoAP (*Constrained Application Protocol*) este destinat dispozitivelor și rețelelor cu resurse limitate: noduri cu microcontrolere de mică putere, memorie redusă și legături cu debit mic și rată ridicată de pierdere a pachetelor. Utilizează un model orientat către resurse, asemănător celui web, cu operațiile GET, POST, PUT și DELETE, dar transportă mesajele peste UDP, iar mesajele pot fi confirmabile sau neconfirmabile [178].

Diferența față de o interfață web obișnuită este cantitativă și explică întregul domeniu de utilizare. Antetul fix al unui mesaj CoAP are patru octeți, astfel încât o cerere completă, cu antetul UDP și cel IPv4, se încadrează uzual sub 50 de octeți. O cerere HTTP echivalentă, cu anteturile sale textuale, ajunge de regulă la câteva sute de octeți și necesită în prealabil stabilirea unei conexiuni TCP. Pentru un senzor alimentat din baterie, care transmite o valoare la cinci minute, raportul dintre cele două variante se traduce direct în durata de viață a bateriei.

Protocolul include mecanisme pentru descoperirea resurselor, pentru observarea unei resurse – prin care serverul notifică modificările fără interogare repetată – și pentru transferul în blocuri al reprezentărilor care depășesc dimensiunea unei datagrame [179]. Acolo unde infrastructura de rețea nu permite traficul UDP, aceleași cereri și răspunsuri pot fi transportate peste TCP, TLS sau WebSockets [180].

Securizarea variantei peste UDP se realizează prin DTLS, cu chei preîmpărtășite sau certificate, iar administrarea acestor credențiale pe un parc de dispozitive constrânse este, în practică, dificultatea principală a implementării.

CoAP este adecvat pentru senzori alimentați din baterii, rețele cu debit redus și pierderi, monitorizarea unor mărimi cu variație lentă, dispozitive care transmit mesaje scurte și aplicații în care consumul energetic este prioritar. Nu este destinat controlului industrial determinist și nu înlocuiește un protocol de câmp.

HTTP este utilizat frecvent pentru interfețe de programare, configurare, integrarea aplicațiilor și transferuri inițiate la cerere; semantica sa este definită în specificația actuală a protocolului [181]. REST nu este un protocol distinct, ci un stil arhitectural aplicat de regulă peste HTTP: resursele sunt identificate prin adrese, iar operațiile sunt exprimate prin metodele protocolului.

Interfețele HTTP/REST sunt potrivite pentru integrarea dintre aplicații MES, ERP și servicii informatice, pentru configurarea dispozitivelor și a gateway-urilor industriale, pentru solicitarea rapoartelor și a datelor istorice, pentru administrarea utilizatorilor și a resurselor, pentru transmiterea loturilor de date și pentru integrarea cu aplicații web. Nu trebuie utilizate ca substitut generic pentru comunicația ciclică dintre automatul programabil și periferia distribuită, din două motive care se cumulează. Primul este modelul: într-o interogare periodică, latența informației este dictată de perioada de interogare, nu de viteza rețelei, iar reducerea perioadei multiplică numărul de cereri. Al doilea este costul pe mesaj: un schimb cerere–răspuns securizat, cu anteturile aferente, depășește cu un ordin de mărime dimensiunea unui mesaj publicat prin MQTT pentru aceeași valoare, calculat în secțiunea 6.4.5.

Proiectarea unei interfețe REST industriale trebuie să includă criptarea prin TLS, autentificarea și autorizarea, limitarea numărului de solicitări, tratarea explicită a erorilor, versionarea interfeței și definirea operațiilor care pot fi repetate fără efecte nedorite. Ultima cerință este cea mai des omisă: o comandă de pornire retransmisă după expirarea unui interval de așteptare nu trebuie să producă două porniri.

6.2.5. AMQP

AMQP (*Advanced Message Queuing Protocol*) este un protocol de mesagerie destinat schimbului fiabil de mesaje între aplicații. Definește un transport binar, formatul mesajelor, mecanismele de confirmare, controlul fluxului bazat pe credite acordate consumatorului, precum și elemente pentru securitate și tranzacții [182]. Specificația este preluată și ca standard internațional, sub numărul ISO/IEC 19464. Structura sa este mai complexă decât cea a MQTT, dar oferă control mai detaliat asupra fluxurilor de mesaje.

Domeniile în care acest control se justifică sunt integrarea dintre servicii informatice, transferul mesajelor între aplicații MES, ERP și sisteme logistice, fluxurile

în care confirmarea și trasabilitatea sunt esențiale, distribuirea sarcinii între mai mulți consumatori și integrarea centrelor de date și a platformelor distribuite. Mecanismul de credite merită subliniat: consumatorul declară câte mesaje poate prelua, iar producătorul nu poate depăși această limită. Într-un flux în care aplicația consumatoare execută o prelucrare costisitoare pentru fiecare mesaj, mecanismul previne acumularea necontrolată a cozilor – situație în care MQTT, care nu are un echivalent direct, lasă problema în seama configurării brokerului.

Persistența și garanțiile efective depind însă de configurația brokerului, de modul de confirmare a mesajelor și de tratarea erorilor în aplicație. Un mesaj declarat persistent într-o coadă nedurabilă se pierde la repornirea serviciului, indiferent de protocol.

AMQP nu trebuie utilizat automat în locul MQTT pentru simplul motiv că oferă mecanisme mai bogate. Pentru telemetrie frecventă și mesaje scurte, costul suplimentar de antet și de administrare nu se justifică; regula practică este ca protocolul de mesagerie să fie ales în funcție de granularitatea la care este necesară confirmarea – pe fiecare mesaj, pentru tranzacții, sau pe flux, pentru telemetrie.

6.2.6. LoRaWAN și 5G industrial

LoRaWAN și 5G nu îndeplinesc același rol ca OPC UA, MQTT sau CoAP. Ele furnizează conectivitatea necesară transportării datelor, peste care sunt utilizate protocoale de aplicație. Confuzia dintre nivelul de acces la rețea și nivelul aplicației conduce la comparații lipsite de sens, de tipul „LoRaWAN sau MQTT".

LoRaWAN este optimizat pentru dispozitive alimentate din baterii, amplasate la distanțe mari și care transmit cantități reduse de date. Specificația definește clasele de dispozitive, mecanismul de adaptare a ratei de transmisie și structura cadrelor la nivelul legăturii de date [183]. Este potrivit pentru monitorizarea mediului, contoare, rezervoare, instalații dispersate și senzori exteriori.

Limitarea decisivă nu este debitul brut, ci regimul de utilizare a canalului impus de reglementările radio regionale. Ordinul de mărime se obține imediat: un mesaj de câteva zeci de octeți, transmis cu factorul de dispersie maxim, ocupă canalul aproximativ o secundă; dacă reglementarea aplicabilă limitează utilizarea canalului la 1 %, intervalul minim dintre două transmisii ale aceluiași dispozitiv depășește o sută de secunde. Valorile exacte depind de banda utilizată, de parametrii regionali și de dimensiunea mesajului și se verifică în documentul de parametri regionali, dar concluzia de proiectare rămâne aceeași: LoRaWAN nu este adecvat volumelor mari, actualizărilor frecvente sau controlului cu latență strictă, iar o aplicație care presupune o valoare pe secundă de la fiecare dispozitiv nu poate fi realizată pe această tehnologie.

5G industrial poate susține rețele private, mobilitatea echipamentelor, conectarea unui număr mare de dispozitive și aplicații cu cerințe diferite de latență și

disponibilitate. Este utilizat pentru roboți mobili, vehicule autonome, terminale de operator și monitorizarea echipamentelor distribuite. Cerințele de serviciu pentru aplicațiile de control ciber-fizic, inclusiv cele privind disponibilitatea comunicației și sincronizarea ceasurilor, sunt formulate în specificația 3GPP TS 22.104.

Utilizarea 5G nu garantează singură determinismul aplicației. Timpul total depinde de rețeaua radio, de infrastructura locală, de rutare, de protocolul de aplicație, de platforma de prelucrare și de comportamentul sistemului la pierderea conexiunii. Din perspectiva bugetului de latență construit în secțiunea 6.3.4, un segment radio nu adaugă doar un termen suplimentar, ci mărește în primul rând variația bugetului, iar variația este mărimea care determină dacă o funcție poate fi susținută. Funcțiile critice trebuie validate cap-coadă, prin măsurare, și păstrate local atunci când continuitatea lor nu poate depinde de rețeaua mobilă.

6.2.7. Utilizarea complementară a OPC UA și MQTT

OPC UA și MQTT nu trebuie tratate ca alternative echivalente. OPC UA este orientat către accesul structurat și contextualizat la informații industriale, în timp ce MQTT este orientat către distribuirea eficientă a mesajelor între sisteme separate. Ele ocupă poziții diferite pe același traseu, iar întrebarea corectă nu este care dintre ele se adoptă, ci unde se termină rolul fiecăruia.

Așa cum arată Figura 6.8, datele sunt preluate de la un PLC sau de la un server OPC UA de către un gateway industrial aflat la nivelul edge. Gateway-ul organizează datele într-un mesaj și îl transmite prin MQTT către un broker, care îl distribuie mai departe către baza de date și aplicații.

Tabelul 6.2 – Delimitarea rolurilor OPC UA și MQTT

Criteriu	**OPC UA**	**MQTT**
Rol principal	Accesarea, modelarea și contextualizarea informațiilor industriale	Distribuirea mesajelor între producători și consumatori
Model uzual	Client–server; este disponibil și OPC UA PubSub	Publicare–abonare prin broker
Structura informației	Spațiu de adrese, noduri, referințe și modele informaționale	Subiecte și payload definite de aplicație
Calitatea datelor	Valoare, cod de stare și mărci temporale, transportate implicit	Trebuie inclusă explicit în contractul de date
Utilizare tipică	PLC–SCADA–MES–gateway industrial	Gateway industrial–broker–platformă–bază de date
Securitate	Certificate, canale securizate, sesiuni, identități și drepturi	TLS, autentificare și politici aplicate clienților și subiectelor
Comenzi	Servicii de scriere și apelare a metodelor, controlate prin drepturi	Mesaje de comandă definite de aplicație și validate la destinație
Comportament la întrerupere	Reconectare, sesiuni, abonamente și coduri de stare	Sesiuni, niveluri QoS, mesaj de testament și stocare configurată

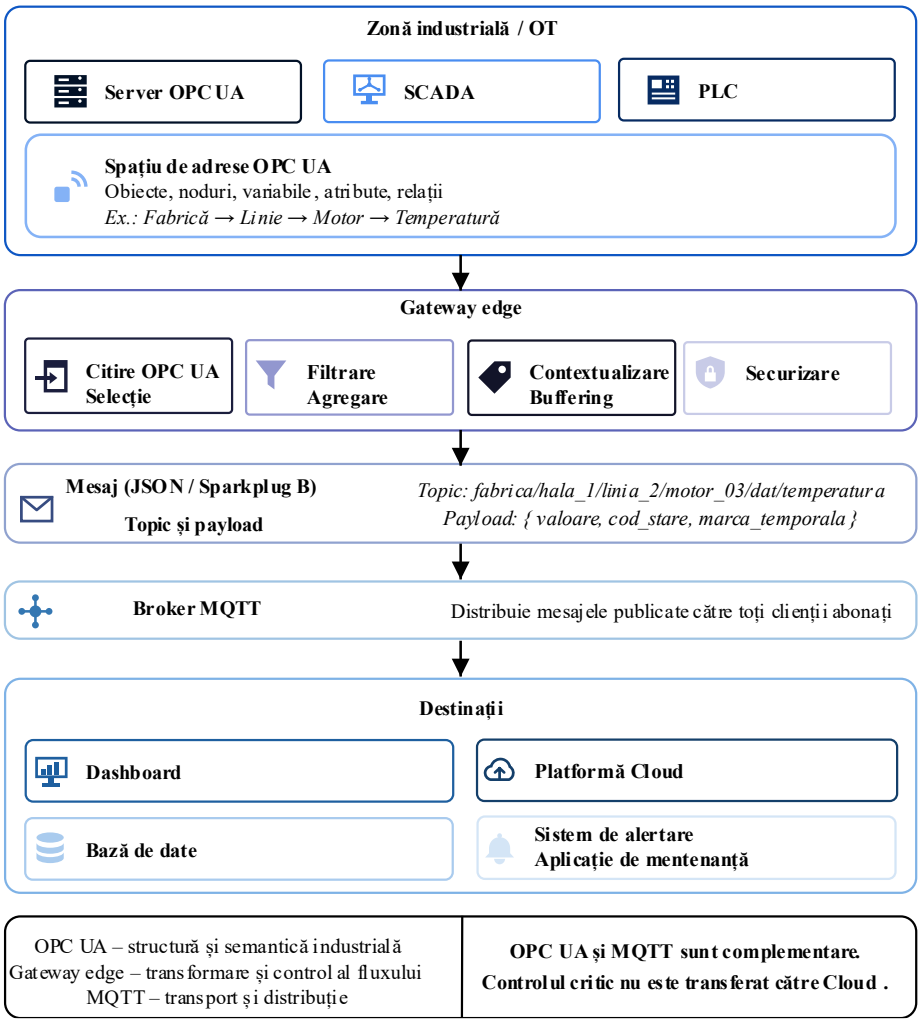


Figura 6.8 – Complementaritatea OPC UA și MQTT pe traseul datelor

Gateway-ul citeşte numai informaţiile necesare, verifică starea acestora, aplică filtrarea şi agregarea, adaugă identificatorii şi mărcile temporale, apoi publică mesajele; aplicaţiile abonate utilizează aceleaşi date pentru vizualizare, stocare, analiză sau notificare. Regulile concrete de construcţie a subiectelor şi corespondenţa dintre nodul OPC UA şi câmpurile mesajului sunt stabilite în secţiunea 6.2.8. Delimitarea rolurilor este sintetizată în Tabelul 6.2.

Validarea acestei frontiere se face pe segmente. Pentru partea OPC UA, se explorează spaţiul de adrese al unui server şi se identifică, pentru o variabilă, identificatorul de nod, tipul de date, valoarea, codul de stare, marca temporală, drepturile de citire şi scriere şi comportamentul unui abonament la modificarea valorii. Pentru partea MQTT, un mesaj se urmăreşte de la clientul care publică până la broker şi apoi la clientul abonat, confirmând subiectul, payloadul, nivelul QoS, identitatea

clientului, politica de acces şi marca temporală. Sunt necesare şi teste pentru pierderea conexiunii, apariţia duplicatelor, recepţionarea unei valori reţinute şi respingerea unui client neautorizat; procedura etapizată este detaliată în secţiunea 6.5.

Comenzile provenite dintr-o aplicaţie externă nu se aplică direct asupra ieşirilor. Mesajul reprezintă o solicitare, iar automatul programabil sau controlerul local verifică identitatea sursei, modul de funcţionare, interblocările, limitele tehnologice şi funcţiile de siguranţă înainte de executare. Pierderea sau compromiterea canalului IIoT nu trebuie să anuleze logica locală de protecţie – principiu enunţat în introducerea capitolului şi verificabil în fiecare exemplu din secţiunile următoare.

6.2.8. Convenția pentru subiectele MQTT și corespondența cu spațiul de adrese OPC UA

Delimitarea rolurilor prezentată anterior rămâne o afirmaţie de principiu până când sunt fixate două artefacte concrete: arborele subiectelor de mesagerie şi contractul de date al mesajului. Fără ele, o implementare cu câteva zeci de semnale funcţionează, iar una cu câteva mii devine neadministrabilă: drepturile de acces nu pot fi formulate, adăugarea unui echipament impune modificarea aplicaţiilor consumatoare, iar corelarea unei valori cu sursa ei industrială depinde de convenţii nescrise.

Structura adoptată în această carte ca referinţă are şase niveluri şi separă locaţia de clasa traficului. Exerciţiile din capitolele 5, 7, 8 şi 9 folosesc variante locale, simplificate sau extinse, declarate ca atare în fiecare loc; principiile rămân cele de aici:

```
<intreprindere>/<hala>/<linie>/<echipament>/<clasa>/<marime>
```

Clasa traficului ia una dintre valorile „dat" pentru telemetrie, „evt" pentru evenimente şi alarme, „cmd" pentru comenzi, „sts" pentru starea conexiunii şi „cfg" pentru parametri de configurare. Aşezarea clasei înaintea mărimii permite formularea drepturilor de acces prin prefix, ceea ce este singurul mod practic de a administra un broker cu sute de clienţi. Subiectele rezultate pentru un echipament sunt enumerate în Tabelul 6.3.

Tabelul 6.3 – Subiectele definite pentru un echipament, pe clase de trafic

Clasa	Subiect	Publică	Se abonează	QoS
Telemetrie	fabrica/hala_1/linia_2/motor_03/dat/temperatura	gateway	istoric, analiză, tablou de bord	1
Eveniment	fabrica/hala_1/linia_2/motor_03/evt/prag_temperatura	gateway	notificare, MES	1
Stare	fabrica/hala_1/linia_2/motor_03/sts/conexiune	gateway (mesaj reținut și testament)	supraveghere	1
Comandă	fabrica/hala_1/linia_2/motor_03/cmd/reset_contor	aplicația autorizată	gateway	1
Configurare	fabrica/hala_1/linia_2/motor_03/cfg/interval_publicare	administrare	gateway	1

Arborele respectă reguli stricte. Nivelurile includ identificatori stabili ai echipamentelor; starea, lotul, schimbul şi operatorul rămân în date, deoarece introducerea lor în subiect complică abonarea şi controlul diferenţiat al accesului. Convenţia utilizează litere mici, cifre şi subliniere, fără diacritice sau spaţii, limitând lungimea subiectului transmis în UTF-8 [177]. Subiectele nu încep cu separator şi nu conţin niveluri vide; „+” şi „#” sunt rezervate filtrelor de abonare. Versiunea contractului se declară în payload, păstrând subiectele şi abonamentele stabile la modificarea structurii. Comenzile sunt separate de telemetrie. Recepţia prin „cmd” nu autorizează declanşarea funcţiilor de siguranţă sau ridicarea interblocărilor: automatul programabil verifică local condiţiile de execuţie şi poate refuza comanda.

Metacaracterul „+" înlocuieşte exact un nivel, iar „#" înlocuieşte restul arborelui şi poate apărea numai pe ultima poziţie. Un serviciu de arhivare care preia toată telemetria unei hale se abonează la „fabrica/hala_1/+/+/dat/#"; un tablou de bord dedicat unei singure linii, la „fabrica/hala_1/linia_2/+/dat/+"; un sistem de supraveghere a disponibilităţii, la „fabrica/+/+/+/sts/conexiune". Gateway-ul declară la conectare un mesaj de testament pe subiectul propriu de stare, publicat de broker automat la pierderea conexiunii; acelaşi subiect poartă, ca mesaj reţinut, starea curentă, astfel încât o aplicaţie nou conectată să afle imediat dacă sursa este activă, fără să aştepte următoarea publicare.

În partea dinspre proces, aceleaşi mărimi sunt identificate prin noduri. Fiecare nod are un identificator format dintr-un indice de spaţiu de nume şi un identificator propriu, iar notaţia textuală consacrată este „ns=<indice>;<tip>=<identificator>", unde tipul poate fi „i" pentru numeric, „s" pentru şir de caractere, „g" pentru identificator global şi „b" pentru formă binară [184]. Pentru variabila discutată, formele reale sunt:

```
ns=3;s=Linia_2.Motor_03.Temperatura    identificator de tip șir
ns=3;i=6045                            identificator numeric, același nod
/3:Linia_2/3:Motor_03/3:Temperatura    calea de navigare corespunzătoare
```

Indicele 3 nu este o proprietate a nodului, ci poziţia spaţiului de nume în tabloul serverului. El se poate modifica la o reconfigurare, iar un client care îl codifică rigid se va conecta la un nod greşit fără nicio eroare vizibilă. Procedura corectă este ca, imediat după deschiderea sesiunii, clientul să citească tabloul spaţiilor de nume din nodul „i=2255", să caute identificatorul uniform al modelului propriu şi să folosească indicele returnat. Când nici identificatorul de nod nu este stabil între versiuni ale programului, alternativa este navigarea prin cale şi traducerea ei în identificator la fiecare pornire.

Gateway-ul încheie sesiunea OPC UA şi construieşte mesajul MQTT; traducerea trebuie definită explicit, element cu element.

Conversia stării merită enunţată separat, pentru că este locul în care se pierde cel mai frecvent informaţie. Codul de stare OPC UA este o valoare pe 32 de biţi în care primii doi biţi codifică severitatea: bună, incertă sau necorespunzătoare.

Consumatorii uzuali – sisteme SCADA, servere de date istorice, tablouri de bord – folosesc scara compactă moştenită din OPC Classic, unde 192 înseamnă bună, 64 incertă şi 0 necorespunzătoare. Contractul de date adoptat în carte transmite în câmpul „q" valoarea de pe această scară, obţinută din severitatea codului OPC UA. Regula asociată este că gateway-ul publică mesajul indiferent de stare, dar nu publică niciodată valoarea fără câmpul „q": o temperatură de 74,6 °C cu stare necorespunzătoare nu este o măsurare, iar suprimarea codului transformă o defecţiune de senzor într-o valoare aparent validă în baza de date.

În forma grupată, un singur câmp „*q*" la nivel de mesaj este admisibil numai dacă toate mărimile provin din aceeaşi sursă şi au aceeaşi stare. Când o singură mărime are altă stare, ea se publică separat sau structura grupată se extinde cu un câmp de calitate pentru fiecare valoare. Simplificarea contrară – un „*q*" unic care raportează starea cea mai favorabilă – este o eroare de proiectare, nu o economie de bandă.

Odată delimitate rolurile, rămâne de stabilit cum se combină aceste protocoale într-un traseu complet şi ce se întâmplă la trecerea de la o tehnologie la alta. Subcapitolul următor tratează stiva de comunicaţie IIoT, zonele arhitecturii şi frontierele la care o stivă se termină şi alta începe.

Corespondenţa dintre atributele nodului şi câmpurile mesajului publicat este prezentată în Tabelul 6.4.

Tabelul 6.4 – Corespondența dintre nodul OPC UA și mesajul MQTT

Element în serverul OPC UA	Formă reală	Destinația în mesaj
Identificatorul nodului	ns=3;s=Linia_2.Motor_03.Temperatura	determină subiectul .../motor_03/dat/temperatura; se păstrează în câmpul src
Atributul Value	74.6	câmpul v
Marca temporală a sursei	2026-08-12T09:15:03.250Z	câmpul ts
Marca temporală a serverului	–	câmpul ts_srv, numai dacă diferă de cea a sursei
Codul de stare	Good	câmpul q, după conversia descrisă mai jos
Proprietatea EngineeringUnits	°C	câmpul u
Proprietatea EURange	-40 … 150	nu se transmite ciclic; se publică pe ramura cfg la modificare

6.3. Stiva de comunicare în IIoT

Comunicarea într-un sistem IIoT nu este realizată de un singur protocol. Datele traversează o stivă de tehnologii cu funcţii distincte: transmiterea semnalului, accesul la mediul de comunicaţie, adresarea, transportul, securizarea, codificarea şi interpretarea informaţiei la nivelul aplicaţiei.

Trebuie diferenţiate două perspective complementare. Perspectiva verticală descrie protocoalele şi formatele suprapuse într-o singură conexiune. Perspectiva orizontală descrie traseul datelor de la echipamentul industrial la gateway-ul industrial şi apoi la aplicaţiile care le utilizează. O arhitectură poate folosi Modbus RTU între un instrument de măsurare şi un automat programabil, OPC UA între automat şi gateway, MQTT între gateway şi platformă, apoi HTTP pentru accesarea datelor de către o aplicaţie web. Fiecare segment are propria stivă, propriul comportament la întrerupere şi propriile mecanisme de securitate – iar confundarea celor două perspective este cauza obişnuită a afirmaţiei, incorecte, că o instalaţie „foloseşte MQTT".

6.3.1. Modelul stratificat al comunicației

Modelul de referinţă OSI împarte comunicaţia în şapte niveluri şi oferă un cadru pentru corelarea standardelor, fără a constitui o specificaţie de implementare obligatorie [185]; interpretarea nivelurilor în comunicaţiile IIoT este sintetizată în Tabelul 6.5. În sistemele reale, unele niveluri sunt reunite, iar anumite tehnologii industriale îndeplinesc funcţii aparţinând mai multor niveluri simultan.

Încadrarea are rol orientativ. PROFINET, EtherNet/IP şi EtherCAT nu pot fi reduse la un singur nivel, deoarece combină mecanisme Ethernet, servicii de comunicaţie şi modele de date. În mod asemănător, OPC UA poate utiliza mai multe codificări şi mecanisme de transport, între care UA Binary, JSON, OPC UA TCP, HTTPS şi WebSockets [184]. La nivelul transportului, TCP asigură livrarea ordonată şi retransmiterea [186], în timp ce UDP transmite datagrame fără garanţii, ceea ce îl face potrivit traficului ciclic de intrări şi ieşiri şi mesajelor scurte ale dispozitivelor constrânse [187]. La nivelul prezentării, alegerea dintre o codificare textuală, precum JSON [188], şi una binară determină simultan lizibilitatea la depanare şi dimensiunea mesajului.

Tabelul 6.5 – Interpretarea nivelurilor modelului OSI în comunicațiile IIoT

Nivel	Funcția principală	Exemple relevante
Fizic	Transmiterea semnalelor electrice, optice sau radio	RS-485, conductoare Ethernet, fibră optică, interfețe radio Wi-Fi, 5G și LoRa
Legătură de date	Formarea cadrelor, accesul la mediu și transferul local	Ethernet IEEE 802.3, CAN, rețele fără fir, mecanisme de sincronizare și de prioritizare
Rețea	Adresarea logică și rutarea între rețele	IPv4 și IPv6
Transport	Transferul datelor între punctele terminale, controlul fluxului și ordonarea	TCP și UDP
Sesiune	Stabilirea și menținerea interacțiunilor dintre aplicații	Funcții implementate, de regulă, în bibliotecile și protocoalele aplicației
Prezentare	Codificarea, serializarea și transformarea datelor	UA Binary, JSON, XML, CBOR și Protocol Buffers
Aplicație	Servicii de comunicare și interpretarea informației	Modbus TCP, OPC UA, MQTT, AMQP, CoAP și HTTP

Securitatea trebuie tratată transversal, nu ca un nivel. TLS este utilizat frecvent între protocolul de aplicaţie şi TCP pentru asigurarea confidenţialităţii, integrităţii şi autenticităţii comunicaţiei, dar nu se asociază rigid unui singur nivel OSI; specificaţia actuală a TLS 1.3 este publicată prin RFC 9846 [189].

Valoarea practică a modelului este diagnostică. Atunci când o valoare nu ajunge la destinaţie, întrebarea utilă nu este „ce protocol este de vină?", ci la ce nivel se opreşte informaţia: dacă interfaţa nu are legătură fizică, dacă adresa nu este rutabilă, dacă portul este blocat de un paravan de protecţie, dacă negocierea TLS eşuează din cauza unui certificat expirat, dacă payloadul nu se decodifică sau dacă aplicaţia refuză mesajul pe motiv de drepturi. Fiecare dintre aceste situaţii are un semn distinct, iar ordinea verificării, de jos în sus, evită modificarea simultană a mai multor componente. Modelul explică şi de ce suprapunerea nivelurilor are un cost măsurabil: fiecare nivel adaugă propriul antet, iar pentru mesaje industriale scurte antetele ajung să depăşească informaţia utilă – efect cuantificat în secţiunea 6.4.5.

6.3.2. Suprapunerea protocoalelor peste zonele arhitecturii

Din perspectivă funcţională, traseul comunicaţiei IIoT se împarte în trei zone. Stiva de comunicaţie corespunzătoare este reprezentată în Figura 6.9.

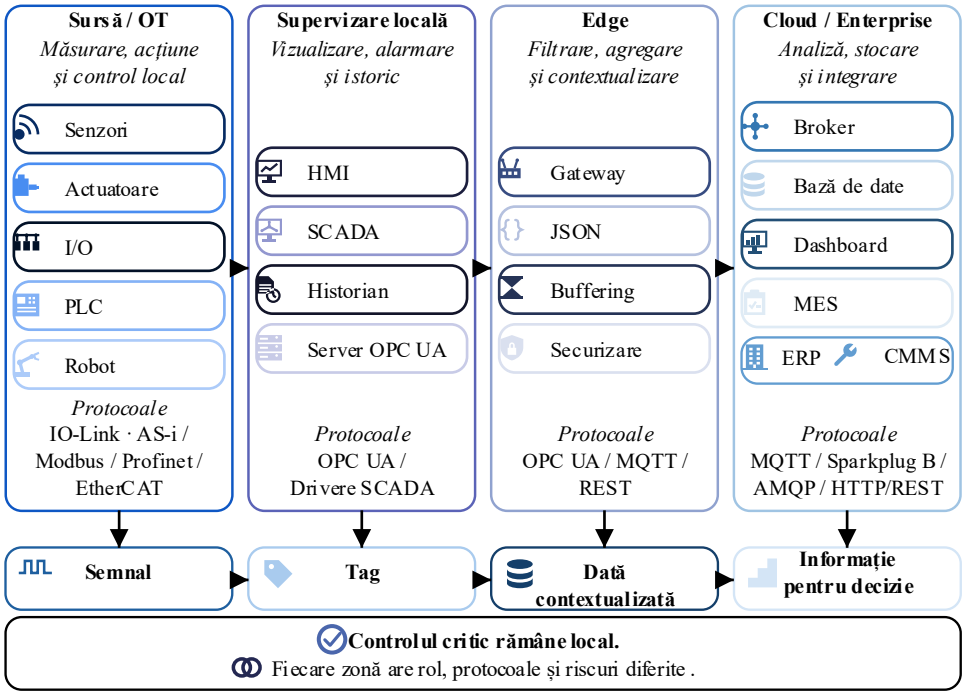


Figura 6.9 – Stiva de comunicaţie IIoT pe zone

Zona sursei și a controlului cuprinde senzorii, actuatoarele, modulele de intrare și ieșire, automatele programabile, controlerele de mișcare, sistemele DCS și echipamentele locale de supraveghere. Aici sunt prioritare timpii de răspuns, sincronizarea și continuarea controlului chiar dacă legătura cu nivelurile superioare este întreruptă. Se utilizează protocoalele tratate în subcapitolul 6.1.

Zona de edge cuprinde gateway-urile industriale, calculatoarele industriale și serviciile software amplasate între rețeaua de control și sistemele superioare. Această zonă realizează conectarea la sursele de date, selecția variabilelor necesare, verificarea calității și a vechimii informației, filtrarea și agregarea, conversia tipurilor și a unităților de măsură, adăugarea identificatorilor și a mărcilor temporale, structurarea mesajelor, stocarea temporară, aplicarea mecanismelor de securitate și publicarea datelor către alte sisteme.

Gateway-ul nu este un releu. Într-un flux OPC UA–MQTT, el încheie sesiunea OPC UA, interpretează nodurile și codurile de stare, construiește un payload nou și inițiază o conexiune MQTT. La edge se termină, prin urmare, o stivă de comunicație și începe alta. Consecința nu este doar tehnică, ci și de securitate: fiecare frontieră de acest tip este un punct în care garanțiile stivei anterioare încetează și trebuie restabilite explicit.

Zona platformei și a aplicațiilor include brokerul, serviciile de rutare, bazele de date, aplicațiile de analiză, tablourile de bord și sistemele MES sau ERP. Aici sunt importante scalabilitatea, distribuirea informației, persistența, integrarea aplicațiilor și administrarea unui număr mare de surse.

Un traseu minimal al datelor pornește de la sursa industrială și continuă, printr-un protocol de control sau de achiziție, către un PLC ori un server de date. Datele sunt apoi transferate prin OPC UA către un gateway industrial, care le transmite prin MQTT securizat către un broker, de unde ajung la sistemele de stocare și la aplicații.

Fluxul către platformă nu face parte din bucla critică de control. Automatul programabil continuă procesul pe baza programului local, a interblocărilor și a funcțiilor de siguranță atunci când gateway-ul, brokerul sau conexiunea externă nu sunt disponibile. Bugetul de latență din secțiunea 6.3.4 arată numeric această separare: lanțul local însumează câteva zeci de milisecunde, în timp ce traseul de observare depășește o secundă, fără ca aceasta să afecteze conducerea procesului.

6.3.3. Exemple de stive de comunicație

Proiectarea unei stive IIoT începe de la cerințele procesului, nu de la lista protocoalelor disponibile. Pentru fiecare variabilă trebuie stabilite cel puțin sursa și semnificația tehnologică, frecvența de achiziție, frecvența de publicare, întârzierea maximă acceptată, precizia și unitatea de măsură, modul de reprezentare a calității, comportamentul la pierderea comunicației, perioada de păstrare, aplicațiile autorizate să utilizeze informația și drepturile de citire, scriere sau comandă. Această listă constituie specificația de date a proiectului și trebuie completată înainte de alegerea produselor.

Tabelul 6.6 – Trei stive de comunicație, pe segmente

Segment	A · Linie de ambalare existentă	B · Celulă robotizată nouă	C · Instalație dispersată, autonomă energetic
Cerința dominantă	Integrare fără oprirea producției	Sincronizarea axelor	Autonomie energetică și acoperire
Sursă	Traductoare 4–20 mA, contoare Modbus	Servomotoare, senzori pe magistrală	Senzori alimentați din baterii
Protocol de câmp	Modbus RTU, PROFIBUS DP existent	EtherCAT	LoRaWAN
Punct de agregare	Automat programabil existent	Controler de mișcare și PLC	Server de rețea LoRaWAN
Protocol de integrare	OPC UA, server în PLC	OPC UA, server în controler	Interfață a serverului de rețea
Transport spre platformă	MQTT peste TLS	MQTT peste TLS	MQTT sau HTTPS, în loturi
Frecvență de publicare	1 s, plus evenimente la prag	1 s agregat; datele de ciclu rămân locale	La modificare, cu publicare periodică de siguranță
Comportament la întrerupere	Stocare temporară în gateway, retransmitere	Idem; ciclul de control nu este afectat	Retransmitere limitată de regimul radio

Rezultatul acestei analize este o stivă diferită pentru fiecare tip de instalație. Tabelul următor prezintă trei configurații complete, construite pentru cerințe distincte.

Cele trei coloane ilustrează aceeași regulă: protocolul rapid rămâne jos, protocolul scalabil rămâne sus, iar punctul de agregare este locul unde se decide ce urcă. În coloana B, datele ciclului de control, produse la fiecare câteva sute de microsecunde, nu sunt publicate: ar genera un volum inutilizabil, iar valoarea lor pentru analiză este acoperită de agregate. În coloana C, tehnologia de acces impune ea însăși frecvența de publicare, potrivit limitelor discutate în secțiunea 6.2.6.

Frecvența de achiziție nu trebuie confundată cu frecvența de publicare. Un automat programabil poate prelua o valoare la fiecare ciclu, gateway-ul o poate citi la 100 ms, iar către platformă poate publica o medie la fiecare secundă; în același timp, depășirea unui prag poate fi transmisă imediat, ca eveniment. Această separare limitează traficul fără să elimine informația necesară.

Mărcile temporale trebuie atribuite cât mai aproape de sursă. Într-un flux complet apar momentul măsurării, momentul preluării de către automat, momentul citirii de către gateway, momentul publicării mesajului, momentul recepționării de către platformă și momentul stocării în baza de date. Pentru analize temporale, momentul măsurării este de regulă cel mai relevant; marca temporală adăugată în platformă indică momentul recepționării și nu poate fi utilizată ca substitut. Sincronizarea ceasurilor și păstrarea referinței UTC sunt necesare pentru corelarea informațiilor provenite din surse diferite – cerință fără de care nici bugetul de latență din secțiunea 6.3.4 nu poate fi verificat prin măsurare.

Calitatea datelor trebuie păstrată la trecerea dintre stive. Dacă serverul OPC UA indică o valoare necorespunzătoare sau incertă, gateway-ul nu trebuie să publice

numai valoarea numerică, pierzând codul de stare. Mesajul rezultat trebuie să conţină suficiente informaţii pentru ca aplicaţia consumatoare să deosebească o măsurare validă de o valoare veche, estimată sau indisponibilă, potrivit contractului de date stabilit în secţiunea 6.2.8.

La întreruperea conexiunii, gateway-ul poate păstra temporar datele şi le poate transmite după reconectare. Strategia necesită reguli explicite pentru capacitatea maximă a memoriei tampon, ordinea retransmiterii, expirarea datelor, identificarea duplicatelor, marcarea valorilor întârziate, prioritatea evenimentelor şi alarmelor şi comportamentul după umplerea memoriei. Ultima regulă este cea mai des omisă şi cea mai consecventă: la umplere, sistemul fie suprascrie cele mai vechi valori, fie opreşte colectarea, iar alegerea trebuie făcută conştient, nu moştenită din configuraţia implicită a produsului.

Securitatea trebuie restabilită la fiecare frontieră unde o stivă se termină. O conexiune OPC UA securizată până la gateway nu protejează mesajul MQTT transmis mai departe; sunt necesare identităţi, certificate, drepturi şi jurnale pentru fiecare segment. Gateway-ul devine astfel simultan punct de integrare şi frontieră de încredere, iar compromiterea lui expune ambele zone.

Diagnosticarea se realizează tot pe segmente. Dacă o valoare apare în serverul OPC UA, dar nu ajunge în baza de date, verificarea parcurge succesiv sursa OPC UA şi codul de stare, clientul implementat în gateway, funcţia de structurare a mesajului, clientul MQTT şi conexiunea TLS, brokerul şi politica aplicată subiectului, regula de rutare, operaţia de scriere şi, în final, aplicaţia care citeşte datele. Abordarea localizează defectul şi evită modificarea simultană a mai multor componente.

Traseul fiind definit, rămâne de stabilit cât durează parcurgerea lui. Secţiunea următoare transformă această întrebare într-un calcul.

6.3.4. Bugetul de latenţă pe lanţul de date

Latenţa până la afişarea valorii în tabloul de bord rezultă din însumarea întârzierilor întregului traseu, depăşind evaluarea unui singur protocol. Predomină parametrii de configurare: perioada conversiei modulului de intrare, ciclul programului, intervalele de eşantionare şi publicare OPC UA şi gruparea temporală a scrierilor în baza de date. Bugetul de latenţă, figura 6.7, evidenţiază contribuţia fiecărui segment şi localizează intervenţiile eficiente.

Se consideră o maşină de sigilat dintr-o linie de ambalare. Variabila urmărită este presiunea din circuitul pneumatic, măsurată de un traductor cu semnal 4–20 mA. Cerinţa procesului, formulată de beneficiar, este ca valoarea să fie vizibilă în tabloul de bord în cel mult 2 s de la modificarea mărimii fizice. Valorile din tabel sunt ipoteze de proiectare preluate din fişele tehnice şi din parametrii configuraţi, nu măsurători; fiecare trebuie înlocuită cu o valoare măsurată înainte ca bugetul să fie folosit drept criteriu de recepţie.

Timpul total de observare se obţine prin însumarea termenilor în cazul cel mai defavorabil:

Tabelul 6.7 – Bugetul de latență pentru o variabilă analogică publicată către o bază de date de serie temporală

Segment	Mărimea care determină întârzierea	Valoare de proiectare	Originea valorii
S1 · Traductor de presiune	timp de răspuns t_{10-90}	20 ms	fișa tehnică
S2 · Modul de intrare analogică	perioada de conversie și filtrare	5 ms	parametru configurat
S3 · Ciclul programului PLC	durata unui ciclu, caz defavorabil	10 ms	timp de ciclu configurat
S4 · Eșantionarea elementului monitorizat	interval de eșantionare	100 ms	parametru configurat
S5 · Publicarea notificării de abonament	interval de publicare	100 ms	parametru configurat
S6 · Prelucrarea în gateway	validare, conversie, construirea payloadului	10 ms	măsurabil în gateway
S7 · Transmisia gateway – broker	jumătate din timpul dus-întors, plus serializarea	30 ms	latența măsurată a legăturii
S8 · Distribuirea broker – serviciu de ingestie	prelucrarea internă a brokerului	10 ms	parametru de exploatare
S9 · Scrierea în baza de date	intervalul de grupare a scrierilor	1000 ms	parametru configurat

$$T_{obs} = \Sigma\, t_i\,,\ i = 1\ldots9$$

$$T_{obs} = 20 + 5 + 10 + 100 + 100 + 10 + 30 + 10 + 1.000 = 1.285 \text{ ms}$$

Rezultatul se încadrează în cerința de 2.000 ms, cu o marjă de 715 ms, adică 36 % din bugetul disponibil. Distribuția termenilor este însă mai instructivă decât suma. Scrierea grupată în baza de date reprezintă 1.000 ms, adică 78 % din total; cele două intervale ale abonamentului OPC UA adaugă împreună 200 ms, adică 16 %; întregul lanț local, de la traductor până la imaginea de proces a automatului programabil, contribuie cu 35 ms, sub 3 %. Reducerea intervalelor de eșantionare și publicare de la 100 ms la 20 ms, operație care încarcă suplimentar serverul OPC UA, scade totalul la 1.125 ms – un câștig de 12 %. Reducerea intervalului de grupare a scrierilor de la 1.000 ms la 200 ms scade totalul la 485 ms, un câștig de 62 %, fără nicio modificare în zona de control. Regula de proiectare care rezultă este că optimizarea trebuie aplicată termenului dominant, nu segmentului cel mai vizibil.

Bugetul descrie exclusiv observabilitatea, nu controlul. Bucla care închide o interblocare pe pragul de presiune folosește numai segmentele S1–S3, are un timp total de 35 ms și se execută integral în automatul programabil. Indisponibilitatea gateway-ului, a brokerului sau a legăturii externe nu o afectează. Un flux de publicare nu trebuie proiectat niciodată astfel încât o funcție de siguranță sau o interblocare să depindă de disponibilitatea lui.

Suma cazurilor defavorabile supraestimează în mod deliberat, pentru că termenii nu ating simultan valoarea maximă. Termenii determinați de o eșantionare periodică – S2, S3, S4, S5 și S9 – contribuie cu o valoare cuprinsă între zero și perioada completă, în funcție de momentul în care evenimentul cade în raport cu instanța de eșantionare. Termenii ficși însumează 70 ms. Latența observată variază, prin

urmare, între aproximativ 70 ms și 1.285 ms, iar această variație de circa 1.215 ms, nu valoarea medie, este mărimea care trebuie declarată atunci când datele sunt corelate temporal cu alte surse.

Bugetul are limite care trebuie enunțate odată cu el. Nu descrie o distribuție statistică, ci două valori extreme; validarea cere măsurarea unor percentile, uzual al 95-lea și al 99-lea. Nu include timpul de restabilire după o întrerupere a comunicației și nici retransmiterea datelor păstrate temporar în gateway, care pot produce întârzieri cu două ordine de mărime mai mari pentru valorile recuperate. Nu include retransmisiile la nivel TCP, cozile brokerului în regim de încărcare și timpul de așteptare al bazei de date, care se manifestă ca majorări ale termenilor S7–S9. În sfârșit, măsurarea efectivă a timpului cap-coadă presupune ceasuri sincronizate pe tot lanțul; fără sincronizare, diferența dintre marca temporală a sursei și cea a platformei măsoară deriva ceasurilor, nu latența.

6.4. Considerații privind alegerea protocolului

Alegerea protocolului de comunicație pornește de la cerințele procesului și ale fiecărui flux de date. Nu există un protocol universal care să ofere simultan determinism strict, modelare informațională avansată, consum minim de resurse, integrare directă cu aplicațiile informatice și administrare simplă. Fiecare tehnologie optimizează câteva dintre aceste dimensiuni în detrimentul celorlalte, iar afirmația contrară, oricât de des repetată în materialele comerciale, nu rezistă unei verificări cantitative.

Într-o arhitectură IIoT sunt utilizate, prin urmare, mai multe protocoale: unul asigură schimbul ciclic dintre controler și dispozitivele de teren, altul furnizează acces structurat la informații, iar un protocol de mesagerie distribuie datele către platforme și aplicații externe. Întrebarea corectă nu este care este cel mai bun protocol, ci ce protocol este potrivit pentru fiecare segment și pentru fiecare categorie de date. Subcapitolul stabilește mai întâi cum se formulează cerințele, apoi criteriile de departajare, un ghid orientativ pe scenarii, metoda de selecție și validare și, în final, calculul de dimensionare a benzii necesare.

6.4.1. Definirea cerințelor fluxului de comunicație

Selectarea începe cu identificarea fluxurilor care trebuie implementate. În aceeași instalație coexistă, de regulă, date ciclice pentru controlul intrărilor și ieșirilor; valori de referință și reacții pentru controlul mișcării; semnale asociate funcțiilor de siguranță; stări, alarme și evenimente; date de monitorizare și diagnosticare; informații despre producție și calitate; serii temporale utilizate pentru analiză; comenzi sau rețete provenite de la sistemele superioare; și date destinate sistemelor MES, ERP sau platformelor cloud.

Pentru fiecare flux trebuie stabilite sursa şi destinaţia, sensul comunicaţiei, frecvenţa de actualizare, volumul şi dimensiunea mesajelor, întârzierea maximă acceptată, variaţia admisă a întârzierii, comportamentul acceptabil la pierderea unui mesaj, ordinea necesară a mesajelor, numărul iniţial şi estimat al nodurilor, perioada în care datele rămân relevante, necesitatea păstrării calităţii şi a mărcilor temporale, drepturile de citire, scriere şi comandă, precum şi comportamentul sistemului la întreruperea comunicaţiei.

Cerinţele trebuie exprimate măsurabil. Formulări precum „latenţă redusă", „reţea rapidă" sau „fiabilitate ridicată" nu pot fi verificate şi, prin urmare, nu pot fi impuse contractual. O cerinţă utilizabilă are forma: valoarea trebuie să fie disponibilă în baza de date în cel mult 2 s de la modificarea mărimii fizice, în 99 % dintre cazuri, la o încărcare de 240 de semnale publicate simultan. Formulată astfel, ea poate fi verificată prin bugetul de latenţă din secţiunea 6.3.4 şi prin calculul de bandă din secţiunea 6.4.5, iar la recepţie poate fi măsurată.

Distanţa dintre cerinţe este adesea de ordine de mărime. O temperatură destinată analizei energetice poate fi publicată la câteva secunde şi tolerează pierderea ocazională a unei măsurări; valorile utilizate pentru sincronizarea unor axe trebuie schimbate într-un ciclu predictibil de ordinul sutelor de microsecunde, iar variaţia întârzierii afectează direct comportamentul mecanismului. Tratarea celor două fluxuri prin aceeaşi tehnologie este posibilă tehnic şi greşită economic.

6.4.2. Criterii de selecţie

Determinismul şi cerinţele de timp real

Pentru controlul mişcării, sincronizarea roboţilor, acţionarea servomotoarelor şi schimbul ciclic rapid sunt necesare tehnologii proiectate pentru comunicaţie deterministă. EtherCAT şi PROFINET IRT oferă mecanisme de sincronizare precisă şi comunicaţie izocronă [169], [171], iar performanţele lor pot fi comparate prin indicatorii definiţi în standardul de profiluri, nu prin declaraţii de produs [24].

Determinismul nu echivalează cu latenţa medie redusă: variaţiile ocazionale pot perturba procesul. Evaluarea include timpul maxim, variaţia întârzierii, pierderea cadrelor, comportamentul la congestie şi durata recuperării după o defecţiune.

MQTT, AMQP şi interfeţele HTTP nu se includ în buclele critice de control. Ele sunt adecvate distribuirii datelor, integrării aplicaţiilor şi transmiterii solicitărilor către controler, dar executarea efectivă a comenzilor se validează local. Determinismul comunicaţiei nu certifică, la rândul lui, funcţia de siguranţă: o funcţie care protejează operatorii sau echipamentele se implementează prin componente şi profiluri de siguranţă adecvate, conform analizei de risc şi cerinţelor aplicabile.

Topologia și infrastructura existentă

Selecția se corelează cu mediul fizic: distanțele dintre echipamente, numărul și distribuția nodurilor, mediile electrice, optice sau radio disponibile, topologia magistrală, linie, stea, arbore sau inel, necesitatea redundanței, condițiile electromagnetice, existența echipamentelor seriale, posibilitatea instalării unor cabluri sau comutatoare suplimentare și delimitarea zonelor de securitate.

Modbus RTU rămâne justificat pentru conectarea unui număr redus de echipamente seriale existente. Înlocuirea sa nu este obligatorie dacă îndeplinește cerințele locale – verificabile prin calculul din secțiunea 6.1.3 – și dacă este separat corespunzător de rețelele externe. Pentru integrarea cu aplicații moderne se utilizează un gateway industrial care convertește și contextualizează datele. Într-o rețea extinsă, alegerea trebuie să includă și comportamentul la defectarea unei legături sau a unui echipament central: compatibilitatea unui protocol cu topologia proiectată nu garantează disponibilitatea în absența redundanței, a diagnosticării și a procedurilor de recuperare.

Scalabilitatea și flexibilitatea

Scalabilitatea nu este determinată numai de numărul dispozitivelor. Contează numărul conexiunilor simultane, frecvența și dimensiunea mesajelor, numărul abonamentelor, volumul datelor reținute sau stocate temporar, încărcarea controlerelor și a gateway-urilor, capacitatea brokerului, extinderea cu noi linii, fabrici sau aplicații și administrarea identităților și a certificatelor.

MQTT facilitează distribuirea aceloraşi date către mai mulți consumatori, dar capacitatea efectivă depinde de broker, de politicile de păstrare, de nivelurile QoS și de comportamentul clienților; specificația definește mecanismele protocolului, nu dimensionarea platformei [177]. Un aspect adesea omis este multiplicarea traficului la ieșirea din broker: un mesaj publicat o dată și consumat de cinci aplicații generează șase transferuri, iar banda calculată în secțiunea 6.4.5 se raportează la un singur consumator. OPC UA susține dezvoltarea graduală prin spațiul de adrese, tipurile reutilizabile și modelele informaționale, însă scalabilitatea serverului trebuie verificată pentru numărul de sesiuni, abonamente, elemente monitorizate și frecvența notificărilor.

Integrarea cu sistemele informatice și platformele externe

Atunci când aplicația necesită descoperirea echipamentelor, navigarea prin variabile, păstrarea relațiilor și accesarea unor informații contextualizate, OPC UA este opțiunea potrivită, prin mecanismele sale de interoperabilitate, modelare a informației și comunicație securizată [173]. Atunci când aceleași date trebuie distribuite către mai multe aplicații independente, MQTT reduce dependența directă dintre producători și consumatori, cu condiția completării prin structura subiectelor, contractul de date, politicile de acces și regulile pentru starea mesajelor stabilite în

secţiunea 6.2.8. Pentru integrarea tranzacţională dintre aplicaţii informatice pot fi adecvate AMQP sau interfeţele HTTP/REST, alegerea ţinând seama de confirmări, persistenţă, trasabilitate, tratarea erorilor şi posibilitatea repetării controlate a operaţiilor.

Integrarea cu nivelul IT nu presupune conectarea directă a reţelei de control la internet. Datele se transferă prin componente şi zone intermediare, cu drepturi, filtrare şi monitorizare corespunzătoare; arhitectura acestor zone este tratată în secţiunea 8.2.

Securitatea comunicaţiei

Existenţa unor mecanisme de criptare sau autentificare nu face o implementare sigură. Trebuie verificate autentificarea aplicaţiilor şi a utilizatorilor, criptarea şi integritatea comunicaţiei, autorizarea separată pentru citire, scriere, publicare şi abonare, administrarea certificatelor şi a cheilor, jurnalizarea operaţiilor, limitarea variabilelor şi a subiectelor expuse, comportamentul la expirarea sau revocarea unei identităţi, disponibilitatea componentelor intermediare şi actualizarea produselor şi bibliotecilor utilizate.

Protocoalele industriale vechi, lipsite de mecanisme proprii, se utilizează în zone izolate şi se protejează prin segmentare, controlul accesului şi porţi de integrare. Încapsularea unui protocol nesecurizat într-o conexiune protejată rezolvă numai securitatea acelui segment şi nu elimină vulnerabilităţile echipamentului sau ale reţelei locale – distincţie dezvoltată în subcapitolul 8.2.

Resursele disponibile şi costul ciclului de viaţă

Protocolul trebuie să poată fi implementat în limitele de procesare, memorie, energie şi lăţime de bandă ale dispozitivului. Pentru senzori sau microcontrolere cu resurse reduse pot fi adecvate CoAP, MQTT într-o configuraţie simplă sau un protocol serial existent.

Costul total include licenţe, echipamente, configurare, diagnosticare, dezvoltarea şi testarea aplicaţiilor, administrarea certificatelor, instruire, actualizări, înlocuiri, suport şi menţinerea compatibilităţii. Simplitatea protocolului poate impune costuri pentru un model propriu de date, iar funcţionalităţile extinse ale unui standard pot fi nejustificate pentru transmiterea câtorva valori. Reînnoirea certificatelor constituie o obligaţie periodică, cu termene definite; într-o instalaţie cu sute de identităţi, aceasta trebuie inclusă în mentenanţa curentă, dincolo de punerea în funcţiune.

Standardizarea şi interoperabilitatea

Selectarea unui standard deschis reduce dependenţa de un singur furnizor, dar nu garantează interoperabilitatea. Trebuie verificate versiunea şi profilul implementat, serviciile obligatorii şi opţionale, codificările şi mecanismele de transport acceptate, modelele informaţionale utilizate, politicile de securitate comune,

certificarea produselor şi compatibilitatea demonstrată între echipamentele concrete. Pentru OPC UA se verifică dacă aplicaţiile utilizează aceleaşi modele şi interpretări ale informaţiei; pentru MQTT se verifică contractul payloadului, deoarece protocolul nu defineşte semnificaţia datelor; pentru reţelele industriale se verifică profilurile dispozitivelor, fişierele de configurare şi funcţiile de diagnosticare acceptate.

6.4.3. Alegerea protocolului în funcție de scenariu

Criteriile din secţiunea anterioară conduc, pentru situaţiile industriale întâlnite frecvent, la combinaţii care se repetă. Tabelul 6.8 le sintetizează, oferind un punct de plecare pentru proiectare. El nu înlocuieşte analiza, ci scurtează drumul până la ipoteza care urmează a fi verificată prin fişele de cerinţe din secţiunea 6.4.1 şi prin calculele din secţiunile 6.3.4 şi 6.4.5.

Tabelul 6.8 – Ghid de alegere a protocoalelor în funcție de scenariul industrial

Scenariu	**Cerințe dominante**	**Soluție recomandată**	**Condiții și limitări**
Celulă robotizată cu mai multe servomotoare	Sincronizare, ciclu predictibil, variație redusă a întârzierii, diagnosticare rapidă	EtherCAT sau PROFINET IRT pentru controlul mișcării; OPC UA pentru supraveghere și acces la date	Bucla de control și funcțiile de siguranță rămân locale; fluxul IIoT nu participă la sincronizarea axelor
Linie de producție cu PLC, HMI și SCADA	Schimb ciclic de intrări și ieșiri, alarme, stări, acces contextualizat la variabile	Rețea Ethernet industrială pentru control; OPC UA între PLC, SCADA și gateway industrial	Se verifică timpii de actualizare, numărul abonamentelor și drepturile de scriere
Modernizarea echipamentelor cu interfețe seriale	Compatibilitate cu instalația existentă, cost redus, integrare graduală	Modbus RTU către un gateway industrial; OPC UA sau Modbus TCP spre sistemele locale; MQTT către platformă	Echipamentele seriale nu se expun rețelelor externe; gateway-ul validează, contextualizează și securizează datele
Monitorizarea mai multor linii sau locații	Distribuirea acelorași date, conectivitate variabilă, extindere, integrare cu baze de date	OPC UA pentru achiziția locală; MQTT cu TLS pentru distribuire; opțional Sparkplug pentru metrici și stare	Sunt necesare memorie tampon, identificarea duplicatelor, mărci temporale, redundanța brokerului și politici pe subiecte
Rețea de senzori autonomi amplasați la distanță	Consum energetic redus, mesaje scurte, transmisii rare	CoAP sau MQTT printr-un gateway industrial; LoRaWAN pentru conectivitate radio, dacă cerințele permit	Nepotrivit pentru control rapid; se evaluează debitul, întârzierea, durata de viață a bateriei și regimul de utilizare a canalului
Integrarea aplicațiilor MES, ERP și logistice	Schimburi între aplicații, confirmări, trasabilitate, versionarea interfețelor	HTTP/REST pentru operații inițiate la cerere; AMQP pentru fluxuri care necesită cozi și confirmări	Operațiile se proiectează pentru repetare controlată; succesul transportului nu înseamnă finalizarea tranzacției

Tabelul nu constituie o regulă rigidă. Produsele disponibile, profilurile implementate, infrastructura existentă şi cerinţele măsurabile pot conduce la alte combinaţii. Înaintea selecţiei finale se verifică documentaţia exactă a echipamentelor.

6.4.4. Metoda de selecţie şi validare

Un proces coerent de alegere parcurge opt etape. Se identifică toate fluxurile de date şi se separă controlul local de monitorizare, analiză şi integrarea aplicaţiilor. Se clasifică fluxurile după criticitate şi se stabilesc funcţiile care trebuie să continue la pierderea conexiunii. Se definesc limitele privind ciclul de comunicaţie, întârzierea, variaţia întârzierii, pierderea mesajelor şi timpul de recuperare. Se elimină protocoalele care nu îndeplinesc cerinţele obligatorii. Se compară soluţiile rămase din perspectiva infrastructurii, securităţii, interoperabilităţii, costului şi posibilităţii de extindere. Se selectează protocolul pentru fiecare segment, împreună cu gateway-ul, formatul datelor şi mecanismele de securitate. Se realizează un prototip şi se măsoară comportamentul în condiţii normale şi în situaţii de defect. Se documentează configuraţia, versiunile, identităţile, drepturile, parametrii de comunicaţie şi rezultatele testelor. Etapele sunt sintetizate în Figura 6.10.

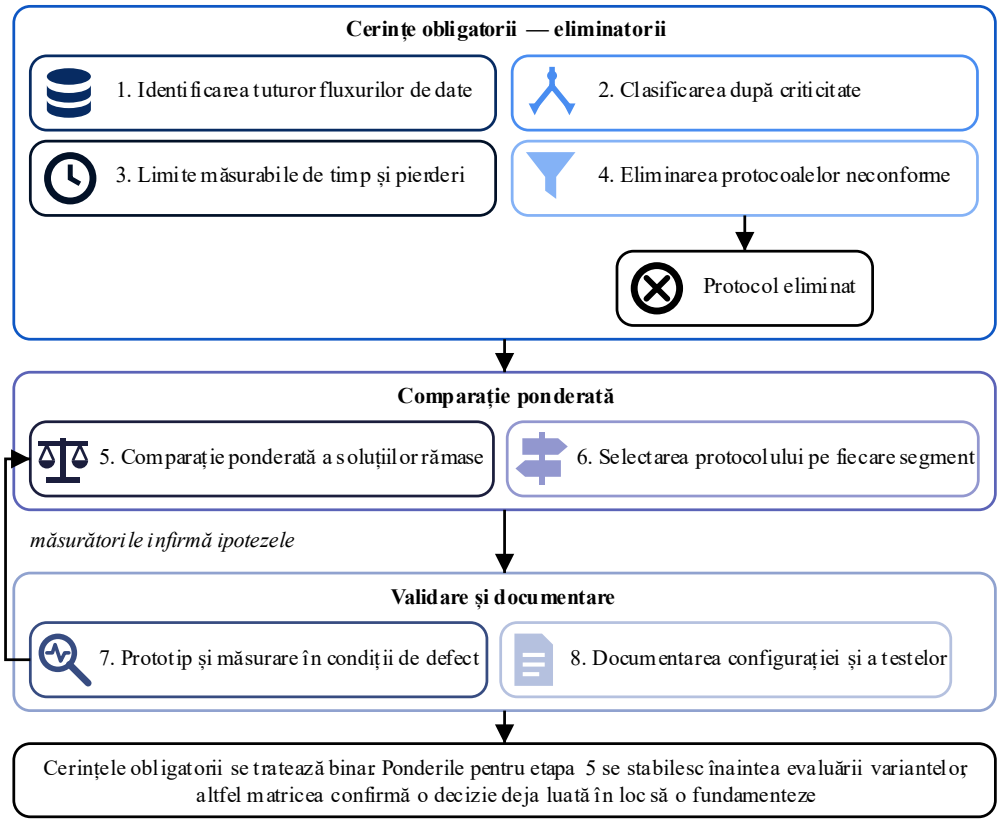


Figura 6.10 – Metoda de selecţie şi validare a protocoalelor

Separarea etapelor a patra și a cincea este esențială și se pierde frecvent în practică. Cerințele obligatorii se tratează binar: un protocol care nu respectă timpul maxim admis sau cerințele de siguranță este eliminat, indiferent de punctajul obținut la celelalte criterii. Abia soluțiile rămase se compară printr-o matrice ponderată. Pentru o linie de ambalare, o repartizare uzuală a ponderilor ar acorda 30 % interoperabilității și integrării, 25 % securității, 20 % costului ciclului de viață, 15 % scalabilității și 10 % compatibilității cu infrastructura existentă; o celulă robotizată ar inversa complet aceste ponderi. Ponderile se stabilesc însă înaintea evaluării variantelor, nu după, altfel matricea confirmă o decizie deja luată în loc să o fundamenteze.

Validarea se efectuează cap-coadă, cu echipamentele și configurațiile care vor fi utilizate în exploatare. Testele urmăresc timpul de transfer și variația acestuia, încărcarea rețelei și a procesoarelor, pierderea, duplicarea și reordonarea datelor, reconectarea după întrerupere, comportamentul memoriei tampon, păstrarea mărcilor temporale și a calității, respingerea accesului neautorizat, expirarea certificatelor, defectarea gateway-ului sau a brokerului, continuarea controlului local și compatibilitatea dintre produsele furnizorilor selectați. Ultimele două elemente se verifică prin provocarea deliberată a defectului, nu prin lectura documentației.

Rezultatul selecției este, de regulă, o arhitectură hibridă: protocoalele deterministe rămân în zona de control, OPC UA asigură accesul contextualizat la informațiile industriale, iar MQTT, AMQP sau HTTP susțin integrarea cu platformele și aplicațiile externe. Înainte de a aplica metoda în exerciții, secțiunea următoare transformă unul dintre criteriile enunțate mai sus – volumul traficului generat – într-un calcul complet.

6.4.5. Dimensionarea lățimii de bandă necesare publicării datelor

Criteriul de selecție discutat anterior – volumul traficului generat către platformă – devine operațional numai dacă este calculat. Calculul este simplu, iar rezultatul contrazice frecvent intuiția: pentru mesaje industriale scurte, cea mai mare parte a benzii consumate nu transportă valori de proces, ci antete.

Dimensiunea unui mesaj publicat prin MQTT peste TLS și TCP/IP se compune astfel:

$$L_{msg} = L_{MQTT} + L_{TLS} + L_{TCP/IP} (+ L_{Ethernet})$$

$$L_{MQTT} = (1 + n_{LR}) + (2 + L_{subiect}) + 2 \cdot \delta(QoS>0) + L_{proprietăți} + L_{payload}$$

Termenul n_{LR} este numărul de octeți ai câmpului de lungime rămasă, unul pentru mesaje sub 128 de octeți; câmpul de proprietăți ocupă minimum un octet, chiar când este vid [177]. Peste acesta, o înregistrare TLS 1.3 adaugă 5 octeți de antet, 1 octet de tip de conținut interior și 16 octeți de etichetă de autentificare, în total 22 de octeți [189]. Antetul TCP fără opțiuni are 20 de octeți [186], iar antetul IPv4 fără opțiuni tot 20 [190]. Cadrul Ethernet adaugă 14 octeți de antet și 4 octeți de

secvență de control, la care se adaugă pe mediu 8 octeți de preambul și echivalentul a 12 octeți de interval între cadre [191].

Cazul A – un mesaj pentru fiecare semnal. Linia publică 240 de semnale, fiecare pe subiectul propriu, cu frecvența de 1 Hz și calitatea serviciului QoS 1. Subiectul „fabrica/hala_1/linia_2/motor_03/dat/temperatura" are 47 de octeți, iar payloadul este:

```
{"ts":"2026-08-12T09:15:03.250Z","v":74.6,"u":"C","q":192}
```

Cazul B — un mesaj pentru fiecare dispozitiv. Aceleași 240 de semnale sunt grupate câte douăsprezece, pe douăzeci de dispozitive, și publicate o dată pe secundă pe subiectul „fabrica/hala_1/linia_2/motor_03/dat", de 35 de octeți:

```
{"ts":"2026-08-12T09:15:03.250Z","q":192,"m":{"p_aer":6.42,
"t_motor":74.6,"i_motor":12.3,"n_motor":1478,"t_sigilare":183.5,
"p_sigilare":2.10,"v_banda":0.62,"n_cicluri":10428,"n_rebut":37,
"stare":3,"t_mediu":27.4,"h_mediu":41.8}}
```

Compunerea dimensiunii mesajului în cele două cazuri este prezentată în Tabelul 6.9.

Tabelul 6.9 – Compunerea dimensiunii unui mesaj MQTT, pentru cele două convenții de publicare

Component	Caz A: un semnal / mesaj	Caz B: un dispozitiv / mesaj
Payload JSON	58 B	228 B
Subiect	47 B	35 B
Pachet MQTT complet	112 B	271 B
+ înregistrare TLS 1.3	134 B	293 B
+ TCP și IPv4	174 B	333 B
+ cadru Ethernet, pe mediu	212 B	371 B
Randament util (payload / octeți pe mediu)	27,4 %	61,5 %
Debit la nivelul pachetelor IP	334,1 kbit/s	53,3 kbit/s
Volum transferat la 30 de zile	108,2 GB	17,3 GB

Debitul rezultat în cazul A, la nivelul pachetelor IP, se obține din relația $B = 8 \cdot f \cdot L$, adică $8 \cdot 240\ s^{-1} \cdot 174\ B = 334{,}1$ kbit/s. Pe segmentul Ethernet local, unde antetele de cadru sunt vizibile, valoarea urcă la 407,0 kbit/s. La aceasta se adaugă confirmările PUBACK impuse de QoS 1, de 104 octeți pe mediu fiecare, adică încă 199,7 kbit/s în sens invers. În cazul B, același calcul conduce la $8 \cdot 20\ s^{-1} \cdot 333\ B = 53{,}3$ kbit/s.

Cantitatea de informație utilă este identică în cele două cazuri – 240 de valori pe secundă – dar banda consumată scade de 6,3 ori. Explicația este integral în tabel: în cazul A, 154 din cei 212 octeți transmiși pe mediu pentru fiecare valoare sunt antete. Gruparea nu comprimă datele, ci amortizează antetele peste mai multe valori. Diferența devine semnificativă atunci când legătura este tarifată la volum sau când platforma facturează datele ingerate.

A treia pârghie este publicarea la modificare, cu bandă moartă (*deadband*). Volumul scade proporţional cu fracţiunea k a eşantioanelor care depăşesc pragul, iar k nu poate fi presupus: se determină prin măsurare pe procesul real, pentru că depinde de zgomotul semnalului şi de regimul de funcţionare. Pentru o valoare ilustrativă k = 0,2, cazul B ar coborî la circa 3,5 GB la 30 de zile. Pragul trebuie ales împreună cu procesul: o bandă moartă prea largă suprimă tocmai variaţiile care interesează analiza, iar o bandă moartă aplicată fără o publicare periodică de siguranţă face imposibilă deosebirea între o valoare constantă şi o sursă oprită.

Calculul nu epuizează încărcarea legăturii. Nu include confirmările TCP, retransmisiile, mesajele de menţinere a conexiunii, restabilirea periodică a sesiunilor TLS şi nici multiplicarea traficului la ieşirea din broker, care creşte proporţional cu numărul abonaţilor la acelaşi subiect. Nu ţine seama nici de mecanismul de aliasuri de subiect din MQTT 5.0, care înlocuieşte subiectul cu un identificator scurt după prima publicare şi reduce sensibil termenul corespunzător în cazul A. Din acest motiv, dimensionarea unei legături nu se face la valoarea calculată, ci cu rezervă: o practică uzuală de proiectare este ca traficul permanent estimat să nu depăşească 30–50 % din capacitatea nominală, pentru a lăsa loc vârfurilor de retransmitere după o întrerupere, când gateway-ul îşi goleşte memoria tampon şi generează, pentru câteva minute, un debit de câteva ori mai mare decât cel de regim.

6.5. Exerciții aplicative pentru validarea comunicațiilor industriale și IIoT

Protocoalele de comunicaţie nu pot fi înţelese complet prin definiţii şi comparaţii. Ele trebuie observate în scenarii în care datele sunt generate, transmise, recepţionate, interpretate şi utilizate de o aplicaţie.

Într-un sistem industrial, stabilirea unei conexiuni nu demonstrează funcţionarea corectă a comunicaţiei. Trebuie verificat dacă informaţia provine din sursa stabilită, dacă este asociată variabilei corecte, dacă ajunge la destinaţie în intervalul admis şi dacă îşi păstrează valoarea, unitatea de măsură, marca temporală şi calitatea. Sistemul trebuie, în plus, să detecteze pierderea conexiunii, valorile neactualizate, mesajele invalide şi accesul neautorizat.

Exerciţiile din acest subcapitol sunt agnostice faţă de produs. Ele nu presupun un anumit automat programabil, mediu de inginerie, broker sau instrument de vizualizare, ci numai disponibilitatea unor funcţii: un broker MQTT care acceptă versiunea 5 a protocolului şi conexiuni TLS; un instrument capabil să publice şi să se aboneze la subiecte; două automate programabile care schimbă date printr-un protocol Ethernet industrial; un sistem SCADA sau o interfaţă HMI care poate afişa starea comunicaţiei. Valorile numerice indicate mai jos sunt parametri de configurare propuşi, iar rezultatele aşteptate se deduc din ei; ele se înlocuiesc cu valorile instalaţiei reale, fără ca metoda să se schimbe.

Cele trei situaţii urmărite sunt distribuirea datelor prin MQTT, schimbul ciclic de comenzi şi stări între două automate programabile şi monitorizarea comunicaţiei într-un sistem SCADA.

6.5.1. Validarea comunicației MQTT

Exerciţiul urmăreşte realizarea şi verificarea unui flux bazat pe modelul publicare–abonare. Un gateway industrial publică periodic temperatura unui motor, iar o aplicaţie de monitorizare se abonează la informaţia respectivă. Traseul datelor porneşte de la sursa de date şi continuă prin clientul publicator către brokerul MQTT, care transmite mesajele clientului abonat, de unde acestea ajung la aplicaţia de monitorizare.

Subiectul şi structura mesajului respectă convenţia stabilită în secţiunea 6.2.8:

```
fabrica/hala_1/linia_2/motor_03/dat/temperatura
{"ts":"2026-08-12T09:15:03.250Z","v":74.6,"u":"C","q":192,
 "src":"ns=3;s=Linia_2.Motor_03.Temperatura"}
```

Parametrii de configurare propuşi sunt: perioadă de publicare 1 s; nivel QoS 1; interval de menţinere a conexiunii 30 s; mesaj de testament publicat pe „fabrica/hala_1/linia_2/motor_03/sts/conexiune", cu indicatorul de reţinere activ; expirarea mesajelor după 300 s; memorie tampon în publicator pentru 600 de mesaje. Câmpul „q" transportă calitatea pe scara compactă, conform regulii de conversie din secţiunea 6.2.8.

Din aceşti parametri rezultă direct comportamentul aşteptat. În regim normal, abonatul recepţionează 60 de mesaje pe minut, cu mărci temporale succesive la 1 s şi fără discontinuităţi în câmpul „ts". La deconectarea publicatorului, brokerul publică mesajul de testament în cel mult 45 s – intervalul de menţinere majorat cu jumătate – iar aplicaţia trebuie să marcheze sursa drept indisponibilă în acest interval, nu la prima valoare lipsă. La restabilirea legăturii după o întrerupere de 30 s, memoria tampon retransmite 30 de mesaje cu mărcile temporale originale, nu cu momentul retransmiterii; verificarea acestui detaliu este scopul principal al exerciţiului, pentru că substituirea mărcii temporale invalidează orice analiză ulterioară.

Pentru validarea iniţială se publică un mesaj simplu, apoi se introduce structura completă. Succesiunea separă problemele de conectivitate de cele de formatare şi interpretare. Testarea parcurge: pornirea şi accesibilitatea brokerului; conectarea clientului abonat; abonarea la subiect; conectarea publicatorului; publicarea unui mesaj de test; recepţionarea lui; validarea structurii JSON; verificarea sursei, unităţii, calităţii şi mărcii temporale; justificarea nivelului QoS ales; şi verificarea comportamentului la întreruperea şi restabilirea conexiunii.

Testarea trebuie să includă cel puţin: neconcordanţa subiectelor de publicare şi abonare; adresă sau port incorect; JSON invalid; respingerea clientului neautorizat; deconectarea publicatorului; mesaje duplicate; valori reţinute neactuale; expirarea sau respingerea certificatului pentru conexiunile securizate.

Nivelul QoS se alege în funcție de consecințele pierderii sau duplicării mesajului. Confirmarea realizată prin MQTT atestă schimbul dintre client și broker, dar nu demonstrează că informația a fost afișată, analizată sau stocată de aplicația finală [177]; aceste etape se verifică separat.

Criterii de reușită: exercițiul este finalizat când sunt îndeplinite simultan patru condiții: un mesaj poate fi urmărit de la publicator până la aplicația abonată, cu toate câmpurile contractului intacte; întreruperea publicatorului este semnalată aplicației în intervalul calculat mai sus; retransmiterea după reconectare păstrează mărcile temporale ale măsurării; iar un client fără drepturi pe subiectul respectiv este respins la conectare sau la publicare, cu înregistrarea tentativei.

6.5.2. Validarea schimbului de date între două automate programabile

Al doilea exercițiu ilustrează comunicația ciclică din zona OT prin schimbul de date dintre două controlere. Primul trimite comenzi, iar al doilea controlează un motor sau un transportor simulat și transmite stările rezultate. Pentru comunicație se utilizează PROFINET sau un protocol industrial echivalent, disponibil în infrastructură. PLC 1 trimite comanda prin rețeaua industrială către PLC 2, care o verifică local și o execută, apoi transmite înapoi confirmarea și informațiile de stare.

Datele schimbate includ cel puțin „*Pornire_Motor*" și „*Oprire_Motor*", transmise de primul controler, respectiv „*Motor_Pornit*", „*Stare_OK*", „*Defect*", „*Confirmare_Comanda*" și „*Puls_Comunicatie*", transmise de al doilea.

Parametrii de configurare propuși: perioadă de actualizare a datelor ciclice 10 ms; semnal periodic de prezență care își schimbă starea la fiecare 500 ms; supraveghere a acestui semnal cu declanșare după trei perioade fără schimbare, adică 1,5 s; interval maxim admis pentru confirmarea unei comenzi 300 ms.

Validarea trebuie să demonstreze o succesiune completă, nu modificarea izolată a unei variabile: primul controler transmite comanda de pornire; al doilea o recepționează; verifică modul de funcționare, interblocările și condițiile locale; execută comanda numai dacă pornirea este permisă; transmite confirmarea recepționării și starea motorului; primul controler verifică primirea confirmării în intervalul stabilit; sistemul de supraveghere afișează comanda, confirmarea și starea procesului.

Comanda și confirmarea sunt informații diferite. Activarea variabilei de pornire în primul controler nu demonstrează că al doilea a recepționat-o și nici că motorul a pornit; al doilea poate refuza justificat comanda din cauza unui defect, a unei interblocări sau a modului local de funcționare. Dacă răspunsul nu este recepționat în cele 300 ms, primul controler generează o stare de depășire a timpului admis, care trebuie diferențiată de defectarea motorului, de refuzarea locală a comenzii, de indisponibilitatea controlerului, de pierderea legăturii de rețea și de asocierea greșită a variabilelor.

Semnalul periodic de prezenţă trebuie să îşi modifice valoarea într-un interval cunoscut. Păstrarea permanentă a valorii 1 nu demonstrează că legătura este activă, deoarece valoarea poate rămâne memorată după întreruperea comunicaţiei – eroare frecventă şi greu de observat, pentru că sistemul pare funcţional.

Testarea se realizează gradual: se verifică accesibilitatea celor două controlere; se transmite o singură variabilă; se confirmă asocierea corectă a datelor; se introduc comenzile şi stările; se adaugă confirmarea comenzii; se configurează semnalul periodic de prezenţă; se introduce supravegherea timpului maxim de răspuns; se simulează pierderea comunicaţiei; se verifică revenirea controlată după restabilirea legăturii.

Criterii de reuşită: deconectarea cablului trebuie semnalată în maximum 1,5 s, iar motorul trebuie să atingă starea sigură stabilită prin analiza de risc, independent de sistemele superioare. Refuzul prin interblocări impune afişarea simultană şi distinctă a comenzii transmise, confirmării recepţiei şi motivului refuzului. Validarea cere diferenţierea demonstrabilă între transmitere, recepţie, execuţie, defectul procesului şi pierderea comunicaţiei.

6.5.3. Monitorizarea comunicației într-un sistem SCADA

Al treilea exerciţiu utilizează schimbul anterior, dar mută accentul de la realizarea comunicaţiei la supravegherea ei. Sistemul SCADA trebuie să indice atât starea procesului, cât şi actualitatea datelor şi disponibilitatea fiecărei conexiuni.

Interfaţa de supraveghere prezintă starea comunicaţiei cu fiecare controler, comanda transmisă, confirmarea recepţionată, starea motorului sau a transportorului, defectele locale, semnalul periodic de prezenţă, depăşirea timpului maxim de răspuns, alarmele de comunicaţie şi jurnalul evenimentelor relevante.

Operatorul trebuie să poată diferenţia şase stări: motor oprit prin comandă; motor oprit din cauza unui defect; comandă transmisă, dar încă neconfirmată; comandă respinsă de logica locală; pierderea comunicaţiei cu unul dintre controlere; valoare veche, care nu mai este actualizată. Confuzia dintre ultimele două este cea mai periculoasă, pentru că prima este vizibilă, iar a doua nu.

Regula de marcare a actualităţii se stabileşte numeric: o valoare se consideră neactualizată dacă vechimea ei depăşeşte de trei ori perioada de actualizare configurată. Afişarea ultimei valori recepţionate fără indicarea vechimii sau a calităţii produce interpretări greşite; la pierderea comunicaţiei, valoarea nu trebuie prezentată ca informaţie curentă şi validă, ci marcată explicit.

În cadrul testării se simulează succesiv oprirea controlerului de execuţie, întreruperea legăturii de reţea, blocarea semnalului periodic de prezenţă, activarea unui defect local, transmiterea unei comenzi fără confirmare, refuzarea unei comenzi de către interblocări şi restabilirea comunicaţiei. Pentru fiecare situaţie se verifică

alarma generată, informaţia prezentată operatorului, marca temporală şi înregistrarea în jurnal.

Alarma de comunicaţie se separă de alarma de proces, deoarece cele două impun intervenţii diferite: prima solicită personalul de automatizare, a doua pe cel de producţie. Într-o instalaţie în care ambele apar sub aceeaşi denumire, timpul de intervenţie creşte fără ca vreo componentă tehnică să fie defectă.

Criterii de reuşită: pentru fiecare dintre cele şapte situaţii simulate (cele şase stări de mai sus şi restabilirea legăturii după întrerupere), interfaţa trebuie să prezinte o stare distinctă, iar jurnalul trebuie să conţină o înregistrare cu marcă temporală şi cauză. Exerciţiul nu repetă integrarea senzor–PLC–SCADA din capitolul 5; urmăreşte exclusiv capacitatea sistemului SCADA de a supraveghea comunicaţia, de a identifica datele neactualizate şi de a prezenta fără ambiguitate relaţia dintre comandă, confirmare şi stare.

6.5.4. Metoda comună de validare etapizată

Cele trei exerciţii folosesc tehnologii diferite, dar se verifică prin aceeaşi metodă: fluxul se împarte în segmente, iar fiecare segment se validează înaintea extinderii către următorul. Verificările sunt grupate în grila din Tabelul 6.10.

Tabelul 6.10 – Grilă generală pentru validarea comunicațiilor industriale și IIoT

Element verificat	**Întrebare de control**	**Dovadă necesară**
Sursa	Valoarea provine din echipamentul și variabila stabilite?	Valoarea poate fi observată direct la sursă
Asocierea datelor	Adresa, eticheta, identificatorul nodului sau subiectul sunt corecte?	Modificarea sursei produce actualizarea variabilei corespunzătoare
Formatul	Mesajul respectă structura și tipurile de date stabilite?	Mesajul poate fi interpretat automat, fără erori
Contextul	Sunt păstrate sursa, unitatea, calitatea și marca temporală?	Valoarea nu este ambiguă și poate fi corelată cu procesul
Actualitatea	Poate fi deosebită o valoare curentă de una neactualizată?	Pierderea actualizării este detectată în intervalul stabilit
Confirmarea	Recepționarea sau executarea unei comenzi este confirmată?	Comanda, confirmarea și starea procesului sunt observabile separat
Securitatea	Sunt verificate identitatea, drepturile și protecția conexiunii?	Accesul autorizat reușește, iar cel neautorizat este respins și înregistrat
Comportamentul la eroare	Sunt tratate întreruperea, mesajele invalide și depășirea timpului?	Sistemul trece într-o stare definită și generează informațiile necesare
Destinația	Datele ajung la aplicația care trebuie să le utilizeze?	Valoarea este recepționată, afișată sau stocată corect
Diagnosticarea	Poate fi localizat segmentul în care a apărut problema?	Verificările disting sursa, clientul, rețeaua, serverul și aplicația

Ordinea recomandată a verificărilor este: valoarea direct la sursă; accesul local la variabilă; asocierea și formatul datelor; conexiunea și parametrii protocolului; recepția la destinație; actualitatea și calitatea informației; întreruperile și situațiile de defect; mecanismele de securitate; documentarea rezultatelor.

Pentru fiecare exercițiu se păstrează configurația utilizată, lista variabilelor, parametrii comunicației, scenariile de test și rezultatele observate. Capturile de ecran pot documenta o etapă, dar nu înlocuiesc explicarea criteriului verificat și a comportamentului sistemului.

O comunicație se consideră validată numai dacă traseul complet este demonstrabil și dacă sistemul reacționează controlat atunci când o etapă devine indisponibilă. Integrarea acestor comunicații într-o arhitectură completă OPC UA–edge–MQTT–platformă este reluată în capitolul 7, unde accentul se mută de la verificarea protocolului la proiectarea întregului sistem.

6.6. Concluzii

Protocoalele de comunicație asigură circulația controlată a datelor, comenzilor, stărilor, alarmelor și informațiilor de diagnosticare între componentele unui sistem industrial. Alegerea lor nu poate fi separată de cerințele procesului, de poziția ocupată în arhitectură și de consecințele întreruperii comunicației.

În zona de control sunt prioritare predictibilitatea, disponibilitatea și respectarea termenelor temporale. Integrarea cu sistemele de supraveghere, bazele de date, aplicațiile MES și ERP sau serviciile cloud cere, în schimb, contextualizarea informației, distribuirea către mai mulți consumatori, securitatea și posibilitatea extinderii. Cele două seturi de cerințe nu pot fi satisfăcute de aceeași tehnologie, iar consecința arhitecturală este constantă în tot capitolul: controlul critic rămâne local și nu depinde de disponibilitatea unei conexiuni externe.

Protocoalele industriale clasice și tehnologiile IIoT nu se exclud. Modbus, PROFIBUS, PROFINET, EtherCAT și EtherNet/IP pot continua să asigure comunicația în zona OT, OPC UA furnizează acces structurat și contextualizat la informații, iar MQTT distribuie mesajele către aplicații independente. Gateway-ul industrial realizează legătura dintre aceste zone prin achiziție, validare, filtrare, contextualizare, conversie, stocare temporară și securizare – și devine, prin aceasta, atât punctul de integrare, cât și frontiera de încredere a instalației.

Coerența fluxului nu rezultă din utilizarea unui singur protocol, ci din definirea clară a rolului fiecărei tehnologii pe fiecare segment. Departajarea se face prin cerințe măsurabile, nu prin comparații generale: capitolul a arătat că aceleași întrebări – cât durează, cât ocupă, ce se întâmplă la întrerupere – au răspunsuri calculabile. Bugetul de latență descompune timpul total pe segmente și indică termenul asupra căruia intervenția are efect; calculul de bandă arată că, pentru mesaje industriale scurte, cea mai mare parte a traficului transportă antete, iar gruparea

mesajelor reduce volumul de câteva ori fără pierdere de informaţie; dimensionarea unei linii seriale sau a unei reţele cu perioade de actualizare stabilite arbitrar scoate la iveală limite pe care nicio schimbare de protocol nu le compensează.

Fiecare segment al traseului oferă garanţii limitate, iar acestea nu se propagă. Recepţionarea unei valori prin OPC UA nu demonstrează publicarea ei prin MQTT, confirmarea publicării către broker nu garantează stocarea în baza de date, iar livrarea exact o dată la nivelul protocolului nu înseamnă executarea o singură dată a operaţiei industriale. Validarea se face cap-coadă şi urmăreşte simultan valoarea, sursa, unitatea de măsură, marca temporală, calitatea şi actualitatea datelor; o comunicaţie în care valoarea circulă, dar contextul se pierde la prima conversie, este o comunicaţie nevalidată.

Securitatea se aplică la fiecare frontieră unde o stivă se încheie şi alta începe. Autentificarea, autorizarea, criptarea, administrarea certificatelor, limitarea drepturilor şi jurnalizarea se configurează separat pentru zona industrială, pentru gateway, pentru broker şi pentru aplicaţiile consumatoare. Încapsularea unui protocol nesecurizat într-o conexiune protejată rezolvă un singur segment şi nu elimină vulnerabilităţile echipamentului sau ale reţelei locale.

Comenzile venite din exterior rămân solicitări. Automatul programabil verifică identitatea sursei, modul de funcţionare, interblocările, limitele tehnologice şi funcţiile de siguranţă înainte de a executa, iar pierderea sau compromiterea canalului IIoT nu anulează logica locală de protecţie. Determinismul comunicaţiei nu certifică, la rândul lui, o funcţie de siguranţă: aceasta se realizează prin componente şi profiluri dedicate, potrivit analizei de risc.

Protocoalele sunt, prin urmare, decizii de arhitectură. Ele influenţează performanţa, disponibilitatea, securitatea, interoperabilitatea şi posibilitatea de diagnosticare a întregului sistem, iar efectele lor se resimt pe toată durata de exploatare a instalaţiei, mult după momentul în care alegerea pare o simplă opţiune tehnică.

Până aici, fiecare protocol a fost analizat pentru segmentul pe care îl deserveşte. Capitolul următor schimbă unitatea de analiză: dispozitivele, controlerele, sistemele SCADA, gateway-urile industriale, protocoalele şi aplicaţiile superioare sunt integrate într-o arhitectură IIoT completă, în care se stabilesc rolurile componentelor, traseele datelor, responsabilităţile de prelucrare şi limitele dintre controlul operaţional şi aplicaţiile informatice.

6.7. Întrebări de verificare

1. *Ce înseamnă determinismul într-o comunicație industrială?*

a) utilizarea exclusivă a protocoalelor bazate pe Ethernet;
b) transmiterea fiecărui mesaj cu cea mai mică latență posibilă, indiferent de variație;
c) existența unei limite superioare cunoscute a timpului de transmisie și a variației acestuia, nu simpla viteză ridicată;
d) viteza maximă de transmisie a rețelei, exprimată în Mbit/s.

2. *O buclă de reglare a temperaturii are constanta de timp dominantă de 30 s. Conform regulii perioadei de eșantionare (de 5–10 ori mai mică decât constanta de timp), ce se poate spune?*

a) este necesară o perioadă de 30 s, egală cu constanta de timp;
b) este necesară o perioadă sub 1 ms, deci o rețea izocronă;
c) perioada de eșantionare nu are legătură cu dinamica procesului;
d) o perioadă de aproximativ 3 s este suficientă, iar o rețea izocronă nu aduce niciun beneficiu pentru această buclă.

3. *Un cadru CAN standard cu opt octeți de date ocupă 111–135 de biți. Cât durează transmisia proprie a cadrului la 500 kbit/s?*

a) între aproximativ 0,22 și 0,27 ms, dar aceasta este durata proprie a cadrului, nu timpul de răspuns;
b) aproximativ 111 ms, egală cu numărul de biți;
c) între aproximativ 22 și 27 ms;
d) aproximativ 0,5 ms, indiferent de numărul de biți.

4. *Ce lipsește protocolului Modbus de bază și ce soluție există pentru implementările compatibile?*

a) autentificarea și confidențialitatea; Modbus Security încapsulează mesajele în TLS, cu certificate X.509v3 pentru autentificare reciprocă;
b) compatibilitatea cu echipamentele existente; soluția este înlocuirea completă a rețelei;
c) determinismul; soluția este un cadru Ethernet cu prelucrare în trecere;
d) modelul de date; soluția este spațiul de adrese OPC UA în fiecare registru.

5. *Care este diferența dintre mesajele explicite și cele implicite în EtherNet/IP?*

a) nu există nicio diferență; termenii desemnează același tip de mesaj;
b) mesajele explicite transportă date ciclice prin UDP, iar cele implicite transportă comenzi de configurare prin TCP;
c) mesajele implicite conțin descrierea completă a serviciului, iar cele explicite conțin numai date;
d) mesajele explicite servesc configurării, diagnosticării și operațiilor cerere–răspuns (de regulă prin TCP); cele implicite transportă periodic date de intrare și ieșire, cu semnificația stabilită la deschiderea conexiunii (de regulă prin UDP).

6. *Care este raportul corect dintre OPC UA și MQTT într-o arhitectură IIoT?*

a) OPC UA înlocuiește MQTT, deoarece este potrivit pentru închiderea buclelor de control rapide;
b) sunt alternative echivalente și trebuie alese una în locul celeilalte;
c) sunt complementare: OPC UA asigură accesul structurat și contextualizat la informații, iar MQTT distribuie eficient mesajele între sisteme separate, de exemplu prin gateway și broker;
d) MQTT înlocuiește OPC UA, deoarece transportă implicit codul de stare și modelul informațional.

7. *Ce informații însoțesc o valoare în OPC UA, astfel încât o temperatură de 45 °C cu stare necorespunzătoare să nu fie echivalentă cu o măsurare validă de 45 °C?*

a) numai adresa IP a clientului și portul de conectare;
b) un cod de stare (bună, incertă sau necorespunzătoare), marca temporală a sursei și marca temporală atribuită de server;
c) numai unitatea de măsură și numele producătorului;
d) numai numărul de ordine al mesajului și nivelul QoS.

8. *Ce garantează nivelul 1 al calității serviciului (QoS 1) în MQTT?*

a) livrarea garantată în mai puțin de o milisecundă;
b) livrarea mesajului cel puțin o dată, astfel încât pot apărea duplicate;
c) livrarea mesajului exact o dată, inclusiv execuția operației industriale;
d) livrarea mesajului cel mult o dată, fără confirmare.

9. *Ce adaugă Sparkplug peste transportul MQTT?*

a) un model client–server cu abonamente la noduri;
b) criptarea implicită a tuturor mesajelor, fără configurarea TLS;
c) o ierarhie standardizată a subiectelor, o reprezentare comună a variabilelor și mecanisme de gestionare a stării (mesaje de naștere și de deces, numerotare secvențială);
d) determinismul necesar închiderii buclelor de reglare.

10. *De ce este așezată clasa traficului (dat, evt, cmd, sts, cfg) înaintea mărimii în structura subiectelor MQTT?*

a) pentru ca brokerul să poată cripta subiectele automat;
b) pentru a reduce dimensiunea payloadului la câțiva octeți;
c) pentru că standardul MQTT impune această ordine a nivelurilor;
d) pentru ca drepturile de acces să poată fi formulate prin prefix, singurul mod practic de a administra un broker cu sute de clienți.

7. ARHITECTURA ȘI INTEGRAREA UNUI SISTEM IIOT COMPLET

Capitolele anterioare au prezentat, pe rând, procesele industriale şi tipurile de producţie, sistemele flexibile de fabricaţie, dispozitivele de măsurare şi automatizare, sistemele de supraveghere şi protocoalele de comunicaţie industrială. Fiecare element a fost tratat prin funcţia proprie şi prin condiţiile în care aceasta poate fi îndeplinită corect. Capitolul de faţă schimbă perspectiva: componentele nu mai sunt privite separat, ci ca părţi ale unui sistem în care trebuie stabilite rolurile, traseele datelor, locul în care este executată fiecare prelucrare şi limitele dintre controlul operaţional şi aplicaţiile informatice.

Diferenţa dintre o instalaţie conectată şi un sistem IIoT proiectat constă tocmai în aceste decizii. Conectarea unui echipament la o reţea produce date; arhitectura stabileşte dacă acele date sunt interpretabile, dacă ajung la sistemul care are nevoie de ele, dacă pot fi corelate cu produsul şi cu ordinul de producţie şi, mai ales, ce se întâmplă cu procesul atunci când o legătură sau o aplicaţie devine indisponibilă. O arhitectură definită corect răspunde la aceste întrebări înaintea implementării, nu după apariţia primei defecţiuni.

Capitolul dezvoltă cinci direcţii. Secţiunea 7.1 defineşte arhitectura stratificată pe baza piramidei CIM şi a modelului ISA-95, standardizat prin IEC 62264 [75], poziţionând componentele din Capitolele 5 şi 6. Secţiunea 7.2 analizează integrarea SCADA–MES–ERP, transformarea informaţiei şi cerinţele interfeţelor. Secţiunea 7.3 compară arhitecturile centralizate, distribuite şi hibride, stabileşte repartizarea funcţiilor între controler, edge, infrastructura fabricii şi cloud şi tratează geamănul digital. Secţiunea 7.4 prezintă lanţul funcţional al platformelor industriale, independent de produse comerciale. Secţiunea 7.5 propune proiectarea integrală a arhitecturii unei linii automatizate de ambalare.

O regulă traversează întregul capitol: funcţiile care influenţează direct siguranţa şi desfăşurarea procesului rămân locale. Nivelurile superioare furnizează ordine, reţete, parametri şi rezultate analitice, însă aplicarea lor este validată de logica din controler. Platforma extinde capacitatea de observare şi de analiză a fabricii, fără să devină o condiţie a funcţionării sigure.

Utilitatea capitolului este dublă. Cititorului cu formaţie tehnică îi oferă instrumentul prin care componentele deja cunoscute pot fi asamblate într-un sistem verificabil şi prin care fiecare interfaţă poate fi specificată complet. Cititorului cu responsabilităţi de conducere îi arată ce decizii de arhitectură determină costul, disponibilitatea şi posibilitatea de extindere a unei investiţii în digitalizare.

Arhitectura construită aici devine referința pentru restul cărții. Capitolul 8 o reia pentru analiza segmentării rețelei, a identității, a protejării comunicațiilor și a monitorizării evenimentelor, iar Capitolul 9 o transpune în mini-proiecte implementabile.

Capitolul presupune parcurse Capitolele 2, 3, 5 și 6. Din Capitolul 2 sunt reluate funcțiile companiei industriale și parcursul unei comenzi; din Capitolul 3, tipurile de producție și consecințele lor asupra cerințelor de date; din Capitolul 5, senzorii, actuatoarele, automatele programabile, sistemele HMI și SCADA, împreună cu elementele fără de care o valoare măsurată nu este interpretabilă – identificatorul sursei, unitatea de măsură, marca temporală și indicatorul de calitate; din Capitolul 6, protocoalele OPC UA și MQTT, modelul publicare–abonare, determinismul comunicației și criteriile de alegere a protocolului. Cititorul care urmează traseul de conducere poate parcurge secțiunile 7.1, 7.2 și 7.3 și poate trata secțiunile 7.4 și 7.5 ca material de referință. Traseul tehnic și traseul de proiectare parcurg integral capitolul; în plus, secțiunea 7.5 presupune disponibilitatea stivei tehnologice declarate în secțiunea 7.5.3, iar exercițiul poate fi refăcut integral numai cu aceasta.

Obiectivele capitolului

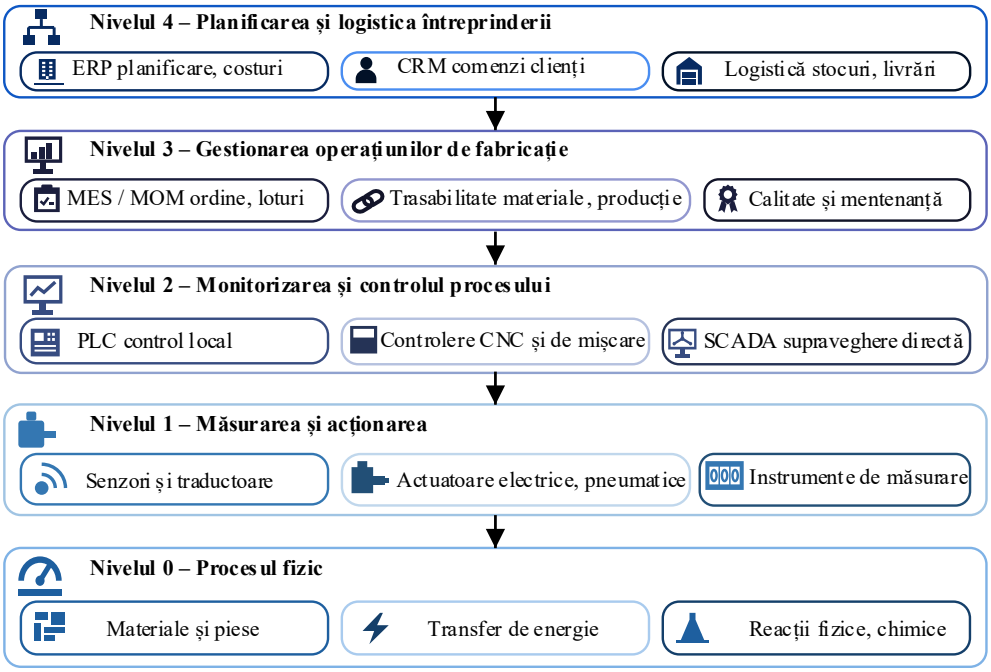
La finalul acestui capitol, cititorul va putea:

- să reprezinte arhitectura stratificată a unui sistem IIoT și să încadreze senzorii, actuatoarele, automatele programabile, sistemele HMI și SCADA, gateway-ul industrial, sistemele MES și ERP și platformele IIoT în nivelurile funcționale corespunzătoare;
- să delimiteze responsabilitățile sistemelor SCADA, MES și ERP, să descrie fluxurile bidirecționale dintre ele și să specifice elementele obligatorii ale unei interfețe de integrare;
- să compare arhitecturile centralizate, distribuite și hibride și să argumenteze alegerea uneia dintre ele pentru un proces industrial dat;
- să distribuie funcțiile pe continuumul *edge–fog–cloud* pe baza unor criterii verificabile: timp de răspuns, criticitate operațională, volum de date, confidențialitate și continuitate a funcționării;
- să calculeze bugetul de latență al unui lanț de achiziție, necesarul de lățime de bandă pentru un set dat de semnale și eficacitatea globală a echipamentelor, interpretând atât rezultatele, cât și limitele acestora;
- să explice rolul geamănului digital și să argumenteze de ce un rezultat obținut în model nu poate fi aplicat direct asupra echipamentului fizic;
- să descrie lanțul funcțional al unei platforme IIoT și să proiecteze traseul complet al datelor, inclusiv comportamentul sistemului la întreruperea comunicației;
- să proiecteze și să valideze etapizat o arhitectură IIoT pentru o linie de ambalare complet automatizată.

7.1. Componentele unei arhitecturi IIoT

O arhitectură IIoT reunește procesul fizic, echipamentele de automatizare, sistemele de supraveghere, aplicațiile de gestionare a producției și infrastructura informatică a întreprinderii. Organizarea pe niveluri permite delimitarea responsabilităților și stabilirea interfețelor prin care sunt transferate datele, comenzile, stările și informațiile de diagnosticare.

Structura stratificată nu trebuie interpretată ca o succesiune rigidă de echipamente prin care trebuie să treacă fiecare valoare. Nivelurile reprezintă domenii funcționale. Într-o implementare concretă, aceeași aplicație poate îndeplini funcții asociate mai multor niveluri, iar unele componente – gateway-ul industrial, platformele IIoT și serviciile de calcul în cloud – pot traversa limitele modelului. Corelarea dintre niveluri și componentele uzuale ale unei instalații este sintetizată în Tabelul 7.1, la finalul secțiunii 7.1.3; ierarhia nivelurilor este reprezentată în Figura 7.1.



** Nivelurile reprezintă domenii funcționale , nu o succesiune rigidă de echipamente prin care trebuie să treacă fiecare valoare.*

Figura 7.1 – Piramida ISA-95 — cele 5 niveluri

7.1.1. Modelul funcțional de referință

Piramida CIM oferă o reprezentare ierarhică a fabricației integrate prin calculator, de la echipamentele care interacționează cu procesul până la aplicațiile pentru planificarea și conducerea întreprinderii [1]. Modelul provine din arhitectura de referință elaborată la Universitatea Purdue, care descrie întreprinderea pe mai

multe straturi şi include, alături de sistemele informatice şi de control, componenta umană şi cea de fabricaţie propriu-zisă [192]. Reprezentarea permite asocierea senzorilor şi actuatoarelor cu nivelul de câmp, a controlerelor cu nivelul de comandă, a sistemelor SCADA cu supravegherea, a sistemelor MES cu gestionarea producţiei şi a sistemelor ERP cu planificarea resurselor.

Pentru definirea mai precisă a funcţiilor şi a schimburilor informaţionale este utilizat modelul ISA-95, standardizat internaţional prin seria IEC 62264. Modelul defineşte cinci niveluri, numerotate de la 0 la 4, şi acordă o atenţie deosebită domeniului de gestionare a operaţiunilor de fabricaţie şi interfeţei dintre nivelul operaţional şi cel al întreprinderii [75], [49]. Partea a treia a seriei detaliază activităţile din acest domeniu şi le poziţionează explicit între funcţiile de planificare şi logistică, atribuite nivelului 4, şi funcţiile de control al procesului, atribuite nivelului 2 [87]. Utilitatea practică a delimitării este că ea nu descrie echipamente, ci activităţi: aceeaşi activitate poate fi executată de produse diferite, iar încadrarea rămâne valabilă.

Piramida CIM şi modelul ISA-95 sunt complementare, dar nivelurile lor nu trebuie echivalate numai pe baza poziţiei grafice. CIM evidenţiază integrarea tehnologică a fabricaţiei, în timp ce ISA-95 defineşte domenii de activitate şi schimburi informaţionale. Corelarea trebuie realizată în funcţie de rolul efectiv al fiecărei componente, nu după eticheta comercială a produsului.

Modelul ierarhic nu este singura reprezentare disponibilă. Modelul de referinţă RAMI 4.0 descrie soluţia industrială într-un spaţiu tridimensional, format din straturile funcţionale ale activului, ciclul său de viaţă şi ierarhia din instalaţie, ceea ce permite tratarea unitară a obiectelor fizice şi a reprezentărilor lor informaţionale [6], [7]; reprezentarea informaţională a activului a fost ulterior standardizată separat, sub forma structurii de administrare a activului [120]. Arhitectura de referinţă a internetului industrial organizează sistemul pe puncte de vedere – de afaceri, de utilizare, funcţional şi de implementare – şi distinge cinci domenii funcţionale: control, operaţiuni, informaţie, aplicaţie şi afaceri [27]. O a patra referinţă, cu domeniu mai larg decât fabricaţia, este arhitectura de referinţă pentru internetul lucrurilor, care descrie sistemul prin puncte de vedere şi entităţi funcţionale independente de sectorul de aplicare [193].

Cele patru modele nu se exclud. ISA-95 răspunde cel mai direct întrebării „ce funcţie se execută unde şi ce informaţii se schimbă între niveluri", motiv pentru care este utilizat ca model de lucru în această carte. RAMI 4.0 este util atunci când discuţia vizează reprezentarea digitală a activului pe durata ciclului de viaţă, arhitectura de referinţă a internetului industrial este utilă atunci când trebuie separate preocupările părţilor interesate înaintea proiectării tehnice, iar arhitectura de referinţă pentru internetul lucrurilor oferă vocabularul comun atunci când soluţia industrială trebuie corelată cu sisteme din afara fabricii. Alegerea unui model de referinţă nu este o formalitate documentară: modelul stabileşte vocabularul comun cu care echipa de automatizări, echipa IT şi furnizorii descriu aceeaşi instalaţie.

Absența unui model asumat nu elimină problema, ci o mută în faza de recepție, unde fiecare participant descrie instalația în termenii produsului pe care îl livrează.

7.1.2. Nivelurile procesului, câmpului și controlului

Nivelul 0 – procesul fizic, reprezintă procesul industrial propriu-zis: deplasarea materialelor, prelucrarea pieselor, transferul energiei, reacțiile fizice sau chimice și transformările prin care sunt realizate produsele. Într-o linie de ambalare, acest nivel include transportul produselor, umplerea recipientelor, sigilarea și etichetarea. Într-o celulă robotizată, include manipularea pieselor, prelucrarea și asamblarea.

Procesul fizic nu este un sistem informatic, dar constituie sursa și destinația finală a datelor și comenzilor. Temperatura, presiunea, poziția, viteza, debitul, forța și prezența unei piese sunt mărimi ale procesului care trebuie observate sau modificate.

Nivelul 1 – măsurarea și acționarea cuprinde componentele care detectează starea procesului și acționează asupra acestuia: senzori și traductoare, instrumente de măsurare, dispozitive inteligente de câmp, actuatoare electrice, pneumatice și hidraulice, valve și elemente de reglare, convertizoare de frecvență și sisteme de acționare, module de intrări și ieșiri distribuite.

Senzorii transformă mărimile fizice în semnale utilizabile de sistemul de control, iar actuatoarele convertesc comenzile în deplasare, forță, debit, temperatură sau alte efecte asupra procesului. Unele dispozitive inteligente realizează suplimentar filtrare, compensare, diagnosticare și comunicație digitală; principiile de măsurare și standardele de semnal au fost tratate în secțiunile 5.1 și 5.2.

Datele de la acest nivel trebuie asociate cu informațiile care permit interpretarea lor: identificatorul sursei, tipul mărimii, unitatea de măsură, domeniul de valori, calitatea și marca temporală. Cerința nu este o convenție locală: modelele de informație utilizate pentru expunerea structurată a datelor de proces asociază explicit fiecărei variabile un identificator de nod, un tip de dată, atribute descriptive și o valoare însoțită de marcă temporală și de indicator de calitate [127]. O valoare numerică transmisă fără aceste elemente poate deveni ambiguă la nivelurile superioare, iar ambiguitatea nu se corectează ulterior, în platformă: contextul pierdut la sursă nu mai poate fi reconstituit cu certitudine.

Nivelul 2 – monitorizarea și controlul procesului, include componentele care execută logica de automatizare și mențin procesul în limitele stabilite: automate programabile, controlere de mișcare, controlere pentru roboți, sisteme DCS, controlere CNC, RTU-uri, sisteme de siguranță, interfețe HMI locale și componentele SCADA asociate supravegherii directe. Delimitarea dintre aceste familii de echipamente este funcțională, nu tehnologică: aceleași cerințe de disponibilitate și de răspuns predictibil au condus la soluții diferite în industria de proces, în fabricația discretă și în infrastructurile distribuite geografic [153].

Controlerele citesc intrările, execută algoritmii și secvențele programate – realizate în limbajele definite de IEC 61131-3, verifică interblocările și transmit comenzile către actuatoare. Ediția în vigoare a standardului menține textul structurat, diagrama cu contacte, diagrama blocurilor funcționale și diagrama funcțională secvențială și renunță la lista de instrucțiuni, declarată învechită încă din ediția anterioară [123]; cerințele privind echipamentul pe care rulează aceste programe fac obiectul unei părți distincte a seriei [152]. Tot aici sunt gestionate funcțiile care necesită răspuns predictibil: reglarea, sincronizarea mișcărilor, oprirea controlată și protecția procesului.

Controlul critic trebuie să rămână local. O buclă de reglare, o interblocare sau o funcție de siguranță nu trebuie să depindă de disponibilitatea unei baze de date externe, a unei platforme IIoT sau a unei conexiuni la internet. Cerința nu este o precauție de proiectare, ci o consecință a modului în care sunt tratate sistemele de control industrial: acestea sunt supuse unor constrângeri de disponibilitate, de timp de răspuns și de consecință fizică a defectării, diferite de cele ale sistemelor informatice de birou [25]. Funcțiile de siguranță fac obiectul unor sisteme dedicate, proiectate și validate conform cerințelor pentru siguranța funcțională [44] și, în cazul echipamentelor de lucru, conform standardelor sectoriale care stabilesc nivelurile de performanță și de integritate cerute părților de comandă relevante pentru siguranță [45], [142]. Aceste funcții nu pot fi preluate de aplicații de monitorizare. Nivelurile superioare pot furniza valori de referință, rețete și ordine, dar aplicarea acestora este verificată de logica locală.

Sistemele HMI și SCADA pot ocupa poziții diferite în funcție de întinderea lor. O interfață HMI conectată direct la un automat programabil aparține nivelului de control. Un sistem SCADA care supraveghează mai multe linii, gestionează alarme la nivelul fabricii și transmite informații către sistemul MES poate îndeplini și funcții asociate nivelului 3. Încadrarea trebuie realizată după funcție, nu după denumirea produsului.

7.1.3. Nivelurile operațiunilor de fabricație și întreprinderii

Nivelul 3 – gestionarea operațiunilor de fabricație, coordonează activitățile prin care planul de producție este transformat în operații executabile. Acesta poate include sisteme MES sau MOM, sisteme SCADA la nivelul fabricii, baze de date istorice, aplicații pentru gestionarea calității și a mentenanței, sisteme pentru urmărirea materialelor și a producției și servicii pentru calcularea indicatorilor operaționali.

Standardul organizează acest domeniu într-un model de activități recurente: administrarea definițiilor de producție, administrarea resurselor, programarea detaliată, lansarea lucrărilor, execuția, colectarea datelor, urmărirea producției și analiza performanței [87]. Modelul este util în practică pentru că oferă un criteriu de delimitare: dacă o funcție aparține uneia dintre aceste activități, ea nu trebuie implementată nici în automatul programabil, nici în ERP.

Aici sunt gestionate ordinele de producţie, loturile, reţetele, resursele, trasabilitatea, genealogia produsului, cantităţile şi abaterile de la plan. Datele de control arată ce s-a produs, pe ce echipament, cu ce materiale, în ce condiţii şi cu ce rezultat al verificării calităţii. Tot aici se calculează indicatorii operaţionali conform ISO 22400 [50], [51], detaliaţi în secţiunea 7.2.3.

Nivelul 3 nu trebuie să preia funcţiile temporale ale controlerelor. Sistemul MES poate transmite o operaţie sau o reţetă, însă automatul programabil verifică starea instalaţiei şi decide momentul în care comanda poate fi executată în siguranţă.

Nivelul 4 – planificarea şi logistica întreprinderii, cuprinde activităţile de planificare şi gestionare a întreprinderii. Sistemele reprezentative sunt ERP, CRM, aplicaţiile pentru aprovizionare şi logistică, sistemele pentru gestiunea stocurilor, aplicaţiile financiare şi comerciale şi instrumentele de planificare a resurselor şi capacităţilor.

La acest nivel sunt gestionate comenzile clienţilor, necesarul de materiale, planurile generale de producţie, costurile, livrările şi relaţiile cu furnizorii. Datele au o granularitate diferită de cea utilizată în control: un automat programabil lucrează cu stări şi valori actualizate în intervale scurte, în timp ce sistemul ERP utilizează comenzi, cantităţi, termene, stocuri și costuri [78].

Tabelul 7.1 – Corelarea nivelurilor ISA-95 cu principalele componente ale arhitecturii IIoT

Nivel	Domeniu funcțional	Componente reprezentative	Responsabilitate dominantă	Informații caracteristice
0	Proces fizic	mașini, instalații, materiale, produse	realizarea transformării fizice	temperatură, poziție, debit, mișcare, stare fizică
1	Măsurare și acționare	senzori, traductoare, actuatoare, sisteme de acționare, intrări și ieșiri distribuite	observarea și modificarea procesului	semnale, valori măsurate, comenzi de acționare, diagnosticare
2	Monitorizare și control	PLC, DCS, CNC, controlere robotice, RTU, HMI local, sisteme de siguranță	controlul local, interblocarea și supravegherea procesului	stări, comenzi, valori de referință, alarme, confirmări
3	Operațiuni de fabricație	MES/MOM, SCADA la nivelul fabricii, baze de date istorice, aplicații pentru calitate și mentenanță	coordonarea și urmărirea execuției producției	ordine de lucru, loturi, rețete, cantități, trasabilitate, indicatori
4	Planificare și logistică	ERP, CRM, aplicații logistice și financiare	planificarea și gestionarea resurselor întreprinderii	comenzi clienți, planuri, stocuri, costuri, termene și livrări

Legătura dintre nivelurile 3 şi 4 trebuie să transforme cerinţele comerciale în instrucţiuni operaţionale şi să returneze rezultatele reale ale execuției. Seria IEC 62264 defineşte pentru această legătură un set de tranzacţii tipice – cereri, confirmări, notificări şi răspunsuri asociate schimbului de informaţii între cele două niveluri – care pot fi utilizate ca punct de plecare la specificarea interfeţei [194]. Interconectarea este dezvoltată în secţiunea 7.2, iar corespondenţa dintre cele cinci

niveluri şi componentele uzuale ale unei instalaţii industriale este prezentată în Tabelul 7.1. Ierarhia celor cinci niveluri este reprezentată în Figura 7.1.

7.1.4. Determinismul şi comunicarea în timp real

Un sistem de control nu are nevoie de comunicaţie rapidă, ci de comunicaţie predictibilă. Determinismul înseamnă că timpul de livrare a unui mesaj se încadrează într-o limită superioară cunoscută şi că variaţia acestui timp, numită fluctuaţie (jitter), rămâne suficient de mică pentru ca aplicaţia să funcţioneze corect [195]. O reţea care transmite de obicei în 2 ms, dar ocazional în 400 ms, este rapidă şi nedeterministă; pentru o buclă de reglare, a doua caracteristică o anulează pe prima.

Cerinţele nu sunt identice în toată instalaţia. Literatura de specialitate şi practica industrială disting trei clase de exigenţă: controlul mişcării, în care ciclurile coboară sub o milisecundă şi fluctuaţia admisă este de ordinul microsecundelor; automatizarea de fabricaţie, cu cerinţe uzuale de ordinul milisecundelor; supravegherea proceselor lente şi monitorizarea, unde întârzieri de sute de milisecunde sunt acceptabile [26], [196]. Standardele pentru reţelele industriale bazate pe Ethernet formalizează această diferenţiere printr-un set de indicatori de performanţă – timpul de livrare, numărul de staţii, topologia şi comportamentul la pierderea unui cadru – care permit compararea profilurilor de comunicaţie pe criterii verificabile, nu prin declaraţii comerciale de tipul „timp real” [24].

Pentru a putea corela evenimentele provenite de la componente diferite este necesară şi o referinţă de timp comună. Sincronizarea la nivelul echipamentelor de automatizare se realizează prin protocoale dedicate, care distribuie timpul cu precizie ridicată în reţeaua locală [35], în timp ce nivelurile superioare pot utiliza mecanisme de sincronizare mai puţin precise [157]. Diferenţa are consecinţe practice: două valori marcate temporal de surse nesincronizate pot apărea în ordine inversată faţă de succesiunea reală din proces, iar o analiză construită pe această ordonare va fi greşită indiferent de calitatea algoritmului.

Convergenţa dintre traficul determinist şi traficul obişnuit pe aceeaşi infrastructură este tratată prin mecanismele de reţea cu sensibilitate temporală, iar profilul dedicat automatizărilor industriale selectează dintre acestea funcţiile, opţiunile şi procedurile aplicabile echipamentelor de câmp, punţilor şi reţelelor locale industriale [197]. Existenţa acestor mecanisme nu transformă însă întregul lanţ IIoT într-unul determinist: garanţiile se opresc la limita reţelei administrate. Segmentul care traversează internetul, brokerul MQTT (MQTT broker) şi serviciile cloud nu oferă limite superioare garantate şi nu pot fi incluse într-o buclă de control.

Bugetul de latenţă al unui lanţ IIoT – exemplu de calcul

Un buget de latenţă descompune întârzierea totală pe segmente şi arată unde se consumă efectiv timpul. Exemplul următor este un scenariu didactic: valorile sunt

orientative şi servesc demonstrării metodei, nu caracterizării unui echipament anume.

Date şi ipoteze – se consideră lanţul senzor, automat programabil, gateway industrial, broker MQTT, bază de date, pentru semnalul de detectare a unui produs neconform pe o linie de ambalare. Ciclul programului din automatul programabil este T_{ciclu} = 10 ms, iar imaginea intrărilor este actualizată la începutul ciclului. Serverul OPC UA publică variabila la un interval de publicare Tpub = 100 ms. Gateway-ul transmite fiecare mesaj individual, fără fereastră de agregare. Legătura cu platforma este o conexiune securizată prin TLS [189], cu timp de propagare dus de aproximativ 15 ms. Toate valorile sunt exprimate în milisecunde şi reprezintă cazul cel mai defavorabil pe fiecare segment.

Formula:

$$\boldsymbol{T_{total} = t_{senzor} + t_{PLC} + t_{OPC} + t_{gateway} + t_{reţea} + t_{broker} + t_{BD}}$$

Înlocuirea numerică:

- t_{senzor} – timpul de răspuns al senzorului şi filtrarea modulului de intrare: 2 ms
- t_{PLC} – în cazul cel mai defavorabil, tranziţia apare imediat după actualizarea imaginii intrărilor şi este preluată la ciclul următor, deci 2 × T_{ciclu}: 20 ms
- t_{OPC} – aşteptarea până la următoarea publicare, în cazul cel mai defavorabil T_{pub}: 100 ms
- $t_{gateway}$ – validare, contextualizare şi serializarea mesajului: 5 ms
- $t_{reţea}$ – transmiterea prin conexiunea securizată: 15 ms
- t_{broker} – recepţia, evaluarea regulii de rutare şi direcţionarea: 30 ms
- t_{BD} – scrierea şi indexarea în baza de date pentru serii temporale: 20 ms

T_{total} = 2 + 20 + 100 + 5 + 15 + 30 + 20 = 192 ms

Interpretarea – datele ajung în baza de date în cel mult aproximativ 0,2 secunde de la apariţia evenimentului în proces. Distribuţia contează mai mult decât suma: intervalul de publicare OPC UA reprezintă singur peste jumătate din buget, în timp ce segmentul de reţea, adesea suspectat primul, contribuie cu mai puţin de 8 %. Într-un asemenea caz, negocierea unei legături mai rapide cu furnizorul de internet nu ar produce o îmbunătăţire perceptibilă, în timp ce reducerea intervalului de publicare de la 100 ms la 20 ms ar scurta bugetul cu circa 40 %. Dacă tabloul de bord se reîmprospătează la 5 secunde, întârzierea percepută de operator este dominată de acest ultim interval, iar optimizarea segmentelor anterioare devine irelevantă pentru el.

Bugetul arată şi ce nu poate fi făcut. Respingerea fizică a unui produs neconform, care trebuie executată în mai puţin de 10 ms la viteza liniei, nu poate fi plasată nici măcar imediat după automatul programabil: numai segmentele t_{senzor} şi t_{PLC} însumează 22 ms în cazul cel mai defavorabil. Soluţia aparţine nivelului de control – reducerea timpului de ciclu, utilizarea unei intrări rapide sau a unui modul specializat, nu arhitecturii IIoT. Aceasta este utilizarea corectă a bugetului de latenţă: nu

de a optimiza lanţul de date, ci de a stabili înaintea proiectării ce funcţii pot fi plasate pe el.

Limitele calculului – bugetul însumează valori de caz defavorabil care nu apar, de regulă, simultan; latenţa medie observată va fi sensibil mai mică. Nu sunt incluse retransmisiile, reconectarea cu renegocierea sesiunii securizate, acumularea mesajelor în coadă la încărcare mare şi nici întârzierile introduse de o eventuală fereastră de agregare la nivelul gateway-ului. Valorile trebuie confirmate prin măsurare în instalaţia reală; un buget nemăsurat este o ipoteză de proiectare, nu un rezultat.

7.1.5. Componentele transversale ale arhitecturii

Gateway-ul industrial, infrastructura de procesare la edge şi platformele IIoT nu corespund unui singur nivel ISA-95. Acestea trebuie poziţionate în funcţie de rol, de locul instalării şi de datele la care au acces. Arhitecturile de referinţă pentru internetul industrial tratează explicit această situaţie, organizând sistemul pe niveluri de implementare – echipamentele din apropierea procesului, platforma şi aplicaţiile întreprinderii – care se suprapun peste, dar nu se confundă cu, nivelurile funcţionale [27].

Gateway-ul industrial – realizează legătura controlată dintre echipamente, reţele şi aplicaţii care utilizează protocoale sau modele de date diferite. Funcţiile sale pot include achiziţia datelor din automatul programabil, din SCADA sau din dispozitivele de câmp, conversia protocoalelor, asocierea adreselor tehnice cu identificatori semnificativi, validarea tipurilor şi a domeniilor de valori, filtrarea şi agregarea, adăugarea contextului şi a mărcilor temporale, stocarea temporară la întreruperea conexiunii, precum şi autentificarea şi protejarea comunicaţiei cu sistemele externe.

Gateway-ul nu trebuie tratat ca un simplu convertor. Acesta constituie o frontieră funcţională şi, simultan, o frontieră de încredere: aici se stabilesc sursele permise, operaţiile autorizate, frecvenţele de transfer şi comportamentul la pierderea comunicaţiei. Standardele pentru securitatea sistemelor de automatizare industrială tratează explicit acest tip de componentă prin cerinţe privind identificarea, autentificarea, controlul utilizării şi integritatea datelor [156]. Consecinţele de securitate ale poziţiei sale – segmentarea reţelei, DMZ industrial , controlul identităţii şi al accesului – sunt tratate în Capitolul 8.

Procesarea edge – componentele de procesare la edge execută funcţii în apropierea procesului. Acestea pot elimina valorile nerelevante, calcula indicatori, detecta abateri, comprima serii temporale şi păstra local datele până la restabilirea conexiunii. Motivaţia nu este doar tehnică: apropierea prelucrării de sursa datelor răspunde simultan problemelor de latenţă, de volum transmis şi de confidenţialitate, care nu pot fi rezolvate prin creşterea capacităţii de calcul centralizate [111].

Decizia de a executa o funcţie la edge nu depinde numai de performanţa echipamentului. Trebuie analizate timpul maxim de răspuns, volumul datelor, costul comunicaţiei, necesitatea funcţionării fără conexiune externă, confidenţialitatea

informației, posibilitatea administrării și actualizării componentei și consecințele unei decizii eronate. Prelucrarea locală poate reduce traficul și întârzierile, dar nu trebuie să dubleze necontrolat logica automatului programabil și nici să introducă o a doua sursă pentru aceeași decizie de control. Criteriile detaliate de repartizare sunt prezentate în secțiunea 7.3.3.

Platforma IIoT și serviciile de calcul în cloud

Platforma IIoT poate primi date de la mai multe linii, fabrici sau organizații și poate asigura rutarea, stocarea, analiza și vizualizarea acestora. Serviciile de calcul în cloud reprezintă un mod de implementare a acestor funcții, nu un nivel funcțional suplimentar al modelului ISA-95; caracteristicile care le definesc – autoservirea, accesul prin rețea, punerea în comun a resurselor, elasticitatea și măsurarea utilizării – privesc modul de furnizare, nu rolul aplicației [159].

În cloud pot fi găzduite aplicații asociate nivelului 3, nivelului 4 sau unor funcții analitice suplimentare. Poziționarea unei aplicații în cloud nu îi schimbă responsabilitatea: un sistem MES găzduit extern continuă să îndeplinească funcții de gestionare a operațiunilor, iar o aplicație ERP găzduită în cloud rămâne o aplicație pentru planificarea și gestionarea întreprinderii. Această diferențiere previne asocierea greșită a tuturor serviciilor cloud cu partea superioară a piramidei. Locul în care rulează aplicația și rolul pe care îl îndeplinește sunt două caracteristici distincte.

7.1.6. Fluxurile și limitele dintre niveluri

Fluxul ascendent pornește de la proces și transferă către aplicațiile superioare valori măsurate, stări și alarme, cantități realizate, timpi de funcționare și de oprire, consumuri, rezultate ale controlului calității, identificatori de produs și informații de trasabilitate.

Fluxul descendent transferă planuri și ordine de producție, rețete, parametri tehnologici, valori de referință, priorități, instrucțiuni și aprobări.

Fluxul descendent nu trebuie să formeze o comandă directă și necontrolată de la o aplicație externă către actuator. Instrucțiunile primite sunt validate succesiv, iar controlerul local aplică interblocările și condițiile de siguranță înaintea executării. Această regulă este consecința directă a delimitării stabilite în secțiunea 7.1.2 și se regăsește, în forme diferite, în toate secțiunile capitolului.

Pentru fiecare interfață trebuie stabilite explicit: producătorul și consumatorul datelor; identificatorii și semnificația variabilelor; unitățile de măsură și tipurile de date; frecvența sau condiția transferului; marca temporală și sursa timpului; informația privind calitatea; drepturile de citire și de scriere; comportamentul la întreruperea conexiunii; responsabilitatea pentru stocare, reconectare și eliminarea duplicatelor.

Lista pare administrativă, dar fiecare element absent devine, la punerea în funcțiune, o discuție între furnizori despre cine este responsabil pentru o valoare greșită. Arhitectura stratificată devine astfel un instrument pentru definirea responsabilităților, nu numai pentru reprezentarea componentelor: ea permite identificarea

locului în care trebuie executată fiecare funcție, a interfețelor care trebuie securizate şi a sistemelor care trebuie să continue să funcţioneze independent.

Arhitectura reprezentată în Figura 7.2 constituie referinţa pentru capitolele următoare. Secţiunile dedicate interconectării, modelelor de arhitectură, platformelor şi securităţii utilizează aceleaşi niveluri şi aceleaşi limite funcţionale, fără reluarea descrierii individuale a componentelor.

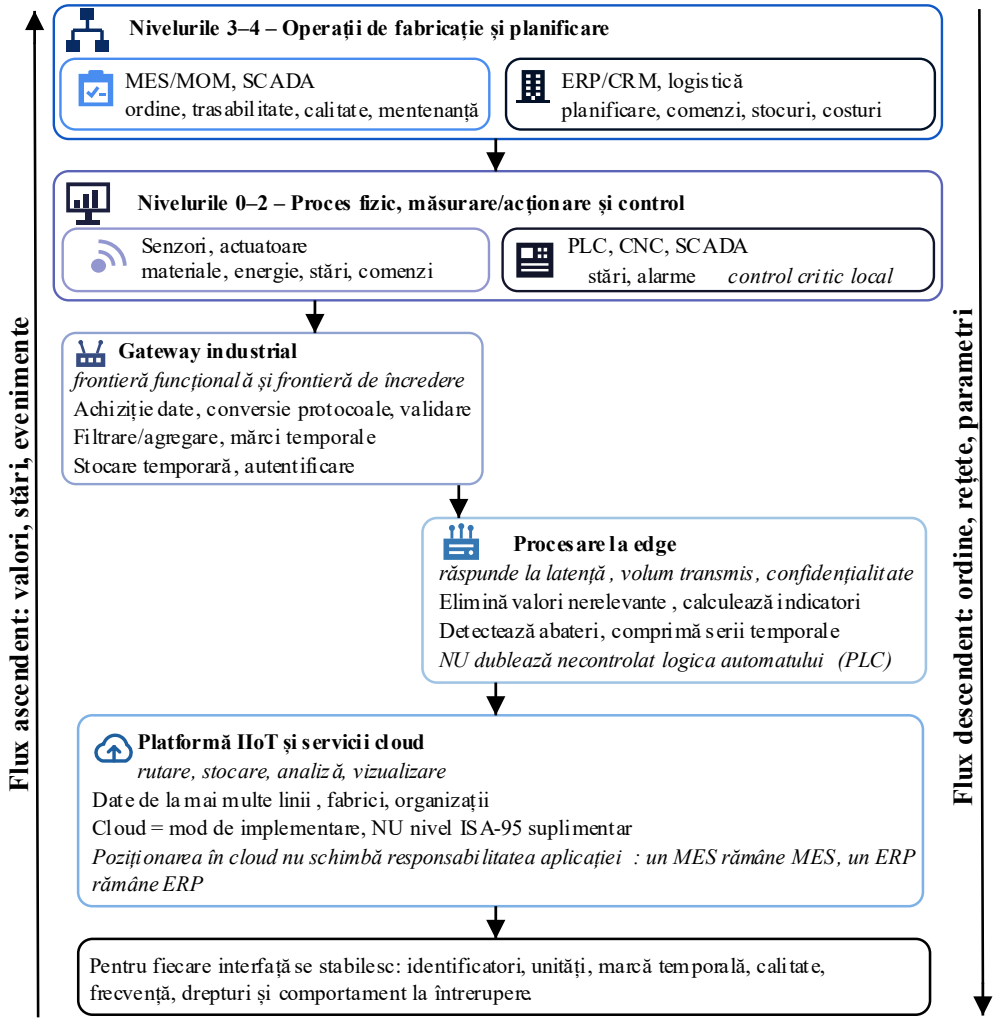


Figura 7.2 – Arhitectura IIoT: niveluri ISA-95 și componente transversale

7.2. Interconectarea SCADA–MES–ERP

Interconectarea sistemelor SCADA, MES şi ERP realizează integrarea verticală dintre procesul fizic, gestionarea operaţiunilor de fabricaţie şi planificarea întreprinderii. Scopul acestei integrări nu este transferarea tuturor datelor către toate

sistemele, ci furnizarea informaţiei potrivite, în forma şi la momentul necesar fiecărui nivel decizional.

Integrarea verticală se distinge de integrarea orizontală. Prima leagă nivelurile ierarhice ale aceleiaşi unităţi de producţie, de la senzor până la aplicaţia de planificare; a doua leagă etapele lanţului de valoare – furnizori, fabrici, distribuţie, service – şi, în interiorul fabricii, procesele succesive ale aceluiaşi flux de fabricaţie [4]. Cele două direcţii ridică probleme diferite: integrarea verticală se confruntă cu diferenţe de granularitate temporală şi de criticitate, în timp ce integrarea orizontală se confruntă cu limite organizaţionale, formate de date incompatibile şi responsabilităţi distribuite între entităţi juridice distincte. Capitolul de faţă tratează în principal integrarea verticală; consecinţele integrării orizontale asupra securităţii sunt reluate în Capitolul 8.

SCADA, MES şi ERP utilizează perspective diferite asupra aceluiaşi proces. Sistemul SCADA urmăreşte starea curentă a echipamentelor şi a variabilelor tehnologice [161]. Sistemul MES corelează aceste date cu ordinele de producţie, loturile, materialele, personalul şi rezultatele obţinute. Sistemul ERP utilizează informaţii agregate pentru planificarea resurselor, aprovizionare, logistică, gestiunea stocurilor, calculul costurilor şi gestionarea comenzilor clienţilor [78].

Integrarea trebuie să păstreze responsabilităţile fiecărui sistem. ERP nu trebuie să controleze direct actuatoarele, MES nu trebuie să înlocuiască interblocările automatului programabil, iar SCADA nu trebuie să devină sistemul principal pentru gestionarea comenzilor comerciale. Fiecare instrucţiune transmisă către nivelurile inferioare este verificată şi transformată progresiv, până când poate fi executată în condiţiile impuse de proces.

7.2.1. Delimitarea funcţională a sistemelor

Sistemul SCADA – asigură supravegherea operaţională a procesului. Acesta achiziţionează valori şi stări de la automate programabile, RTU-uri şi alte controlere, le prezintă operatorului şi gestionează alarmele, evenimentele şi tendinţele. Modul în care alarmele sunt definite, prioritizate şi evaluate face obiectul unui standard dedicat, care tratează gestionarea alarmelor ca proces cu ciclu de viaţă propriu, nu ca simplă listă de praguri [46].

Informaţiile caracteristice acestui nivel includ valori măsurate şi valori de referinţă, stări ale echipamentelor, comenzi şi confirmări, moduri de funcţionare, alarme şi evenimente, timpi de funcţionare şi de oprire, identificatori ai reţetelor active şi informaţii privind calitatea şi actualitatea datelor.

SCADA lucrează, în principal, cu variabile individuale şi evenimente apropiate temporal de proces. O valoare precum temperatura unui cuptor, viteza unui transportor sau starea unui motor are semnificaţie operaţională imediată, dar nu indică singură produsul realizat, comanda căreia îi aparţine sau consumul total al unui lot.

Sistemul MES – gestionează execuţia producţiei. Acesta transformă planurile şi comenzile primite de la ERP în activităţi care pot fi urmărite la nivelul fabricii şi corelează datele provenite din zona de control cu semnificaţia lor de producţie.

Standardul grupează aceste responsabilităţi în activităţi recurente, aplicabile deopotrivă producţiei, calităţii, mentenanţei şi gestiunii materialelor: administrarea definiţiilor, administrarea resurselor, programarea detaliată, lansarea lucrărilor, execuţia, colectarea datelor, urmărirea şi analiza performanţei [87]. În practică, funcţiile MES pot include preluarea şi verificarea ordinelor de producţie, programarea detaliată şi repartizarea operaţiilor, lansarea lucrărilor către liniile şi echipamentele disponibile, gestionarea reţetelor şi a instrucţiunilor de lucru, urmărirea producţiei în curs, gestionarea loturilor şi a seriilor, trasabilitatea materialelor şi a produselor, construirea genealogiei produsului, înregistrarea rezultatelor controlului calităţii, clasificarea opririlor şi a pierderilor, urmărirea consumurilor şi a cantităţilor realizate, calcularea indicatorilor operaţionali şi raportarea progresului şi a abaterilor către ERP.

Gestionarea reţetelor merită o precizare. În industriile de proces, reţeta nu este o simplă listă de parametri, ci un obiect structurat, separat conceptual de echipamentul pe care se execută: reţeta descrie ce trebuie realizat, iar procedurile echipamentului descriu cum poate fi realizat de o instalaţie anume [95]. Separarea permite modificarea reţetei fără reprogramarea instalaţiei şi transferul aceleiaşi reţete între linii echivalente, iar în absenţa ei parametrii tehnologici ajung să fie codificaţi în programul automatului programabil, unde nu mai pot fi nici versionaţi, nici auditaţi.

MES nu se limitează la agregarea valorilor SCADA. Acesta adaugă contextul necesar pentru a stabili ce produs a fost realizat, în cadrul cărei comenzi, cu ce materiale, pe ce echipament, în ce interval, conform cărei versiuni a reţetei şi cu ce rezultat.

Sistemul ERP – gestionează planificarea şi resursele întreprinderii. Acesta lucrează cu informaţii comerciale, logistice şi economice: comenzile clienţilor, planurile generale de producţie, necesarul de materiale, stocurile şi aprovizionarea, capacităţile planificate, termenele de livrare, consumurile raportate, cantităţile de produse finite, costurile şi rezultatele financiare.

ERP trebuie să primească informaţii suficient de agregate şi validate pentru a susţine deciziile întreprinderii. Transferarea directă a fiecărei valori provenite din senzori către ERP ar mări volumul datelor fără a aduce contextul necesar planificării.

Delimitarea funcţională dintre cele trei sisteme, cu obiectele urmărite, granularitatea datelor, orizontul temporal şi dependenţele admise, este sintetizată în Tabelul 7.2.

Intervalele temporale din tabel sunt orientative. Clasificarea trebuie realizată după responsabilitatea funcţională, nu după viteza actualizării. Un sistem MES poate recepţiona evenimente în câteva secunde, fără a deveni sistem de control în timp real.

Tabelul 7.2 – Delimitarea funcțională dintre SCADA, MES și ERP

Caracteristică	SCADA	MES	ERP
Domeniu dominant	supravegherea și operarea procesului	gestionarea operațiunilor de fabricație	planificarea și gestionarea întreprinderii
Obiect urmărit	variabilă, echipament, alarmă, eveniment	operație, ordin de producție, lot, produs	comandă client, material, resursă, cost, livrare
Granularitatea datelor	ridicată, apropiată de proces	medie, contextualizată operațional	agregată, economică și logistică
Orizont temporal dominant	momentul curent, secunde și minute	minute, schimburi, zile, durata ordinului	zile, săptămâni, luni, perioade de planificare
Utilizatori principali	operatori, automatiști, personal de mentenanță	responsabili de producție, calitate, trasabilitate și planificare operațională	planificatori, logisticieni, personal comercial, financiar și managerial
Informații descendente	valori de referință aprobate, rețete și comenzi operaționale	ordine, operații, rețete, priorități și instrucțiuni	comenzi, cantități, termene, necesar de materiale și priorități
Informații ascendente	valori, stări, alarme, evenimente și cantități	progres, consumuri, trasabilitate, calitate, opriri și indicatori	situația consolidată a producției, stocurilor, costurilor și livrărilor
Dependență admisă	controlul local trebuie să continue fără MES și ERP	poate funcționa temporar cu informațiile deja lansate	indisponibilitatea temporară nu trebuie să oprească buclele de control

7.2.2. Fluxurile bidirecționale dintre niveluri

Seria ISA-95, adoptată şi în cadrul IEC 62264, defineşte modele şi schimburi informaţionale pentru integrarea funcţiilor întreprinderii cu cele de control şi acordă o atenţie deosebită interfeţei dintre gestionarea operaţiunilor de fabricaţie şi activităţile întreprinderii [75], [49].

În sens descendent, informaţia este transformată progresiv dintr-o cerinţă comercială într-o activitate executabilă, parcurgând succesiv sistemul ERP, sistemul MES, sistemul SCADA sau serviciul de integrare şi automatul programabil, până la nivelul procesului.

ERP poate transmite către MES identificatorul ordinului de producţie, produsul şi versiunea acestuia, cantitatea solicitată, termenul şi prioritatea, materialele planificate, cerinţele de calitate şi restricţiile sau instrucţiunile asociate comenzii.

MES verifică disponibilitatea resurselor, corelează ordinul cu planificarea detaliată şi îl descompune în operaţii. Pentru fiecare operaţie sunt stabilite linia, echipamentul, lotul, reţeta, cantitatea, succesiunea şi condiţiile de executare.

Către zona de control nu trebuie transmisă întreaga structură comercială a comenzii. Sunt transferate numai informaţiile necesare execuției: identificatorul

operației, identificatorul produsului sau al lotului, versiunea rețetei, parametrii tehnologici aprobați, cantitatea care trebuie realizată, condițiile de pornire și de oprire și identificatorii necesari trasabilității.

Automatul programabil validează starea instalației, modul de funcționare, interblocările și limitele locale înaintea aplicării parametrilor. Faptul că o operație a fost lansată de MES nu demonstrează că aceasta poate fi executată imediat.

În sens ascendent, datele pornesc din proces și ajung la automatul programabil, apoi trec prin SCADA sau prin serviciul de integrare către MES și ERP. Pe acest traseu, datele sunt grupate și completate cu informațiile necesare interpretării lor.

Automatul programabil furnizează valori, stări, confirmări, contoare și coduri de defect. SCADA le prezintă operatorului, gestionează alarmele și poate păstra istoricul detaliat. MES asociază evenimentele cu ordinul, operația, produsul, lotul, materialele și intervalul de producție. ERP primește rezultatele consolidate necesare planificării și gestiunii: cantitatea realizată și cantitatea acceptată, cantitatea rebutată, consumul real de materiale, stadiul ordinului, momentul începerii și al finalizării, abaterile semnificative, produsul finit introdus în stoc, necesarul actualizat de materiale și datele necesare calculării costurilor.

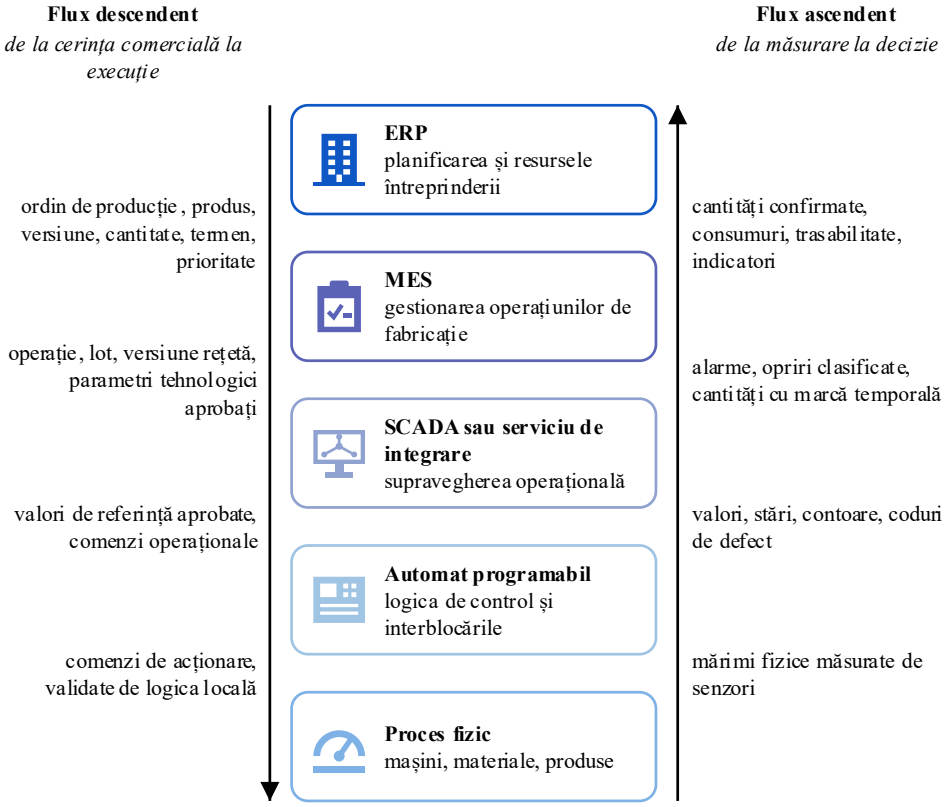


Figura 7.3 – Fluxurile bidirecționale dintre ERP, MES, SCADA și automatul programabil

Cele două sensuri nu se implementează simetric. Schimbul dintre nivelurile 3 şi 4 este structurat, în modelul standardizat, ca un set de tranzacţii cu roluri şi confirmări explicite – cerere, răspuns, notificare, confirmare, tocmai pentru ca fiecare transfer să aibă un iniţiator identificabil şi un rezultat verificabil [194]. Fluxul ascendent poate fi tratat, în bună măsură, ca o publicare de evenimente, în timp ce fluxul descendent are, aproape întotdeauna, caracter tranzacţional: lansarea unui ordin trebuie confirmată, iar o confirmare pierdută nu are aceleaşi consecinţe ca o valoare de proces pierdută.

O eroare frecventă de proiectare este tratarea acestui lanţ ca un traseu unic prin care fiecare informaţie trebuie să treacă. Nu SCADA transportă obligatoriu datele către MES: în multe instalaţii, MES citeşte direct dintr-un server OPC UA sau primeşte evenimente printr-un serviciu de integrare [127], iar SCADA rămâne dedicat operării. Criteriul nu este ordinea din desen, ci sistemul care deţine informaţia de referinţă şi responsabilitatea pentru validarea ei.

Fluxurile descrise, cu transformarea informaţiei la trecerea prin fiecare nivel, sunt reprezentate sintetic în Figura 7.3.

7.2.3. Contextualizarea datelor şi funcţiile MES

MES realizează asocierea dintre datele tehnice şi obiectele gestionate în producţie. Un contor din automatul programabil poate indica faptul că au fost executate 100 de cicluri, dar sistemul MES trebuie să stabilească ordinul în cadrul căruia au fost executate ciclurile, produsul şi versiunea realizată, loturile de materiale utilizate, echipamentul şi reţeta activă, operatorul sau schimbul, numărul produselor acceptate şi respinse, intervalul de timp corespunzător şi cauzele opririlor şi ale abaterilor.

Trasabilitatea permite urmărirea deplasării şi transformării materialelor, semifabricatelor şi produselor. Aceasta răspunde unor întrebări precum: unde se află un lot, prin ce operaţii a trecut şi ce rezultate au fost înregistrate. În anumite sectoare, capacitatea de a răspunde la aceste întrebări nu este o opţiune de proiectare, ci o obligaţie legală: legislaţia alimentară europeană impune identificarea, în amonte şi în aval, a oricărui operator care a furnizat sau a primit un produs, la fiecare etapă a lanţului [198].

Genealogia produsului descrie relaţiile dintre produsul finit şi elementele care au contribuit la realizarea lui: loturile materiilor prime, subansamblurile, echipamentele, programele, reţetele, parametrii, rezultatele verificărilor şi eventualele reprelucrări.

Pentru construirea unei genealogii corecte, identificatorii trebuie păstraţi pe întregul traseu. Dacă automatul programabil raportează numai o creştere a contorului, fără identificatorul operaţiei sau al lotului activ, asocierea ulterioară poate deveni incertă. Contextul trebuie stabilit cât mai aproape de momentul producerii evenimentului: reconstituirea lui ulterioară, prin corelarea mărcilor temporale cu

programul de producţie, funcţionează în regim normal şi eşuează exact în situaţiile care interesează – la schimbarea lotului, la repornirea după o oprire sau la producţia simultană a două variante de produs.

Indicatorii operaţionali şi calculul OEE

MES calculează indicatori ai performanţei operaţionale. Seria ISO 22400 oferă un cadru neutru pentru definirea, compunerea, schimbul şi utilizarea indicatorilor-cheie de performanţă în gestionarea operaţiunilor de fabricaţie [50], [51]. Cel mai utilizat este eficacitatea globală a echipamentelor (*overall equipment effectiveness, OEE*), formulată iniţial în cadrul mentenanţei productive totale ca produs al trei rapoarte independente [65]:

$$\boldsymbol{OEE = D \times P \times C}$$

unde *D* este disponibilitatea, raportul dintre timpul efectiv de producţie şi timpul planificat pentru producţie; *P* este performanţa, raportul dintre timpul teoretic necesar realizării cantităţii produse şi timpul efectiv de producţie; iar *C* este rata de calitate, raportul dintre cantitatea acceptată şi cantitatea totală realizată.

Scenariu didactic – o linie de ambalare, un schimb. Datele de mai jos sunt construite pentru demonstrarea metodei; ele nu provin dintr-o instalaţie reală.

Date şi ipoteze. Schimb de 8 ore, adică 480 min. Pauzele planificate însumează 30 min, deci timpul planificat pentru producţie este de 450 min. Opririle neplanificate înregistrate sunt: defectarea mecanismului de etichetare, 22 min; lipsa materialului de ambalare, 14 min; reglaj după schimbarea lotului, 9 min – în total 45 min. Timpul de ciclu de referinţă, preluat din definiţia produsului, este de 1,2 s/produs, adică 0,02 min/produs. Contorul liniei indică 16 200 de produse realizate, dintre care 486 au fost respinse la inspecţia finală. Toate valorile se referă la aceeaşi linie, la acelaşi schimb şi la acelaşi produs.

Înlocuirea numerică:

Timpul efectiv de producţie: 450 − 45 = 405 min.

$$D = 405 / 450 = 0{,}900$$

Timpul teoretic necesar pentru cantitatea realizată: 16 200 × 0,02 = 324 min.

$$P = 324 / 405 = 0{,}800$$

Cantitatea acceptată: 16 200 − 486 = 15 714 produse.

$$C = 15\,714 / 16\,200 = 0{,}970$$

$$OEE = 0{,}900 \times 0{,}800 \times 0{,}970 = 0{,}698, \text{ adică } 69{,}8\ \%$$

Verificare: Rezultatul se poate obţine şi direct, ca raport între timpul care ar fi fost necesar pentru realizarea numai a produselor acceptate şi timpul planificat: 15 714 × 0,02 = 314,3 min, iar 314,3 / 450 = 0,698. Coincidenţa celor două căi confirmă coerenţa datelor; o diferenţă între ele indică, de regulă, un timp de ciclu de referinţă

care nu corespunde produsului sau o cantitate raportată din altă sursă decât cea utilizată la calculul disponibilității.

Interpretarea: din cele 450 de minute planificate, aproximativ 136 se pierd. Repartizarea lor este informația utilă, nu procentul global: 45 min se pierd prin opriri, circa 81 min prin funcționare sub viteza de referință și circa 10 min prin produse respinse. Cea mai mare pierdere nu este vizibilă în jurnalul de alarme, pentru că nu corespunde niciunei opriri înregistrate – linia a funcționat, dar la 1,5 s/produs în loc de 1,2 s/produs. Acest tip de pierdere provine, de regulă, din micro-opriri sub pragul de înregistrare, din reduceri deliberate de viteză pentru evitarea rebuturilor sau dintr-un timp de ciclu de referință stabilit optimist. Concluzia practică este că o intervenție asupra fiabilității mecanismului de etichetare ar recupera cel mult 22 min, în timp ce identificarea cauzei pierderii de viteză vizează de aproape patru ori mai mult.

Limitele indicatorului: OEE depinde integral de convenția privind timpul planificat: dacă schimbul fără comenzi este exclus din numitor, valoarea crește fără nicio îmbunătățire reală a procesului. Indicatorul nu spune dacă producția era necesară – o linie care fabrică stoc nevandabil poate avea OEE ridicat. Compararea valorilor între linii, fabrici sau furnizori este validă numai dacă definițiile timpului planificat, ale opririlor înregistrabile și ale timpului de ciclu de referință sunt identice; standardul insistă asupra acestui punct, condiționând compararea indicatorilor de declararea completă a elementelor din care sunt compuși [51]. În lipsa acestei condiții, două valori aparent comparabile măsoară lucruri diferite. În sfârșit, indicatorul este valid numai dacă toate datele provin din același interval și de la același echipament, iar cantitatea, opririle și timpul de referință au o singură sursă de referință declarată.

Această ultimă condiție explică de ce calculul aparține sistemului MES și nu sistemului SCADA. Cantitatea provine din contorul automatului programabil, stările și duratele din SCADA, clasificarea cauzelor de oprire din intervenția operatorului, iar timpul de ciclu de referință din definiția produsului. Numai nivelul care deține simultan ordinul, produsul și intervalul poate corela corect aceste patru surse.

7.2.4. Proiectarea interfețelor de integrare

Interconectarea nu trebuie realizată prin acces necontrolat al unui sistem la structurile interne ale altuia. Utilizarea unei baze de date comune, în care SCADA, MES și ERP modifică direct aceleași tabele, creează dependențe puternice între aplicații și face imposibilă stabilirea responsabilității pentru o valoare greșită. Costul acestei soluții nu apare la punerea în funcțiune, ci la prima actualizare a unuia dintre sisteme.

Integrarea trebuie realizată prin interfețe definite și administrate: servere OPC UA pentru expunerea structurată a datelor operaționale [127]; mesagerie MQTT pentru distribuirea evenimentelor și a stărilor [177]; cozi de mesaje sau un broker

pentru transfer asincron; interfețe API pentru operații tranzacționale, construite, de regulă, peste semantica protocolului de transfer al hipertextului [181]; fișiere structurate, atunci când actualizarea nu necesită transfer imediat; servicii de integrare care transformă și validează mesajele.

Alegerea mecanismului depinde de natura schimbului. Actualizarea unei stări de echipament, lansarea unui ordin și confirmarea recepției unui lot reprezintă operații diferite: prima este o informare repetitivă, a doua o tranzacție care trebuie confirmată, a treia un eveniment cu efect asupra stocurilor. Tratarea lor prin același tip de mesaj, fără analiză prealabilă, este una dintre cauzele frecvente ale integrărilor care funcționează în regim normal și eșuează la prima anomalie.

Pentru fiecare interfață se precizează: cine deține informația de referință, cine produce și cine consumă mesajul; structura și versiunea datelor; identificatorii ordinului, operației, produsului, lotului și echipamentului; tipurile și unitățile de măsură; marca temporală și sursa timpului; când se transmite și cum se confirmă; regulile repetării și eliminării duplicatelor; reacția la destinația indisponibilă; drepturile de citire, scriere și administrare; cerințele de jurnalizare și audit.

Trei dintre aceste elemente merită dezvoltate, pentru că sunt cel mai des omise.

Tratarea repetărilor: un mesaj trebuie să poată fi prelucrat în siguranță și atunci când este recepționat de două ori. Proprietatea se numește idempotență și se obține prin asocierea unui identificator unic fiecărei tranzacții, pe care destinația îl păstrează și îl verifică înainte de aplicare. Necesitatea ei nu ține de calitatea implementării, ci de protocol: nivelul de calitate a serviciului utilizat în mod obișnuit pentru mesageria industrială garantează livrarea cel puțin o dată, nu exact o dată, iar duplicatele sunt un rezultat normal al retransmisiei [177]. În absența idempotenței, o simplă retransmitere după o întrerupere de rețea poate produce lansarea dublă a aceluiași ordin sau înregistrarea de două ori a aceleiași cantități – erori care nu se manifestă imediat, ci la închiderea lunii, în conturile de stoc.

Sincronizarea timpului: Corelarea evenimentelor este posibilă numai dacă sistemele utilizează o referință de timp comună. La nivelul echipamentelor de automatizare este utilizat un protocol de sincronizare de precizie ridicată [35], în timp ce serverele și aplicațiile întreprinderii sunt sincronizate, de regulă, prin protocolul de timp al rețelei [157]. Diferența de precizie dintre cele două mecanisme este acceptabilă atât timp cât este cunoscută și consemnată; problema apare atunci când o componentă rămâne nesincronizată, iar ordinea aparentă a evenimentelor diferă de succesiunea reală din proces. Trebuie stabilite, pentru fiecare interfață, sursa timpului, fusul orar utilizat și convenția de reprezentare – recomandabil, timpul universal coordonat, cu conversia realizată numai la afișare.

Comportamentul la întrerupere: la întreruperea conexiunii dintre SCADA și MES, controlul local trebuie să continue. Datele pot fi păstrate temporar și transferate după restabilirea legăturii, cu menținerea mărcilor temporale inițiale, iar MES

trebuie să diferenţieze datele produse în prezent de cele recuperate ulterior. Dacă legătura MES–ERP este indisponibilă, ordinele deja lansate pot continua în limitele aprobate, însă introducerea unor ordine noi, modificarea priorităţilor şi actualizarea stocurilor trebuie tratate printr-o procedură prestabilită. Reconectarea nu trebuie să producă pierderea, dublarea sau reordonarea necontrolată a tranzacţiilor; capacitatea de stocare locală şi durata maximă de funcţionare autonomă se dimensionează explicit, nu se descoperă la prima întrerupere prelungită. Metoda de dimensionare este prezentată în secţiunea 7.5.5, pe datele exerciţiului.

7.2.5. Exemplu de integrare a unei comenzi de producţie

Exemplul următor este un scenariu didactic, construit pentru a urmări transformarea informaţiei de-a lungul lanţului descris anterior. Este utilizată aceeaşi linie de ambalare la care se referă calculul din secţiunea 7.2.3, pentru ca cele două tratări să poată fi citite împreună.

Se consideră că ERP primeşte o comandă de 5.000 de produse, cu produsul, cantitatea, termenul de livrare şi prioritatea specificate de client.

I. Traseul descendent

- ERP verifică necesarul de materiale, disponibilitatea stocului şi capacitatea planificată, apoi creează ordinul de producţie.
- Ordinul este transmis către MES împreună cu identificatorul produsului şi versiunea acestuia, cantitatea, termenul şi prioritatea. Transferul este o tranzacţie: MES confirmă preluarea, iar ERP păstrează starea „ordin lansat” numai după primirea confirmării.
- MES verifică disponibilitatea liniei, a materialelor, a reţetei aprobate şi a resurselor necesare, inclusiv calificarea personalului, dacă procedura o impune.
- MES descompune ordinul în operaţii şi stabileşte succesiunea de execuţie, alocând fiecărei operaţii linia, echipamentul, lotul şi intervalul planificat.
- Către zona de control sunt transmise numai informaţiile necesare execuţiei: identificatorul operaţiei, identificatorul lotului, versiunea reţetei, parametrii tehnologici aprobaţi şi cantitatea care trebuie realizată. Structura comercială a comenzii – clientul, preţul, termenul contractual – rămâne în ERP.
- Operatorul confirmă pregătirea liniei, dacă procedura impune această verificare.
- Automatul programabil verifică interblocările, starea echipamentelor şi condiţiile locale: presiunea aerului, temperatura staţiei de sigilare, prezenţa materialului de ambalare, poziţia iniţială a mecanismelor.
- Producţia începe numai după îndeplinirea condiţiilor de pornire. Dacă o condiţie nu este îndeplinită, operaţia rămâne în aşteptare, iar MES primeşte motivul întârzierii, nu o simplă absenţă a confirmării.

Etapa a opta merită subliniată. Ordinul lansat de MES este o autorizare, nu o comandă de pornire. Distincția pare formală, dar determină comportamentul sistemului în situațiile anormale: dacă lansarea ar echivala cu pornirea, o eroare de planificare s-ar transforma direct într-o mișcare a instalației.

II. Traseul ascendent

Pe parcursul execuției, automatul programabil transmite către SCADA stările echipamentelor, contoarele, viteza liniei, alarmele și codurile de defect. SCADA prezintă informațiile operatorului și păstrează evenimentele necesare diagnosticării.

MES preia informațiile relevante și le asociază ordinului activ, actualizând cantitatea realizată, cantitatea acceptată și cea rebutată, materialele consumate, durata operației, opririle și cauzele acestora, rezultatele verificărilor și progresul ordinului. Frecvențele sunt diferite pentru fiecare categorie: contoarele pot fi citite la fiecare minut, alarmele la apariție, iar consumurile de materiale la închiderea fiecărui recipient de alimentare.

La finalizarea operației, MES transmite către ERP cantitățile confirmate, consumurile reale, produsele introduse în stoc și abaterile relevante. ERP actualizează stocurile, situația comenzii clientului, necesarul de aprovizionare și informațiile pentru calcularea costurilor.

Comportamentul în caz de abatere

Dacă un senzor detectează lipsa materialului de ambalare, automatul programabil oprește controlat echipamentul – finalizează ciclul în curs, oprește transportorul și menține temperatura stației de sigilare în regimul de așteptare, iar SCADA generează alarma. MES asociază oprirea cu operația și ordinul activ, o clasifică drept oprire cauzată de lipsa materialului și actualizează progresul producției. ERP poate primi informația consolidată necesară reaprovizionării, dar nu comandă direct repornirea transportorului.

Traseul acestei singure opriri arată de ce contextul trebuie stabilit la nivelul potrivit. Automatul programabil știe că un senzor a comutat; SCADA știe că a apărut o alarmă cu un anumit cod, la un anumit moment; numai MES poate stabili că oprirea de 14 minute aparține lotului 245, că a fost cauzată de lipsa materialului și că trebuie inclusă în componenta de disponibilitate a indicatorului calculat în secțiunea 7.2.3. Dacă această clasificare nu se face la momentul opririi, ea se face ulterior, prin reconstituire, iar rezultatul este un indicator în care o parte semnificativă a pierderilor apare ca „cauză neidentificată”.

Ce demonstrează exemplul

Informația se transformă progresiv, iar fiecare nivel lucrează cu propriul obiect:

- ERP lucrează cu necesarul comenzii;

- MES lucrează cu execuţia ordinului şi contextul producţiei;
- SCADA lucrează cu starea procesului;
- automatul programabil execută logica locală;
- senzorii şi actuatoarele interacţionează cu procesul fizic.

Integrarea este corectă atunci când aceeaşi comandă poate fi urmărită de la cerinţa clientului până la produsul realizat, fără ca limitele dintre planificare, gestionarea operaţiunilor, supraveghere şi control să fie eliminate. Un test practic al acestei corectitudini este întrebarea inversă: pornind de la un produs livrat, sistemul trebuie să poată indica lotul, intervalul, echipamentul, reţeta aplicată şi rezultatele verificărilor, fără intervenţie manuală şi fără corelări bazate exclusiv pe mărci temporale.

Delimitarea funcţională stabilită până aici nu impune însă o singură implementare. Aceleaşi responsabilităţi pot fi distribuite diferit între infrastructura locală şi serviciile externe, în funcţie de timpul de răspuns, de volumul datelor şi de disponibilitatea cerută. Secţiunea următoare prezintă modelele arhitecturale prin care se realizează această distribuire şi criteriile după care se decide locul de execuţie al fiecărei funcţii.

7.3. Modele de arhitectură IIoT

Modelul arhitectural stabileşte locul în care sunt executate funcţiile sistemului, datele care sunt păstrate la fiecare nivel şi dependenţele admise între infrastructura locală şi serviciile externe. Aceleaşi componente prezentate în secţiunea 7.1 pot fi organizate diferit în funcţie de timpul de răspuns, volumul datelor, criticitatea procesului, distribuţia geografică şi cerinţele de disponibilitate.

Alegerea arhitecturii nu trebuie redusă la decizia „local sau cloud". Pentru fiecare funcţie trebuie stabilit dacă aceasta este executată în controler, la edge, pe un server al fabricii sau într-o infrastructură externă. Rezultatul este, de regulă, o distribuire controlată a prelucrării, stocării şi analizei între mai multe niveluri, nu adoptarea unui model pur. Modelele descrise în continuare sunt tipuri de referinţă utile pentru analiză; instalaţiile reale se situează aproape întotdeauna între ele.

7.3.1. Arhitecturi centralizate, distribuite şi hibride

Într-o *arhitectură centralizată*, datele provenite de la mai multe echipamente sau linii sunt transferate către un sistem principal în care sunt realizate stocarea, analiza şi administrarea aplicaţiilor. Sistemul central poate fi amplasat în fabrica proprie, într-un centru de date al organizaţiei sau într-o platformă găzduită în cloud.

Centralizarea simplifică administrarea aplicaţiilor şi a utilizatorilor, aplicarea uniformă a modelelor de date, corelarea informaţiilor provenite din mai multe surse, realizarea copiilor de siguranţă, actualizarea algoritmilor şi a tablourilor de bord şi analiza comparativă între linii sau unităţi de producţie.

Modelul devine însă vulnerabil atunci când funcționarea locală depinde de disponibilitatea sistemului central sau a conexiunii cu acesta. Transmiterea continuă a tuturor valorilor brute poate încărca rețeaua, poate crește costurile de stocare și poate introduce întârzieri incompatibile cu procesul. Îndrumările pentru securitatea tehnologiei operaționale tratează explicit această situație, cerând ca disponibilitatea funcțiilor de operare să nu depindă de servicii aflate în afara perimetrului administrat [25].

Vulnerabilitatea este cuantificabilă. Dacă o funcție depinde simultan de mai multe componente înseriate, disponibilitatea rezultată este produsul disponibilităților individuale. Pentru un lanț format din gateway, legătură de comunicație și serviciu extern, fiecare cu o disponibilitate de 99,5 %, disponibilitatea funcției devine $0{,}995^3 \approx 0{,}985$, adică aproximativ 10,7 ore de indisponibilitate pe lună, față de 3,6 ore pentru o singură componentă. Calculul este simplificator – presupune defectări independente și ignoră duratele de restabilire, dar este suficient pentru a arăta de ce o funcție necesară operării nu se plasează la capătul unui lanț de dependențe externe.

Centralizarea este adecvată pentru raportare, analiză istorică, gestionarea mai multor unități și aplicarea unor modele comune. Aceasta nu este adecvată pentru buclele de reglare, interblocări sau alte funcții care trebuie să răspundă predictibil și să continue în lipsa conexiunii externe.

Într-o *arhitectură distribuită*, funcțiile sunt repartizate între mai multe componente apropiate de proces. Automatele programabile execută logica de control, gateway-urile filtrează și contextualizează datele, serverele locale corelează informațiile la nivelul fabricii, iar sistemele superioare primesc numai datele necesare.

Avantajele principale sunt reducerea timpului de răspuns, funcționarea locală în cazul întreruperii comunicației, diminuarea volumului transmis, izolarea mai ușoară a unei defecțiuni, adaptarea funcțiilor la particularitățile fiecărei linii și păstrarea locală a datelor sensibile.

Distribuirea introduce și dificultăți. Configurațiile, modelele de date și versiunile aplicațiilor trebuie administrate pe mai multe componente, iar efortul crește proporțional cu numărul acestora. Rezultatele calculate local trebuie să utilizeze definiții compatibile – două linii care calculează același indicator după reguli diferite produc valori care nu pot fi comparate [51], iar sincronizarea după restabilirea comunicației trebuie să prevină pierderea, dublarea sau reordonarea datelor.

O arhitectură distribuită nu presupune duplicarea aceleiași logici în automatul programabil, în gateway și în platformă. Fiecare funcție trebuie să aibă un proprietar clar și o singură sursă de referință; altfel, la prima divergență între două rezultate, nu există niciun criteriu pentru a stabili care este cel corect.

Arhitectura hibridă – combină infrastructura locală cu serviciile de calcul în cloud. Funcțiile critice, datele necesare operării și aplicațiile care trebuie să

continue în lipsa conexiunii sunt păstrate local. Funcțiile care necesită scalare, corelarea mai multor fabrici sau resurse de calcul variabile pot fi executate în cloud, unde alocarea rapidă a resurselor și plata proporțională cu utilizarea constituie caracteristici definitorii ale modelului de furnizare [159].

O distribuire posibilă este:

- PLC-urile, interblocări și protecții;
- HMI și SCADA locale pentru operare, alarmare și supraveghere;
- gateway industrial pentru conversie, filtrare și stocare temporară;
- server local pentru agregare, bază de date istorică și aplicații ale fabricii;
- cloud pentru analiză la scară mare, comparații între unități, instruirea modelelor și raportare centralizată.
- Modelul hibrid permite modernizarea graduală a unei instalații. Sistemele existente pot continua să funcționeze local, iar serviciile externe pot fi adăugate fără transferarea controlului critic în afara fabricii. Costul acestei flexibilități este dublu: trebuie administrate două medii cu practici diferite de operare și securitate, iar limita dintre ele trebuie definită explicit, altfel dependențele se acumulează necontrolat, funcție cu funcție.
- Cele trei modele sunt comparate în Tabelul 7.3 din punctul de vedere al locului prelucrării, al dependenței de comunicație, al timpului de răspuns, al volumului transmis, al efortului de administrare și al continuității locale.

Tabelul 7.3 – Compararea modelelor de arhitectură IIoT

Caracteristică	**Arhitectură centralizată**	**Arhitectură distribuită**	**Arhitectură hibridă**
Locul prelucrării dominante	sistem central local sau cloud	controlere, gateway-uri și servere distribuite	distribuit între infrastructura locală și cloud
Dependența de comunicație	ridicată pentru funcțiile centralizate	redusă pentru funcțiile locale	stabilită separat pentru fiecare funcție
Timp de răspuns	depinde de rețea și de sistemul central	redus pentru prelucrarea apropiată de proces	redus local, variabil pentru funcțiile externe
Volumul transmis	poate fi ridicat	poate fi redus prin filtrare și agregare	datele sunt selectate în funcție de destinație
Administrare	concentrată	distribuită și mai complexă	necesită coordonarea celor două medii
Continuitatea locală	trebuie proiectată explicit	poate fi asigurată prin autonomie locală	funcțiile critice rămân locale
Utilizare adecvată	analiză centrală, raportare și gestionare multi-site	procese cu latență redusă și conectivitate variabilă	sisteme industriale care combină operarea locală cu analiza scalabilă

7.3.2. Continuumul marginea rețelei–nivel intermediar–cloud

Prelucrarea datelor poate fi distribuită de-a lungul unui continuum format din edge, nivelul intermediar şi serviciile de calcul în cloud. Acestea nu reprezintă niveluri ISA-95 suplimentare, ci locuri în care pot fi implementate funcţii aparţinând diferitelor domenii ale arhitecturii. Arhitecturile de referinţă pentru internetul industrial utilizează aceeaşi separare, sub forma nivelurilor de implementare: nivelul din apropierea procesului, nivelul platformei şi nivelul aplicaţiilor întreprinderii [27].

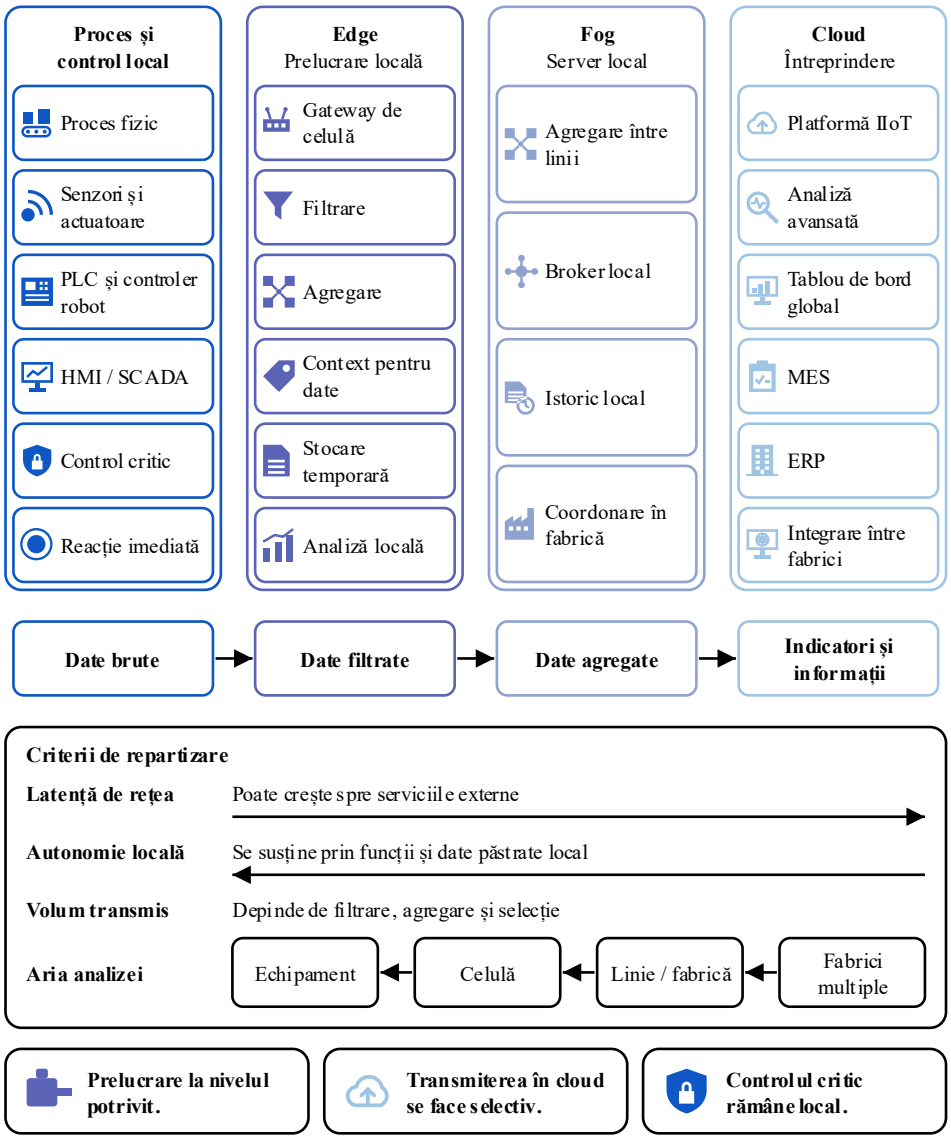


Figura 7.4 – Distribuirea prelucrării între marginea rețelei, nivelurile intermediare și serviciile de calcul în cloud

Distribuirea prelucrării de-a lungul acestui continuum este reprezentată în Figura 7.4.

Procesarea edge este executată în apropierea sursei datelor. Aceasta poate fi realizată într-un controler, într-un gateway industrial, într-un calculator industrial sau într-o componentă instalată la nivelul mașinii ori al liniei. Motivația este simultan tehnică și economică: apropierea prelucrării de sursă reduce latența, reduce volumul transmis și permite păstrarea locală a informațiilor care nu trebuie să părăsească fabrica, trei probleme care nu se rezolvă prin creșterea capacității de calcul centralizate [111].

Funcțiile potrivite pentru acest nivel includ filtrarea valorilor nerelevante, validarea tipului și a domeniului de măsurare, conversia protocoalelor, agregarea pe intervale scurte, calcularea unor indicatori locali, detectarea rapidă a abaterilor, stocarea temporară și retransmiterea, precum și anonimizarea sau eliminarea informațiilor care nu trebuie transferate.

O componentă de edge poate detecta o abatere și poate genera o notificare, dar nu trebuie să preia necontrolat funcțiile deterministe ale automatului programabil. Dacă rezultatul analizei influențează procesul, acesta este transmis printr-o interfață definită către sistemul responsabil de validarea și executarea comenzii. Distincția este esențială: o funcție de edge poate lipsi temporar fără consecințe asupra siguranței, ceea ce nu este valabil pentru o funcție de control.

Nivelul intermediar, asociat conceptului de calcul distribuit de tip fog, este amplasat între echipamentele de edge și serviciile centralizate. Acesta poate fi reprezentat de un server al secției, de un grup de servere al fabricii sau de o infrastructură distribuită care deservește mai multe linii. Conceptul a fost formulat inițial ca extindere a modelului cloud către marginea rețelei, pentru aplicații care necesită latență redusă, distribuție geografică și mobilitate [158], iar modelul conceptual elaborat ulterior îl descrie ca o distribuire a aplicațiilor, administrării și analizei în interiorul rețelei, ca răspuns la volumul, eterogenitatea și latența sistemelor IoT [199].

La acest nivel pot fi realizate agregarea datelor provenite de la mai multe echipamente, corelarea evenimentelor la nivelul liniei sau al fabricii, păstrarea unui istoric operațional local, coordonarea unor aplicații distribuite, aplicarea unor modele analitice comune, sincronizarea datelor cu sistemele MES și administrarea componentelor de edge.

Nivelul intermediar este util atunci când informațiile trebuie corelate la o scară mai mare decât cea a unei singure mașini, dar nu este justificată transmiterea imediată a tuturor datelor către cloud. În instalațiile mici, acest nivel poate lipsi complet, iar funcțiile sale se împart între gateway și platformă; introducerea lui devine justificată atunci când numărul surselor face administrarea individuală a componentelor de edge nepracticabilă.

Serviciile de calcul în cloud oferă resurse scalabile pentru stocare, analiză și integrare. Acestea sunt adecvate pentru păstrarea datelor pe termen lung, analiza unor volume mari de date, compararea performanțelor mai multor fabrici,

instruirea modelelor de învățare automată, gestionarea centralizată a rapoartelor, integrarea cu aplicații externe și furnizarea serviciilor către utilizatori distribuiți geografic.

Cloudul nu trebuie considerat destinația obligatorie a tuturor datelor. Frecvența, granularitatea și perioada de păstrare se stabilesc în funcție de cazul de utilizare: pentru evaluarea consumului zilnic poate fi suficientă transmiterea unor valori agregate, în timp ce diagnosticarea unui defect poate necesita temporar serii de date cu rezoluție ridicată. Această asimetrie – regim normal cu volum redus, regim de diagnosticare cu volum ridicat, activat la cerere – este, de regulă, mai eficientă decât transmiterea permanentă la rezoluție maximă și constituie punctul de plecare al calculului din secțiunea următoare.

7.3.3. Criterii pentru distribuirea funcțiilor

Distribuirea unei funcții trebuie realizată pornind de la cerințele procesului, nu de la disponibilitatea unui anumit produs software. Pentru fiecare funcție trebuie analizate următoarele criterii.

Timpul de răspuns. Funcțiile care necesită răspuns în intervale scurte trebuie executate în controler sau în apropierea procesului. Analizele care acceptă întârzieri mai mari pot fi transferate către nivelurile superioare. Criteriul se aplică pe baza bugetului de latență construit în secțiunea 7.1.4, nu pe baza unei aprecieri calitative.

Criticitatea operațională. Dacă indisponibilitatea funcției poate opri procesul sau poate afecta siguranța, aceasta nu trebuie să depindă exclusiv de o conexiune externă.

Volumul datelor. Semnalele cu frecvență ridicată pot fi filtrate, comprimate sau transformate în indicatori înaintea transmiterii. Datele brute pot fi păstrate local pentru diagnosticare și transmise numai la apariția unui eveniment. Consecințele cantitative ale acestei decizii sunt calculate mai jos.

Necesitatea corelării. Analiza unei singure mașini poate fi executată la edge. Compararea mai multor linii necesită un nivel al fabricii, iar analiza mai multor unități poate justifica utilizarea cloudului.

Confidențialitatea și proprietatea datelor. Rețetele, parametrii tehnologici, imaginile procesului sau datele despre clienți pot necesita păstrare locală, anonimizare ori politici speciale de transfer.

Continuitatea funcționării. Trebuie stabilit ce se întâmplă la întreruperea conexiunii, cât timp pot fi păstrate datele local și cum sunt acestea sincronizate după reconectare.

Resursele de calcul. Unele modele necesită resurse care nu sunt disponibile în controler sau în gateway. În acest caz, instruirea modelului poate fi realizată centralizat, iar executarea unei versiuni optimizate poate avea loc la edge.

Administrarea și actualizarea. O funcție distribuită pe sute de componente trebuie să dispună de mecanisme pentru inventariere, configurare, actualizare, revenire la versiunea anterioară și jurnalizare. Acest criteriu este cel mai des subestimat: o funcție care se execută corect pe o componentă poate deveni imposibil de întreținut pe cincizeci.

O regulă practică este executarea funcției cât mai aproape de proces, atât timp cât resursele locale și administrarea permit acest lucru, și transferarea către nivelurile superioare numai a operațiilor care beneficiază efectiv de centralizare sau de scalare.

Calculul necesarului de lățime de bandă – exemplu

Criteriul volumului nu poate fi aplicat prin apreciere. Exemplul următor este un scenariu didactic care arată cum se dimensionează transferul și cât de mult depinde rezultatul de decizia luată la edge.

Date și ipoteze. O linie generează 120 de semnale destinate monitorizării, eșantionate la 10 Hz. Un mesaj individual conține identificatorul activului, identificatorul semnalului, marca temporală, valoarea, unitatea de măsură și indicatorul de calitate; serializat în format text, ocupă aproximativ 180 de octeți, la care se adaugă circa 70 de octeți pentru antetele protocolului de mesagerie și ale stivei de comunicație, deci $L \approx 250$ de octeți. Se neglijează retransmisiile și mesajele de confirmare. Debitul se exprimă în octeți pe secundă și se convertește în biți pe secundă prin înmulțire cu 8.

Formula: $$\boldsymbol{Q = N \times f \times L}$$

Varianta A – un mesaj pentru fiecare valoare.

$$Q = 120 \times 10 \times 250 = 300\,000 \text{ octeți/s} \approx 300 \text{ kB/s} \approx 2{,}4 \text{ Mbit/s}$$

Volumul zilnic: 300 000 × 86 400 ≈ 25,9 GB/zi, adică aproximativ 778 GB pe lună.

Varianta B – gruparea valorilor într-un singur mesaj la fiecare 100 ms. Contextul comun – activul, marca temporală, versiunea schemei – se scrie o singură dată, aproximativ 120 de octeți, iar fiecare valoare se reduce la circa 45 de octeți.

$$Q = (120+120\times45+70)\times10 = 5.590\times10 = 55.900 \text{ octeți/s} \approx 55{,}9 \text{ kB/s} \approx 0{,}45 \text{ Mbit/s}$$

Volumul zilnic scade la aproximativ 4,8 GB/zi, adică o reducere de circa 81 % față de varianta A, fără nicio pierdere de informație: se transmit exact aceleași valori.

Varianta C – gruparea, plus selecția frecvențelor. Numai 20 de semnale justifică 10 Hz; celelalte 100 sunt relevante la 1 Hz. Mesajele se grupează la o secundă.

Numărul de valori transmise: 20 × 10 + 100 × 1 = 300 valori/s

$$Q = (120+300\times45+70)\times1 = 13.690 \text{ octeți/s} \approx 13{,}7 \text{ kB/s} \approx 0{,}11 \text{ Mbit/s}$$

Volumul zilnic devine aproximativ 1,18 GB/zi, o reducere de circa 95 % față de varianta A.

Interpretarea – cele trei variante transportă aceeaşi informaţie utilă pentru monitorizare, dar diferă printr-un factor de peste douăzeci. Debitul absolut nu este problema – 2,4 Mbit/s nu saturează o legătură industrială, însă trei consecinţe indirecte contează: legătura către exterior este, de regulă, partajată cu alte servicii şi nu este dimensionată pentru un flux permanent; traficul şi stocarea în serviciile externe se facturează proporţional cu volumul, conform modelului de furnizare bazat pe resurse măsurate [159]; iar la zece linii identice valorile se înmulţesc cu zece, iar varianta A ajunge la aproximativ 7,8 TB pe lună. Decizia care produce cea mai mare parte a economiei – gruparea mesajelor – nu implică nicio pierdere de date şi se ia integral la nivelul gateway-ului.

Limitele calculului – dimensiunea reală a mesajului depinde de denumirile utilizate în model, de formatul de serializare şi de eventuala comprimare; un format binar poate reduce suplimentar volumul cu un factor semnificativ, cu preţul lizibilităţii la depanare [110]. Nu sunt incluse traficul de confirmare, retransmisiile, restabilirea periodică a sesiunii securizate şi traficul de administrare a dispozitivelor. Nu este luat în calcul nici regimul de diagnosticare, în care rezoluţia se ridică temporar la valoarea maximă şi debitul revine la ordinul de mărime din varianta A. Valorile trebuie confirmate prin măsurare pe o durată reprezentativă, care să includă cel puţin un schimb complet şi o schimbare de lot.

7.3.4. Geamănul digital

Termenul geamăn digital , figura 7.5, este utilizat astăzi pentru realităţi tehnice foarte diferite, de la un model tridimensional până la o replică sincronizată bidirecţional cu instalaţia. Distincţia utilă în practică se face după gradul de integrare a datelor între obiectul fizic şi modelul său: în modelul digital, transferul este manual în ambele sensuri; în umbra digitală, datele circulă automat de la obiectul fizic către model, dar nu şi invers; în geamănul digital propriu-zis, ambele sensuri sunt automate, iar o modificare a modelului se reflectă în comportamentul instalaţiei [200]. Cele mai multe implementări industriale prezentate comercial drept gemeni digitali sunt, conform acestei clasificări, umbre digitale – ceea ce nu le diminuează utilitatea, dar schimbă complet cerinţele de validare şi de securitate.

Indiferent de gradul de integrare, modelul are nevoie de o reprezentare standardizată a activului, prin care identitatea, caracteristicile, documentaţia şi interfeţele acestuia să poată fi regăsite de aplicaţii diferite; structura de administrare a activului defineşte o astfel de reprezentare, organizată pe submodele independente de furnizor [120].

Se consideră o celulă formată dintr-un robot industrial, un dispozitiv de prindere, un transportor, senzori de prezenţă, un automat programabil, un sistem HMI şi echipamente de siguranţă. Geamănul digital poate integra modelul geometric al robotului şi al spaţiului de lucru, cinematica axelor şi limitele de deplasare, geometria dispozitivului de prindere şi a pieselor, amplasarea transportorului şi a

dispozitivelor auxiliare, succesiunea operaţiilor, timpii de ciclu, stările şi alarmele controlerului, contoarele de cicluri şi orele de funcţionare, datele privind sarcina, viteza, curentul sau temperatura axelor şi rezultatele verificărilor de calitate.

Relaţia dintre obiectul fizic şi modelul său, cu cele trei grade de integrare a datelor, este reprezentată în Figura 7.5.

În etapa de proiectare, modelul poate fi utilizat pentru verificarea accesibilităţii, identificarea coliziunilor, analiza timpului de ciclu şi compararea variantelor de amplasare. Înaintea instalării, logica de comandă poate fi verificată într-un mediu de simulare, reducând numărul intervenţiilor necesare în timpul punerii în funcţiune.

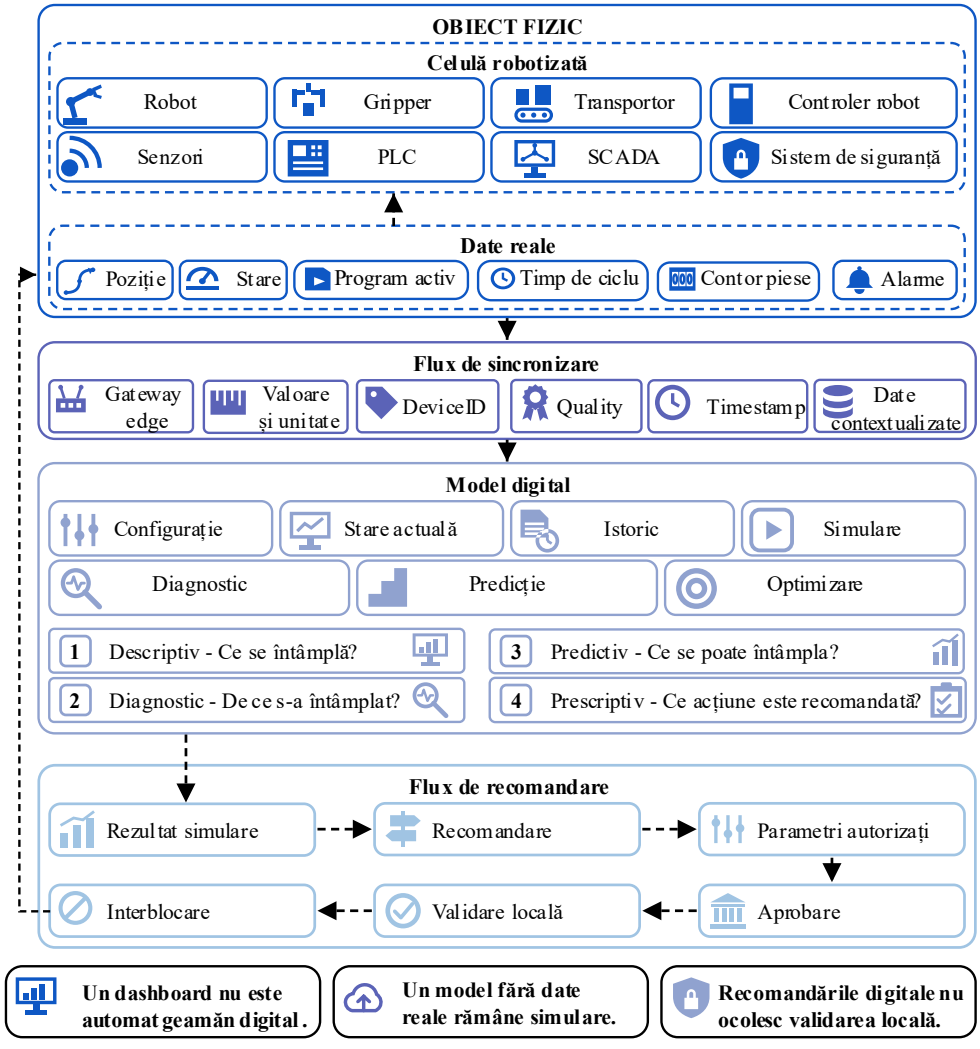


Figura 7.5 – Geamănul digital – sincronizarea dintre obiectul fizic şi modelul digital

După pornirea celulei fizice, datele operaţionale sunt utilizate pentru sincronizarea modelului. Poziţiile, modurile de funcţionare, durata ciclurilor, alarmele şi starea dispozitivului de prindere permit compararea comportamentului real cu cel estimat. Diferenţele persistente pot indica uzură, modificarea proprietăţilor piesei, o calibrare incorectă sau o reprezentare incompletă. Această comparaţie este, de fapt, principala sursă de valoare a modelului în exploatare: nu predicţia în sine, ci divergenţa dintre model şi instalaţie, care semnalează o schimbare pe care niciun prag de alarmă nu o detectează.

În exploatare, geamănul digital poate fi utilizat pentru evaluarea unei noi traiectorii, verificarea unei modificări de program, estimarea efectului schimbării vitezei, analiza unei noi variante de produs, identificarea riscului de coliziune, anticiparea necesarului de mentenanţă, instruirea operatorilor şi pregătirea reconfigurării celulei. Studiile privind gemenii digitali pentru sisteme robotizate identifică aceleaşi categorii de utilizare de-a lungul întregului ciclu de viaţă – proiectare, testare, punere în funcţiune şi reconfigurare operaţională – şi subliniază că utilitatea depinde de completitudinea componentelor modelate: geometrie, cinematică, logică de comandă, senzori şi interacţiunea cu operatorul [201].

Rezultatele obținute în mediul virtual nu trebuie aplicate automat asupra celulei. O traiectorie care nu produce coliziuni în model poate fi periculoasă dacă geometria, poziția piesei, sarcina sau starea dispozitivelor de siguranță nu sunt reprezentate corect. Modificarea trebuie validată progresiv: mai întâi în model, apoi în regim controlat, cu viteză redusă și zonă de lucru restrânsă, și abia în final în condițiile reale de producție. Cu atât mai puțin poate un model să preia funcțiile echipamentelor de siguranță: acestea rămân implementate în componentele dedicate, iar validarea celulei robotizate se realizează pe instalația fizică, prin procedurile impuse de standardele de securitate aplicabile aplicațiilor robotizate [128], indiferent de fidelitatea reprezentării digitale. Succesiunea validării este reprezentată în Figura 7.6.

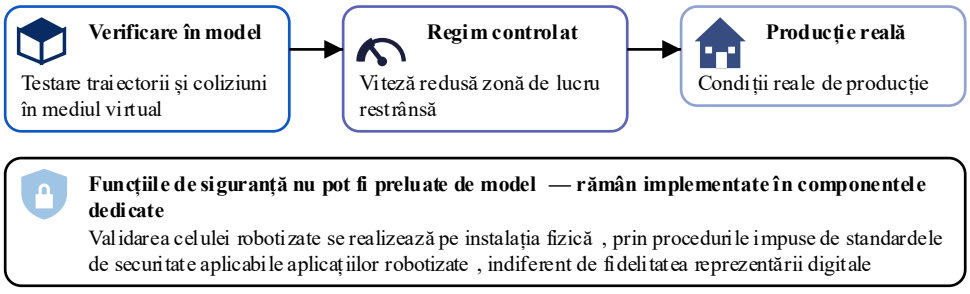


Figura 7.6 – Validarea progresivă: model, regim controlat, producție

Modelul arhitectural stabileşte infrastructura pe care sunt implementate aceste funcţii. Geamănul digital poate utiliza prelucrarea locală pentru actualizarea rapidă

a stării, serverele fabricii pentru corelarea datelor şi serviciile de calcul în cloud pentru simulări complexe sau analiza mai multor sisteme. Secţiunea următoare prezintă lanţul funcţional al platformelor care recepţionează, transformă, stochează şi valorifică aceste date.

7.4. Platforme industriale care furnizează servicii de calcul în cloud

Platformele industriale cloud asigură infrastructura necesară pentru recepţionarea, gestionarea, stocarea şi valorificarea datelor provenite din sisteme IIoT. Acestea nu trebuie înţelese numai ca spaţii de stocare externe sau ca aplicaţii pentru realizarea tablourilor de bord. O platformă completă implementează un lanţ funcţional care începe cu identificarea sursei şi recepţionarea mesajului şi continuă cu rutarea, transformarea, persistenţa, analiza şi integrarea rezultatelor cu aplicaţiile organizaţiei.

Funcţiile unei platforme pot fi furnizate printr-o suită industrială integrată sau pot fi construite prin combinarea mai multor servicii specializate. Implementarea poate fi realizată într-un centru de date propriu, într-un cloud public, într-un cloud privat ori într-o arhitectură hibridă; cele patru variante corespund modelelor de implementare definite pentru serviciile de calcul în cloud [159]. Distribuirea funcţiilor între infrastructura locală şi serviciile externe trebuie stabilită conform criteriilor prezentate în secţiunea 7.3.3.

Platforma nu înlocuieşte controlul local, sistemul SCADA, MES sau ERP. Rolul său este de a conecta sursele, de a administra fluxurile de date şi de a furniza servicii scalabile pentru analiză şi aplicaţii. Interblocările, protecţiile şi comenzile care necesită răspuns determinist rămân în automatul programabil sau în controlerele specializate.

Prezentarea care urmează este organizată pe funcţii, nu pe produse. Motivul este practic: denumirile comerciale, modelele de licenţiere şi grupările de servicii se modifică frecvent, în timp ce rolurile arhitecturale – recepţie, intermediere, rutare, persistenţă, analiză, vizualizare – rămân stabile şi pot fi regăsite, sub alte nume, în oferta oricărui furnizor.

7.4.1. Lanțul funcțional al unei platforme IIoT

Această succesiune reprezintă traseul logic, nu obligaţia ca fiecare funcţie să fie implementată într-un serviciu separat. O platformă poate grupa mai multe funcţii, iar unele operaţii pot fi executate la edge.

Recepţia datelor asigură punctul de intrare în platformă. Mesajele pot proveni de la gateway-uri industriale, aplicaţii SCADA, servere OPC UA, calculatoare industriale sau dispozitive capabile să comunice direct prin protocoalele acceptate.

Intermedierea mesajelor separă producătorii datelor de aplicaţiile care le consumă. Într-un model de publicare–abonare, sursa publică informaţia într-un

subiect de mesagerie, iar una sau mai multe aplicații se abonează la subiectele relevante [177]. Consecința arhitecturală a acestei separări este că adăugarea unui nou consumator nu impune nicio modificare la sursă – proprietate esențială într-o instalație în care sursele sunt echipamente greu accesibile.

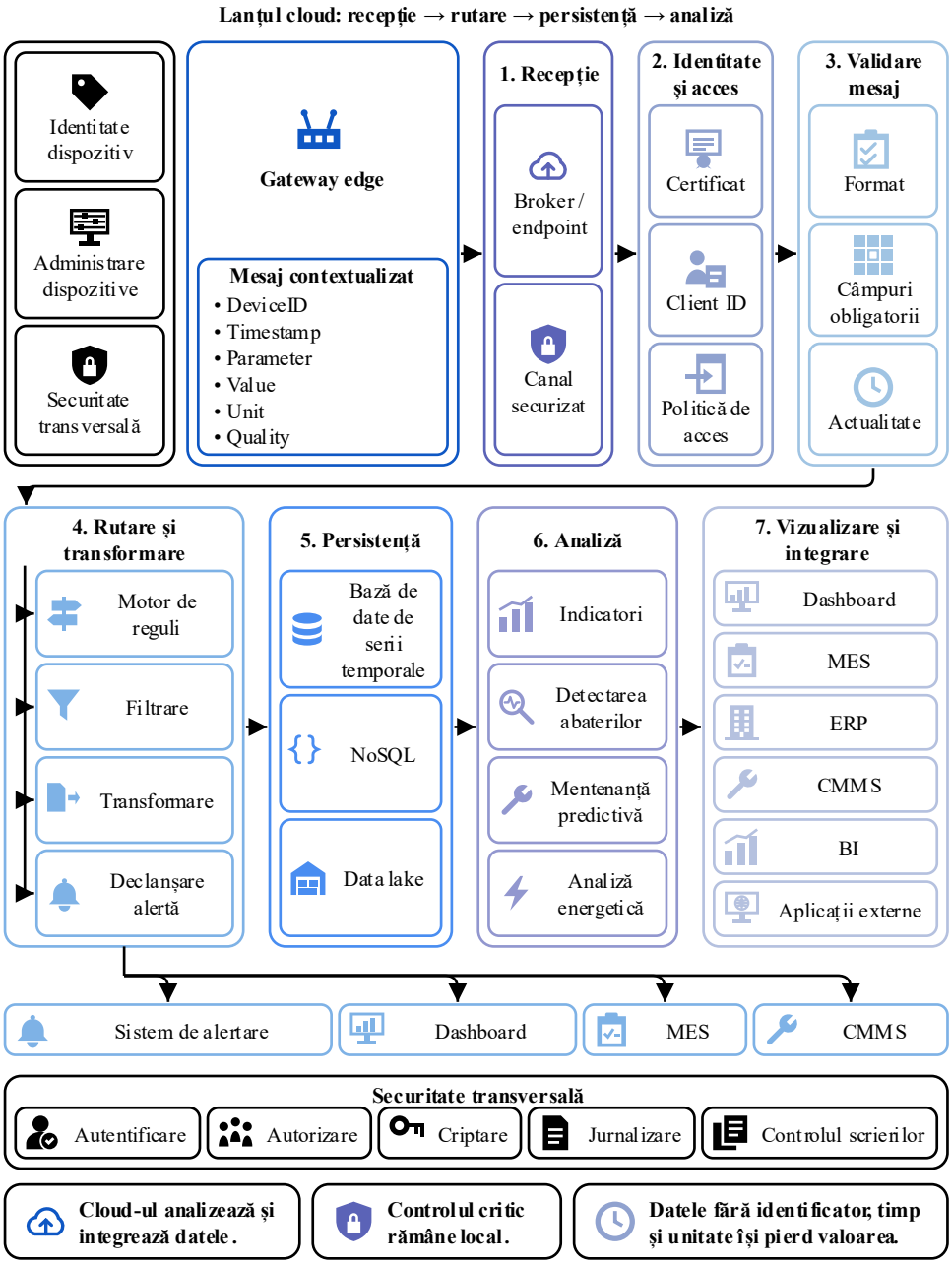


Figura 7.7 – Lanțul funcțional al serviciilor de calcul în cloud

Datele provin de la o sursă industrială și trec printr-un gateway industrial, apoi sunt transportate în condiții de securitate. După recepție și intermediere, acestea sunt direcționate și transformate, apoi stocate pentru a fi păstrate în timp. În continuare, datele sunt analizate și utilizate pentru vizualizare și integrare.

Rutarea și transformarea stabilesc destinația mesajului și forma în care acesta va fi transmis. Un motor de reguli poate filtra datele, poate selecta anumite câmpuri, poate adăuga informații contextuale și poate trimite același mesaj către mai multe servicii.

Persistența păstrează datele pe perioadele necesare utilizării lor. Alegerea mecanismului de stocare depinde de tipul datelor, frecvența actualizării, modul de interogare și durata de păstrare.

Analiza transformă datele în indicatori, alerte, estimări sau recomandări. Aceasta poate fi executată imediat asupra fluxului recepționat sau ulterior, asupra datelor istorice.

Lanțul complet, cu funcțiile transversale reprezentate separat, este redat în Figura 7.7, iar rolurile funcționale și informațiile gestionate de fiecare verigă sunt detaliate în Tabelul **Eroare! Fără sursă de referință.**.

Vizualizarea și integrarea prezintă rezultatele utilizatorilor și le transmit către aplicații precum MES, ERP, CMMS sau alte sisteme organizaționale.

Administrarea dispozitivelor și securitatea sunt funcții transversale. Acestea se aplică întregului lanț și includ identitatea dispozitivelor, certificatele, politicile de acces, inventarierea, monitorizarea conexiunilor și administrarea configurațiilor.

Tabelul 7.4 – Rolurile funcționale ale unei platforme IIoT

Funcție	**Rol principal**	**Exemple de informații gestionate**
Recepție	acceptarea conexiunilor și a mesajelor	identificator client, protocol, subiect, payload
Administrarea dispozitivelor	evidența identității și a stării surselor	certificat, versiune, configurație, ultima conectare
Intermediere	distribuirea mesajelor către consumatori	publicare, abonare, nivel de calitate a serviciului
Rutare și transformare	selectarea, validarea și modificarea mesajelor	reguli, filtre, conversii, versiunea schemei
Persistență	păstrarea datelor pentru interogare și analiză	valori temporale, evenimente, fișiere, configurații
Analiză	detectarea situațiilor relevante și calcularea rezultatelor	praguri, indicatori, anomalii, predicții
Vizualizare	prezentarea informației în funcție de utilizator	tendințe, alarme, indicatori, comparații
Integrare	schimbul de informații cu alte aplicații	API, evenimente, comenzi, rapoarte
Securitate și audit	protejarea accesului și înregistrarea operațiilor	identitate, permisiuni, jurnale, trasabilitate

Arhitecturile industriale prezentate de Veneri şi Capasso [202] separă în mod similar conectivitatea, distribuirea fluxurilor, stocarea seriilor temporale, registrul activelor şi funcţiile de analiză. Produsele şi serviciile utilizate pentru implementarea acestor funcţii se modifică în timp, însă rolurile arhitecturale rămân relativ stabile.

7.4.2. Recepţia datelor şi administrarea dispozitivelor

Punctul de recepţie trebuie să gestioneze simultan conectivitatea, identitatea şi volumul mesajelor. Acceptarea unei conexiuni nu este suficientă pentru a demonstra că sursa este autorizată să publice orice informaţie. Identitatea clientului trebuie verificată, iar drepturile sale trebuie limitate la operaţiile şi subiectele necesare; cerinţele tehnice de securitate pentru componentele sistemelor de automatizare tratează separat identificarea şi autentificarea, pe de o parte, şi controlul utilizării, pe de altă parte [156]; distincţia este reprezentată în Figura 7.8.

Într-o implementare bazată pe MQTT, gateway-ul utilizează adresa punctului terminal al platformei, un identificator unic al clientului, un certificat sau alte credenţiale acceptate, un set de subiecte în care poate publica sau la care se poate abona, parametrii conexiunii securizate, nivelul de calitate a serviciului şi politica pentru reconectare şi retransmitere [177].

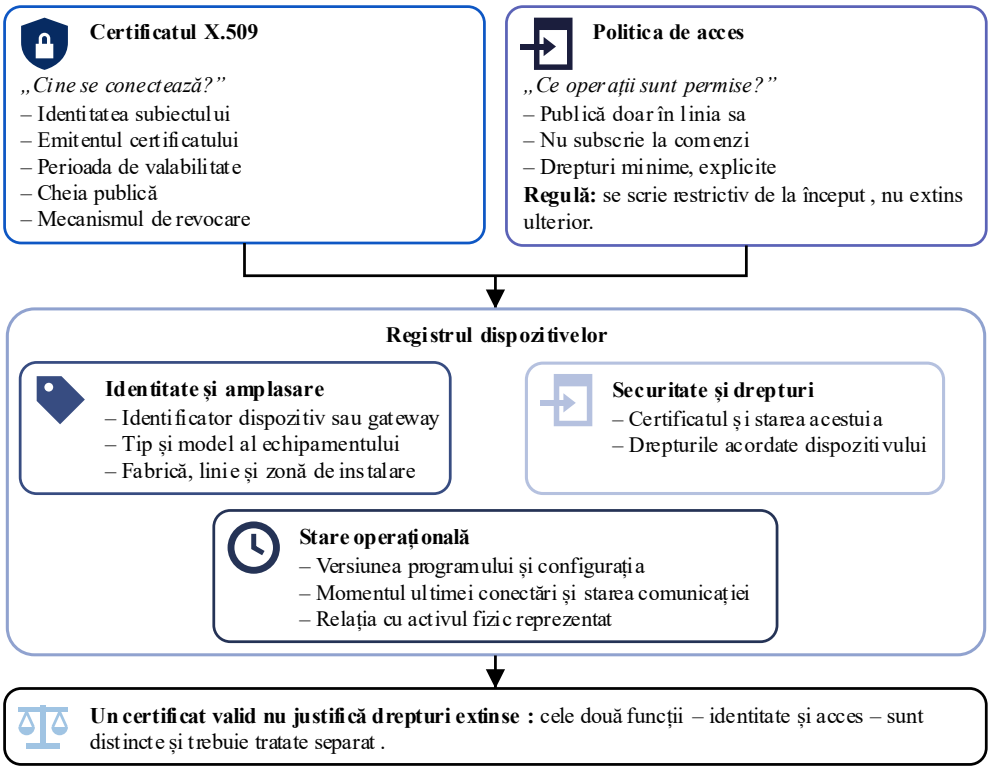


Figura 7.8 – Certificat X.509 vs. politică de acces şi registrul dispozitivelor

Certificatul X.509 poate fi utilizat pentru autentificarea dispozitivului. Formatul este standardizat şi include, alături de cheia publică, identitatea subiectului, emitentul, perioada de valabilitate şi extensiile care limitează utilizarea cheii, precum şi mecanismele prin care un certificat poate fi revocat înainte de expirare [203]. Politica asociată stabileşte acţiunile pe care dispozitivul le poate executa. Cele două funcţii trebuie delimitate: certificatul răspunde întrebării „cine se conectează?", iar politica de acces răspunde întrebării „ce operaţii sunt permise?". Documentaţia AWS IoT Core descrie aceeaşi separare între comunicaţia securizată cu certificate X.509, intermedierea mesajelor şi motorul de reguli [204].

Delimitarea are o consecinţă practică frecvent ignorată: un certificat valid nu justifică drepturi extinse. Un gateway care publică datele unei singure linii nu trebuie să poată publica în subiectele altei linii şi nu trebuie să se poată abona la subiectele de comandă. Politica se scrie restrictiv de la început, pentru că extinderea ei ulterioară este o operaţie controlată, în timp ce restrângerea unei politici permisive, după ce zeci de dispozitive funcţionează pe ea, devine un proiect în sine.

Registrul dispozitivelor păstrează informaţiile necesare administrării surselor conectate: identificatorul dispozitivului sau al gateway-ului, tipul şi modelul echipamentului, fabrica, linia şi zona în care este instalat, certificatul şi starea acestuia, versiunea programului, configuraţia aplicată, momentul ultimei conectări, starea comunicaţiei, drepturile acordate şi relaţia cu activul fizic reprezentat. Menţinerea acestui inventar nu este o formalitate administrativă: programele de securitate pentru sistemele industriale îl tratează ca element de bază, întrucât un activ neinventariat nu poate fi nici actualizat, nici retras din exploatare în mod controlat [205].

Identitatea clientului de comunicaţie nu trebuie confundată cu identitatea activului industrial. Un singur gateway poate publica date pentru mai multe echipamente, iar un echipament poate avea mai multe surse de date. Modelul trebuie să permită diferenţierea dintre dispozitivul care transmite mesajul, activul observat şi subsistemul sau semnalul la care se referă valoarea. Specificaţia Sparkplug tratează explicit această problemă, definind o ierarhie de subiecte cu roluri distincte pentru nodul de margine şi pentru dispozitivele aflate în spatele lui, precum şi mesaje dedicate pentru anunţarea conectării şi a deconectării, astfel încât starea fiecărei surse să fie cunoscută de consumatori fără interogare suplimentară [110], [206].

Ultimul element merită subliniat. Într-un model de publicare–abonare, absenţa mesajelor este ambiguă: sursa poate fi oprită, poate fi deconectată sau poate să nu aibă valori de raportat. Un mecanism explicit de anunţare a stării transformă această ambiguitate într-o informaţie verificabilă, iar tabloul de bord poate distinge între „valoare constantă" şi „sursă indisponibilă" – distincţie esenţială, pentru că a doua situaţie este cea care necesită intervenţie.

La întreruperea conexiunii, datele importante sunt păstrate temporar la edge. După reconectare, acestea sunt retransmise cu mărcile temporale originale.

Platforma trebuie să poată diferenția mesajele produse în momentul curent de mesajele recuperate ulterior și să trateze duplicatele fără înregistrări sau acțiuni repetate necontrolat.

7.4.3. Rutarea, transformarea și contextualizarea mesajelor

Brokerul MQTT recepționează datele, însă nu stabilește singur modul în care acestea sunt utilizate. Această responsabilitate revine regulilor de rutare și serviciilor de prelucrare.

O regulă poate utiliza subiectul în care a fost publicat mesajul, identificatorul clientului, tipul evenimentului, valorile din payload, fabrica, linia sau echipamentul, nivelul de severitate, versiunea schemei și momentul producerii evenimentului.

De exemplu, mesajele publicate în subiectul destinat telemetriei pot fi trimise către o bază de date pentru serii temporale, alarmele pot fi transmise către un serviciu de notificare, iar rezumatele de producție pot fi trimise către MES. Motoarele de reguli ale platformelor cloud pot filtra și îmbogăți mesajele și le pot direcționa către servicii de stocare sau de procesare. În AWS IoT Core, regulile sunt evaluate pe baza fluxului de subiecte MQTT și pot transmite rezultatul către servicii precum DynamoDB sau sisteme de stocare a obiectelor [207].

Eficacitatea acestui mecanism depinde direct de o decizie luată înainte: convenția de denumire a subiectelor. O ierarhie construită de la general la particular – organizație, fabrică, linie, echipament, tip de mesaj – permite abonarea selectivă și scrierea unor reguli stabile, în timp ce o denumire plată sau inconsecventă obligă la filtrarea în aplicație a unor mesaje care nu ar fi trebuit recepționate. Convenția trebuie stabilită o singură dată, la începutul proiectului, pentru că modificarea ei ulterioară afectează simultan toate sursele și toți consumatorii. Structura de referință adoptată în această carte este definită în secțiunea 6.2.8; exercițiul din secțiunea 7.5.4 aplică o variantă proprie, declarată acolo.

Transformarea poate include selectarea câmpurilor relevante, conversia unităților de măsură, normalizarea denumirilor, validarea tipurilor și a domeniilor, calcularea unor valori derivate, adăugarea identificatorilor activului și procesului, eliminarea datelor sensibile și conversia între versiuni ale modelului de date.

Mesajele trebuie să respecte un contract de date definit. Pentru fiecare câmp sunt stabilite denumirea, tipul, unitatea de măsură, semnificația, caracterul obligatoriu și regulile de validare. Un mesaj industrial poate conține identificatorul dispozitivului care transmite, identificatorul activului observat, marca temporală a măsurării, marca temporală a recepției, valorile și unitățile de măsură, calitatea datelor, starea echipamentului, identificatorul operației sau al lotului, versiunea schemei mesajului și identificatorul unic al mesajului.

Cele două mărci temporale nu sunt redundante. Diferența dintre ele măsoară întârzierea reală a lanțului și permite distingerea datelor curente de cele

retransmise după o întrerupere; un mesaj cu marcă de măsurare veche de patruzeci de minute şi marcă de recepţie curentă este o valoare recuperată, nu o valoare recentă, iar tratarea lui ca valoare curentă ar declanşa alarme false sau ar deplasa incorect o medie.

Contextualizarea realizată în platformă trebuie coordonată cu MES şi cu modelele definite în secţiunea 7.2. Platforma poate adăuga informaţii despre activ, amplasare şi tipul semnalului, dar nu trebuie să inventeze contextul ordinului de producţie atunci când sursa de referinţă pentru această informaţie este MES. Regula generală este că fiecare câmp adăugat pe traseu trebuie să aibă un proprietar declarat; un câmp completat de două componente diferite, după reguli diferite, produce inconsistenţe care se descoperă abia la prima analiză comparativă.

Versiunea schemei este necesară deoarece structura mesajelor se modifică pe durata exploatării. Regula practică de compatibilitate este următoarea: adăugarea unui câmp opţional nu trebuie să blocheze aplicaţiile existente, care îl ignoră; eliminarea unui câmp, modificarea tipului sau schimbarea semnificaţiei unui câmp existent reprezintă modificări incompatibile şi impun incrementarea versiunii majore, o perioadă de funcţionare în paralel a celor două versiuni şi actualizarea coordonată a consumatorilor. Cazul cel mai periculos nu este eliminarea unui câmp – care produce o eroare vizibilă imediat, ci schimbarea tăcută a unităţii de măsură sau a semnificației: mesajul rămâne valid din punct de vedere structural, iar eroarea se propagă în indicatori fără niciun semnal.

7.4.4. Persistența datelor industriale

Nu toate datele trebuie păstrate în acelaşi sistem. Selectarea mecanismului de persistenţă se realizează în funcţie de structura informaţiei şi de modul în care aceasta va fi interogată; corespondenţa dintre categoriile de date industriale şi mecanismele adecvate este sintetizată în Tabelul 7.5.

Tabelul 7.5 – Corelarea datelor industriale cu mecanismele de stocare

Tip de informație	Mecanism adecvat	Utilizare dominantă
Valori măsurate periodic	bază de date pentru serii temporale sau sistem istoric	tendințe, agregări, monitorizare și diagnosticare
Evenimente și alarme	depozit de evenimente sau bază NoSQL	căutare, corelare și audit
Configurații și date de referință	bază de date relațională	administrare, validare și integrare
Mesaje semistructurate	bază de date NoSQL	starea dispozitivelor și aplicații flexibile
Fișiere, imagini și date brute	stocare de obiecte sau lac de date	arhivare, analiză avansată și instruirea modelelor
Rezultate agregate	bază analitică sau depozit de date	indicatori, raportare și comparații între unități

Bazele de date pentru serii temporale sunt potrivite pentru valori asociate unui moment şi unui activ: temperatura, presiunea, viteza, curentul, vibraţiile sau

consumul energetic. Acestea facilitează interogările pe intervale, agregarea temporală şi calcularea tendinţelor.

Bazele de date NoSQL sunt potrivite pentru mesaje semistructurate, stări ale dispozitivelor şi înregistrări cu seturi variabile de atribute. Flexibilitatea structurii nu elimină necesitatea unui model de date şi a unor identificatori stabili.

Bazele de date relaţionale sunt adecvate pentru informaţii structurate şi relaţii bine definite: configuraţii, utilizatori, produse, reţete şi înregistrări tranzacţionale.

Stocarea obiectelor sau lacul de date poate fi utilizată pentru fişiere voluminoase, imagini, înregistrări brute, arhive şi seturi pregătite pentru analiza ulterioară.

Sistemul istoric industrial rămâne relevant pentru valorile operaţionale apropiate de SCADA. Transferarea datelor către cloud nu obligă înlocuirea istoricului local; cele două sisteme pot utiliza perioade de păstrare şi niveluri de agregare diferite. Menţinerea istoricului local are şi o funcţie de continuitate: el este sursa care rămâne disponibilă atunci când legătura externă lipseşte, exact în situaţiile în care este cel mai probabil să fie consultat.

Datele pot fi repartizate între trasee cu cerinţe diferite. Traseul rapid păstrează informaţia recentă necesară monitorizării şi detectării abaterilor, iar traseul lent păstrează volume mai mari pentru procesare în lot şi analiză istorică. Separarea dintre fluxul rapid şi cel lent este utilizată în arhitecturile de date pentru a combina analiza cu latenţă redusă şi prelucrarea completă a datelor istorice [208].

Pentru datele provenite de la dispozitive, o structură frecventă utilizează identificatorul sursei drept cheie de partiţie şi marca temporală drept cheie de sortare. Astfel, valorile aceluiaşi dispozitiv pot fi recuperate şi ordonate temporal. Serviciile DynamoDB permit interogarea înregistrărilor care au aceeaşi cheie de partiţie şi ordonarea lor după cheia de sortare [209].

O structură formată numai din identificatorul dispozitivului şi marca temporală este adecvată pentru demonstrarea traseului datelor. Într-o implementare industrială, proiectarea cheilor trebuie reevaluată în funcţie de numărul dispozitivelor, frecvenţa mesajelor, distribuţia încărcării şi interogările necesare. Concentrarea unui volum foarte mare într-o singură partiţie poate limita performanţa, iar soluţia uzuală este includerea unui element suplimentar în cheia de partiţie – de exemplu ziua sau intervalul orar, astfel încât încărcarea să se distribuie, cu preţul unor interogări puţin mai complexe pe intervale lungi.

Dimensionarea stocării. Volumul rezultă direct din calculul realizat în secţiunea 7.3.3. Pentru varianta C – 300 de valori pe secundă, la aproximativ 60 de octeţi per înregistrare stocată, inclusiv indexul, rezultă circa 18 kB/s, adică aproximativ 1,55 GB pe zi şi 566 GB pe an pentru o singură linie. Valoarea nu este mare în sine, dar se multiplică cu numărul liniilor şi cu numărul de ani de păstrare, iar costul stocării

în serviciile externe se facturează recurent. Acesta este motivul pentru care politica de păstrare nu poate fi decisă după punerea în funcţiune.

Politica de păstrare trebuie stabilită înaintea colectării. Pentru fiecare categorie de date se precizează rezoluţia iniţială, perioada păstrării în formă detaliată, agregările care trebuie calculate, perioada păstrării agregatelor, condiţiile de arhivare, cerinţele de ştergere, responsabilitatea pentru copiile de siguranţă şi condiţiile de restaurare.

O politică uzuală păstrează datele la rezoluţie completă câteva săptămâni, mediile la un minut câteva luni şi mediile orare câţiva ani, cu arhivarea seturilor brute numai pentru intervalele în care s-a produs un incident. Alegerea perioadelor nu este arbitrară: ea trebuie corelată cu durata reală a analizelor efectuate – o analiză de defect se realizează, de regulă, în zilele următoare evenimentului, în timp ce o comparaţie între campanii de producţie se realizează după luni.

Păstrarea nelimitată a tuturor datelor brute măreşte costul fără a garanta utilitatea lor. Datele trebuie colectate la rezoluţia justificată de cazul de utilizare şi păstrate atât timp cât sunt necesare tehnic, contractual sau legal. Cerinţele legale şi contractuale trebuie identificate explicit, pentru că ele stabilesc atât o durată minimă – de exemplu, pentru trasabilitatea produselor [198], cât şi, în cazul datelor cu caracter personal, o durată maximă şi o obligaţie de ştergere.

7.4.5. Analiza, vizualizarea şi integrarea rezultatelor

Analiza poate fi realizată asupra fluxului curent sau asupra istoricului. Prelucrarea fluxului este adecvată pentru detectarea depăşirilor, a modificărilor rapide şi a combinaţiilor de evenimente care necesită notificare imediată. Prelucrarea în lot este adecvată pentru rapoarte, comparaţii între perioade, identificarea tendinţelor şi instruirea modelelor.

Rezultatele pot avea niveluri diferite de elaborare: o valoare filtrată sau agregată, o condiţie logică, o alarmă sau notificare, un indicator operaţional, o clasificare a stării, o estimare a degradării, o probabilitate de defectare, o recomandare pentru intervenţie sau un scenariu de optimizare. Această succesiune corespunde, în domeniul monitorizării stării echipamentelor, unui lanţ de prelucrare standardizat, care separă achiziţia, prelucrarea semnalului, detectarea stării, evaluarea sănătăţii, prognoza şi consilierea [42]. Distanţa dintre primul şi ultimul element al listei nu este numai tehnică, ci şi de responsabilitate: o valoare agregată poate fi verificată de oricine reface calculul, în timp ce o probabilitate estimată de un model necesită cunoaşterea datelor de instruire, a ipotezelor şi a condiţiilor în care estimarea încetează să fie validă.

Un rezultat analitic nu trebuie transformat automat într-o comandă asupra procesului. Dacă analiza indică necesitatea modificării unui parametru, recomandarea este transmisă către sistemul şi persoana responsabile. Aplicarea se realizează printr-o interfaţă autorizată, cu verificarea limitelor, a stării instalaţiei şi a

interblocărilor locale. Regula are două motive independente. Primul este de siguranță: modelul nu cunoaște starea completă a instalației în momentul aplicării. Al doilea este de securitate: o cale prin care un rezultat calculat extern devine comandă asupra procesului constituie, prin construcție, o cale de atac dinspre rețeaua de întreprindere către rețeaua industrială [25], tratată în Capitolul 8.

Tabloul de bord trebuie proiectat în funcție de utilizator și de decizia pe care acesta trebuie să o ia. Operatorul are nevoie de starea curentă și de abateri, personalul de mentenanță urmărește degradarea și istoricul intervențiilor, iar conducerea utilizează indicatori agregați. Principiile de proiectare a interfețelor de operare pornesc de la aceeași cerință: afișarea trebuie să susțină conștientizarea situației și decizia, nu să reproducă schema instalației [162], [160]. Afișarea acelorași grafice tuturor utilizatorilor nu reprezintă contextualizare, ci absența ei.

Un test simplu al utilității unui element vizual este întrebarea: ce decizie se schimbă în funcție de valoarea afișată? Un grafic care nu poate primi un răspuns la această întrebare ocupă spațiu și atenție fără a le justifica [47].

Pentru fiecare element vizual trebuie cunoscute sursa datelor, perioada analizată, unitatea de măsură, frecvența actualizării, momentul ultimei valori, starea calității datelor, echipamentul și fabrica, regula de calcul și pragurile utilizate. Momentul ultimei valori și starea calității merită afișate, nu doar cunoscute: un indicator care rămâne pe ecran după oprirea sursei este mai periculos decât un indicator absent, pentru că sugerează o normalitate care nu mai este verificată.

Integrarea cu MES, ERP și CMMS trebuie realizată prin interfețele definite în secțiunea 7.2.4. Platforma poate transmite către MES o abatere asociată unui activ, către CMMS o solicitare de evaluare și către ERP un rezultat agregat privind consumul. Accesul direct și necontrolat la bazele de date interne ale acestor aplicații trebuie evitat.

7.4.6. Criterii pentru alegerea platformei

Alegerea unei platforme trebuie pornită de la cazul de utilizare și de la arhitectura existentă. Lista funcțiilor comerciale nu demonstrează că soluția poate fi integrată și operată în condițiile fabricii.

Conectivitatea industrială. Se verifică protocoalele, conectorii, compatibilitatea cu serverele OPC UA, integrarea cu SCADA și posibilitatea utilizării gateway-urilor existente.

Funcționarea la edge. Platforma trebuie evaluată în raport cu filtrarea locală, stocarea temporară, reluarea transmisiei și administrarea aplicațiilor instalate în fabrică.

Modelul de date. Trebuie analizată capacitatea de a reprezenta active, ierarhii, relații, unități de măsură, rețete, stări și versiuni.

Administrarea dispozitivelor. Sunt importante inventarierea, identitatea, starea conexiunii, configurarea, actualizarea și retragerea sigură din exploatare [205].

Securitatea. Se verifică autentificarea, autorizarea granulară, administrarea certificatelor, criptarea, jurnalizarea și integrarea cu sistemul organizației pentru gestionarea identităților [156].

Disponibilitatea. Trebuie stabilit comportamentul la întreruperea conexiunii, perioada de funcționare autonomă, mecanismul de recuperare și obiectivele pentru restaurarea serviciului.

Scalabilitatea și performanța. Evaluarea trebuie să utilizeze numărul estimat de dispozitive, frecvența mesajelor, dimensiunea payloadului, numărul utilizatorilor și tipurile de interogări – mărimi care rezultă din calculele prezentate în secțiunile 7.3.3 și 7.4.4, nu din estimări generale.

Integrarea aplicațiilor. Sunt analizate interfețele API, mesageria, conectarea la MES, ERP și CMMS, precum și exportul datelor către alte medii.

Portabilitatea. Datele, modelele și aplicațiile trebuie să poată fi exportate într-un format utilizabil. Standardele pentru cloud disting portabilitatea datelor de portabilitatea aplicațiilor și de interoperabilitatea dintre servicii; cele trei nu se obțin simultan și nu decurg una din alta [53]. Întrebarea practică nu este dacă exportul este posibil, ci ce se poate face efectiv cu datele exportate: o arhivă lipsită de model de date, de ierarhia activelor și de definițiile indicatorilor conține valori, nu informație reutilizabilă.

Administrarea operațională. Platforma trebuie să permită monitorizarea serviciilor, urmărirea erorilor, controlul versiunilor, automatizarea configurării și auditarea modificărilor.

Costul total. Analiza include licențele, numărul dispozitivelor, volumul mesajelor, stocarea, interogările, traficul de ieșire, conectorii, dezvoltarea, instruirea și operarea. În modelul de furnizare bazat pe resurse măsurate, costul crește odată cu utilizarea [159]; o arhitectură care transmite date brute permanent produce un cost recurent proporțional cu volumul, în timp ce filtrarea la edge îl reduce o singură dată, prin proiectare.

Localizarea și proprietatea datelor. Trebuie cunoscute regiunile de stocare, regulile pentru transfer, drepturile asupra datelor și condițiile de recuperare la încetarea contractului.

O soluție cu numeroase funcții predefinite poate reduce timpul inițial de dezvoltare, dar poate limita personalizarea. O arhitectură construită din servicii independente oferă flexibilitate, însă necesită integrare, administrare și competențe suplimentare. Alegerea trebuie justificată prin cerințele aplicației și prin costul întregului ciclu de viață, nu prin comparația listelor de funcții.

7.4.7. Exemple de platforme și evoluția serviciilor

Platformele comerciale pot fi grupate în două categorii principale. Prima este reprezentată de suitele industriale care integrează conectivitatea, modelarea activelor, analiza şi dezvoltarea aplicaţiilor. A doua este reprezentată de serviciile cloud compozabile, prin care organizaţia selectează separat intermedierea mesajelor, motorul de reguli, stocarea, analiza şi vizualizarea. Poziţionarea funcţională a câtorva soluţii reprezentative pentru cele două categorii este prezentată în Tab. 7.6.

Siemens a integrat capabilităţile MindSphere în Insights Hub, ca parte a portofoliului Industrial Operations X. Schimbarea ilustrează evoluţia denumirilor şi a poziţionării comerciale, fără eliminarea rolurilor de conectare şi de valorificare a datelor operaţionale [210].

AVEVA poziţionează CONNECT ca platformă deschisă, neutră faţă de furnizor şi găzduită în cloud, destinată integrării datelor, modelelor, aplicaţiilor şi funcţiilor analitice industriale [211].

Tabelul 7.6 – Poziționarea funcțională a unor soluții IIoT

Soluție	Accent funcțional	Observație privind utilizarea
Siemens Insights Hub	valorificarea datelor despre active și operațiuni, aplicații industriale și analiză locală sau cloud	relevantă pentru integrarea cu ecosistemul industrial Siemens, dar nu limitată conceptual la acesta
AVEVA CONNECT	gestionarea, contextualizarea și distribuirea datelor industriale	adecvată pentru integrarea datelor operaționale și colaborarea între aplicații și organizații
ThingWorx (până în 2026, PTC ThingWorx)	dezvoltarea și administrarea aplicațiilor IIoT, conectivitate, analiză și experiențe digitale	oferă flexibilitate pentru aplicații personalizate și implementări locale, cloud sau hibride
Servicii cloud compozabile	recepție, mesagerie, reguli, baze de date, analiză și vizualizare selectate separat	permit controlul detaliat al arhitecturii, dar transferă integratorului responsabilitatea pentru asamblare și administrare

ThingWorx oferă capabilităţi pentru conectarea activelor, dezvoltarea aplicaţiilor IIoT, analiză, administrarea dispozitivelor şi realizarea interfeţelor digitale sau de realitate augmentată. Platforma poate fi utilizată în implementări locale, cloud sau hibride, iar în martie 2026 PTC a finalizat vânzarea ei către un fond de investiţii – o ilustrare suplimentară a instabilităţii denumirilor şi a apartenenţei corporative [212].

Serviciile cloud compozabile permit realizarea aceluiaşi lanţ prin asocierea mai multor componente. De exemplu, AWS IoT Core poate asigura recepţia şi intermedierea mesajelor, o regulă poate realiza rutarea, iar DynamoDB poate asigura persistenţa. Alte servicii pot fi adăugate pentru analiză, notificare şi vizualizare.

Tabelul nu reprezintă un clasament. Capabilităţile, denumirile, licenţierea şi disponibilitatea regională a serviciilor se pot modifica. Înaintea unei achiziţii, comparaţia trebuie refăcută pe baza documentaţiei oficiale, a unei probe de concept realizate cu date proprii şi a cerinţelor reale ale organizaţiei. Proba de concept este elementul decisiv: ea arată nu ce poate platforma, ci cât efort presupune integrarea

ei cu instalația existentă – singura mărime pe care documentația comercială nu o comunică.

Traseul generalizat utilizat în continuarea capitolului pornește de la un server OPC UA și continuă către un gateway industrial, unde datele sunt organizate într-un mesaj structurat. Mesajul este transmis prin MQTT securizat, cu utilizarea unui certificat X.509, către platforma cloud, apoi direcționat printr-o regulă de rutare către o bază de date. Datele stocate sunt ulterior utilizate într-un tablou de bord sau într-o aplicație.

În acest traseu, fiecare componentă are o responsabilitate distinctă. Serverul OPC UA expune datele procesului, gateway-ul le selectează și le structurează, MQTT asigură transportul, platforma autentifică sursa și intermediază mesajul, regula stabilește destinația, baza de date păstrează informația, iar aplicația o prezintă utilizatorului. Exercițiul următor utilizează aceste roluri pentru proiectarea completă a arhitecturii unei linii automatizate.

7.5. Exercițiu – Proiectarea unei arhitecturi IIoT pentru o linie de ambalare complet automatizată

Exercițiul urmărește proiectarea sistemică a unei arhitecturi IIoT pentru o linie de ambalare. Cititorul trebuie să stabilească funcțiile care rămân în sistemul local de automatizare, datele care sunt transmise către nivelurile superioare, protocoalele utilizate și modul în care informațiile sunt stocate și valorificate.

Activitatea este un exercițiu de proiectare și documentare, nu o cerință de implementare integrală. Implementarea efectivă a unor fluxuri similare este abordată în mini-proiectele din Capitolul 9.

Linia descrisă în continuare este un scenariu didactic. Valorile parametrilor sunt alese pentru a fi realiste și coerente între ele, astfel încât calculele să poată fi refăcute și verificate, dar nu provin dintr-o instalație existentă. Este aceeași linie utilizată în calculul indicatorului din secțiunea 7.2.3 și în calculul de lățime de bandă din secțiunea 7.3.3; cele trei tratări pot fi citite împreună.

7.5.1. Scenariul tehnologic

Se consideră o linie complet automatizată pentru ambalarea unui produs alimentar în recipiente individuale. Procesul include următoarele operații:

1. detectarea produsului la intrarea pe transportor;
2. poziționarea recipientului în stația de lucru;
3. verificarea greutății;
4. sigilarea ambalajului;
5. aplicarea și verificarea etichetei;
6. inspectarea produsului ambalat;
7. eliminarea produselor neconforme;

8. evacuarea şi numărarea produselor conforme.

Tabelul 7.7 – Parametrii procesului pentru linia de ambalare

Mărime	Valoare	Observație
Timp de ciclu de referință	1,2 s/produs	50 de produse pe minut la viteză nominală
Viteza transportorului	0,25 m/s nominal, reglabilă 0,10–0,35 m/s	acționare prin convertizor de frecvență
Greutate nominală a produsului ambalat	500 g, toleranță ±5 g	criteriu de conformitate
Temperatura de sigilare	valoare prescrisă 175 °C, toleranță ±3 °C	reglare cu revenire în bandă în cel mult 20 s
Program de lucru	trei schimburi a câte 8 ore	pauze planificate de 30 min pe schimb

Parametrii procesului sunt prezentaţi în Tabelul 7.7, iar echipamentele instalate şi interfeţele lor, în Tabelul 7.8.

Funcţiile care influenţează direct desfăşurarea procesului trebuie executate local: secvenţa de ambalare, controlul transportorului, poziţionarea produsului, reglarea temperaturii, interblocările, oprirea de urgenţă şi eliminarea produselor neconforme. Platforma IIoT poate monitoriza şi analiza aceste funcţii, dar nu trebuie să devină o componentă obligatorie a buclelor critice de control.

Tabelul 7.8 – Echipamentele instalate pe linia de ambalare și interfețele acestora

Componentă	Caracteristici relevante	Interfață
Senzori fotoelectrici de prezență (4 buc.)	timp de răspuns ≤ 1 ms	intrare digitală 24 V c.c.
Senzori inductivi de poziție (3 buc.)	detectarea poziției stațiilor	intrare digitală 24 V c.c.
Celulă de sarcină	domeniu 0–1 000 g, precizie ±0,5 g, 10 măsurări/s	4–20 mA sau Modbus TCP
Traductor de temperatură Pt100	domeniu 0–300 °C, precizie ±1 °C, constantă de timp ≈ 2 s	intrare analogică
Contor de energie	rezoluție 0,01 kWh, actualizare la 1 s	Modbus TCP
Sistem de inspecție vizuală	rezultat conform/neconform și cod de defect	intrare digitală și interfață de date
Actuatoare pneumatice de respingere și poziționare	timp de acționare ≈ 80 ms	ieșire digitală
Mecanism de etichetare	verificarea prezenței și a lizibilității etichetei	intrare digitală și interfață de date
Automat programabil	timp de ciclu 10 ms	rețea industrială Ethernet
Sistem HMI local, sistem SCADA, gateway industrial	operare, supraveghere, achiziție și transfer	rețea industrială Ethernet

Trei constrângeri temporale rezultă direct din datele de mai sus şi trebuie verificate de cititor înainte de orice decizie de arhitectură. Respingerea unui produs neconform trebuie executată în intervalul dintre inspecţie şi punctul de evacuare, adică în mai puţin de 1,2 s la viteză nominală, dar cu marja redusă de timpul de acţionare al actuatorului; decizia aparţine automatului programabil. Reglarea

temperaturii de sigilare admite întârzieri de ordinul secundelor și rămâne, de asemenea, locală. Calculul indicatorilor de producție și analiza tendințelor admit întârzieri de ordinul secundelor sau minutelor și pot fi transferate către platformă.

7.5.2. Cerințele sistemului

Cerințele sunt formulate astfel încât fiecare să poată fi verificată. O cerință care nu poate fi testată nu poate fi nici recepționată.

Cerințe funcționale de control și supraveghere

1. Succesiunea celor opt operații este executată automat, cu interblocările și condițiile de pornire verificate local, la fiecare ciclu.
2. Operatorul poate urmări starea liniei prin HMI local și prin SCADA, poate confirma pregătirea liniei și poate acționa oprirea controlată și oprirea de urgență.
3. Alarmele și evenimentele sunt înregistrate cu marcă temporală, cod, categorie și durată, iar clasificarea cauzelor de oprire este disponibilă operatorului la momentul confirmării.
4. Numărul produselor conforme și neconforme este contorizat local, iar contoarele nu se pierd la repornirea sistemului de supraveghere.

Cerințe de monitorizare și date

5. Temperatura de sigilare este raportată la 1 Hz; greutatea este raportată pentru fiecare produs cântărit; viteza transportorului și contoarele, la 1 Hz; consumul energetic, la 0,1 Hz.
6. Fiecare valoare transmisă poartă identificatorul activului, marca temporală a măsurării, unitatea de măsură și indicatorul de calitate.
7. Datele sunt asociate produsului, lotului și intervalului de producție, astfel încât orice valoare să poată fi atribuită unui lot fără corelare manuală.
8. Latența totală de la producerea evenimentului până la disponibilitatea valorii în baza de date a platformei nu depășește 2 s în regim normal, măsurată conform metodei din secțiunea 7.1.4.

Cerințe de valorificare

9. Sunt calculați și afișați: producția realizată pe interval, proporția produselor neconforme, evoluția temperaturii de sigilare, abaterea greutății față de valoarea prescrisă, durata ciclului, consumul energetic raportat la producție, durata opririlor și distribuția alarmelor pe categorii.
10. Indicatorul de eficacitate globală a echipamentelor este calculat pe schimb, cu definițiile stabilite în secțiunea 7.2.3, iar componentele sale sunt afișate separat.

Cerințe de continuitate

11. La întreruperea conexiunii externe, producția continuă fără nicio degradare a funcțiilor de control, supraveghere și siguranță.

12. Gateway-ul păstrează local datele nelivrate cel puțin 24 de ore la debitul nominal de raportare și le retransmite după reconectare, cu mărcile temporale originale.
13. Datele retransmise sunt marcate ca recuperate și pot fi distinse de cele curente în toate aplicațiile consumatoare.
14. Retransmiterea nu produce înregistrări duplicate; fiecare mesaj poartă un identificator unic verificat la destinație.

Cerințe de securitate

15. Gateway-ul se autentifică la platformă cu identitate proprie și are drept de publicare numai în subiectele liniei proprii; nu are drept de abonare la subiecte de comandă.
16. Toate transferurile către exterior sunt protejate criptografic, iar operațiile relevante sunt jurnalizate.
17. Nicio comandă provenită din platformă nu poate ajunge la nivelul de control fără validare locală explicită.

Cititorul trebuie să diferențieze între datele necesare controlului, datele utilizate pentru supraveghere și datele transferate pentru analiză. Valoarea instantanee a unui senzor de poziție este necesară automatului programabil la fiecare ciclu de 10 ms, în timp ce platforma are nevoie numai de numărul opririlor, de durata acestora și de momentul apariției unei abateri. Cerința 5 este consecința directă a acestei distincții: ea limitează volumul transmis la valorile din planul de raportare din Tabelul 7.10 (aproximativ cinci valori pe secundă), aplicând aceleași principii ca varianta C din secțiunea 7.3.3, dar la scara acestei linii, nu la cea a exemplului de 120 de semnale.

7.5.3. Stiva tehnologică de referință

Exercițiul se realizează pe o stivă declarată explicit, astfel încât configurațiile, mesajele și rezultatele să poată fi reproduse și verificate. Stiva de referință este alcătuită integral din componente care pot fi instalate local, fără cont la un furnizor de servicii cloud și fără costuri variabile:

- *PLC*: S7-1500, programat în TIA Portal, cu timp de ciclu de 10 ms;
- *proces*: simulat în Factory I/O, cu semnalele conectate la PLC;
- *expunerea datelor*: serverul OPC UA integrat în automatul programabil;
- *gateway industrial*: Node-RED, instalat pe un calculator industrial sau pe o placă de dezvoltare din rețeaua fabricii;
- *broker MQTT*: Eclipse Mosquitto, cu TLS și autentificare prin certificat;
- *persistență*: InfluxDB, bază de date pentru serii temporale;
- *vizualizare*: Grafana.

Stiva este o alegere de referință, nu o cerință a exercițiului. Cerințele din secțiunea 7.5.2, criteriile de reușită și metoda de validare sunt formulate independent de

produs; numai secţiunile 7.5.4 şi 7.5.5, care conţin identificatori, fişiere de configurare şi interogări concrete, depind de componentele enumerate mai sus. Un cititor care dispune de un alt automat programabil, de un alt broker sau de o altă bază de date poate parcurge integral exerciţiul, transpunând elementele din aceste două secţiuni în echivalentele stivei proprii.

Alegerea acestei stive nu invalidează exemplele cu servicii cloud prezentate în secţiunile 7.4.2, 7.4.3 şi 7.4.7. Rolurile arhitecturale rămân aceleaşi, iar componentele se pot înlocui una cu alta fără modificarea structurii soluţiei. Corespondenţa este prezentată în Tabelul 7.9 şi trebuie citită ca o confirmare a principiului enunţat în secţiunea 7.4: rolurile sunt stabile, produsele sunt interschimbabile.

Migrarea de la o variantă la alta nu este gratuită, dar este delimitată: se modifică adresa punctului terminal, modul de autentificare şi componenta de persistenţă, în timp ce convenţia de subiecte, structura mesajului şi logica de validare rămân neschimbate. Această delimitare este ea însăşi un rezultat al proiectării şi trebuie urmărită de cititor ca obiectiv al exerciţiului.

Tabelul 7.9 – Corespondența rolurilor între stiva de referință și serviciile cloud

Rol arhitectural	Stiva de referință (locală)	Echivalent în serviciile cloud	Ce nu se schimbă la înlocuire
Recepție și intermediere	Mosquitto	AWS IoT Core – broker de mesaje	modelul publicare–abonare, identitatea sursei, subiectele
Administrarea identității	fișier de configurare și listă de control al accesului	registrul de dispozitive și politicile de acces	separarea dintre autentificare și autorizare
Rutare și transformare	fluxuri Node-RED	motorul de reguli al platformei	criteriul de selecție, destinația, contractul de date
Persistență	InfluxDB OSS 2.x	DynamoDB sau bază de date pentru serii temporale	cheia de identificare a sursei și ordonarea temporală
Vizualizare	Grafana	tablou de bord al platformei	panourile, pragurile, indicatorii afișați
Prelucrare la edge	fluxuri Node-RED pe gateway	componentă de edge administrată de platformă	filtrarea, gruparea, stocarea temporară

7.5.4. Convenţia de denumire a subiectelor şi structura mesajelor

Convenţia de denumire se stabileşte înaintea primei implementări, deoarece modificarea ei ulterioară afectează simultan toate sursele şi toţi consumatorii. Convenţia de mai jos este proprie acestui exerciţiu: urmează principiile structurii de referinţă din secţiunea 6.2.8 – ierarhie de la general la particular, separarea tipurilor de mesaje, câmpuri explicite pentru timp, unitate şi calitate –, dar foloseşte cinci niveluri, denumiri de câmpuri în limba română şi un mesaj grupat, pentru a ilustra versionarea schemei şi marcarea datelor recuperate. Într-un proiect real se adoptă o singură convenţie pentru toate liniile.

Structura subiectelor

```
{organizatie}/{fabrica}/{linie}/{activ}/{tip}
```

Segmentele se scriu cu litere mici, fără diacritice şi fără spaţii. Pentru linia din exerciţiu rezultă:

```
fabrica-demo/f01/amb01/sig01/telemetrie
fabrica-demo/f01/amb01/cant01/telemetrie
fabrica-demo/f01/amb01/plc01/evenimente
fabrica-demo/f01/amb01/plc01/productie
fabrica-demo/f01/amb01/gw01/stare
```

Ierarhia permite abonarea selectivă: o aplicaţie interesată numai de telemetria liniei se abonează la fabrica-demo/f01/amb01/+/telemetrie, iar un sistem de supraveghere a mai multor linii se abonează la fabrica-demo/f01/+/+/evenimente. Fără această structură, aceleaşi aplicaţii ar recepţiona toate mesajele şi le-ar filtra intern, consumând inutil trafic şi resurse.

Regulile asociate sunt:

- fiecare tip de mesaj are subiectul său; telemetria, evenimentele şi rezumatele de producţie nu se amestecă;
- telemetria periodică se publică la nivelul de calitate a serviciului 0; înregistrările individuale ale cântăririlor, evenimentele şi rezumatele de producţie se publică la nivelul 1. Înregistrările cântăririlor se păstrează în coada locală pentru retransmitere, iar duplicatele sunt eliminate la destinaţie pe baza identificatorului cântăririi;
- subiectul stare conţine un mesaj reţinut, astfel încât orice consumator nou să afle imediat starea sursei;
- gateway-ul îşi declară la conectare un mesaj de testament, publicat automat de broker în subiectul stare la pierderea legăturii;
- niciun subiect nu este utilizat pentru comenzi către proces; comenzile nu fac parte din acest exerciţiu.

Structura mesajului

Mesajul de telemetrie grupează înregistrările unui singur activ, disponibile într-o fereastră de o secundă. Fiecare înregistrare păstrează marca temporală a măsurării, momentul primei recepţii în gateway şi indicatorul de calitate. Momentul publicării aparţine mesajului şi nu înlocuieşte momentele individuale ale măsurărilor. Înregistrările provenite de la active diferite se publică separat, pe subiectele corespunzătoare. Exemplul următor prezintă un mesaj al staţiei de cântărire:

```
{
  "idMesaj": "b3c1f0a2-8d54-4b17-9a6e-2f7c1d0e5a91",
  "versiuneSchema": "1.2",
  "sursa": {
    "gateway": "gw-amb01",
    "activ": "F01-AMB01-CANT01",
```

```
        "amplasare": "F01/Hala2/Linia-Ambalare-01"
      },
      "timp": {
        "publicareInitiala": "2026-03-17T09:42:16.000Z"
      },
      "context": {
        "ordin": "OP-2026-004512",
        "lot": "L-20260317-03",
        "produs": "PRD-500G-A",
        "schimb": "S1"
      },
      "masuratori": [
        {
          "idCantarire": "CANT01-S20260317-000125",
          "semnal": "greutate_produs",
          "valoare": 498.7,
          "unitate": "g",
          "calitate": "buna",
          "timpMasurare": "2026-03-17T09:42:15.300Z",
          "timpReceptie": "2026-03-17T09:42:15.462Z",
          "sursaTimp": "PLC01"
        }
      ],
      "recuperat": false
    }
```

Fiecare câmp are o justificare care poate fi verificată:

- idMesaj identifică mesajul şi se păstrează la retransmitere; idCantarire identifică rezultatul individual, inclusiv atunci când aceeaşi înregistrare este transmisă în alt mesaj;
- versiuneSchema permite identificarea structurii pe care consumatorul trebuie să o interpreteze;
- sursa.gateway identifică echipamentul care transmite datele, iar sursa.activ identifică echipamentul observat;
- timp.publicareInitiala indică momentul primei publicări a mesajului; acesta se păstrează la retransmitere;
- timpMasurare aparţine fiecărei înregistrări şi indică momentul achiziţiei la sursă; timpReceptie indică prima recepţie a înregistrării în gateway, iar sursaTimp identifică dispozitivul care a atribuit momentul măsurării. Compararea momentelor provenite de la dispozitive diferite presupune ceasuri sincronizate;
- context conţine ordinul, lotul, tipul produsului şi schimbul asociate înregistrărilor. Câmpul produs identifică tipul produsului, nu exemplarul fizic. Înregistrările cu contexte diferite se transmit în mesaje separate;
- calitate însoţeşte fiecare valoare şi se păstrează la stocare, pentru a permite diferenţierea rezultatelor valide de cele invalide;
- recuperat marchează retransmiterea după o întrerupere, fără modificarea identificatorilor şi a momentelor originale.

Timpul se exprimă în timp universal coordonat, cu conversia realizată numai la afișare, conform regulii din secțiunea 7.2.4.

Modificările compatibile – adăugarea unui câmp opțional, adăugarea unui semnal nou în masuratori – incrementează versiunea minoră. Eliminarea unui câmp, modificarea unei unități de măsură sau schimbarea semnificației unui câmp existent incrementează versiunea majoră și impun funcționarea în paralel a celor două versiuni pe durata actualizării consumatorilor.

Greutatea se înregistrează la finalizarea fiecărei cântăriri, indiferent de diferența față de valoarea precedentă. Două produse consecutive cu aceeași greutate generează două înregistrări distincte. Fiecare înregistrare conține un identificator unic al cântăririi, valoarea, unitatea de măsură, marca temporală a sursei și indicatorul de calitate. Banda moartă poate fi utilizată pentru actualizarea unei afișări, dar nu pentru selectarea rezultatelor păstrate în istoricul pe produs.

Planul complet de raportare a semnalelor, cu sursa, frecvența, banda moartă, subiectul și destinația fiecăruia, este prezentat în Tabelul 7.10.

Tabelul 7.10 – Planul de raportare a semnalelor

Semnal	Sursă	Frecvență de raportare	Bandă moartă	Subiect	Destinație
Temperatura de sigilare	Pt100 prin PLC	1 Hz	0,2 °C	…/sig01/telemetrie	serie temporală, panou operator
Greutatea produsului	celulă de sarcină	la finalizarea fiecărei cântăriri	nu se aplică	…/cant01/telemetrie	istoric pe produs, control statistic
Viteza transportorului	convertizor prin PLC	1 Hz	0,01 m/s	…/plc01/telemetrie	serie temporală, calculul performanței
Contoare produse conforme și neconforme	PLC, valori cumulative	1 Hz	–	…/plc01/productie	calculul producției și al calității
Rezultatul inspecției	sistem de inspecție	la fiecare produs neconform	–	…/insp01/evenimente	evidența defectelor
Alarme și opriri	PLC și SCADA	la apariție și la revenire	–	…/plc01/evenimente	calculul disponibilității
Consum energetic	contor Modbus TCP	0,1 Hz	–	…/em01/telemetrie	consum raportat la producție
Starea gatewayului	gateway	la conectare, la deconectare	–	…/gw01/stare	indicator de disponibilitate a sursei

7.5.5. Configurarea componentelor

Configurațiile de mai jos sunt date în forma în care pot fi reaplicate pe stiva declarată în secțiunea 7.5.3. Ele constituie livrabilul 4 din secțiunea 7.5.7.

Automatul programabil și serverul OPC UA

Variabilele destinate monitorizării se grupează într-un bloc de date dedicat, DB_IIoT, cu denumiri stabile și tipuri explicite. Blocul se declară cu acces optimizat,

care se dezactivează numai dacă este necesară adresarea absolută din alte aplicații; pentru serverul OPC UA integrat, accesul optimizat este de preferat, deoarece expunerea se face prin nume, nu prin adresă. Nu se expun adrese absolute de memorie, deoarece acestea se modifică la recompilare.

Serverul OPC UA integrat expune variabilele blocului sub identificatori de nod în spațiul de nume al programului. Forma reală a identificatorului este ns=3;s="DB_IIoT"."nume_variabila", unde indicele 3 corespunde spațiului de nume al programului utilizator, iar identificatorul este un șir care reproduce exact denumirea blocului și a membrului, inclusiv ghilimelele. Nodurile utilizate în exercițiu sunt cele din Tabelul 7.11.

Tabelul 7.11 – Nodurile OPC UA expuse de automatul programabil pentru monitorizare

Semnal	Identificator de nod	Tip de dată	Interval de eșantionare	Bandă moartă absolută
Temperatura de sigilare	ns=3;s="DB_IIoT"."temperatura_sigilare"	Real	100 ms	0,2
Greutatea ultimei cântăriri, pentru afișare	ns=3;s="DB_IIoT"."greutate_produs"	Real	100 ms	0
Viteza transportorului	ns=3;s="DB_IIoT"."viteza_transportor"	Real	100 ms	0,01
Contor produse conforme	ns=3;s="DB_IIoT"."contor_conforme"	DInt	1 000 ms	0
Contor produse neconforme	ns=3;s="DB_IIoT"."contor_neconforme"	DInt	1 000 ms	0
Cod alarmă activă	ns=3;s="DB_IIoT"."cod_alarma"	Int	100 ms	0
Identificator lot activ	ns=3;s="DB_IIoT"."lot_activ"	String	1 000 ms	—
Identificator ordin activ	ns=3;s="DB_IIoT"."ordin_activ"	String	1 000 ms	—

Abonamentul creat de gateway utilizează un interval de publicare de 100 ms pentru semnalele rapide și de 1 000 ms pentru restul, cu filtrul de bandă moartă absolută din tabel; contoarele și codurile de alarmă se citesc fără bandă moartă, pentru că orice modificare este semnificativă. Contoarele se expun ca valori cumulative, nu ca diferențe calculate în automat: o valoare cumulativă pierdută se recuperează la mesajul următor, în timp ce o diferență pierdută dispare definitiv. Gateway-ul primește un cont dedicat pe serverul OPC UA, cu drept exclusiv de citire, iar politica de securitate a punctului terminal se stabilește la semnare și criptare cu certificat, nu la modul fără securitate.

Pentru cântărire, variabila scalară din Tabelul 7.11 servește afișării ultimei valori disponibile. Istoricul pe produs se construiește separat: la finalizarea fiecărei cântăriri, automatul creează o înregistrare completă într-o memorie tampon, accesibilă gateway-ului prin OPC UA. Identificatorul cântăririi nu se reutilizează la repornirea automatului; el poate fi alcătuit din identificatorul sesiunii de funcționare și un număr de secvență. Gateway-ul preia înregistrările în ordinea secvenței și păstrează identificatorii pentru detectarea lipsurilor și eliminarea duplicatelor. Citirea periodică a ultimei greutăți, chiar fără bandă moartă, nu poate înlocui acest mecanism: între două citiri pot apărea mai multe rezultate, inclusiv rezultate identice. Capacitatea memoriei tampon se stabilește în funcție de ritmul maxim al

cântăririlor şi de întreruperea de comunicaţie pe care trebuie să o acopere; depăşirea capacităţii este semnalată.

Gateway-ul. Fluxul are patru etape: citirea prin OPC UA, validarea, gruparea şi publicarea. În Node-RED, acestea corespund unei succesiuni de noduri: un nod client OPC UA configurat pe abonamentul de mai sus; un nod de funcţie pentru validare; un nod de agregare pe fereastră de o secundă; un nod de funcţie pentru construirea mesajului conform schemei 1.2; un nod client MQTT configurat pentru brokerul securizat.

Înregistrările cântăririlor sunt prelucrate individual. Dacă mai multe cântăriri sunt incluse în aceeaşi fereastră de o secundă, gruparea păstrează toate înregistrările, cu identificatorii, mărcile temporale şi indicatorii de calitate proprii. Pentru istoricul pe produs, rezultatele nu se înlocuiesc cu ultima valoare din fereastră şi nu se reduc la o medie. Indicatorii statistici se calculează ulterior, pornind de la înregistrările individuale valide.

Validarea verifică tipul, apartenenţa la domeniul de măsurare şi indicatorul de calitate. Domeniile aplicate sunt cele din Tabelele 7.7 şi 7.8: 0–300 °C pentru temperatură, 0–1 000 g pentru greutate, 0–0,35 m/s pentru viteză. O valoare în afara domeniului nu se elimină tăcut, ci se transmite cu "calitate": "invalida", pentru că absenţa ei ar fi interpretată ca lipsă de eveniment. O valoare al cărei indicator de calitate OPC UA nu este „bun” se transmite cu aceeaşi marcă.

Gruparea se realizează pe o fereastră de o secundă, separat pentru fiecare activ şi context de producţie. Fiecare înregistrare păstrează momentul măsurării şi momentul primei recepţii în gateway. Câmpul timp.publicareInitiala indică prima publicare a mesajului şi nu înlocuieşte momentele individuale ale măsurărilor. Publicarea se face pe subiectul corespunzător activului, la nivelul de calitate a serviciului stabilit în secţiunea 7.5.4.

Stocarea locală se dimensionează pornind de la debitul calculat pentru planul din Tabelul 7.10, cu metoda din secţiunea 7.3.3: aproximativ 4 mesaje şi 5 valori pe secundă dau $Q \approx 4 \times (120 + 70) + 5 \times 45 \approx 1{,}0$ kB/s, adică 1,0 kB/s × 86 400 s ≈ 85 MB pentru 24 de ore. Se alocă 1 GB, pentru a acoperi evenimentele suplimentare, creşterea numărului de semnale şi marja de siguranţă; raportul dintre valoarea alocată şi necesarul calculat, de aproximativ 12, acoperă cerinţa 12 chiar şi la dublarea numărului de semnale. Politica la depăşire este declarată explicit: cele mai vechi mesaje de telemetrie se elimină primele, iar evenimentele şi rezumatele de producţie se păstrează prioritar.

Brokerul. Se configurează un singur punct de acces securizat, cu verificarea obligatorie a certificatului clientului şi utilizarea identităţii din certificat ca nume de utilizator. Fişierul de configurare al brokerului conţine directivele:

```
listener 8883
cafile   /etc/mosquitto/certs/ca.crt
certfile /etc/mosquitto/certs/broker.crt
keyfile /etc/mosquitto/certs/broker.key
```

```
    require_certificate true
    use_identity_as_username true
    allow_anonymous false
    acl_file /etc/mosquitto/acl
    persistence true
    max_queued_messages 10000
```

Lista de control al accesului acordă gateway-ului drept de publicare numai în subarborele liniei proprii şi niciun drept de abonare:

```
    user gw-amb01
    topic write fabrica-demo/f01/amb01/#
```

Numele `gw-amb01` este preluat din câmpul de identitate al certificatului clientului, ceea ce face ca autorizarea să depindă de identitatea criptografică, nu de un identificator declarat de client. Persistenţa brokerului se activează, iar numărul de mesaje în aşteptare se limitează, pentru ca o destinaţie indisponibilă să nu consume memoria brokerului.

Persistenţa. Datele se scriu într-un depozit cu retenţie de 30 de zile la rezoluţie completă. Două sarcini programate calculează agregate la un minut, păstrate 400 de zile, şi agregate orare, păstrate cinci ani. Agregatele numerice utilizează numai valorile cu indicatorul de calitate „buna”; numărul înregistrărilor valide şi al celor invalide se păstrează separat. Absenţa valorilor valide nu se înlocuieşte cu o valoare numerică zero.

Fiecare măsurare se stochează cu valoarea, unitatea, indicatorul de calitate şi marca temporală proprie, preluată din timpMasurare. Înregistrările invalide rămân disponibile pentru diagnostic. Dacă sursa nu furnizează o valoare numerică utilizabilă, se păstrează starea de calitate şi momentul, fără inventarea unei valori.

În exemplul de persistenţă se utilizează InfluxDB OSS 2.x. Pentru cântăriri, etichetele identifică linia, activul, lotul şi cântărirea individuală. Valoarea, unitatea şi calitatea sunt câmpuri ale înregistrării. Marca temporală se transmite în nanosecunde de la epoca Unix.

```
cantariri,linie=amb01,activ=CANT01,lot=L-20260317-03,idCantarire=CANT01-
S20260317-000125 valoare=498.7,unitate="g",calitate="buna"
1773740535300000000
```

În această configuraţie, identitatea punctului este determinată de numele măsurării, ansamblul etichetelor şi marca temporală. Retransmiterea aceleiaşi cântăriri păstrează aceste elemente şi aceleaşi câmpuri, astfel încât nu creează o înregistrare suplimentară. Două cântăriri distincte au identificatori diferiţi şi rămân separate chiar dacă greutăţile sau mărcile temporale coincid. Simpla păstrare a identificatorului într-un câmp obişnuit nu l-ar include în cheia punctului.

Utilizarea unui identificator unic drept etichetă este aleasă aici pentru claritatea exerciţiului. La dimensionarea unei aplicaţii de producţie trebuie evaluat numărul de serii rezultat şi ales un model de stocare adecvat volumului de cântăriri.

Momentele recepției și publicării pot fi păstrate suplimentar pentru diagnostic, dar nu înlocuiesc momentul măsurării. Marcajul recuperat descrie traseul înregistrării și nu face parte din cheia acesteia.

Vizualizarea. Se realizează trei tablouri distincte, conform regulii din secțiunea 7.4.5: un tablou pentru operator, cu temperatura și banda de toleranță 175 ± 3 °C, greutatea față de limitele 500 ± 5 g, contorul de producție și alarmele active; un tablou pentru mentenanță, cu duratele opririlor pe categorii, evoluția abaterii de greutate și consumul raportat la producție; un tablou pentru conducere, cu indicatorul de eficacitate globală pe schimb și componentele sale afișate separat. Fiecare tablou conține momentul ultimei valori recepționate și starea sursei, preluată din subiectul stare.

Comportamentul la pierderea comunicației. Secvența verificabilă este următoarea:

1. La pierderea legăturii, brokerul publică mesajul de testament în subiectul stare; cu un interval de menținere a conexiunii de 30 s, detectarea are loc în cel mult 45 s.
2. Tablourile afișează sursa ca indisponibilă; valorile rămân vizibile, dar marcate ca neactualizate.
3. Gateway-ul trece pe coada locală. Automatul programabil, sistemul SCADA și sistemul HMI nu sunt afectate; producția continuă fără nicio degradare, conform cerinței 11.
4. La restabilire, gateway-ul se reconectează cu întârziere progresivă, publică starea „conectat” și retransmite mesajele în ordine cronologică, cu mărcile temporale originale și cu recuperat marcat.
5. Debitul retransmisiei se limitează la de trei ori debitul nominal, pentru ca recuperarea să nu satureze legătura utilizată simultan de traficul curent.

7.5.6. Validarea etapizată

Validarea se realizează în două faze. Scopul primei faze este localizarea erorilor într-un lanț minimal; scopul celei de-a doua este verificarea comportamentului sistemului complet, inclusiv în situații anormale.

Faza 1 – traseul minimal. Se transmite o singură variabilă, temperatura de sigilare, de la automatul programabil până la panoul de vizualizare.

Rezultate așteptate:

- valoarea afișată coincide cu cea de pe sistemul HMI, cu o abatere de cel mult 0,2 °C, egală cu banda moartă configurată;
- diferența dintre marca temporală a măsurării și cea a recepției rămâne sub 2 s;
- oprirea gateway-ului determină apariția stării „indisponibil” în cel mult 45 s.

Dacă una dintre aceste condiții nu este îndeplinită, cauza se află într-un lanț format din cinci componente, ceea ce face diagnosticarea practicabilă. Trecerea directă la fluxul complet mută aceeași eroare într-un sistem cu peste douăzeci de elemente.

Faza 2 – fluxul complet. Se activează toate semnalele din Tabelul 7.10, contextul de lot și calculul indicatorilor.

Rezultate așteptate, măsurabile:

- debitul mediu către broker se situează în jurul valorii de 1,0 kB/s, cu o abatere de cel mult 20 % față de calculul propriu (livrabilul 6), făcut conform metodei din secțiunea 7.3.3 pentru planul din Tabelul 7.10; o abatere mai mare indică o eroare de configurare a frecvențelor sau a benzilor moarte;
- percentila 95 a întârzierii, calculată din diferența celor două mărci temporale, nu depășește 2 s;
- indicatorul de eficacitate globală calculat pe schimb coincide cu valoarea obținută manual din datele contorizate, cu o abatere de cel mult 0,5 puncte procentuale.

Se execută trei încercări suplimentare:

Încercarea de întrerupere. Legătura externă se întrerupe timp de 15 minute. Producția trebuie să continue nemodificat. La debitul nominal, coada locală acumulează aproximativ 1,0 kB/s × 900 s ≈ 0,9 MB. După restabilire, retransmiterea trebuie finalizată în cel mult 5 minute, la debitul limitat, iar seria temporală trebuie să prezinte, după recuperare, un istoric continuu, fără gol în intervalul întreruperii.

Încercarea de duplicat. Se forțează retransmiterea unui set de mesaje deja livrate. Numărul de puncte din baza de date trebuie să rămână neschimbat, iar indicatorii recalculați trebuie să producă aceleași valori.

Încercarea de securitate. Gateway-ul liniei încearcă publicarea într-un subiect aparținând altei linii și abonarea la un subiect din afara subarborelui propriu. Ambele operații trebuie respinse de broker, iar respingerea trebuie să apară în jurnal. Rezultatul verifică cerințele 15 și 16 și confirmă distincția dintre autentificare și autorizare, tratată în secțiunea 7.4.2.

7.5.7. Livrabile și criterii de reușită

Exercițiul se consideră finalizat atunci când sunt predate următoarele documente:

1. schema arhitecturii, cu nivelurile, componentele și traseele de date, realizată conform modelului din Figura 7.2;
2. tabelul semnalelor, cu sursa, frecvența, banda moartă, subiectul și destinația fiecăruia;
3. convenția de denumire a subiectelor și un mesaj complet, comentat câmp cu câmp;

4. configurațiile componentelor, în forma în care pot fi reaplicate: parametrii serverului OPC UA și identificatorii de nod, fluxul gateway-ului, configurația brokerului și lista de control al accesului, politica de retenție și panourile de vizualizare;
5. delimitarea explicită a funcțiilor care rămân locale, cu justificarea fiecăreia prin timp de răspuns sau prin consecința indisponibilității;
6. bugetul de latență și calculul de lățime de bandă pentru configurația proiectată, realizate conform metodelor din secțiunile 7.1.4 și 7.3.3;
7. procedura pentru comportamentul la întrerupere, cu durata de autonomie calculată și politica declarată la depășirea capacității;
8. raportul de validare, cu rezultatele măsurate ale celor două faze și ale celor trei încercări.
9. Criteriile după care se evaluează fiecare livrabil, împreună cu modul de verificare, sunt prezentate în Tabelul 7.12.

Exercițiul nu urmărește obținerea unei soluții unice. Două arhitecturi diferite pot îndeplini toate criteriile, cu condiția ca fiecare decizie să fie justificată prin cerințele procesului și verificabilă prin calcul sau prin măsurare. Ceea ce nu este acceptabil este o arhitectură corectă în regim normal și nedefinită în situațiile anormale: cele trei încercări din faza a doua au tocmai rolul de a face vizibilă această diferență.

Tabelul 7.12 – Criteriile de reușită ale exercițiului

Criteriu	Condiție de îndeplinire	Mod de verificare
Delimitarea funcțiilor	nicio funcție de control, interblocare sau siguranță nu depinde de platformă	analiza schemei și încercarea de întrerupere
Continuitatea producției	producția continuă nemodificat pe durata întreruperii de 15 min	observarea directă a liniei
Integritatea datelor	istoricul este continuu după recuperare, fără gol și fără duplicate	interogarea seriei temporale, încercarea de duplicat
Trasabilitatea	orice valoare poate fi atribuită unui lot fără corelare manuală	selectarea unui lot și extragerea valorilor asociate
Respectarea bugetului de latență	percentila 95 a întârzierii sub 2 s	diferența mărcilor temporale, pe un interval de o oră
Respectarea dimensionării	debit măsurat în limita de ±20 % față de valoarea calculată	monitorizarea traficului pe gateway
Corectitudinea indicatorilor	abatere de cel mult 0,5 puncte procentuale față de calculul manual	recalcularea indicatorului din datele contorizate
Restricționarea accesului	publicarea și abonarea în afara subarborelui propriu sunt respinse	încercarea de securitate și jurnalul brokerului
Documentarea	toate cele opt livrabile sunt complete și consecvente între ele	verificarea corespondenței dintre schemă, tabel, configurații și raport

7.6. Concluzii

Arhitectura unui sistem IIoT trebuie proiectată ca un ansamblu de niveluri şi responsabilităţi clar delimitate. Senzorii şi actuatoarele interacţionează cu procesul fizic, automatele programabile execută funcţiile de control, sistemele HMI şi SCADA asigură operarea şi supravegherea, gateway-ul industrial prelucrează datele la edge, iar platformele IIoT susţin stocarea, analiza şi integrarea cu aplicaţiile organizaţiei. Modelul stratificat nu descrie un traseu obligatoriu al fiecărei valori, ci o repartizare a responsabilităţilor; componentele transversale se poziţionează după rolul pe care îl îndeplinesc, nu după locul în care rulează.

Integrarea acestor componente nu se reduce la realizarea conexiunilor. Datele trebuie selectate, validate, contextualizate şi asociate unor identificatori stabili pentru active, procese, produse şi loturi, iar contextul trebuie stabilit cât mai aproape de momentul producerii evenimentului, pentru că reconstituirea lui ulterioară eşuează exact în situaţiile care interesează. Fiecare interfaţă devine astfel un obiect de proiectare, cu sursă de referinţă declarată, model de date versionat, comportament definit la întrerupere şi reguli explicite pentru repetare şi eliminarea duplicatelor.

Verificarea cantitativă fundamentează arhitectura. Bugetul de latenţă identifică întârzierile şi exclude funcţiile incompatibile cu lanţul de achiziţie. Calculul traficului confirmă o reducere de peste douăzeci de ori prin gruparea mesajelor şi selectarea frecvenţelor de raportare, fără pierderea informaţiei utile, predominant prin decizii la gateway. Evaluarea eficacităţii globale a echipamentelor evidenţiază relevanţa distribuţiei pierderilor faţă de valoarea agregată şi condiţionează comparabilitatea de utilizarea unor definiţii identice.

Alegerea între prelucrarea locală, la edge şi în cloud depinde de timpul de răspuns, de criticitatea funcţiei, de volumul datelor, de confidenţialitate şi de comportamentul necesar la pierderea comunicaţiei. Secvenţele de control, interblocările şi funcţiile de siguranţă rămân locale. Platforma IIoT extinde capacitatea de monitorizare şi de analiză, fără a deveni o condiţie pentru funcţionarea sigură a procesului; un rezultat analitic se transmite ca recomandare către sistemul responsabil, nu ca acţiune directă asupra procesului.

Platformele industriale se evaluează prin lanţul funcţional pe care îl implementează – recepţie, administrarea dispozitivelor, intermediere, rutare, transformare, persistenţă, analiză, vizualizare şi integrare – şi nu prin lista funcţiilor comerciale. Rolurile arhitecturale rămân stabile, în timp ce denumirile, gruparea serviciilor şi modelele de licenţiere se modifică frecvent. Din acelaşi motiv, dimensionarea, politica de păstrare şi condiţiile de portabilitate trebuie stabilite înaintea colectării datelor, nu după punerea în funcţiune.

Proiectarea trebuie să pornească de la cazul de utilizare şi să includă modelul de date, continuitatea funcţionării, administrarea dispozitivelor, politica de păstrare şi integrarea cu MES, ERP şi CMMS. Exerciţiul din secţiunea 7.5 arată că această

proiectare poate fi dusă până la nivelul identificatorilor de nod, al fișierelor de configurare și al criteriilor numerice de recepție, iar validarea progresivă, mai întâi a traseului minimal și apoi a fluxului complet, permite localizarea controlată a erorilor și verificarea trasabilității datelor de la sursă până la aplicația finală.

Conectarea nivelurilor industriale și extinderea fluxurilor de date către infrastructuri distribuite măresc însă suprafața expusă amenințărilor. Fiecare element care a făcut arhitectura funcțională – gateway-ul care traversează frontiera dintre rețele, identitatea cu care se autentifică, subiectele în care are drept de publicare, interfețele către MES și ERP – devine, din perspectiva securității, un element care trebuie protejat și monitorizat. Din acest motiv, arhitectura funcțională trebuie completată cu segmentarea rețelei, controlul identității și accesului, protejarea comunicațiilor și monitorizarea evenimentelor. Capitolul următor tratează aceste cerințe și prezintă principiile de securitate cibernetică aplicabile sistemelor IIoT, folosind ca punct de plecare exact arhitectura construită aici.

7.7. Întrebări de verificare

1. *Cum trebuie interpretate piramida CIM și modelul ISA-95 în raport una cu alta?*

a) ISA-95 înlocuiește complet piramida CIM, care nu mai este utilizată;
b) sunt identice, deci nivelurile se suprapun exact una peste alta;
c) sunt complementare, dar nivelurile lor nu se echivalează doar după poziția grafică, ci după rolul efectiv al fiecărei componente;
d) corelarea se face după eticheta comercială a produsului.

2. *Unde se încadrează un sistem SCADA care supraveghează mai multe linii, gestionează alarme la nivelul fabricii și transmite informații către MES?*

a) la nivelul 2 și, prin extinderea funcțiilor, poate îndeplini și funcții asociate nivelului 3; încadrarea se face după rolul efectiv;
b) exclusiv la nivelul 0, deoarece lucrează cu procesul fizic;
c) exclusiv la nivelul 4, alături de ERP;
d) la niciun nivel, deoarece SCADA nu face parte din modelul ISA-95.

3. *În exemplul de buget de latență (senzor 2 ms, PLC 20 ms, OPC UA 100 ms, gateway 5 ms, rețea 15 ms, broker 30 ms, baza de date 20 ms), care este latența totală în cazul cel mai defavorabil și care segment contribuie cel mai mult?*

a) 172 ms; rețeaua este segmentul dominant;
b) 100 ms; celelalte segmente se execută în paralel și nu se însumează;
c) 192 ms; rețeaua contribuie cu peste 30 % din buget;
d) 192 ms; intervalul de publicare OPC UA reprezintă singur peste jumătate din buget.

4. *De ce nu poate fi plasată respingerea fizică a unui produs neconform, care trebuie executată în mai puțin de 10 ms, în lanțul prin gateway, broker și bază de date?*

a) deoarece baza de date pentru serii temporale nu poate stoca evenimente;

b) deoarece brokerul MQTT nu acceptă mesaje de alarmă;
c) deoarece chiar segmentele senzor și PLC însumează 22 ms în cazul cel mai defavorabil; funcția aparține nivelului de control, local;
d) deoarece respingerea produselor este o funcție exclusivă a sistemului ERP.

5. *Cum se determină, în cartea de față, valoarea OEE a liniei de ambalare din scenariul didactic (480 min schimb, 30 min pauze, 45 min opriri, 16 200 produse, 486 respinse, 0,02 min/produs)?*

a) OEE = D × P × C = 0,900 × 0,800 × 0,970 ≈ 0,698, adică 69,8 %;
b) OEE = 0,900 + 0,800 + 0,970 = 2,67, ca sumă a factorilor;
c) OEE = 15 714 / 16 200 = 97,0 %, doar rata de calitate;
d) OEE = 405 / 480 = 84,4 %, doar raportul timpului efectiv la durata schimbului.

6. *Care este cea mai mare componentă a pierderilor din scenariul OEE și de ce nu este vizibilă în jurnalul de alarme?*

a) produsele respinse (circa 81 min); apar doar în rapoartele de calitate;
b) funcționarea sub viteza de referință (circa 81 min); nu corespunde niciunei opriri înregistrate;
c) pauzele planificate (30 min); sunt trecute în jurnalul de alarme;
d) opririle neplanificate (45 min); sunt înregistrate doar prin alarme.

7. *De ce calculul OEE aparține sistemului MES și nu sistemului SCADA?*

a) deoarece numai nivelul care deține simultan ordinul, produsul și intervalul poate corela cantitatea, duratele, cauzele opririlor și timpul de ciclu de referință;
b) deoarece ERP interzice calculul indicatorilor în afara sa;
c) deoarece SCADA nu poate înregistra stările echipamentelor;
d) deoarece MES are întotdeauna un timp de răspuns mai mic decât SCADA.

8. *Ce reprezintă ordinul de producție lansat de MES către zona de control?*

a) o simplă informare, fără legătură cu execuția;
b) o comandă pe care o poate anula doar ERP;
c) o comandă directă de pornire, executată imediat de actuatoare;
d) o autorizare, nu o comandă de pornire; automatul programabil verifică interblocările și condițiile locale înaintea pornirii.

9. *De ce nu este recomandată utilizarea unei baze de date comune, în care SCADA, MES și ERP modifică direct aceleași tabele?*

a) deoarece bazele de date relaționale nu pot fi accesate de mai multe aplicații;
b) creează dependențe puternice între aplicații și face imposibilă stabilirea responsabilității pentru o valoare greșită;
c) deoarece reduce prea mult timpul de răspuns al sistemelor;
d) deoarece este permisă numai în sistemele cu un singur automat programabil.

10. *O linie transmite 120 de semnale la 10 Hz, câte 250 de octeți pe mesaj (varianta A). Ce debit rezultă și cum se schimbă acesta prin gruparea valorilor într-un mesaj la fiecare 100 ms (varianta B)?*

a) 30 000 octeți/s în varianta A; 28 000 octeți/s în varianta B;

b) 2,4 Mbit/s în varianta A; 0,02 Mbit/s în varianta B, cu pierderea valorilor intermediare;
c) 300.000 octeți/s în ambele variante, deoarece numărul de valori nu se schimbă;
d) 300.000 octeți/s ≈ 2,4 Mbit/s în varianta A; 55.900 octeți/s ≈ 0,45 Mbit/s în varianta B, o reducere de circa 81 %, fără pierdere de informație.

8. SECURITATE CIBERNETICĂ ÎN IIOT

Extinderea conectivității dintre echipamentele industriale, sistemele de automatizare, aplicațiile organizației și serviciile cloud creează posibilități noi pentru monitorizare, analiză și optimizare. În același timp, fiecare interfață, fiecare dispozitiv conectat și fiecare serviciu adăugat poate deveni o cale de acces către infrastructura industrială. Securitatea nu poate fi adăugată ulterior, ca un strat separat: ea trebuie integrată în arhitectura IIoT din etapa de proiectare și menținută pe întreaga durată de exploatare, cerință formulată explicit în standardul dedicat ciclului securizat de dezvoltare a produselor industriale [213].

În sistemele de tehnologie operațională, un incident cibernetic nu afectează numai informațiile. Modificarea neautorizată a programului unui PLC, transmiterea unor valori false, blocarea comunicației sau compromiterea unei stații de inginerie poate produce oprirea procesului, deteriorarea echipamentelor, realizarea unor produse neconforme ori apariția unor riscuri pentru personal și mediu. Din acest motiv, protejarea sistemelor OT trebuie corelată cu cerințele specifice privind performanța, fiabilitatea și siguranța procesului [25].

Securitatea industrială nu se obține prin transferul mecanic al practicilor din sistemele IT. Echipamentele au durate lungi de exploatare, posibilități limitate de actualizare și intervale scurte în care pot fi oprite. Unele componente utilizează protocoale proiectate fără mecanisme de autentificare și criptare, iar orice intervenție asupra configurației trebuie verificată pentru a nu perturba funcționarea procesului. Disponibilitatea serviciilor, integritatea comenzilor și menținerea instalației într-o stare sigură au aici o importanță pe care modelul clasic al securității informației nu o reflectă complet, iar literatura de specialitate arată că soluțiile dezvoltate pentru rețelele de birou nu pot fi aplicate identic în mediile de control industrial [214].

Analiza din acest capitol nu pornește de la o arhitectură nouă. Traseul construit în Capitolul 7 – serverul OPC UA, gateway-ul industrial, conexiunea MQTT, platforma IIoT, baza de date și tabloul de bord – este reluat din perspectiva activelor protejate, a amenințărilor, a vulnerabilităților, a identităților și a drepturilor de acces. Această continuitate permite asocierea fiecărei măsuri de securitate cu o componentă și cu o legătură de comunicație concrete, fără reconstruirea separată a arhitecturii funcționale.

Protecția eficientă se bazează pe apărarea în profunzime (*defence in depth*). Nicio măsură individuală nu elimină toate riscurile: inventarierea activelor, segmentarea, autentificarea, autorizarea, criptarea, consolidarea configurațiilor, monitorizarea, copiile de siguranță și pregătirea răspunsului la incidente produc efect numai

atunci când sunt aplicate coordonat [215]. Seria ISA/IEC 62443 organizează această coordonare prin responsabilități distribuite între proprietarii activelor, integratorii de sistem, furnizorii de produse și prestatorii de servicii, precum și prin corelarea oamenilor, proceselor și tehnologiei [85], [205].

Capitolul prezintă mai întâi riscurile și vulnerabilitățile specifice arhitecturilor IIoT, apoi măsurile de control al identității și accesului, protejarea comunicațiilor, segmentarea rețelei industriale și schimbul controlat de date printr-un DMZ. Sunt corelate în continuare ISA/IEC 62443, NIST CSF 2.0, ISO/IEC 27001 și MITRE ATT&CK for ICS, cu precizarea rolului distinct al fiecăreia. Partea aplicativă reia arhitectura din capitolul anterior pentru identificarea riscurilor, delimitarea zonelor și conductelor, stabilirea măsurilor de protecție și verificarea comportamentului sistemului în situații de atac, de configurare greșită sau de indisponibilitate.

Obiectivele capitolului

După parcurgerea capitolului, cititorul va putea:

- să diferențieze prioritățile securității în mediile OT de cele ale sistemelor IT și să argumenteze de ce măsurile IT nu pot fi transferate mecanic în producție;
- să identifice activele, limitele de încredere și suprafața de atac a unei arhitecturi IIoT, delimitând corect amenințarea, vulnerabilitatea, vectorul de atac, consecința și riscul;
- să analizeze consecințele tehnice și de proces ale compromiterii PLC-urilor, stațiilor de inginerie, sistemelor SCADA, gateway-urilor industriale și comunicațiilor industriale;
- să selecteze și să justifice măsuri de identificare, autentificare și autorizare pentru utilizatori, dispozitive și aplicații, inclusiv certificate X.509 și control al accesului bazat pe roluri;
- să proiecteze segmentarea unei rețele industriale și schimbul controlat de date printr-un DMZ industrial, incluzând accesul la distanță al personalului de mentenanță și al furnizorilor;
- să explice rolul complementar al ISA/IEC 62443, NIST CSF 2.0, ISO/IEC 27001 și MITRE ATT&CK for ICS și să aplice conceptele de zonă, conductă și nivel de securitate;
- să evalueze securitatea traseului OPC UA – gateway industrial – MQTT – platformă IIoT și să stabilească comportamentul sigur la pierderea comunicației sau la invalidarea unui certificat;
- să valideze într-un mediu izolat eficacitatea măsurilor implementate și să documenteze riscurile, contramăsurile, responsabilitățile și criteriile de verificare.

8.1. Riscuri și vulnerabilități în automatizările industriale

Conectarea echipamentelor de producţie la sisteme SCADA, gateway-uri industriale, aplicaţii ale organizaţiei şi servicii cloud extinde funcţionalitatea sistemului, dar creează şi noi căi prin care acesta poate fi perturbat sau compromis. Riscul trebuie analizat pe întregul traseu al datelor, de la senzor şi actuator până la aplicaţia utilizatorului, nu doar la limita dintre reţeaua industrială şi internet.

În acest context, termenii utilizaţi au semnificaţii distincte, iar tratarea lor ca sinonime este una dintre cauzele frecvente ale analizelor de securitate neconcludente:

- activul este echipamentul, aplicaţia, informaţia, serviciul sau funcţia care trebuie protejată;
- ameninţarea reprezintă cauza potenţială a unui incident;
- vulnerabilitatea este o slăbiciune de proiectare, configurare, implementare sau exploatare;
- vectorul de atac este calea prin care ameninţarea poate exploata vulnerabilitatea;
- consecinţa reprezintă efectul asupra procesului, organizaţiei, personalului sau mediului;
- riscul rezultă din asocierea probabilităţii unui scenariu cu gravitatea consecinţelor sale.

Aceste delimitări corespund vocabularului definit în partea introductivă a seriei ISA/IEC 62443 şi utilizat în metoda de evaluare a riscului pentru proiectarea sistemelor de automatizare şi control industrial [216], [85]; ele sunt folosite consecvent în restul capitolului.

Existenţa unei vulnerabilităţi nu înseamnă că incidentul se va produce, dar nici o probabilitate aparent redusă nu poate justifica ignorarea unui scenariu cu efecte severe asupra siguranţei sau a procesului tehnologic.

8.1.1. Specificul riscului în mediile OT

În sistemele informatice convenţionale, analiza securităţii este orientată frecvent către confidenţialitatea, integritatea şi disponibilitatea informaţiilor. Aceste atribute rămân importante şi în mediile industriale, dar trebuie corelate cu funcţionarea procesului fizic.

În multe sisteme OT, disponibilitatea serviciilor şi integritatea comenzilor au prioritate operaţională. O măsură de securitate care blochează nejustificat comunicaţia poate produce oprirea instalaţiei, în timp ce acceptarea unei comenzi false poate genera o stare periculoasă. Confidenţialitatea nu dispare din analiză, deoarece reţetele, parametrii procesului, programele controlerelor şi datele privind producţia pot avea valoare tehnică sau comercială. Ghidul dedicat securităţii tehnologiei operaţionale formulează explicit această diferenţă de priorităţi şi

recomandă selectarea măsurilor astfel încât să nu afecteze determinismul, timpul de răspuns şi funcţiile de siguranţă ale procesului [25].

Consecinţele unui incident pot include:

- pierderea vizibilităţii asupra procesului;
- pierderea sau degradarea funcţiei de control;
- oprirea producţiei;
- modificarea neautorizată a parametrilor;
- realizarea unor produse neconforme;
- deteriorarea echipamentelor;
- pierderea protecţiilor şi a interblocărilor;
- afectarea siguranţei personalului;
- producerea unor efecte asupra mediului;
- compromiterea informaţiilor operaţionale;
- pierderi financiare şi contractuale.

Sistemele OT au, de asemenea, particularităţi care pot menţine vulnerabilităţile perioade îndelungate. Echipamentele pot fi exploatate timp de mai multe decenii, iar oprirea lor pentru actualizare poate fi posibilă numai în intervale planificate. Unele dispozitive au resurse limitate, utilizează sisteme de operare care nu mai sunt susţinute sau nu permit instalarea mecanismelor moderne de protecţie. Analizele comparative ale incidentelor industriale arată că un număr important dintre acestea exploatează vulnerabilităţi cunoscute şi corectate de mult timp în echivalentul lor din zona IT, dar rămase neremediate în instalaţie tocmai din cauza acestor constrângeri de exploatare [217].

Actualizările trebuie testate înaintea aplicării, deoarece o modificare aparent minoră poate afecta timpul de răspuns, comunicaţia sau compatibilitatea cu alte componente. Din acest motiv, gestionarea corecţiilor de securitate într-un mediu industrial este tratată separat de practica IT, printr-un proces care asociază proprietarul activului şi furnizorul produsului şi care prevede evaluarea aplicabilităţii, validarea şi planificarea instalării fiecărei corecţii [218].

Securitatea OT trebuie deci proiectată în raport cu cerinţele de performanţă, fiabilitate şi siguranţă ale procesului, nu aplicată independent de acestea [25].

8.1.2. Suprafaţa de atac a unei arhitecturi IIoT

Suprafaţa de atac cuprinde toate componentele şi interfeţele prin care un sistem poate fi accesat, observat, influenţat sau perturbat. Într-o arhitectură IIoT, aceasta nu se limitează la echipamentele conectate direct la internet.

Modelul Purdue, formulat iniţial ca arhitectură de referinţă pentru integrarea întreprinderii industriale [192], poate fi utilizat ca hartă pentru identificarea punctelor expuse. La nivelul procesului se află senzorii şi actuatoarele. Nivelurile de control includ PLC-urile, controlerele de acţionare şi componentele de siguranţă.

Sistemele HMI, SCADA, staţiile de inginerie şi serverele istorice asigură operarea şi supravegherea. DMZ-ul industrial intermediază schimburile dintre reţeaua OT şi infrastructura IT, iar nivelurile superioare includ aplicaţiile organizaţiei, accesul la distanţă şi serviciile cloud. Figura 8.1 reprezintă această distribuţie a punctelor expuse pe niveluri.

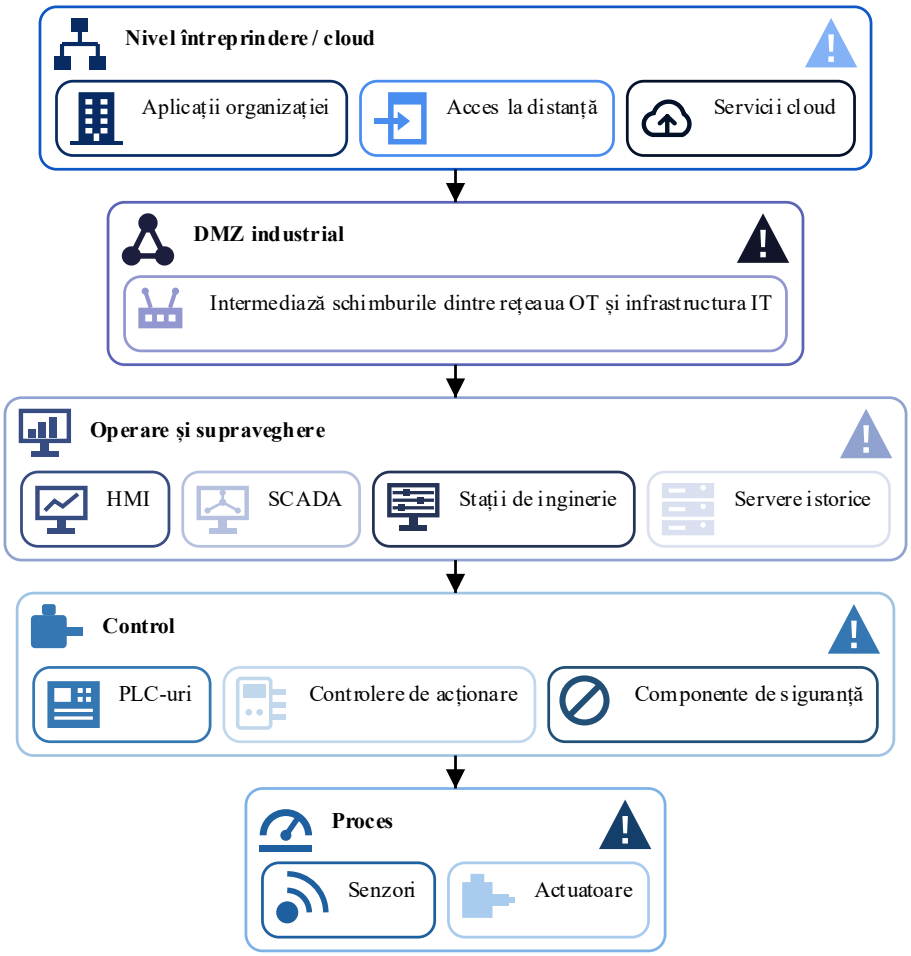


Figura 8.1 – Suprafaţa de atac a unei arhitecturi IIoT pe niveluri

Punctele de intrare pot fi reprezentate de:

- servicii expuse direct sau configurate necorespunzător;
- conexiuni de mentenanţă la distanţă;
- conturi implicite, partajate sau insuficient protejate;
- staţii de inginerie conectate succesiv la mai multe reţele;
- gateway-uri industriale care au interfeţe atât în reţeaua OT, cât şi în reţele externe;
- calculatoare portabile şi medii de stocare detaşabile;

- reţele wireless şi dispozitive mobile;
- aplicaţii web, interfeţe API şi tablouri de bord;
- certificate, chei şi parole păstrate necorespunzător;
- componente software sau actualizări provenite din lanţul de aprovizionare;
- acces fizic la dulapuri, porturi de comunicaţie şi echipamente.

O arhitectură izolată logic poate fi compromisă printr-un calculator temporar, o conexiune de mentenanţă sau un mediu de stocare infectat. Această observaţie nu este teoretică: literatura consacrată securităţii reţelelor industriale arată că izolarea fizică declarată se dovedeşte frecvent incompletă la o inventariere riguroasă, din cauza legăturilor introduse pentru diagnoză, raportare sau mentenanţă şi nedocumentate ulterior [219]. În mod similar, un gateway industrial bine protejat nu compensează existenţa unui PLC expus direct ori utilizarea aceloraşi credenţiale pentru mai multe dispozitive. Punctele de intrare sunt grupate în Figura 8.2.

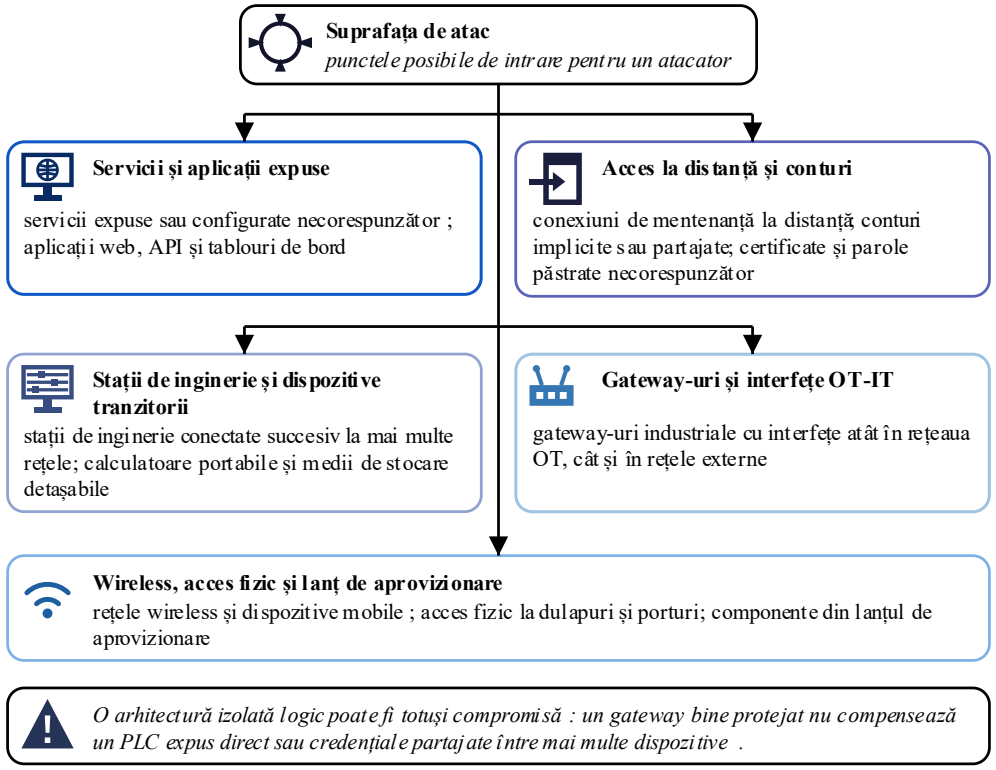


Figura 8.2 – Ierarhia punctelor de intrare - 5 grupe

Ameninţările nu sunt exclusiv deliberate. O clasificare utilă pentru inventarierea surselor de risc distinge atacurile intenţionate, acţiunile accidentale, defectările tehnice, deficienţele organizaţionale, evenimentele fizice şi compromiterea lanţului de aprovizionare; Tabelul 8.1 asociază fiecărei categorii exemple concrete şi consecinţele posibile asupra procesului.

Tabelul 8.1 – Surse de risc pentru sistemele OT și IIoT

Sursa riscului	Exemple	Consecințe posibile
acțiune intenționată	acces neautorizat, program malițios, furtul credențialelor, blocarea comunicației	manipularea procesului, exfiltrarea datelor, oprirea producției
eroare umană	încărcarea unui program greșit, modificarea unei politici, conectarea incorectă a unui echipament	pierderea comunicației, comandă eronată, expunerea unui serviciu
defectare tehnică	defect hardware, eroare software, umplerea spațiului de stocare, expirarea certificatului	indisponibilitate, pierderea datelor, imposibilitatea autentificării
deficiență organizațională	inventar incomplet, drepturi excesive, responsabilități neclare, copii de siguranță neverificate	detectare întârziată, recuperare dificilă, modificări netrasabile
eveniment fizic sau de mediu	întreruperea alimentării, temperatură excesivă, incendiu, acces fizic neautorizat	oprirea echipamentelor, deteriorare, pierderea controlului
compromiterea lanțului de aprovizionare	firmware modificat, bibliotecă software vulnerabilă, actualizare neautorizată	introducerea unei căi persistente de acces în sistem

8.1.3. Atacuri asupra PLC-urilor și sistemelor de supraveghere

PLC-ul execută secvenţele, reglarea şi interblocările procesului. Compromiterea sa poate modifica direct comportamentul echipamentelor. Atacatorul nu trebuie să înlocuiască integral programul pentru a produce un efect: poate fi suficientă schimbarea unui parametru, a unei valori de referinţă, a modului de funcţionare sau a unei condiţii logice.

Acţiunile posibile includ:

- modificarea programului sau a sarcinilor controlerului;
- încărcarea unui proiect alterat;
- schimbarea modului de funcţionare;
- modificarea firmware-ului;
- alterarea imaginii intrărilor şi ieşirilor;
- schimbarea limitelor şi parametrilor tehnologici;
- transmiterea unor comenzi neautorizate;
- blocarea sau întârzierea mesajelor;
- repornirea ori oprirea controlerului;
- dezactivarea alarmelor, protecţiilor sau interblocărilor;
- suprasolicitarea resurselor de comunicaţie şi procesare.

Posibilitatea acestor acţiuni nu ține numai de configurare, ci și de capabilităţile pe care componenta le oferă. Cerințele tehnice aplicabile controlerelor şi celorlalte componente ale unui sistem de automatizare – protejarea integrităţii firmware-ului și a programului, verificarea autenticității actualizărilor, limitarea modificărilor la identităţi autorizate – sunt formulate explicit în partea 4-2 a seriei ISA/IEC 62443

[156]. Un controler care nu oferă aceste funcţii nu poate fi adus la nivelul cerut prin configurare, ci numai prin măsuri compensatorii la nivelul sistemului.

MITRE ATT&CK for ICS grupează astfel de acţiuni în tactici care includ accesul iniţial, execuţia, persistenţa, deplasarea laterală, inhibarea funcţiilor de răspuns, perturbarea controlului procesului şi producerea impactului. Printre tehnicile documentate se află modificarea programului sau a firmware-ului, manipularea imaginilor intrărilor şi ieşirilor, blocarea mesajelor OT, modificarea parametrilor şi suprimarea alarmelor [220]. Utilizarea acestei clasificări în proiectare este tratată în secţiunea 8.3.6.

Staţia de inginerie este un activ deosebit de important, deoarece poate conţine proiectele controlerelor, programele de configurare şi drepturile necesare pentru descărcarea modificărilor. Compromiterea acesteia poate oferi atacatorului o cale legitimă din punct de vedere tehnic pentru modificarea PLC-ului. Acesta este şi mecanismul prin care programul maliţios cunoscut sub numele de Stuxnet a acţionat: componenta care intercepta comunicaţia mediului de inginerie Siemens permitea introducerea unui bloc de program modificat în controler şi, simultan, returnarea codului original la operaţiile de citire, astfel încât inginerul care verifica programul nu observa nicio diferenţă [221], [222]. Cazul arată de ce integritatea trebuie verificată printr-un mecanism independent de calea prin care se face modificarea.

Sistemele HMI şi SCADA pot fi utilizate pentru influenţarea operatorului. Un atacator poate modifica valorile afişate, poate ascunde o alarmă sau poate prezenta o stare aparent normală în timp ce procesul se află în afara limitelor. Trebuie diferenţiată pierderea controlului de pierderea vizibilităţii: procesul poate continua să funcţioneze fără ca operatorul să-i cunoască starea reală sau poate fi controlat neautorizat în timp ce interfaţa afişează date false. Distincţia nu este terminologică. Ea este consemnată ca atare şi în clasificarea efectelor din MITRE ATT&CK for ICS, unde pierderea controlului, pierderea vizibilităţii şi manipularea vizibilităţii sunt tehnici distincte, cu surse de detectare şi cu măsuri de limitare diferite [220].

8.1.4. Interceptarea şi manipularea comunicațiilor

Protocoalele industriale clasice au fost proiectate frecvent pentru reţele izolate şi nu includ întotdeauna mecanisme native de autentificare, autorizare şi criptare. Această moştenire este documentată sistematic în literatura dedicată reţelelor de control industrial, care arată că majoritatea magistralelor de câmp şi a protocoalelor de nivel superior derivate din ele au fost concepute pentru determinism şi simplitate, într-un context în care accesul fizic la mediul de transmisie era considerat suficient ca protecţie [153]. Cazul cel mai răspândit este Modbus: specificaţia de aplicaţie nu prevede autentificarea solicitantului, verificarea integrităţii mesajului sau criptarea, iar aceste funcţii au fost adăugate ulterior printr-un profil separat, bazat pe TLS şi pe certificate X.509, care nu este însă implementat de echipamentele mai vechi [155], [168].

Dacă traficul poate fi accesat, un atacator poate observa structura mesajelor, adresele dispozitivelor, variabilele procesului și succesiunea comenzilor. Principalele scenarii sunt:

- ascultarea pasivă, prin captarea valorilor și comenzilor;
- uzurparea identității, prin imitarea unui dispozitiv sau client legitim;
- injectarea mesajelor, prin transmiterea unor comenzi ori valori falsificate;
- retransmiterea, prin repetarea unui mesaj valid într-un moment necorespunzător;
- atacul de interpunere (*man-in-the-middle*), prin interceptarea și modificarea comunicației;
- blocarea sau întârzierea mesajelor, inclusiv a alarmelor și comenzilor;
- refuzul serviciului, prin consumarea resurselor dispozitivului sau rețelei;
- manipularea sincronizării temporale, care afectează ordonarea evenimentelor și corelarea datelor.

Ultimul scenariu este frecvent omis din analize, deși sincronizarea timpului este ea însăși o funcție care trebuie protejată. Atât protocolul de timp în rețea, cât și protocolul de precizie utilizat în automatizări prevăd mecanisme de autentificare, dar acestea sunt opționale și rămân deseori dezactivate în configurațiile implicite [157], [35]. Un atacator care modifică referința temporală a mai multor echipamente simultan poate reordona evenimentele într-un jurnal, poate deplasa datele unui schimb de producție în altul și poate face imposibilă corelarea unui incident, fără să fi modificat nicio valoare de proces.

Un mesaj fals nu trebuie să aibă o valoare evident imposibilă. Valorile pot fi menținute în limite plauzibile, dar modificate suficient pentru a influența analiza, calitatea produsului sau decizia operatorului. Din acest motiv, verificarea domeniului numeric nu este suficientă; trebuie analizate și ritmul variației, relația cu alte mărimi și starea procesului. Distincția dintre marca temporală a măsurării și marca temporală a recepției, tratată în secțiunea 6.3, devine aici un element de securitate, nu doar de calitate a datelor.

OPC UA și MQTT pot utiliza mecanisme moderne de securitate, dar simpla alegere a protocolului nu garantează protecția. Modelul de securitate OPC UA prevede autentificarea aplicațiilor, semnarea și criptarea mesajelor și autorizarea utilizatorilor, însă lasă administratorului alegerea modului de securitate efectiv activat [223]. Un server configurat cu politici slabe, acces anonim sau drepturi de scriere excesive rămâne vulnerabil. În mod similar, specificația MQTT nu impune un mecanism de autorizare, ci trimite explicit această responsabilitate către implementarea brokerului și către proiectant [177]; o conexiune MQTT poate fi astfel compromisă prin credențiale partajate, certificate neverificate, drepturi prea largi asupra subiectelor sau configurarea necorespunzătoare a brokerului MQTT. Configurațiile care elimină aceste slăbiciuni sunt prezentate în secțiunea 8.2.4.

8.1.5. Vulnerabilități în stratul edge și în serviciile cloud

Gateway-ul industrial este o limită de încredere între sistemele industriale și platformele externe. Rolul său arhitectural – prelucrare, filtrare și contextualizare a datelor cât mai aproape de sursă – îl obligă să dețină simultan acces la servere OPC UA, baze de date locale, brokere MQTT și servicii de administrare, ceea ce concentrează într-un singur punct drepturi care, în restul arhitecturii, sunt separate [111]. Compromiterea lui poate permite observarea datelor, modificarea mesajelor sau deplasarea între segmente de rețea.

Vulnerabilitățile pot proveni din:

- sisteme de operare și componente software neactualizate;
- servicii inutile rămase active;
- conturi implicite sau drepturi administrative excesive;
- interfețe de administrare expuse;
- biblioteci și module provenite din surse neverificate;
- certificate și chei private păstrate neprotejat;
- fluxuri de prelucrare care nu validează datele de intrare;
- absența jurnalizării modificărilor;
- stocarea temporară necriptată;
- actualizări nesemnate sau insuficient verificate;
- lipsa separării dintre funcțiile de achiziție și cele de administrare.

Cele mai multe dintre aceste slăbiciuni nu sunt defecte de proiectare ale produsului, ci consecințe ale punerii în funcțiune cu configurația din fabrică. Cerințele de consolidare aplicabile unui astfel de echipament – dezactivarea serviciilor neutilizate, individualizarea credențialelor, protejarea materialului criptografic și restricționarea interfețelor de administrare – sunt formulate ca cerințe verificabile pentru componente în ISA/IEC 62443 [156] și trebuie tratate ca parte a recepției, nu ca o îmbunătățire ulterioară.

În platformă, identitatea dispozitivului, politica de acces și destinația mesajelor trebuie corelate. O politică prea permisivă poate permite unui gateway să publice date în numele altui activ, să citească informații care nu îi sunt destinate sau să trimită mesaje către funcții de comandă.

Interfețele API, bazele de date și tablourile de bord pot introduce alte riscuri: configurarea incorectă a drepturilor, expunerea cheilor de acces, validarea insuficientă a cererilor, vulnerabilități ale aplicației și păstrarea necontrolată a datelor. Indisponibilitatea furnizorului sau a conexiunii trebuie tratată separat de atacul cibernetic, deoarece efectul asupra procesului poate fi asemănător, dar tratarea și responsabilitatea diferă. Distincția are și o consecință contractuală: într-un serviciu cloud, responsabilitatea este partajată între furnizor și utilizator, iar limita dintre cele două depinde de modelul de serviciu adoptat [159]. Elementele aflate în sarcina utilizatorului – identitățile, drepturile, configurația și păstrarea datelor –

rămân ale organizației industriale, indiferent de garanțiile de disponibilitate oferite de furnizor.

Menținerea controlului critic la nivel local limitează consecințele. Dacă platforma este utilizată numai pentru monitorizare, compromiterea datelor poate afecta analiza și deciziile, dar nu trebuie să modifice direct secvențele PLC-ului. Dacă platformei i se permite transmiterea comenzilor, apare o suprafață de atac suplimentară, cu efecte potențiale asupra procesului fizic; această opțiune trebuie justificată explicit, nu adoptată implicit pentru comoditatea integrării [25].

8.1.6. Rețele wireless, acces fizic și lanțul de aprovizionare

Comunicațiile wireless extind conectivitatea în zone în care instalarea cablurilor este dificilă, dar mediul de transmisie nu poate fi delimitat fizic la perimetrul fabricii. Un atacator aflat în exterior poate încerca să detecteze rețeaua, să capteze traficul, să imite un nod legitim sau să introducă un punct de acces neautorizat. Din acest motiv, ghidurile dedicate securității OT tratează legăturile wireless ca fiind, prin natura lor, expuse și impun autentificarea reciprocă a nodurilor, criptarea la nivelul legăturii și inventarierea explicită a fiecărui punct de acces, inclusiv a celor instalate temporar pentru punerea în funcțiune [25].

Bruiajul poate reduce sau elimina disponibilitatea comunicației. Efectul său depinde de rolul legăturii. Pierderea unei conexiuni utilizate pentru raportare poate întârzia datele, în timp ce perturbarea unei comunicații implicate în comandă poate afecta funcționarea procesului. Proiectarea trebuie să precizeze comportamentul sigur al echipamentului la pierderea legăturii, iar cerințele de fiabilitate și latență ale legăturii trebuie stabilite înaintea alegerii tehnologiei, nu deduse din specificațiile comerciale ale acesteia [22].

Accesul fizic poate permite conectarea la porturi de programare, înlocuirea unui dispozitiv, copierea configurației sau introducerea unui mediu de stocare. Dulapurile, panourile de comandă și echipamentele amplasate în zone accesibile trebuie incluse în analiza de securitate.

Riscurile lanțului de aprovizionare apar atunci când în sistem sunt introduse produse, firmware, biblioteci, actualizări sau servicii compromise. Acestea pot ocoli protecțiile perimetrale, deoarece componenta este acceptată inițial ca fiind legitimă. Tratarea lor presupune extinderea analizei dincolo de perimetrul propriu: identificarea furnizorilor critici, formularea cerințelor de securitate în documentele de achiziție, verificarea provenienței și integrității componentelor livrate și monitorizarea modificărilor pe durata contractului [224]. În mediul industrial, aceste cerințe sunt corelate cu procesul securizat de dezvoltare impus furnizorului de produs și cu cerințele aplicabile prestatorilor de servicii de integrare și mentenanță [213], [91]. Verificarea provenienței, integrității și autenticității trebuie aplicată atât echipamentelor noi, cât și actualizărilor utilizate pe durata exploatării.

Calculatoarele personalului de mentenanță și ale furnizorilor reprezintă active tranzitorii. Ele pot fi conectate succesiv la mai multe instalații și pot transporta programe, proiecte, credențiale sau cod malițios. Accesul temporar nu trebuie să însemne acces nelimitat.

8.1.7. Incidente documentate și evaluarea riscului

Incidentele cunoscute demonstrează că atacurile industriale pot depăși nivelul furtului de informații. Stuxnet a exploatat vulnerabilități ale mediului Siemens și a vizat componente utilizate pentru configurarea și controlul procesului industrial [221]. Atacul asupra rețelei electrice ucrainene din decembrie 2015 a arătat că un atacator poate obține și utiliza acces legitim: după o perioadă îndelungată de recunoaștere, operatorii au fost deposedați de controlul stațiilor prin sesiuni de administrare la distanță aparent normale, iar refacerea alimentării a fost întârziată prin ștergerea unor componente software și prin blocarea centrului de relații cu clienții [225]. CrashOverride, cunoscut și ca Industroyer, a fost conceput ca o platformă modulară, extensibilă, pentru atacarea infrastructurilor critice prin protocoalele proprii sistemelor de control [226]. HatMan, denumit și TRITON sau TRISIS, a vizat controlerele unui sistem instrumentat de siguranță și a demonstrat că pot fi atacate inclusiv funcțiile destinate protejării procesului [227].

Incidentele recente arată aceleași riscuri. În mai 2021, Colonial Pipeline a oprit preventiv conducta după un atac cu program de extorcare asupra rețelei IT, deși controlul nu fusese vizat direct [228]. În aprilie 2022, autoritățile americane au avertizat asupra unor instrumente pentru automate Schneider Electric și OMRON și servere OPC UA, întâlnite în arhitecturile cărții [229]. În ianuarie 2024, FrostyGoop a comandat prin Modbus TCP controlerele unei companii de termoficare din Lviv; peste 600 de clădiri rezidențiale au rămas fără încălzire [230]. Exemplul ilustrează riscul protocolului fără autentificare accesibil prin rețea, explicat în capitolul 6.

Aceste incidente nu trebuie utilizate ca șabloane exclusive. Un sistem poate fi afectat și printr-o eroare de configurare, un cont legitim compromis, o actualizare necorespunzătoare sau propagarea unui program de extorcare (*ransomware*) din rețeaua IT. Ultima situație este raportată mai frecvent decât atacurile concepute special pentru sisteme industriale: în multe cazuri producția se oprește nu pentru că echipamentele de automatizare au fost atacate, ci pentru că sistemele de planificare, de expediție sau de facturare au devenit indisponibile, iar operatorul a oprit preventiv instalația [217]. Analiza trebuie să pornească, prin urmare, de la arhitectura concretă și de la dependențele reale ale procesului, nu numai de la programele malițioase cunoscute.

Pentru fiecare risc se construiește un scenariu care precizează:

1. activul și funcția care trebuie protejate;
2. sursa amenințării;

3. condiţiile necesare pentru producerea incidentului;
4. vulnerabilitatea exploatată;
5. acţiunea posibilă;
6. efectul tehnic asupra sistemului;
7. consecinţa asupra procesului şi organizaţiei;
8. măsurile existente;
9. probabilitatea şi impactul rezidual;
10. responsabilitatea pentru tratarea şi acceptarea riscului.

Această succesiune nu este arbitrară: ea reproduce, într-o formă adaptată unei lucrări didactice, etapele evaluării detaliate a riscului cerute pentru fiecare zonă şi conductă în metoda de proiectare a securităţii sistemelor de automatizare, care prevede identificarea ameninţării şi a vulnerabilităţii, determinarea consecinţei, estimarea riscului înainte şi după tratare şi consemnarea deciziei de acceptare [85].

În traseul analizat în Capitolul 7, un scenariu poate porni de la compromiterea certificatului gateway-ului industrial. Dacă politica MQTT îi permite să publice în orice subiect, atacatorul poate introduce date în numele altor active. Valorile false pot fi stocate şi afişate în tabloul de bord, afectând indicatorii şi deciziile. Dacă platforma nu are acces la funcţiile de control, procesul local continuă să funcţioneze. Dacă aceeaşi cale permite transmiterea comenzilor către PLC, consecinţele pot deveni fizice.

Contextul determină riscul: un scenariu didactic de evaluare

Evaluarea nu trebuie să se limiteze la gravitatea intrinsecă a unei vulnerabilităţi software. Se consideră acelaşi model de gateway industrial, cu aceeaşi versiune de firmware, afectat de o slăbiciune care permite execuţia de cod la distanţă prin interfaţa de administrare. Probabilitatea şi impactul se apreciază pe o scară ordinală cu trei trepte (1 – redus, 2 – mediu, 3 – ridicat), iar riscul se obţine ca produs al celor două valori, pe un domeniu de la 1 la 9:

$$R = P \times I$$

Cazul A – bancul de testare. Gateway-ul este amplasat într-o reţea de laborator, fără legătură cu instalaţia, cu date simulate. Interfaţa de administrare este accesibilă doar din laborator: P = 2. Compromiterea afectează un mediu de test care poate fi reinstalat: I = 1. Rezultă R = 2 × 1 = 2, risc scăzut.

Cazul B – instalaţia în funcţiune. Acelaşi gateway este amplasat în DMZ-ul industrial, are un cont cu drepturi de scriere asupra serverului OPC UA şi publică datele a trei linii de producţie. Expunerea este comparabilă: P = 2. Compromiterea permite însă falsificarea datelor de producţie şi scrierea în noduri ale procesului: I = 3. Rezultă R = 2 × 3 = 6, risc semnificativ, care impune tratare.

Cazul B după tratare. Se aplică măsurile din secţiunea 8.2: consolidarea configuraţiei şi eliminarea interfeţei de administrare expuse (P scade la 1), retragerea drepturilor de scriere şi limitarea contului la citirea celor şapte variabile necesare,

împreună cu monitorizarea publicărilor neautorizate (I scade la 2). Rezultă R = 1 × 2 = 2, valoare care poate fi acceptată formal de responsabilul desemnat.

Interpretare și limite. Comparația arată că aceeași vulnerabilitate produce un risc de trei ori mai mare într-un context și un risc echivalent celui inițial după aplicarea a două măsuri ieftine. Valorile obținute sunt însă instrumente de prioritizare, nu estimări ale pierderii: scara este ordinală, iar produsul a două valori ordinale nu are semnificație fizică și nu poate fi interpretat ca valoare monetară așteptată. Scorurile nu se însumează între scenarii și nu se compară între instalații evaluate de echipe diferite. Un scenariu cu consecințe asupra siguranței personalului trebuie tratat indiferent de scorul obținut, iar pragul de acceptare se stabilește înaintea evaluării, nu după obținerea rezultatelor.

Identificarea suprafeței de atac și a scenariilor de risc constituie baza pentru alegerea contramăsurilor. Autentificarea, autorizarea, criptarea, segmentarea, DMZ-ul industrial și controlul accesului trebuie aplicate în funcție de riscurile identificate. Aceste măsuri sunt dezvoltate în secțiunea 8.2.

8.2. Măsuri de securitate – Autentificare, criptare, segmentare și DMZ industrial

Protejarea unui sistem IIoT nu poate fi realizată printr-o singură măsură aplicată la limita rețelei. Un firewall nu compensează utilizarea unor conturi comune, criptarea comunicației nu limitează drepturile unui client autentificat, iar segmentarea nu protejează un echipament configurat necorespunzător. Măsurile trebuie organizate în straturi, astfel încât compromiterea unei componente să nu permită accesul necontrolat la întregul sistem.

Apărarea în profunzime combină măsuri de prevenire, detectare, limitare și recuperare. Pentru fiecare flux trebuie stabilite identitatea sursei, destinația permisă, protocolul utilizat, sensul comunicației și comportamentul la pierderea legăturii. Controalele trebuie adaptate cerințelor OT privind disponibilitatea, timpul de răspuns și menținerea procesului într-o stare sigură [215], [25]. Formularea lor ca cerințe verificabile, nu ca intenții, se face pe structura celor șapte cerințe fundamentale ale seriei ISA/IEC 62443, prezentate în secțiunea 8.3.3 și utilizate ca fir organizator al măsurilor din acest subcapitol [68].

8.2.1. Principiile aplicării măsurilor de securitate

Proiectarea securității pornește de la riscurile identificate în secțiunea 8.1 și urmărește câteva principii generale:

- acordarea privilegiului minim necesar;
- blocarea implicită a comunicațiilor care nu au fost autorizate;
- separarea responsabilităților operaționale de cele administrative;
- utilizarea unor identități individuale pentru utilizatori, dispozitive și aplicații;

- separarea funcţiilor de monitorizare de cele care pot modifica procesul;
- limitarea comunicaţiilor la sursele, destinaţiile şi protocoalele necesare;
- protejarea cheilor, certificatelor şi credenţialelor;
- jurnalizarea operaţiilor relevante;
- menţinerea funcţiilor critice de control la nivel local;
- verificarea periodică a configuraţiilor şi a capacităţii de recuperare.

Primele două principii formează nucleul modelului de arhitectură cu încredere zero, în care nicio poziţie în reţea nu conferă prin ea însăşi drepturi, iar fiecare cerere de acces este evaluată în raport cu identitatea, starea dispozitivului şi resursa solicitată [231]. Transpunerea acestui model în mediul industrial este parţială şi trebuie făcută cu prudenţă: verificarea repetată a fiecărei cereri introduce întârzieri şi dependenţe de servicii de identitate care nu pot fi acceptate în bucla de control, iar indisponibilitatea unui astfel de serviciu nu trebuie să oprească procesul. Principiul se aplică, în consecinţă, fluxurilor de date, accesului administrativ şi accesului de la distanţă, nu comunicaţiei deterministe dintre controler şi echipamentele de teren.

Accesul permis trebuie justificat printr-o necesitate funcţională. Dacă un gateway industrial trebuie să citească şapte variabile dintr-un server OPC UA, nu este justificată acordarea accesului de scriere asupra întregului spaţiu de adrese. În mod similar, un client MQTT care publică datele unei linii de producţie nu trebuie să poată publica în subiectele altor linii sau să se aboneze la fluxuri care nu îi sunt destinate.

Aceste principii nu sunt independente unele de altele. Privilegiul minim este verificabil numai dacă identităţile sunt individuale; blocarea implicită este utilă numai dacă regulile permise sunt documentate; jurnalizarea produce dovezi numai dacă acţiunile pot fi atribuite unei identităţi. Aplicarea parţială a setului reduce semnificativ efectul fiecărei măsuri luate separat.

8.2.2. Identificarea, autentificarea şi autorizarea

Identificarea, autentificarea şi autorizarea reprezintă operaţii diferite. Identificarea declară cine este entitatea, autentificarea verifică această identitate, iar autorizarea stabileşte ce operaţii îi sunt permise. Jurnalizarea asociază acţiunile efectuate cu identitatea autentificată. Această separare nu este o convenţie didactică: în ISA/IEC 62443 ea corespunde primelor două cerinţe fundamentale, tratate ca familii distincte de cerinţe de sistem – identificarea şi autentificarea, respectiv controlul utilizării [68]. Confuzia dintre ele este una dintre cauzele frecvente ale configuraţiilor nesigure: un sistem în care toate dispozitivele se autentifică corect, dar primesc aceleaşi drepturi, nu este mai sigur decât unul fără autentificare.

Într-o arhitectură IIoT trebuie gestionate cel puţin trei categorii de identităţi:

- identităţi umane, pentru operatori, personalul de mentenanţă, ingineri, administratori şi furnizori;

- identități ale dispozitivelor, pentru controlere, gateway-uri industriale, senzori inteligenți și alte echipamente conectate;
- identități ale aplicațiilor și serviciilor, pentru servere OPC UA, clienți MQTT, baze de date, interfețe API și componente de analiză.

Conturile comune reduc trasabilitatea și trebuie evitate. Fiecare utilizator trebuie să aibă o identitate proprie, iar fiecare dispozitiv trebuie să utilizeze credențiale distincte. Compromiterea unei parole sau a unui certificat nu trebuie să permită imitarea întregii categorii de dispozitive.

Pentru accesul administrativ și accesul la distanță al utilizatorilor este recomandată autentificarea multifactor. Robusteţea ei depinde însă de tipul factorului utilizat, nu de simpla lor înmulțire: ghidul de referință în materie clasifică autentificatorii pe niveluri de asigurare și tratează diferit factorii rezistenți la interceptare și la falsificarea destinației, precum cheile criptografice legate de domeniul solicitat, față de codurile transmise printr-un canal separat, care pot fi obținute prin inginerie socială [232]. Autentificarea multifactor nu înlocuiește controlul drepturilor și nu trebuie aplicată fără verificarea efectului asupra operării. Operatorul trebuie să poată utiliza sistemul în condițiile prevăzute, dar funcțiile administrative, modificarea programelor și accesul extern necesită controale suplimentare. Un caz care trebuie tratat explicit este autentificarea în situații de urgență: procedura de acces alternativ trebuie definită, jurnalizată și limitată în timp, nu improvizată prin păstrarea unui cont comun activ „pentru orice eventualitate".

Tabelul 8.2 – Exemplu de repartizare a drepturilor pe roluri

Rol	Vizualizarea procesului	Comenzi operaționale	Modificarea parametrilor	Modificarea programului PLC	Administrarea securității
operator	permisă	permisă în limitele procesului	limitată la valorile aprobate	interzisă	interzisă
tehnician de mentenanță	permisă	permisă în modul de mentenanță	permisă pentru echipamentele alocate	condiționată	interzisă
inginer de automatizare	permisă	permisă	permisă	permisă prin procedură de modificare	limitată
administrator de securitate	permisă pentru verificare	interzisă în mod obișnuit	interzisă	interzisă	permisă
aplicație de monitorizare	permisă pentru variabilele aprobate	interzisă	interzisă	interzisă	interzisă
gateway industrial	permisă pentru datele selectate	interzisă în configurația de monitorizare	interzisă	interzisă	numai asupra propriei identități

Autorizarea poate fi implementată prin controlul accesului bazat pe roluri. Rolul grupează drepturile necesare unei funcții, fără ca acestea să fie configurate separat pentru fiecare utilizator; avantajul modelului nu este economia de configurare, ci faptul că drepturile devin verificabile prin raportare la funcția organizațională, iar modificarea atribuțiilor unei persoane se reduce la schimbarea rolului atribuit [233]. Tabelul 8.2 prezintă o repartizare posibilă a drepturilor pentru rolurile uzuale dintr-o instalație conectată IIoT.

Drepturile trebuie aplicate atât în interfața utilizatorului, cât și la nivelul serviciului care execută operația. Ascunderea unui buton într-un tablou de bord nu reprezintă un control de acces dacă aceeași funcție poate fi apelată printr-o interfață API.

Separarea responsabilităților reduce posibilitatea ca o singură persoană să modifice simultan logica procesului, politicile de acces și înregistrările de audit. Cerința este formulată ca atare și în sistemul de management al securității informației, alături de cea privind revizuirea periodică a drepturilor acordate [234]. Pentru schimbările cu impact ridicat pot fi necesare aprobarea prealabilă, verificarea independentă și păstrarea versiunii anterioare.

8.2.3. Certificatele X.509 și infrastructura cu chei publice

Parolele partajate sunt dificil de administrat în sisteme care includ numeroase dispozitive. Schimbarea lor poate necesita intervenții asupra fiecărui echipament, iar compromiterea unei parole comune afectează toate dispozitivele care o utilizează. Certificatele X.509 permit asocierea unei identități cu o cheie publică și pot susține autentificarea individuală a dispozitivelor și aplicațiilor; structura certificatului, regulile de validare a lanțului și mecanismele de revocare sunt definite în profilul de infrastructură cu chei publice al internetului [203].

Într-un mecanism bazat pe chei asimetrice, fiecare dispozitiv deține:

- o cheie privată, care trebuie păstrată secretă;
- o cheie publică;
- un certificat care asociază cheia publică identității dispozitivului;
- lanțul certificatelor necesar verificării autorității emitente.

Certificatul poate fi transmis pentru verificare, dar cheia privată nu trebuie copiată, publicată sau inclusă în proiecte și capturi de ecran. Atunci când echipamentul permite, cheia privată trebuie generată și păstrată într-un modul hardware securizat, astfel încât să nu poată fi extrasă printr-o operație obișnuită. Regula generală de administrare a materialului criptografic este ca o cheie privată să nu părăsească niciodată mediul în care a fost generată și ca fiecare cheie să aibă o singură utilizare declarată, o perioadă de valabilitate stabilită și o procedură definită de retragere [235].

În autentificarea mutuală, clientul verifică identitatea serverului, iar serverul verifică identitatea clientului. Verificarea trebuie să acopere lanţul până la o autoritate de certificare de încredere, perioada de valabilitate, numele sau identificatorul aplicaţiei înscris în certificat, utilizarea permisă a cheii şi starea de revocare. Ultima verificare este cea mai des omisă în practică, deoarece presupune fie distribuirea şi actualizarea unei liste de certificate revocate, fie interogarea în timp real a unui serviciu de stare a certificatului [236]. Într-o reţea industrială izolată, ambele mecanisme trebuie proiectate explicit, împreună cu comportamentul sistemului atunci când serviciul de verificare nu este accesibil.

Acceptarea oricărui certificat prezentat, fără aceste verificări, elimină cea mai mare parte a protecţiei şi transformă autentificarea într-o formalitate. Lanţul complet, de la certificat la autorizare, este reprezentat în Figura 8.3.

Autentificarea prin certificat nu acordă automat accesul la resurse. După verificarea certificatului, identitatea trebuie asociată unei politici care stabileşte:

- operaţiile permise;
- resursele asupra cărora pot fi executate;
- direcţia comunicaţiei;
- intervalul sau contextul în care accesul este valabil;
- condiţiile suplimentare care trebuie îndeplinite.

În OPC UA, această separare este vizibilă în însăşi structura modelului de securitate: certificatul autentifică aplicaţia, iar drepturile efective ale utilizatorului sau ale aplicaţiei se stabilesc separat, prin roluri şi permisiuni asociate nodurilor din spaţiul de adrese [223].

Gestionarea certificatelor trebuie să acopere întregul ciclu de viaţă:

1. înregistrarea dispozitivului;
2. emiterea şi instalarea certificatului;
3. activarea identităţii;
4. monitorizarea perioadei de valabilitate;
5. reînnoirea sau rotaţia înaintea expirării;
6. revocarea în cazul compromiterii ori retragerii dispozitivului;
7. eliminarea sigură a cheilor şi actualizarea inventarului.

Perioadele de valabilitate se stabilesc prin politica organizaţiei. Ca ordin de mărime, în instalaţiile industriale se utilizează frecvent certificate de dispozitiv cu valabilitate de unu până la trei ani, reînnoite automat după consumarea a aproximativ două treimi din perioadă, şi certificate ale autorităţii de certificare cu valabilitate mult mai mare, păstrate în afara sistemelor operaţionale. Aceste valori sunt orientative: perioadele scurte reduc fereastra de exploatare a unei chei compromise, dar impun un mecanism de reînnoire automat şi testat, iar perioadele lungi reduc efortul administrativ cu preţul unui risc mai mare.

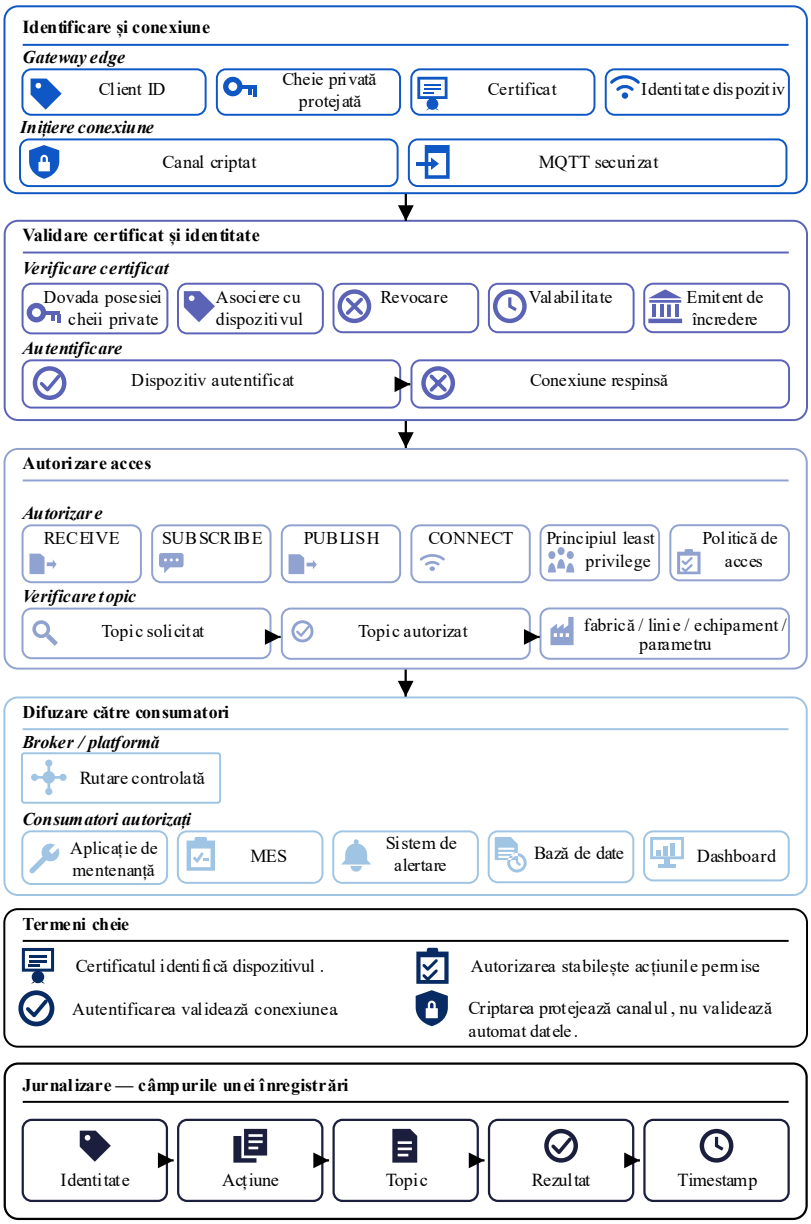


Figura 8.3 – Lanțul de încredere certificat–autentificare–autorizare

Un calcul de dimensionare a reînnoirilor

Consecința practică a politicii de reînnoire poate fi ilustrată printr-un calcul simplu. Se consideră o instalație cu 180 de identități de dispozitiv și de aplicație: gateway-uri industriale, clienți și servere OPC UA, clienți MQTT și servicii de bază de date. Fiecare identitate utilizează un certificat valabil 24 de luni. Reînnoirea este

programată după consumarea a două treimi din această perioadă, adică la 16 luni de la emitere.

Dacă fiecare reînnoire reuşită produce un certificat nou, cu aceeaşi valabilitate şi aceeaşi regulă de înlocuire, ciclul efectiv de reînnoire este de 16 luni. Pentru un inventar constant şi reînnoiri distribuite uniform în timp, volumul mediu rezultă din relaţia:

$$N = 180 / 16 = 11{,}25 \text{ reînnoiri/lună}$$

Aceasta înseamnă, în medie, aproximativ o reînnoire la două–trei zile. Perioada de valabilitate de 24 de luni determină momentul expirării, dar nu reprezintă intervalul dintre reînnoirile succesive în politica aleasă.

La punerea în funcţiune, certificatele pot fi emise în aceeaşi campanie de instalare, uneori în aceeaşi zi. În această situaţie, primele 180 de reînnoiri ajung la termen în aceeaşi perioadă, la aproximativ 16 luni după emitere. Media lunară nu mai descrie sarcina de vârf: mecanismul trebuie să poată procesa campania de reînnoire şi eventualele reîncercări, în intervalul planificat.

Dacă prima încercare de reînnoire eşuează pentru 5% dintre certificate, rezultă:

$$N_eşec = 180 \times 0{,}05 = 9 \text{ certificate}$$

Aceste nouă eşecuri nu produc automat pierderea imediată a conexiunilor. Certificatele existente mai au aproximativ opt luni de valabilitate, dacă nu sunt revocate şi dacă procedura de actualizare nu le înlocuieşte prematur cu unele inutilizabile. Eşecul trebuie însă înregistrat şi semnalat, iar reînnoirea reluată până la instalarea şi verificarea certificatului nou. Fereastra rămasă este o rezervă pentru remediere, nu un motiv pentru amânarea intervenţiei.

Dacă problema persistă până la expirare, autentificarea cu certificatul expirat poate fi respinsă, inclusiv la următoarea reconectare. De aceea, succesul procedurii nu se verifică numai prin emiterea certificatului nou, ci şi prin instalarea lui, asocierea cu cheia corespunzătoare şi testarea comunicaţiei autentificate.

Interpretare şi limite. Calculul nu stabileşte o durată universală de valabilitate. El arată că inventarul certificatelor, intervalul de reînnoire şi concentrarea termenelor trebuie analizate împreună. Distribuirea deliberată a momentelor de reînnoire reduce vârfurile de sarcină, iar testarea mecanismului trebuie să includă reînnoiri simultane şi încercări nereuşite. Monitorizarea urmăreşte atât apropierea expirării, cât şi eşecul unei reînnoiri programate.

Valorile utilizate sunt ipoteze pentru o instalaţie de dimensiune medie. Pentru un alt inventar sau o altă politică, se recalculează volumul mediu şi sarcina de vârf. Distincţia rămâne aceeaşi: momentul programat pentru reînnoire precedă expirarea, iar nereuşita unei încercări nu este echivalentă cu pierderea imediată a valabilităţii certificatului.

8.2.4. Protejarea comunicațiilor și a datelor

Criptarea în tranzit protejează confidențialitatea datelor, dar mecanismele criptografice trebuie să asigure și integritatea mesajelor și autentificarea punctelor terminale. O conexiune criptată către un server neverificat protejează traficul față de observatori, fără a demonstra că destinația este cea legitimă.

Pentru comunicațiile IIoT se utilizează, în mod uzual, TLS în versiunea 1.2 sau 1.3, cu autentificare mutuală și cu suite criptografice care asigură confidențialitatea perfectă înainte (*forward secrecy*). Versiunea 1.3 elimină din protocol o serie de mecanisme învechite, reduce numărul de schimburi necesare stabilirii sesiunii și interzice explicit negocierea versiunilor 1.0 și 1.1 [189]. Acestea din urmă, împreună cu SSL, au fost declarate depășite și nu trebuie utilizate în instalații noi [237].

Costul stabilirii sesiunii, exprimat numeric

Diferența dintre cele două versiuni nu este numai una de igienă criptografică; ea are un efect măsurabil asupra timpului de reconectare. O sesiune TLS 1.2 completă necesită două schimburi dus-întors înaintea primului mesaj util, în timp ce TLS 1.3 necesită unul singur. Pe o legătură cu timp de propagare dus-întors de 40 ms – valoare orientativă pentru o conexiune între o platformă externă și un gateway industrial dintr-o rețea de întreprindere, rezultă aproximativ 80 ms față de aproximativ 40 ms consumați exclusiv de schimburile de protocol, la care se adaugă durata operațiilor criptografice propriu-zise, dependentă de procesorul echipamentului. Diferența este neglijabilă pentru o conexiune stabilită o dată pe zi și devine semnificativă pentru un dispozitiv care se reconectează după fiecare întrerupere de rețea: la o legătură instabilă, cu treizeci de reconectări pe oră, economia ajunge la aproximativ 14 minute de indisponibilitate cumulată pe lună.

Limite – valorile de mai sus izolează numai componenta de propagare; ele nu includ timpul de validare a lanțului de certificate, care depinde de mecanismul de verificare a revocării, nici încărcarea procesorului, care pe echipamentele cu resurse reduse poate depăși contribuția rețelei. Aceste componente se măsoară pe echipamentul utilizat efectiv, nu se estimează.

OPC UA include mecanisme pentru autentificarea aplicațiilor și a utilizatorilor, semnarea mesajelor, criptare și autorizare bazată pe roluri [223]. Configurația trebuie să utilizeze un mod de securitate care asigură cel puțin semnarea mesajelor, iar pentru datele sensibile semnarea și criptarea. Politicile de securitate construite pe funcții de dispersie învechite, precum Basic128Rsa15 și Basic256, se sprijină pe SHA-1, au fost retrase din profilurile recomandate și nu trebuie utilizate; se aleg politici bazate pe SHA-256 sau mai puternice [238]. Accesul anonim și modul fără semnare rămân justificate numai într-un server de test izolat, declarat ca atare.

MQTT nu criptează implicit conținutul mesajelor. Protejarea comunicației se realizează prin TLS, împreună cu autentificarea clientului și politicile aplicate de brokerul MQTT. Standardul precizează necesitatea utilizării mecanismelor de

autentificare, autorizare şi comunicaţie securizată pentru aplicaţiile care prelucrează informaţii sensibile sau sunt asociate infrastructurilor critice, dar nu impune o sintaxă a politicilor de acces; acestea sunt specifice implementării brokerului [177]. În consecinţă, convenţia de denumire a subiectelor trebuie stabilită la nivel de proiect, înaintea configurării, deoarece de ea depinde direct granularitatea drepturilor care pot fi acordate.

Convenţia de subiecte şi politica de acces utilizate în exemplele acestui capitol

Subiectele se construiesc ierarhic, de la general la particular, folosind numai litere mici, cifre şi cratimă, fără diacritice şi fără spaţii:

```
fabrica/<sit>/<linie>/<echipament>/<tip-mesaj>
```

unde `<tip-mesaj>` aparţine mulţimii telemetrie, stare, eveniment, comanda, raspuns, config. Structura este o variantă simplificată a convenţiei de referinţă din secţiunea 6.2.8 (aici nivelurile sunt separate prin cratimă, iar clasele de mesaje sunt cele enumerate mai sus, nu cele din 6.2.8), aleasă pentru a pune în evidenţă granularitatea drepturilor. Un exemplu complet de subiect este `fabrica/sit01/linie01/umplere/telemetrie`.

Pentru gateway-ul industrial al liniei 01, autentificat cu certificat individual şi identificat prin `gw-linie01`, politica brokerului se formulează astfel:

- publicare permisă în fabrica/sit01/linie01/+/telemetrie, fabrica/sit01/linie01/+/stare şi fabrica/sit01/linie01/+/eveniment;
- abonare permisă numai la fabrica/sit01/linie01/gw-linie01/config, subiectul propriu de configurare;
- orice altă operaţie este respinsă implicit.

Aplicaţia de analiză primeşte o identitate distinctă, cu abonare permisă la fabrica/sit01/+/+/telemetrie şi fără drept de publicare. Trei reguli suplimentare se aplică indiferent de implementare: nu se acordă niciodată drepturi asupra rădăcinii ierarhiei prin metacaracterul #; subiectele de comandă se separă de cele de telemetrie şi se atribuie unor identităţi diferite; subiectele de administrare ale brokerului se restricţionează la contul administrativ. Identificatorul clientului facilitează administrarea conexiunilor şi corelarea jurnalelor, dar nu constituie o dovadă a identităţii – aceasta rezultă din certificatul verificat, nu din numele declarat la conectare.

Ierarhia trebuie proiectată de la început cu granularitatea drepturilor în minte. Dacă situl şi linia nu apar în subiect, ci numai echipamentul, nicio politică nu mai poate separa liniile între ele fără enumerarea individuală a fiecărui echipament; corectarea ulterioară presupune reconfigurarea tuturor clienţilor şi a tuturor abonărilor, deci o oprire planificată. Aceasta este o decizie de proiectare cu consecinţe operaţionale, nu o convenţie de denumire.

O rețea virtuală privată poate proteja comunicația dintre două puncte sau poate susține accesul la distanță. Aceasta nu înlocuiește însă autentificarea aplicației, controlul drepturilor și segmentarea internă. După stabilirea tunelului, utilizatorul sau dispozitivul trebuie să aibă acces numai la resursele necesare – cerință care corespunde direct principiului că poziția în rețea nu conferă prin ea însăși drepturi [231].

Datele trebuie protejate și în repaus. Bazele de date, copiile de siguranță și spațiile temporare ale gateway-ului industrial pot conține informații despre proces, configurații și evenimente. Criptarea suportului de stocare trebuie completată cu limitarea accesului, păstrarea controlată a cheilor și verificarea copiilor de siguranță. Cheile utilizate pentru datele în repaus se administrează separat de cele utilizate pentru comunicație, cu perioade de valabilitate și proceduri de retragere proprii [235]; păstrarea lor pe același suport cu datele pe care le protejează anulează măsura.

Introducerea criptării crește timpul de inițializare a sesiunii și consumul de resurse, în special pe echipamentele cu capacitate redusă de procesare. Funcțiile cu cerințe deterministe se mențin local și se separă de fluxurile către platformă, astfel încât costul criptării să nu intre în bucla de control.

8.2.5. Segmentarea rețelei industriale

Segmentarea împarte infrastructura în zone cu funcții, niveluri de criticitate și cerințe de încredere similare. Scopul nu este numai separarea rețelei IT de rețeaua OT, ci și limitarea deplasării laterale între linii, celule, servicii și funcții administrative. Delimitarea acestor zone și a legăturilor dintre ele nu este o operație de rețea, ci rezultatul evaluării riscului, tratat ca cerință explicită de metoda de proiectare a securității sistemelor de automatizare [85] și dezvoltat în secțiunea 8.3.2.

O structură posibilă, reprezentată în Figura 8.4, poate include:

- zona dispozitivelor de câmp și a controlului local;
- zona sistemelor HMI, SCADA și a serverelor istorice;
- zona stațiilor de inginerie și mentenanță;
- DMZ-ul industrial;
- zona aplicațiilor IT și a serviciilor organizației;
- zona serviciilor externe și a platformelor cloud;
- zona distinctă pentru accesul furnizorilor.

Rețelele locale virtuale permit separarea logică a traficului, dar nu constituie singure un mecanism suficient de protecție. Comunicația dintre zone trebuie să treacă prin echipamente care aplică reguli de filtrare și permit jurnalizarea traficului [25].

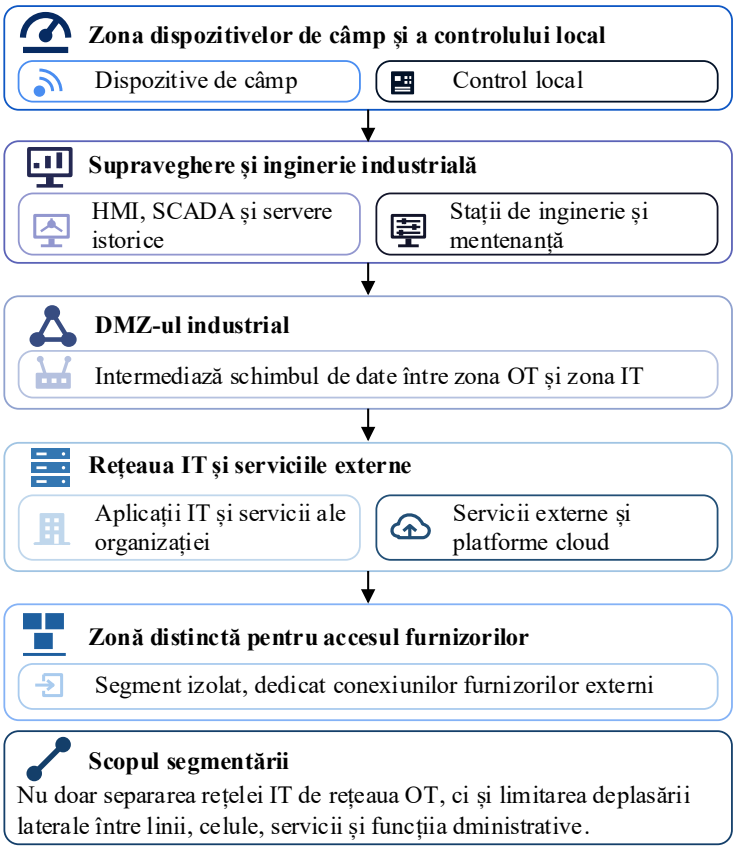


Figura 8.4 – Cele 7 zone ale segmentării industriale

Fiecare regulă trebuie documentată prin sursă, destinaţie, protocol, port şi sensul iniţierii conexiunii. Documentaţia trebuie să includă serviciul sau procesul justificativ, responsabilul pentru aprobare, necesitatea jurnalizării, perioada de valabilitate şi comportamentul la indisponibilitatea conexiunii.

Câmpul „perioada de valabilitate" merită o observaţie. În lipsa lui, regulile introduse pentru o punere în funcţiune, o probă sau o intervenţie rămân active ani de zile, iar setul de reguli creşte monoton, fiindcă nimeni nu are motivul documentat pentru a elimina o regulă pe care nu a introdus-o. Revizuirea periodică a drepturilor şi a regulilor de acces este, din acest motiv, o cerinţă a sistemului de management, nu o bună practică opţională [234].

Regulile generale de tipul „permite orice trafic între reţeaua de producţie şi reţeaua organizaţiei" anulează avantajele segmentării. Trebuie autorizate numai fluxurile necesare. Un PLC poate comunica cu serverul SCADA şi cu staţia de inginerie aprobată, dar nu trebuie să aibă acces direct la internet. Gateway-ul industrial poate iniţia o conexiune MQTT către destinaţia stabilită, fără a accepta conexiuni externe nejustificate către reţeaua de control.

Segmentarea limitează și consecințele erorilor. Configurarea greșită a unei aplicații din zona IT nu trebuie să genereze trafic necontrolat către PLC-uri, iar compromiterea unui dispozitiv dintr-o celulă nu trebuie să ofere acces automat la celelalte linii de producție. Această proprietate este utilă și în afara contextului de securitate: o rețea segmentată corect este mai ușor de diagnosticat atunci când apare o problemă de comunicație.

8.2.6. Zona demilitarizată industrială

DMZ-ul industrial este un segment intermediar între infrastructura OT și rețelele IT sau externe; în reprezentările pe niveluri este notat convențional ca „nivelul 3.5", pentru că se situează între nivelul 3 (gestionarea operațiunilor de fabricație) și nivelul 4 (întreprindere) din Figura 7.1. Schimburile dintre aceste domenii sunt realizate prin servicii intermediare, evitând conexiunile directe către sistemele de control. Intermedierea printr-o astfel de zonă, în locul conexiunilor directe, este una dintre recomandările centrale ale practicilor de apărare în profunzime pentru sistemele de control industrial [215]. Poziția ei între zona IT și zona OT este reprezentată în Figura 8.5.

În DMZ-ul industrial pot fi instalate servere proxy și proxy inverse, servere care intermediază transferul fișierelor și replici ale serverelor de date istorice. Tot aici pot funcționa servicii pentru actualizare și distribuirea controlată a pachetelor, brokere sau relee care intermediază mesajele, puncte de acces la distanță, servere intermediare pentru administrare și sisteme care monitorizează activitatea și colectează jurnalele.

Amplasarea unui serviciu în DMZ nu îl face automat sigur. Acesta trebuie consolidat, actualizat, monitorizat și configurat cu drepturi limitate. Echipamentele cu două interfețe de rețea nu trebuie utilizate pentru a crea căi necontrolate care ocolesc firewall-urile și politicile dintre zone – o legătură care ocolește punctul de control anulează întreaga separare, indiferent de calitatea regulilor configurate pe firewall.

Pentru transferul datelor către platforma IIoT se utilizează un mecanism de tip stocare și retransmitere. Gateway-ul industrial colectează și contextualizează datele în zona industrială, apoi inițiază o conexiune securizată către un serviciu intermediar sau către platformă. Sensul inițierii este esențial: nicio conexiune din internet nu trebuie să permită accesul direct la serverul OPC UA sau la PLC.

Dacă aplicațiile IT au nevoie de date istorice, acestea pot consulta o replică amplasată în DMZ, fără a interoga direct serverul SCADA. Pentru instalațiile cu cerințe ridicate poate fi analizată utilizarea unui transfer unidirecțional, realizat prin echipamente care permit fizic circulația datelor într-un singur sens [25]. Soluția se adoptă numai dacă funcția aplicației nu necesită transmiterea informațiilor în sens invers, deoarece elimină prin construcție confirmările de recepție, actualizările de configurare și diagnoza de la distanță.

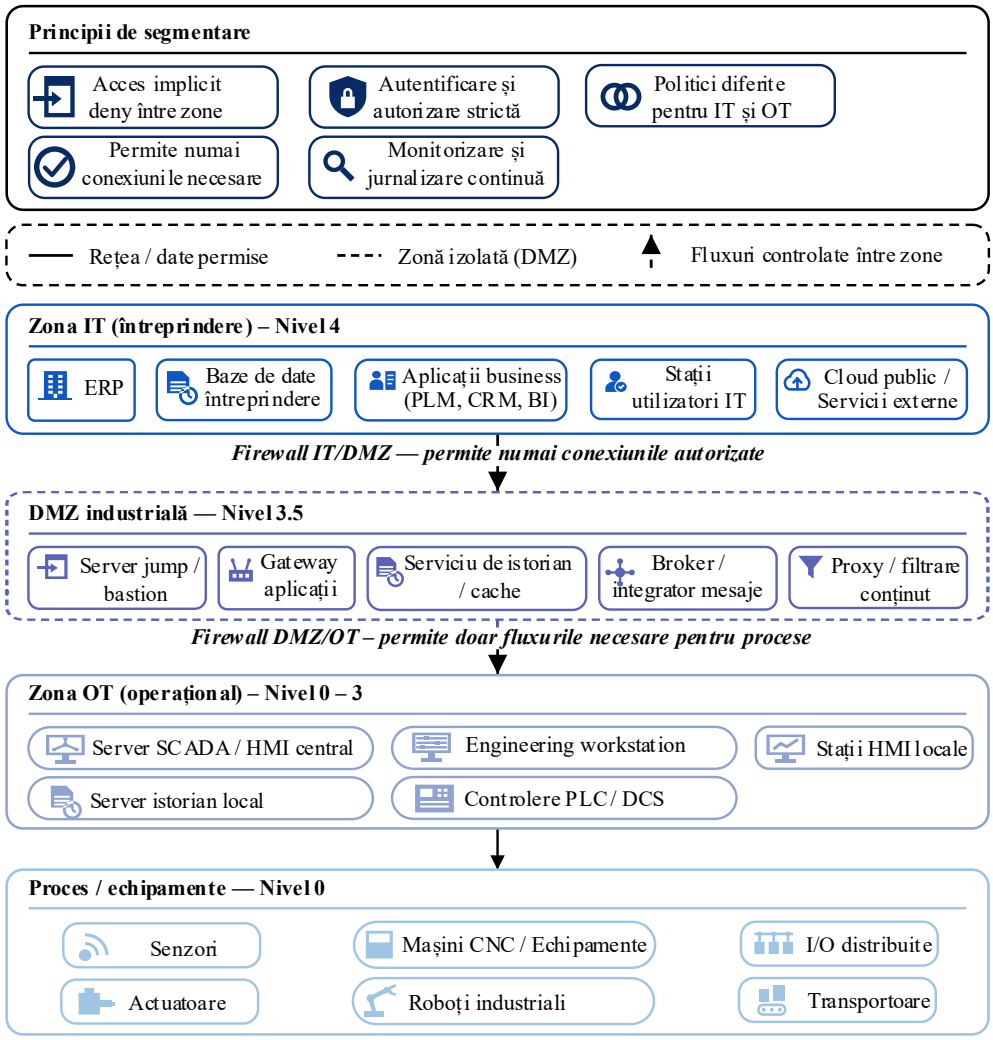


Figura 8.5 – Segmentarea IT–OT cu DMZ industrial

8.2.7. Accesul la distanță

Accesul la distanţă este necesar pentru diagnosticare, mentenanţă şi asistenţă tehnică, dar creează o cale suplimentară către sistemele industriale. Conectarea directă a unui calculator extern la un PLC, la o interfaţă HMI sau la o staţie de inginerie trebuie evitată.

Accesul trebuie să se facă printr-un punct controlat, fiecare utilizator având o identitate proprie şi folosind autentificarea multifactor. Conectarea trebuie aprobată explicit şi permisă numai pentru o durată şi într-un interval stabilite, cu acces doar la sistemele necesare, printr-un server intermediar de administrare. Activitatea trebuie consemnată în jurnale, iar sesiunea trebuie înregistrată atunci când

acest lucru este justificat. Operaţiile executate trebuie monitorizate, accesul trebuie să poată fi revocat imediat, iar conturile care nu mai sunt necesare trebuie dezactivate.

Conturile furnizorilor nu trebuie menţinute permanent active dacă accesul este utilizat numai pentru intervenţii ocazionale. Cerinţele aplicabile prestatorilor de servicii de integrare şi mentenanţă prevăd explicit administrarea conturilor pe durata contractului, retragerea lor la încheierea intervenţiei şi posibilitatea proprietarului activelor de a verifica modul în care furnizorul îşi respectă propriile proceduri [91]. Calculatorul de la distanţă trebuie verificat înaintea conectării, iar transferul fişierelor trebuie realizat printr-un mecanism controlat. Practicile recomandate pentru sistemele de control industrial prevăd segregarea accesului la distanţă şi intermedierea lui printr-un DMZ industrial, nu prin conexiuni directe către reţeaua de control [215].

Alegerea factorilor de autentificare pentru acest tip de acces nu este indiferentă. Un cod transmis printr-un canal separat protejează împotriva reutilizării unei parole compromise, dar nu împotriva unui atac în care utilizatorul este determinat să îl introducă într-o destinaţie falsă; factorii criptografici legaţi de destinaţia solicitată elimină această categorie de atac [232]. Într-o instalaţie în care accesul de la distanţă este singura cale către zona de control, distincţia merită considerată la proiectare, nu după primul incident.

Stabilirea unei sesiuni securizate nu înseamnă că modificarea procesului este automat permisă. Încărcarea unui program, modificarea parametrilor şi actualizarea firmware-ului trebuie să respecte procedurile de aprobare, testare şi revenire la configuraţia anterioară.

8.2.8. Consolidarea configuraţiei, monitorizarea şi recuperarea

Autentificarea, criptarea şi segmentarea trebuie completate prin consolidarea fiecărei componente. Configuraţia iniţială trebuie să elimine serviciile şi conturile inutile, să modifice credenţialele implicite şi să limiteze interfeţele de administrare.

Principalele măsuri pornesc de la inventarierea hardware-ului, software-ului şi firmware-ului şi stabilirea unei configuraţii de referinţă. Serviciile şi porturile neutilizate trebuie dezactivate, iar drepturile administrative trebuie limitate. Actualizările trebuie testate înainte de instalare, modificările configuraţiei trebuie monitorizate, iar fişierele de proiect şi cheile private trebuie protejate. Totodată, sunt necesare sincronizarea sigură a timpului, colectarea şi corelarea jurnalelor şi urmărirea termenelor de expirare a certificatelor. Copiile de siguranţă trebuie realizate, restaurarea lor trebuie testată periodic, iar unele copii trebuie păstrate în condiţii controlate, separat de sistemele operaţionale.

Aceste activităţi nu sunt independente şi nu pot fi întreţinute prin efort individual. Ele constituie obiectul unui program de securitate al proprietarului activelor, care stabileşte responsabilii, procedurile, frecvenţele şi înregistrările pentru

fiecare dintre ele [205], iar tratarea actualizărilor urmează un proces distinct, care asociază furnizorul de produs şi proprietarul instalaţiei în evaluarea aplicabilităţii, validarea şi planificarea fiecărei corecţii [218]. Sincronizarea timpului merită o menţiune separată: fără o referinţă temporală comună şi protejată, jurnalele colectate din zone diferite nu pot fi corelate, iar reconstituirea unui incident devine imposibilă [157], [35].

Monitorizarea defineşte profilul de referinţă al comunicaţiilor OT: dispozitive, protocoale şi perioade de interogare. Traficul repetitiv şi previzibil facilitează detectarea abaterilor comparativ cu IT, susţinând utilizarea modelelor comportamentale în locul detecţiei exclusiv prin semnături [214]. Evenimentele de identificat şi investigat includ conexiuni noi către PLC, modificări neaşteptate ale programelor, publicări în subiecte MQTT neautorizate şi încercări repetate de autentificare.

Detectarea nu are însă valoare fără capacitatea de a reacţiona şi de a reveni. Cele trei funcţii – detectare, răspuns, recuperare – sunt tratate distinct şi în cadrul de management al riscului cibernetic, tocmai pentru că a doua şi a treia trebuie pregătite înaintea incidentului, nu improvizate în timpul lui [239]. Capacitatea de restaurare se demonstrează prin teste, nu prin existenţa copiilor: o copie de siguranţă care nu a fost restaurată niciodată este o ipoteză, nu o măsură [234].

Sistemul trebuie proiectat şi pentru degradarea controlată. La pierderea conexiunii cu platforma, gateway-ul industrial păstrează temporar datele, iar controlul local continuă. La expirarea unui certificat, conexiunea este refuzată şi este generată o alertă, fără trecerea automată la o comunicaţie nesecurizată. La indisponibilitatea serviciului de autentificare, accesul administrativ extern poate fi blocat, dar funcţiile locale necesare operării sigure trebuie menţinute. Regula generală este că o defecţiune a mecanismelor de securitate trebuie să conducă la refuzul accesului, nu la suspendarea protecţiei.

În traseul IIoT analizat în Capitolul 7, măsurile formează un lanţ coerent: serverul OPC UA controlează clienţii şi drepturile de citire sau scriere; gateway-ul industrial este consolidat şi amplasat într-o zonă protejată; conexiunea MQTT utilizează TLS şi un certificat individual; politica brokerului limitează subiectele şi operaţiile conform convenţiei din secţiunea 8.2.4; baza de date aplică drepturi distincte şi copii de siguranţă; tabloul de bord utilizează controlul accesului bazat pe roluri şi jurnalizarea operaţiilor.

Eficienţa acestui lanţ depinde de aplicarea consecventă a măsurilor. O singură politică excesiv de permisivă sau o cheie privată compromisă poate reduce protecţia întregului traseu. Standardele şi cadrele prezentate în secţiunea 8.3 oferă metode sistematice pentru organizarea, evaluarea şi îmbunătăţirea acestor controale.

8.3. Standarde și cadre relevante pentru securitatea IIoT

Securitatea unui sistem IIoT trebuie susținută prin referințe recunoscute, care permit definirea cerințelor, repartizarea responsabilităților, evaluarea riscurilor și verificarea măsurilor implementate. Referințele utilizate în acest domeniu nu au însă același rol. Unele sunt standarde certificabile, altele sunt cadre pentru gestionarea riscului, modele arhitecturale sau baze de cunoștințe privind comportamentul atacatorilor. Confuzia dintre aceste categorii conduce la formulări lipsite de conținut, de tipul „instalația este conformă cu standardele de securitate", care nu precizează ce a fost cerut, ce a fost implementat și cine a verificat.

Pentru arhitecturile industriale sunt relevante în special:

- ISA/IEC 62443 – securitatea automatizării și controlului industrial, cu cerințe verificabile pentru sisteme și componente [216];
- NIST Cybersecurity Framework – gestionarea riscului cibernetic organizațional prin rezultate urmărite, fără prescrierea soluțiilor tehnice [239];
- ISO/IEC 27001 – cerințe certificabile pentru managementul securității informației [234];
- MITRE ATT&CK for ICS – baza de cunoștințe despre tacticile și tehnicile observate în atacuri industriale [220];
- Industrial Internet Security Framework – proprietățile de încredere ale arhitecturilor IIoT distribuite [240].

Aceste referințe sunt complementare. Niciuna nu trebuie tratată ca o listă universală de produse sau configurații care garantează automat securitatea.

8.3.1. Familia ISA/IEC 62443

Seria ISA/IEC 62443 constituie principala referință tehnică pentru securitatea sistemelor de automatizare și control industrial. Aceasta definește cerințe și procese aplicabile pe întregul ciclu de viață, de la proiectarea produselor și integrarea sistemului până la exploatarea și mentenanța instalației. Abordarea urmărește corelarea securității cibernetice cu disponibilitatea, integritatea, fiabilitatea și siguranța procesului industrial.

Responsabilitatea partajată constituie un principiu central al securității instalației, aceasta implicând mai mulți actori, dincolo de operatorul industrial și producătorul PLC-ului. Proprietarul activelor stabilește toleranța la risc, cerințele operaționale și regulile de exploatare, iar integratorul de sistem proiectează arhitectura, selectează componentele și implementează măsurile de securitate. Furnizorul produsului dezvoltă echipamente și aplicații cu funcții de securitate adecvate, în timp ce furnizorul de servicii asigură mentenanța, administrarea, actualizarea sau monitorizarea. Personalul de exploatare utilizează sistemul și aplică procedurile operaționale.

O componentă sigură nu compensează o arhitectură greşită, iar o arhitectură bine segmentată nu compensează utilizarea necorespunzătoare a produselor. Cerinţele trebuie corelate între toţi participanţii şi menţinute pe întreaga durată de exploatare.

Documentele seriei sunt organizate în patru grupe:

- 62443-1-x defineşte terminologia, conceptele, modelele şi elementele generale [216];
- 62443-2-x tratează programele de securitate, politicile, managementul actualizărilor şi cerinţele aplicabile proprietarilor de active şi furnizorilor de servicii [218], [91], [205];
- 62443-3-x tratează evaluarea riscurilor, proiectarea sistemului, zonele, conductele şi cerinţele tehnice aplicabile arhitecturii [68], [85];
- 62443-4-x defineşte cerinţele pentru procesul securizat de dezvoltare şi capabilităţile de securitate ale componentelor [213], [156].

Într-un proiect IIoT, documentele nu se selectează după tipul echipamentului, ci după etapa lucrării. Partea 3-2 se utilizează pentru evaluarea riscului şi stabilirea zonelor, partea 3-3 pentru definirea cerinţelor sistemului, partea 4-2 pentru selectarea componentelor, partea 4-1 pentru evaluarea procesului de dezvoltare al furnizorului, iar documentele din grupa 2 pentru organizarea exploatării şi a mentenanţei.

Distincţia dintre document tehnic şi raport tehnic are, în această serie, o consecinţă practică. Părţile 3-3 şi 4-2 conţin cerinţe verificabile, care pot fi invocate într-un caiet de sarcini şi pot face obiectul unei certificări; partea 2-3, dedicată gestionării corecţiilor, este un raport tehnic, cu caracter de recomandare şi cu un format propus pentru schimbul de informaţii între furnizor şi proprietarul activelor [218]. Confuzia dintre cele două categorii produce cerinţe contractuale care nu pot fi evaluate şi, invers, ignorarea unor documente utile pentru că „nu sunt standarde".

8.3.2. Zonele şi conductele de comunicaţie

ISA/IEC 62443 utilizează conceptele de zonă (zone) şi conductă (*conduit*) pentru structurarea sistemului analizat. O zonă grupează activele fizice sau logice care au cerinţe de securitate comune. O conductă grupează canalele de comunicaţie dintre două sau mai multe zone şi defineşte condiţiile în care informaţiile pot traversa limitele acestora. Partajarea sistemului analizat în zone şi conducte, evaluarea riscului pentru fiecare dintre ele şi stabilirea nivelului de securitate ţintă constituie cerinţe explicite ale metodei de evaluare a riscului pentru proiectarea sistemului [85].

O zonă nu este identică în mod obligatoriu cu o reţea locală virtuală, cu un dulap electric sau cu un nivel al modelului Purdue [192]. Aceste elemente pot fi utilizate

la implementare, dar delimitarea rezultă din analiza funcției, criticității, expunerii și consecințelor compromiterii activelor.

În arhitectura dezvoltată în Capitolul 7 pot fi definite, de exemplu, zonele și conductele din Figura 8.6:

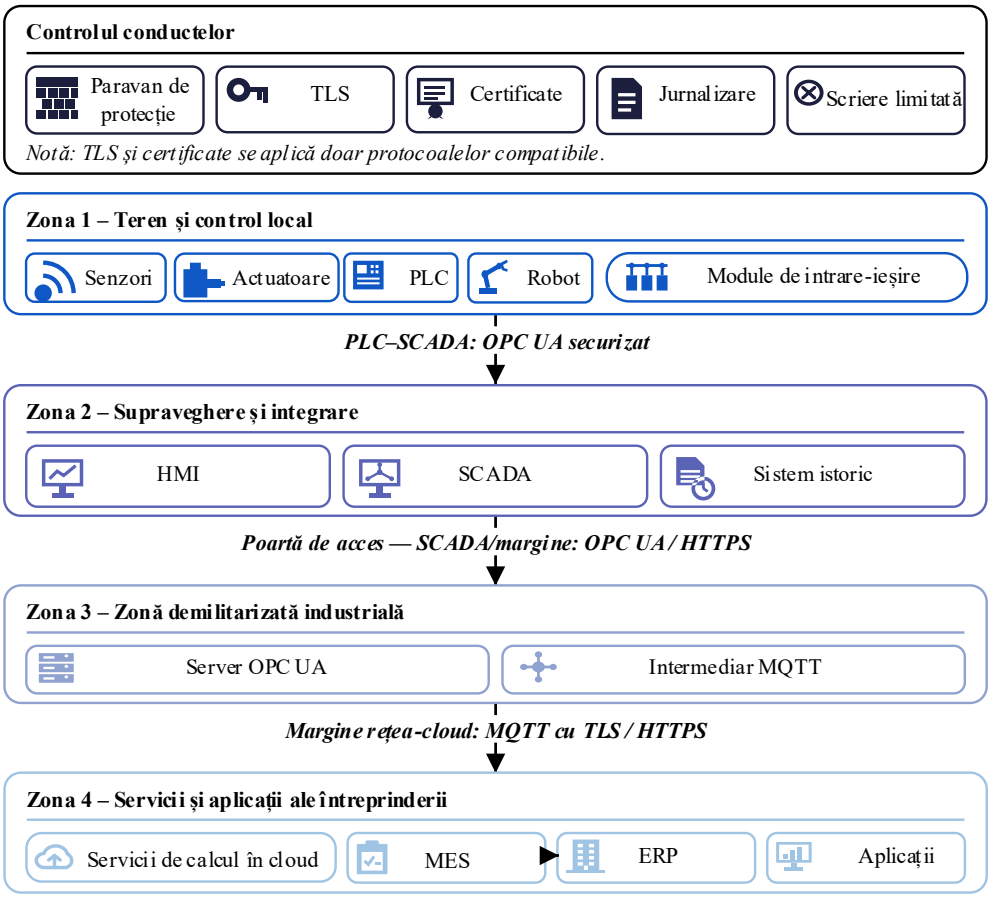


Figura 8.6 – Zonele și conductele IEC 62443 aplicate arhitecturii IIoT

- o zonă pentru senzori, actuatoare și controlerele procesului;
- o zonă pentru sistemele HMI, SCADA și serverul istoric;
- o zonă separată pentru stațiile de inginerie;
- un DMZ industrial pentru serviciile intermediare;
- o zonă pentru aplicațiile MES, ERP și bazele de date ale organizației;
- o zonă pentru platforma IIoT și serviciile cloud;
- o zonă temporară sau distinctă pentru accesul furnizorilor.

Conducta dintre zona de control și cea de supraveghere poate permite numai protocoalele necesare între PLC-uri și serverele aprobate. Conducta către DMZ poate permite replicarea datelor istorice sau transmiterea mesajelor printr-un

gateway industrial. Nu este justificată existența unei conducte directe între platforma externă și PLC.

Pentru fiecare conductă, trebuie precizat ce zone conectează, ce sisteme pot iniția comunicația și ce protocoale, servicii și identități sunt acceptate. Totodată, trebuie stabilite cerințele de criptare și de asigurare a integrității datelor, regulile de filtrare și de înregistrare în jurnale, modul de reacție la pierderea legăturii și nivelul de securitate care trebuie atins.

Delimitarea trebuie să țină cont și de activele care au cerințe diferite de restul sistemului. Un controler de siguranță poate necesita o zonă distinctă față de PLC-urile de proces, chiar dacă este instalat în același dulap; separarea funcțiilor instrumentate de siguranță de cele de control al procesului este o cerință de proiectare independentă de securitatea cibernetică, iar incidentul HatMan a arătat consecințele nerespectării ei [227]. În mod similar, stația de inginerie nu trebuie inclusă automat în zona HMI, deoarece drepturile sale permit modificări mai ample.

8.3.3. Cerințele fundamentale și nivelurile de securitate

Seria ISA/IEC 62443 definește șapte cerințe fundamentale, prezentate conceptual în partea 1-1 [216] și detaliate prin cerințe de sistem verificabile în partea 3-3: identificarea și autentificarea verifică utilizatorii, dispozitivele și aplicațiile; controlul utilizării limitează operațiile permise identităților autentificate; integritatea sistemului previne și detectează modificările neautorizate; confidențialitatea datelor protejează informațiile împotriva divulgării; restricționarea fluxului de date controlează comunicațiile dintre zone; răspunsul la timp la evenimente asigură detectarea, raportarea și tratarea incidentelor; disponibilitatea resurselor menține funcțiile necesare și limitează efectele indisponibilității.

Aceste cerințe permit trecerea de la formulări generale, precum „sistemul trebuie să fie sigur", la cerințe verificabile pentru autentificare, controlul accesului, integritatea comunicațiilor, jurnalizare, segmentare și disponibilitate [68]. Corespondența cu măsurile prezentate în secțiunea 8.2 este directă: identitățile individuale și certificatele X.509 servesc prima cerință, politicile pe subiecte MQTT și rolurile o servesc pe a doua, iar segmentarea și DMZ-ul industrial o servesc pe a cincea.

Nivelurile de securitate exprimă robustețea necesară în raport cu capabilitățile presupuse ale sursei amenințării. Nivelul SL 0 corespunde situației în care nu sunt formulate cerințe specifice, iar nivelurile următoare cresc progresiv:

- SL 1 urmărește protecția împotriva încălcărilor accidentale sau întâmplătoare;
- SL 2 urmărește protecția împotriva acțiunilor intenționate realizate cu mijloace simple, resurse reduse și cunoștințe generale;
- SL 3 presupune un atacator care utilizează mijloace sofisticate, resurse moderate și cunoștințe specifice sistemelor industriale;
- SL 4 presupune mijloace sofisticate, resurse extinse, cunoștințe industriale avansate și o motivație ridicată.

Nivelul nu se alege în funcție de importanța economică declarată a instalației. Acesta rezultă din evaluarea riscului și trebuie stabilit pentru fiecare zonă și conductă. O zonă care include funcții de siguranță poate necesita cerințe mai ridicate decât o zonă utilizată exclusiv pentru raportare.

În aplicarea standardului trebuie diferențiate: nivelul de securitate țintă, SL-T, stabilit prin evaluarea riscului; nivelul de securitate al capabilității, SL-C, pe care un sistem sau o componentă îl poate susține atunci când este integrat și configurat corespunzător [156]; nivelul de securitate realizat, SL-A, corespunzător soluției efectiv implementate și verificate.

Selectarea unui PLC certificat pentru un anumit nivel nu demonstrează că întreaga celulă atinge același nivel. Configurația, infrastructura de rețea, stația de inginerie, politicile de acces și procesele de mentenanță influențează nivelul realizat. Dacă o componentă existentă nu oferă toate funcțiile necesare, pot fi utilizate măsuri compensatorii la nivelul sistemului, dar acestea trebuie justificate și documentate.

Nivelurile pot fi reprezentate și sub forma unui vector asociat celor șapte cerințe fundamentale. Astfel, o zonă poate necesita un nivel ridicat pentru integritatea sistemului și disponibilitatea resurselor, dar un nivel diferit pentru confidențialitatea datelor. Această reprezentare este mai exactă decât atribuirea unui singur număr întreg întregii instalații.

Doi vectori SL-T pentru arhitectura din Capitolul 7:

Valorile de mai jos nu provin din standard, care nu prescrie niveluri pentru situații concrete; ele rezultă dintr-o evaluare de risc ipotetică, prezentată aici pentru a arăta forma pe care o ia rezultatul și tipul de raționament care îl produce.

Pentru zona de teren și control local – senzori, actuatoare, PLC-ul liniei, cu funcțiile instrumentate de siguranță plasate într-o zonă separată – se obține:

$$SL\text{-}T\ (control) = \{\ 2,\ 3,\ 3,\ 1,\ 3,\ 2,\ 3\ \}$$

Justificarea fiecărei componente: identificarea și autentificarea la nivelul 2, deoarece în zonă comunică dispozitive și aplicații cunoscute, nu utilizatori externi; controlul utilizării la 3, pentru că dreptul de scriere într-un nod de proces trebuie limitat strict și individual; integritatea sistemului la 3, pentru că o modificare de program produce efect fizic; confidențialitatea la 1, deoarece valorile instantanee de proces au valoare redusă pentru un atacator extern; restricționarea fluxului la 3, ca justificare a segmentării; răspunsul la evenimente la 2; disponibilitatea la 3, întrucât indisponibilitatea zonei înseamnă oprirea liniei.

Pentru zona platformei IIoT și a serviciilor cloud, în configurația exclusiv de monitorizare, rezultă:

$$SL\text{-}T\ (platformă) = \{\ 3,\ 2,\ 2,\ 3,\ 2,\ 3,\ 1\ \}$$

Aici identificarea urcă la 3, din cauza expunerii externe și a numărului de identități umane implicate; confidențialitatea urcă la 3, pentru că datele agregate de producție au valoare comercială; răspunsul la evenimente urcă la 3, deoarece zona este locul în care o intruziune poate fi detectată; iar disponibilitatea coboară la 1.

Interpretare şi limite. Cei doi vectori sunt aproape complementari: cerinţa cea mai ridicată a unei zone este cea mai coborâtă a celeilalte. Un singur număr atribuit „instalaţiei" ar fi ascuns exact această structură şi ar fi condus fie la supradimensionarea protecţiei datelor de proces, fie la subdimensionarea protecţiei datelor comerciale. A doua observaţie este mai importantă: valoarea 1 pentru disponibilitatea platformei nu este o constatare, ci o decizie de arhitectură – ea este admisibilă numai atât timp cât controlul local rămâne autonom şi procesul continuă în stare sigură fără platformă. Dacă platformei i se acordă vreodată o funcţie de comandă, această componentă trebuie recalculată la 3, iar odată cu ea se modifică segmentarea, cerinţele de redundanţă şi, în consecinţă, costul soluţiei. Vectorul face vizibilă legătura dintre o decizie funcţională aparent minoră şi consecinţele ei tehnice şi economice.

8.3.4. NIST Cybersecurity Framework 2.0

NIST Cybersecurity Framework 2.0 este un cadru pentru organizarea rezultatelor urmărite în gestionarea riscului cibernetic. Nu prescrie o arhitectură industrială şi nu stabileşte ce model de firewall sau ce protocol trebuie utilizat. Acesta oferă un limbaj comun pentru formularea situaţiei existente, a situaţiei urmărite şi a priorităţilor organizaţiei.

Versiunea 2.0, publicată în februarie 2024, este organizată în şase funcţii. Faţă de versiunea 1.1, care conţinea cinci funcţii, a fost introdusă funcţia Guvernează, iar domeniul de aplicare a fost extins de la infrastructurile critice la organizaţii de orice tip [239]:

- *Guvernează* – stabileşte strategia, politicile, responsabilităţile, supravegherea şi modul de integrare a riscului cibernetic în managementul organizaţiei;
- *Identifică* – inventariază activele, dependenţele, vulnerabilităţile şi riscurile;
- *Protejează* – aplică măsurile necesare pentru reducerea probabilităţii şi consecinţelor incidentelor;
- *Detectează* – identifică anomaliile, modificările şi evenimentele relevante;
- *Răspunde* – coordonează analiza, limitarea, comunicarea şi tratarea incidentului;
- *Recuperează* – restabileşte funcţiile şi îmbunătăţeşte sistemul pe baza experienţei acumulate.

Funcţiile nu reprezintă etape executate o singură dată şi nici o succesiune rigidă. Guvernanţa, identificarea, protecţia şi detectarea sunt activităţi continue, iar capacităţile de răspuns şi recuperare trebuie pregătite înaintea incidentului.

Într-un sistem IIoT, aplicarea poate începe prin construirea unui profil curent şi a unui profil ţintă. Profilul curent descrie, de exemplu, existenţa PLC-urilor neinventariate, a conturilor comune şi a conexiunilor care nu sunt monitorizate. Profilul ţintă introduce identităţi individuale, zone şi conducte, jurnalizare, copii de

siguranță verificate și proceduri pentru reacția la incident. Diferența dintre profiluri devine baza planului de îmbunătățire. Transpunerea rezultatelor în măsuri concrete pentru un mediu OT nu este însă furnizată de cadru și trebuie preluată dintr-un ghid specific, care ține cont de constrângerile de disponibilitate, de determinism și de siguranță ale procesului [25].

Nivelurile de implementare ale cadrului descriu caracterul proceselor de gestionare a riscului, de la practici parțiale și reactive până la practici adaptive. Ele nu trebuie interpretate automat ca un scor universal de maturitate și nici utilizate pentru compararea simplistă a unor organizații cu contexte diferite.

8.3.5. ISO/IEC 27001:2022

ISO/IEC 27001:2022 definește cerințele pentru stabilirea, implementarea, menținerea și îmbunătățirea continuă a unui sistem de management al securității informației. Standardul este aplicabil organizațiilor de orice dimensiune și poate include în domeniul său infrastructura IT, sistemele OT, aplicațiile IIoT, datele de producție și serviciile furnizate de terți [234]. Amendamentul publicat în 2024 a introdus cerința de a analiza dacă schimbările climatice constituie un aspect relevant pentru sistemul de management [241].

Aplicarea standardului presupune:

- definirea domeniului sistemului de management;
- înțelegerea contextului organizației și a cerințelor părților interesate;
- stabilirea responsabilităților;
- identificarea și evaluarea riscurilor;
- selectarea și justificarea controalelor;
- documentarea tratării riscurilor;
- monitorizarea performanței;
- efectuarea auditurilor interne;
- tratarea neconformităților;
- îmbunătățirea continuă.

ISO/IEC 27001 nu precizează în detaliu cum trebuie proiectată o celulă robotizată sau cum trebuie configurată o conductă între SCADA și DMZ-ul industrial. Aceste aspecte sunt tratate mai concret de ISA/IEC 62443. În schimb, ISO/IEC 27001 asigură cadrul prin care inventarul, responsabilitățile, furnizorii, schimbările, incidentele, continuitatea și auditarea sunt administrate la nivelul organizației.

Domeniul sistemului de management trebuie definit cu atenție. Excluderea formală a rețelei OT, în timp ce aplicațiile IT depind de datele provenite din aceasta, creează o separare artificială. Interfețele dintre domeniul inclus și componentele excluse trebuie identificate și tratate ca dependențe.

Declarația de aplicabilitate documentează controalele selectate, justificarea includerii sau excluderii lor și starea implementării. Setul de referință al acestor

controale, împreună cu îndrumarea privind implementarea fiecăruia, este cuprins în standardul asociat de bune practici, restructurat în 2022 pe patru teme – organizațională, umană, fizică și tehnologică [242]. Într-un mediu IIoT, declarația trebuie corelată cu arhitectura tehnică, registrul riscurilor și cerințele stabilite pentru zonele și conductele ISA/IEC 62443, astfel încât un control declarat implementat la nivel de organizație să aibă corespondent verificabil în configurația instalației.

8.3.6. MITRE ATT&CK for ICS

MITRE ATT&CK for ICS este o bază de cunoștințe privind tacticile și tehnicile observate în atacurile asupra sistemelor industriale. Aceasta nu este un standard de certificare și nu definește singură cerințele complete ale unui program de securitate.

Matricea grupează comportamentele atacatorului în tactici precum accesul inițial, execuția, persistența, evitarea mecanismelor de protecție, descoperirea sistemului, deplasarea laterală, colectarea datelor, inhibarea funcțiilor de răspuns, afectarea controlului procesului și producerea impactului [220].

Într-o analiză IIoT, matricea poate completa scenariile de risc construite conform secțiunii 8.1.7 și poate ajuta la identificarea punctelor în care o tehnică poate fi detectată. Totodată, permite verificarea măsurii în care mecanismele de monitorizare acoperă tehnicile analizate. Matricea poate fi folosită și pentru pregătirea exercițiilor de răspuns la incidente, corelarea evenimentelor observate în zone diferite și testarea măsurilor de apărare în condiții controlate.

De exemplu, scenariul modificării programului PLC (Figura 8.7) poate fi descompus în accesul la stația de inginerie, obținerea credențialelor, descoperirea controlerului, transferul proiectului alterat și inhibarea alarmelor. Această descompunere permite asocierea fiecărei etape cu sursele de jurnal, regulile de detecție și măsurile de limitare. Valoarea metodei se vede cel mai clar în analizele incidentelor reale: reconstituirea atacului asupra rețelei electrice ucrainene a fost organizată tocmai pe etapele parcurse de atacator, de la accesul inițial prin poștă electronică până la acțiunea asupra procesului, arătând că fiecare etapă a oferit, la momentul ei, o ocazie de detectare care nu a fost valorificată [225].

Absența unei tehnici dintr-un raport de monitorizare nu demonstrează că sistemul este protejat. Poate indica faptul că tehnica nu a fost executată, dar și faptul că infrastructura nu colectează datele necesare pentru detectarea ei. Distincția are consecințe practice: înaintea concluziei că o tehnică nu a fost utilizată, trebuie verificat dacă sursa de jurnal corespunzătoare există, este activă și este păstrată suficient timp.

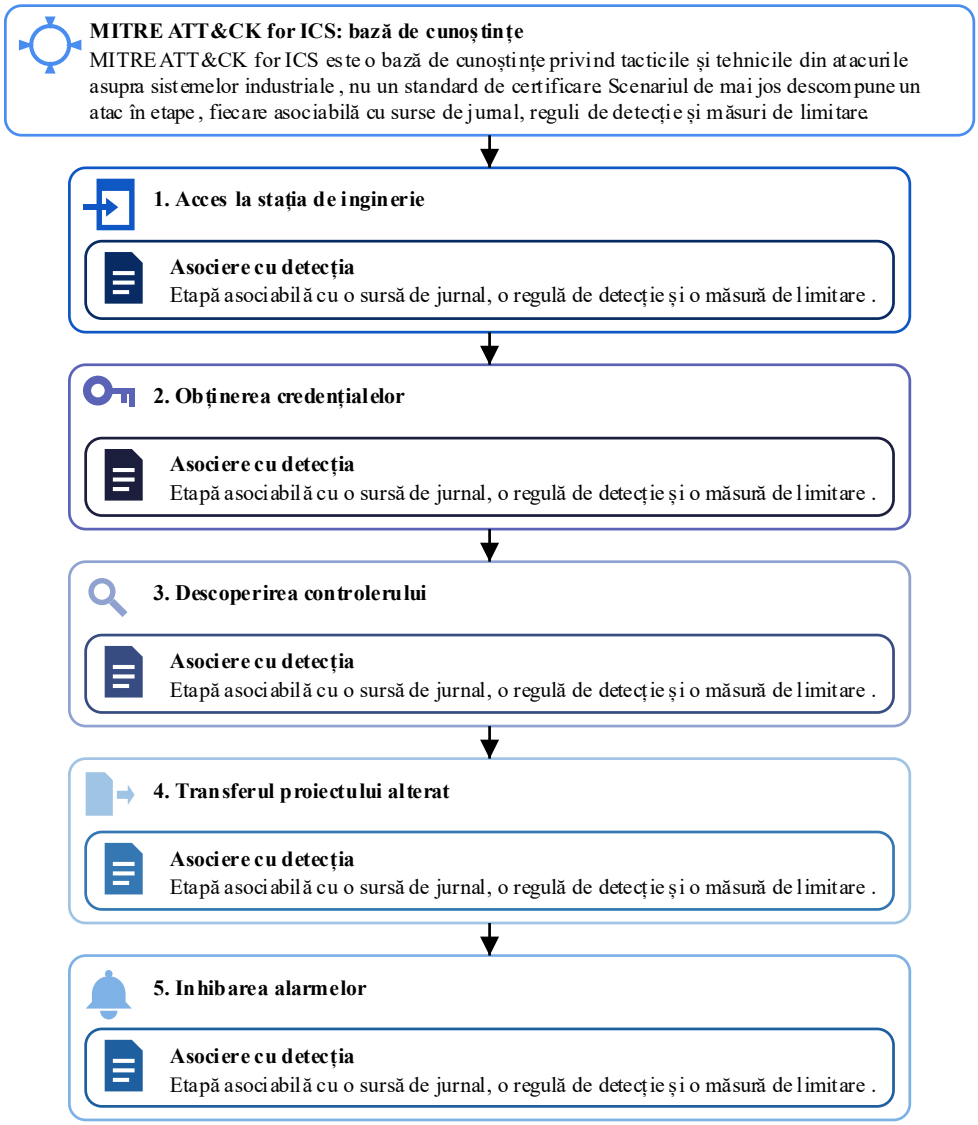


Figura 8.7 – Scenariul modificării programului PLC - 5 etape MITRE

8.3.7. Industrial Internet Security Framework

Industrial Internet Security Framework extinde analiza către sistemele IIoT distribuite, în care securitatea trebuie corelată cu siguranţa, fiabilitatea, rezilienţa şi protecţia informaţiilor. Cadrul tratează arhitecturile, punctele terminale, comunicaţiile, datele şi monitorizarea ca elemente ale unui sistem de încredere [240]. Documentul a fost publicat sub denumirea de atunci a organizaţiei, care astăzi poartă numele Industry IoT Consortium; citarea păstrează denumirea de la data publicării.

Utilitatea sa este mai evidentă în arhitecturile care includ produse şi servicii provenite de la mai mulţi furnizori, gateway-uri industriale, platforme externe, aplicaţii analitice şi schimburi de date între organizaţii. Cadrul sprijină analiza proprietăţilor sistemului la nivel de ansamblu, dar nu înlocuieşte cerinţele tehnice detaliate ale ISA/IEC 62443 şi nici sistemul de management definit de ISO/IEC 27001.

8.3.8. Utilizarea complementară a referinţelor

Referinţele prezentate pot fi utilizate într-un flux comun (Figura 8.8):

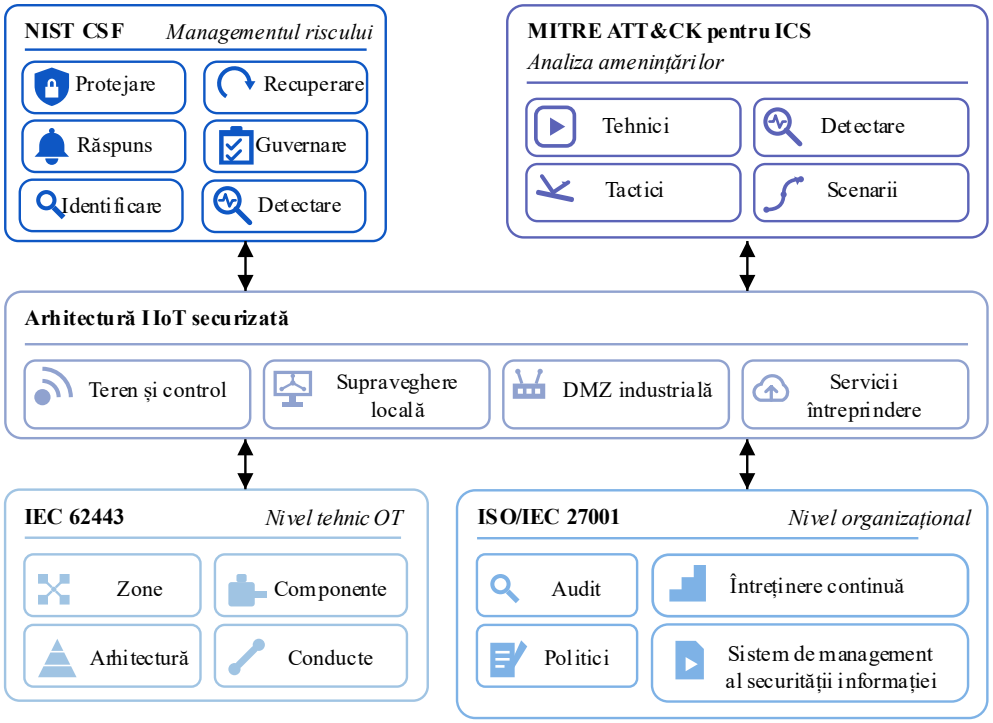


Figura 8.8 – Utilizarea complementară a IEC 62443, NIST CSF, ISO/IEC 27001 şi MITRE ATT&CK pentru ICS

- ISO/IEC 27001 stabileşte sistemul de management, responsabilităţile şi procesul de tratare a riscurilor;
- NIST CSF 2.0 organizează situaţia curentă, rezultatele urmărite şi priorităţile de îmbunătăţire;
- ISA/IEC 62443 structurează sistemul industrial în zone şi conducte şi defineşte cerinţele tehnice;
- MITRE ATT&CK for ICS completează scenariile cu tehnici şi comportamente observabile;
- Industrial Internet Security Framework verifică proprietăţile arhitecturii IIoT distribuite şi relaţia dintre securitate, siguranţă şi reziliență.

Tabelul 8.3 – Corelarea amenințărilor OT cu măsurile și referințele aplicabile

Amenințare sau scenariu	Măsuri principale	Referințe utilizate
acces neautorizat la PLC, HMI sau SCADA	identități individuale, autentificare, roluri, privilegiu minim, jurnalizare	ISA/IEC 62443 – identificare, autentificare și controlul utilizării; ISO/IEC 27001 – controlul accesului; NIST CSF – Protejează
modificarea programului sau a parametrilor	controlul schimbărilor, semnarea și verificarea proiectelor, limitarea stațiilor autorizate, copii de siguranță	ISA/IEC 62443 – integritatea sistemului; ISO/IEC 27001 – gestionarea schimbărilor; MITRE ATT&CK for ICS – modificarea controlului
deplasare laterală între IT și OT	zone și conducte, firewall-uri, DMZ industrial, acces administrativ intermediat	ISA/IEC 62443 – restricționarea fluxului de date; NIST CSF – Protejează și Detectează; MITRE ATT&CK for ICS – deplasare laterală
suprimarea alarmelor sau modificarea valorilor afișate	monitorizare independentă, protejarea jurnalelor, corelarea datelor, alertare	ISA/IEC 62443 – integritatea sistemului și răspunsul la evenimente; NIST CSF – Detectează și Răspunde; MITRE ATT&CK for ICS – inhibarea funcțiilor de răspuns
compromiterea gateway-ului industrial sau a identității MQTT	consolidarea configurației, certificat individual, TLS, politici pe subiecte, rotația cheilor	ISA/IEC 62443 – autentificare, integritate și flux restricționat; ISO/IEC 27001 – criptografie și managementul identităților; NIST CSF – Protejează
indisponibilitatea comunicației sau a platformei	control local autonom, stocare temporară, redundanță, copii de siguranță, plan de recuperare	ISA/IEC 62443 – disponibilitatea resurselor; ISO/IEC 27001 – continuitate; NIST CSF – Răspunde și Recuperează
compromiterea furnizorului sau a actualizării	evaluarea furnizorilor, verificarea proveniență, actualizări semnate, acces temporar și monitorizat	ISA/IEC 62443 – cerințe pentru furnizori și ciclul de dezvoltare; ISO/IEC 27001 – relațiile cu furnizorii; NIST CSF – Guvernează; MITRE ATT&CK for ICS – acces inițial
atac coordonat asupra procesului fizic	corelarea evenimentelor, protejarea funcțiilor de siguranță, proceduri de răspuns și revenire verificată	ISA/IEC 62443 – cerințe sistemice; NIST CSF – Detectează, Răspunde și Recuperează; MITRE ATT&CK for ICS – afectarea controlului procesului și impact

În cazul unei celule robotizate, precum cea din mini-proiectul din secţiunea 9.2.4, aplicarea începe prin separarea controlerelor robotului, PLC-ului şi dispozitivelor de siguranţă de sistemele de supraveghere. Staţia de inginerie formează o zonă cu drepturi controlate, iar gateway-ul industrial şi serviciile care transferă datele sunt amplasate într-o zonă intermediară. Platforma externă primeşte numai datele necesare şi nu are acces direct la funcţiile de control.

Evaluarea riscului stabileşte nivelurile ţintă pentru fiecare zonă şi conductă, sub forma vectorilor exemplificaţi în secţiunea 8.3.3. Cerinţele sunt apoi transformate în reguli de acces, configuraţii de reţea, criterii de selectare a componentelor, surse de jurnal şi proceduri de recuperare. Profilul NIST CSF descrie diferenţa dintre situaţia curentă şi cea urmărită, ISO/IEC 27001 integrează responsabilităţile şi verificarea în sistemul de management, iar MITRE ATT&CK for ICS permite testarea scenariilor şi a capacităţii de detectare. Tabelul 8.3 sintetizează această corelare,

asociind fiecărui tip de ameninţare măsurile principale şi referinţele care le fundamentează.

Standardele oferă astfel o metodă de proiectare şi verificare, nu o garanţie obţinută prin simpla lor menţionare. Aplicarea lor trebuie demonstrată prin arhitectură, configuraţii, proceduri, înregistrări şi rezultate de testare. Secţiunea 8.4 transpune aceste elemente în exerciţii de identificare a riscurilor şi de analiză controlată a măsurilor de securitate.

8.3.9. Cadrul de reglementare al Uniunii Europene

Standardele şi cadrele prezentate în această secţiune sunt, în principiu, voluntare. Produsele şi instalaţiile industriale conectate sunt însă supuse şi unor acte normative obligatorii ale Uniunii Europene, care transformă o parte din bunele practici de securitate în cerinţe legale. Pentru un proiect IIoT sunt relevante, în primul rând, patru astfel de acte.

Regulamentul (UE) 2024/2847 (Cyber Resilience Act) [69] stabileşte cerinţe de securitate cibernetică pentru produsele cu elemente digitale introduse pe piaţa Uniunii: securitate integrată în proiectare, configuraţii implicite sigure, actualizări de securitate pe durata de suport, gestionarea vulnerabilităţilor şi raportarea vulnerabilităţilor exploatate activ şi a incidentelor grave. Regulamentul a intrat în vigoare la 10 decembrie 2024; obligaţiile de raportare se aplică din 11 septembrie 2026, iar ansamblul cerinţelor, din 11 decembrie 2027. Fabricanţii, importatorii şi distribuitorii poartă responsabilităţi distincte, iar un integrator care introduce pe piaţă un produs sub propriul nume este tratat ca fabricant.

Directiva (UE) 2022/2555 (NIS2) [243] se adresează entităţilor esenţiale şi importante, printre care şi o parte din sectoarele de producţie, şi impune măsuri de gestionare a riscurilor de securitate cibernetică, inclusiv pentru securitatea lanţului de aprovizionare, precum şi notificarea incidentelor semnificative (avertizare timpurie în 24 de ore şi notificare în 72 de ore). Spre deosebire de regulamentul precedent, care priveşte produsul, directiva priveşte organizaţia care operează instalaţia şi se aplică prin legislaţia naţională de transpunere.

Regulamentul (UE) 2023/1230 privind maşinile [244], aplicabil din 20 ianuarie 2027, adaugă cerinţe privind protecţia împotriva coruperii sistemelor de comandă legate de siguranţă: o maşină conectată trebuie proiectată astfel încât o conexiune externă sau o actualizare să nu poată compromite funcţiile de siguranţă. Aceasta justifică, în arhitecturile din capitolele 6 şi 7, separarea strictă dintre controlul local şi fluxul de observare.

Regulamentul (UE) 2023/2854 (Data Act) [245] reglementează accesul la datele generate de produsele conectate şi utilizarea lor; implicaţiile pentru proiectarea fluxurilor de date sunt discutate în secţiunea 9.1.4.

Tabelul 8.4 – Acte normative ale Uniunii Europene relevante pentru produsele și instalațiile IIoT

Act normativ	Cine este vizat	Cerințe principale și aplicare
Regulamentul (UE) 2024/2847 (CRA)	Fabricanți, importatori și distribuitori de produse cu elemente digitale	Securitate pe ciclul de viață, gestionarea vulnerabilităților, raportare; raportarea din 11.09.2026, restul cerințelor din 11.12.2027
Directiva (UE) 2022/2555 (NIS2)	Entități esențiale și importante, inclusiv o parte din producție	Gestionarea riscurilor, lanțul de aprovizionare, notificarea incidentelor în 24 h și 72 h; aplicare prin legislația națională
Regulamentul (UE) 2023/1230 (mașini)	Fabricanții de mașini și de componente de siguranță	Protecție împotriva coruperii funcțiilor de siguranță; aplicabil din 20.01.2027
Regulamentul (UE) 2023/2854 (Data Act)	Fabricanți și deținători de date ai produselor conectate	Acces la datele generate; aplicabil din 12.09.2025, iar art. 3 alin. (1) pentru produse introduse după 12.09.2026

Tabelul 8.4 rezumă actele, destinatarii şi cerinţele principale; calendarul de aplicare trebuie verificat în versiunea în vigoare a fiecărui act.

Legătura cu standardele este practică: ISA/IEC 62443 şi ISO/IEC 27001 oferă metode verificabile prin care se poate demonstra îndeplinirea cerinţelor legale, dar respectarea lor nu înlocuieşte evaluarea conformităţii prevăzută de fiecare act. Calendarul de aplicare, categoriile de produse şi standardele armonizate sunt încă în curs de precizare; la proiectare se verifică versiunea în vigoare a fiecărui act pe portalul oficial EUR-Lex.

8.4. Exerciții aplicative: identificarea riscurilor și analiza securității unui sistem IIoT

Exerciţiile din această secţiune urmăresc transformarea principiilor prezentate anterior în activităţi de analiză, proiectare şi validare. Toate testele trebuie realizate într-un mediu izolat, utilizând echipamente de laborator, simulatoare sau copii ale configuraţiilor. Nu se vor executa teste asupra sistemelor aflate în producţie şi nu se vor dezactiva funcţiile de siguranţă ale procesului. Restricţia nu este o precauţie didactică: verificarea comportamentului la conexiuni neautorizate presupune generarea deliberată a unor condiţii de eroare, iar reacţia reală a unui echipament industrial la astfel de condiţii nu poate fi anticipată din documentaţie [25].

Cele trei exerciţii sunt formulate independent de producător: ele pot fi realizate cu orice server OPC UA, orice gateway industrial, orice broker MQTT şi orice bază de date care oferă funcţiile menţionate. Această alegere este deliberată, deoarece obiectul exerciţiilor îl constituie deciziile de securitate, nu deprinderea unei interfeţe de configurare anume. Valorile numerice, structura mesajelor şi criteriile de reuşită sunt însă precizate complet, astfel încât rezultatele obţinute de cititori diferiţi să poată fi comparate.

8.4.1. Exercițiul 1 – Evaluarea riscurilor unei linii de ambalare conectate IIoT

Obiectiv: identificarea și prioritizarea riscurilor asociate unei linii de ambalare care include senzori, actuatoare, un PLC, o interfață HMI, un sistem SCADA, un gateway industrial și o platformă IIoT.

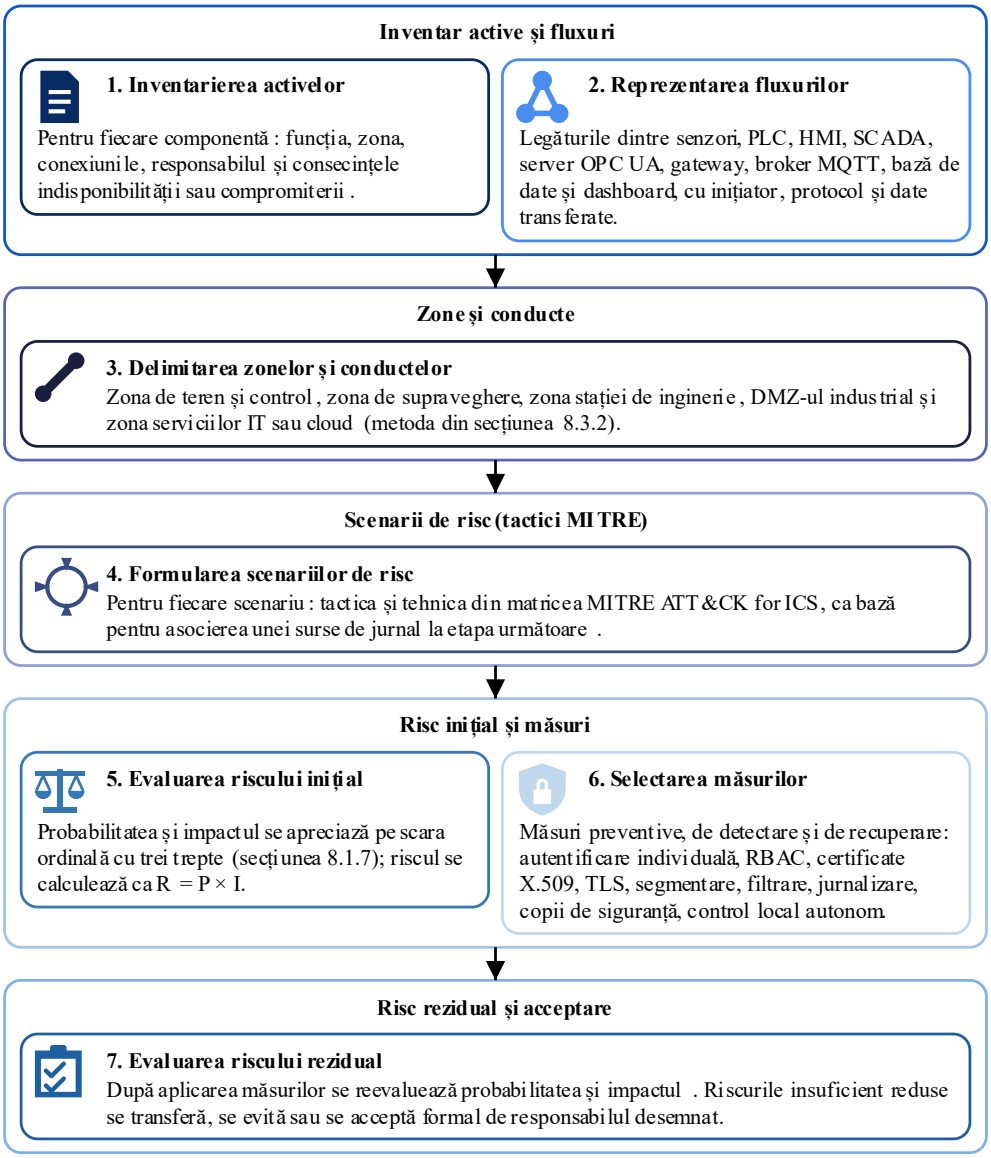


Figura 8.9 – Etapele evaluării riscului pentru linia de ambalare conectată IIoT

Scenariu: senzorii de proximitate, temperatură și presiune furnizează informații unui PLC care controlează transportoarele și actuatoarele liniei. Valorile procesului și stările echipamentelor sunt transmise către sistemul SCADA. Un gateway

industrial citește datele selectate prin OPC UA și le publică, prin MQTT, către o platformă externă. Platforma stochează datele și le afișează într-un tablou de bord.

Controlul procesului trebuie să continue local dacă gateway-ul industrial, conexiunea MQTT sau platforma externă devine indisponibilă.

Etapele exercițiului sintetizate în Figura 8.9

1. Inventarierea activelor. Pentru fiecare componentă se vor preciza funcția, zona în care este amplasată, conexiunile utilizate, responsabilul și consecințele indisponibilității sau compromiterii sale.
2. Reprezentarea fluxurilor. Se vor identifica legăturile dintre senzori, PLC, HMI, SCADA, serverul OPC UA, gateway-ul industrial, brokerul MQTT, baza de date și tabloul de bord. Pentru fiecare legătură se vor indica inițiatorul, protocolul și datele transferate.
3. Delimitarea zonelor și conductelor. Arhitectura va fi împărțită în zona de teren și control, zona de supraveghere, zona stației de inginerie, DMZ-ul industrial și zona serviciilor IT sau cloud, conform metodei prezentate în secțiunea 8.3.2 și cerințelor de partajare din standardul de evaluare a riscului pentru proiectarea sistemului [85].
4. Formularea scenariilor de risc. Analiza va include cel puțin situațiile enumerate mai jos; pentru fiecare se va indica tactica și tehnica corespunzătoare din matricea comportamentelor observate în atacurile asupra sistemelor industriale, astfel încât etapa următoare să poată asocia fiecărui scenariu o sursă de jurnal, nu doar o măsură de prevenire [220].
5. Evaluarea riscului inițial. Probabilitatea și impactul se apreciază pe scara ordinală cu trei trepte definită în secțiunea 8.1.7, iar riscul se calculează ca $R = P \times I$. Impactul se analizează asupra siguranței, disponibilității, calității produsului, integrității procesului și protecției informațiilor, reținându-se valoarea cea mai mare dintre acestea.
6. Selectarea măsurilor. Pentru fiecare scenariu se vor propune măsuri preventive, de detectare și de recuperare. Acestea pot include autentificarea individuală, controlul accesului bazat pe roluri, certificatele X.509, TLS, segmentarea, regulile de filtrare, jurnalizarea, copiile de siguranță și menținerea controlului local autonom.
7. Evaluarea riscului rezidual. După aplicarea măsurilor se reevaluează probabilitatea și impactul. Riscurile care nu pot fi reduse suficient trebuie transferate, evitate sau acceptate formal de responsabilul desemnat, cu consemnarea deciziei și a persoanei care o asumă.

La etapa 4, trebuie analizate cel puțin situațiile în care cineva accesează fără autorizare PLC-ul sau stația de inginerie, modifică logica de control ori parametrii procesului sau compromite un gateway industrial al cărui firmware nu este actualizat. În cazul comunicației MQTT, trebuie luate în considerare conectarea la

broker fără o identitate verificată, publicarea unor valori false într-un subiect autorizat şi abonarea fără permisiune la datele altor linii. Alte scenarii necesare sunt interceptarea sau modificarea comunicaţiei, indisponibilitatea conexiunii către platformă, extragerea neautorizată a datelor de producţie şi pierderea configuraţiei sau a bazei de date.

Tabelul 8.5 prezintă fişa completată pentru cinci dintre scenariile enumerate, cu valorile obţinute prin aplicarea etapelor 5–7. Ea serveşte ca model de lucru: cititorul reia calculul pentru propria instalaţie, unde probabilităţile şi impacturile pot fi diferite.

Tabelul 8.5 – Fișa de evaluare a riscurilor pentru linia de ambalare conectată IIoT

Activ sau flux	Scenariu de amenințare	Vulnerabilitate	Consecințe	P	I	R inițial	Măsuri propuse	P′	I′	R rezidual
PLC și stație de inginerie	modificarea neautorizată a programului	cont comun și acces nesegmentat	oprirea procesului sau comenzi incorecte	2	3	6	identități individuale, roluri, aprobarea modificărilor, jurnalizare, copie verificată a programului	1	3	3
Gateway industrial	compromiterea serviciului de comunicație	firmware neactualizat și servicii inutile active	acces la date și deplasare către zona OT	2	3	6	consolidare, actualizare testată, amplasare în DMZ industrial, monitorizare	1	2	2
Conexiune MQTT	interceptarea sau falsificarea mesajelor	lipsa TLS și a autentificării mutuale	divulgarea ori modificarea datelor	3	2	6	TLS 1.2 sau 1.3, certificat individual, verificarea completă a lanțului	1	2	2
Broker MQTT	publicare sau abonare neautorizată	politici excesiv de permisive	introducerea sau extragerea datelor	3	2	6	politici distincte pe subiecte și operații, refuz implicit	1	2	2
Platformă și bază de date	pierderea ori modificarea datelor	drepturi comune și copii neverificate	rapoarte incorecte, pierderea istoricului	2	2	4	roluri distincte, jurnalizare, copii de siguranță, testarea restaurării	1	2	2

Interpretarea rezultatelor conduce la trei observaţii care nu apar dintr-o citire superficială a tabelului. În primul rând, măsurile propuse reduc aproape exclusiv probabilitatea, nu impactul: consecinţa compromiterii unui PLC rămâne severă indiferent de calitatea controalelor de acces, motiv pentru care linia întâi păstrează un impact de 3 şi un risc rezidual mai mare decât celelalte. Reducerea acestui impact nu se obţine prin măsuri informatice, ci prin interblocări locale şi funcţii de siguranţă independente de sistemul de control. În al doilea rând, scenariile cu risc

inițial egal – patru dintre ele au valoarea 6 – nu au aceeași urgență: cele cu probabilitate 3 provin din absența unor măsuri elementare, care pot fi aplicate imediat și ieftin. În al treilea rând, valorile din coloanele de risc nu se însumează și nu produc un „scor de securitate" al liniei; ele ordonează intervențiile, atât.

Rezultatul exercițiului va fi un raport care conține arhitectura analizată, inventarul activelor, matricea riscurilor, măsurile propuse și justificarea riscurilor reziduale acceptate, cu numele responsabilului care le acceptă.

8.4.2. Exercițiul 2. Analiza securității fluxului OPC UA – edge – MQTT – servicii cloud

Obiectiv: analizarea securității scenariului integrator prezentat în Capitolul 7 și identificarea efectelor produse de eliminarea unor controale esențiale.

Fluxul analizat pornește de la serverul OPC UA și continuă prin gateway-ul industrial, care transmite datele printr-o conexiune MQTT securizată prin TLS către un broker MQTT sau o platformă. Datele sunt apoi stocate într-o bază de date și prezentate într-un tablou de bord.

Parametrii de lucru

Analiza se face pe o singură mărime, urmărită de la traductor până la tabloul de bord, cu valorile următoare, identice pentru toți cititorii:

- mărimea măsurată: presiunea din circuitul de umplere al liniei 01;
- domeniul de măsurare: 0–10 bar;
- precizia traductorului: ±0,5 % din domeniu, adică ±0,05 bar;
- frecvența de eșantionare în PLC: 10 Hz; frecvența de publicare către platformă: 1 Hz;
- valoarea nominală în regim stabilizat: 4,80 bar;
- viteza normală de variație în regim stabilizat: cel mult 0,05 bar/s;
- pragul de alarmă de proces: sub 4,20 bar sau peste 5,60 bar.

Se vor compara variantele degradate din Figura 8.10, rezultate prin eliminarea unor controale din configurația corectă: server OPC UA cu acces anonim și fără diferențierea drepturilor de citire și scriere; gateway industrial cu configurație implicită, în aceeași zonă cu PLC-urile; conexiune MQTT fără TLS și cu parolă comună mai multor dispozitive; broker MQTT cu publicare și abonare prin subiecte generale; bază de date cu un cont administrativ comun și fără copii de siguranță verificate; tablou de bord fără roluri și fără jurnalizarea modificărilor; platformă externă cu posibilitatea inițierii unor conexiuni directe către sistemele de control.

Pentru fiecare variantă, se vor determina limita de încredere traversată, identitatea sau resursa expusă și operația neautorizată care ar deveni posibilă. Analiza va evalua efectele asupra procesului și asupra datelor, posibilitățile de detectare a evenimentului, măsura preventivă necesară și mecanismul de recuperare, precum și riscul rezidual după aplicarea măsurilor.

Variantele 1 și 3 se analizează prin raportare la ceea ce protocolul oferă și la ceea ce lasă în sarcina configurației: OPC UA definește modurile de securitate și autorizarea, dar permite administratorului să le dezactiveze [223], iar TLS protejează canalul numai dacă lanțul de certificate este efectiv validat la ambele capete [203], [189].

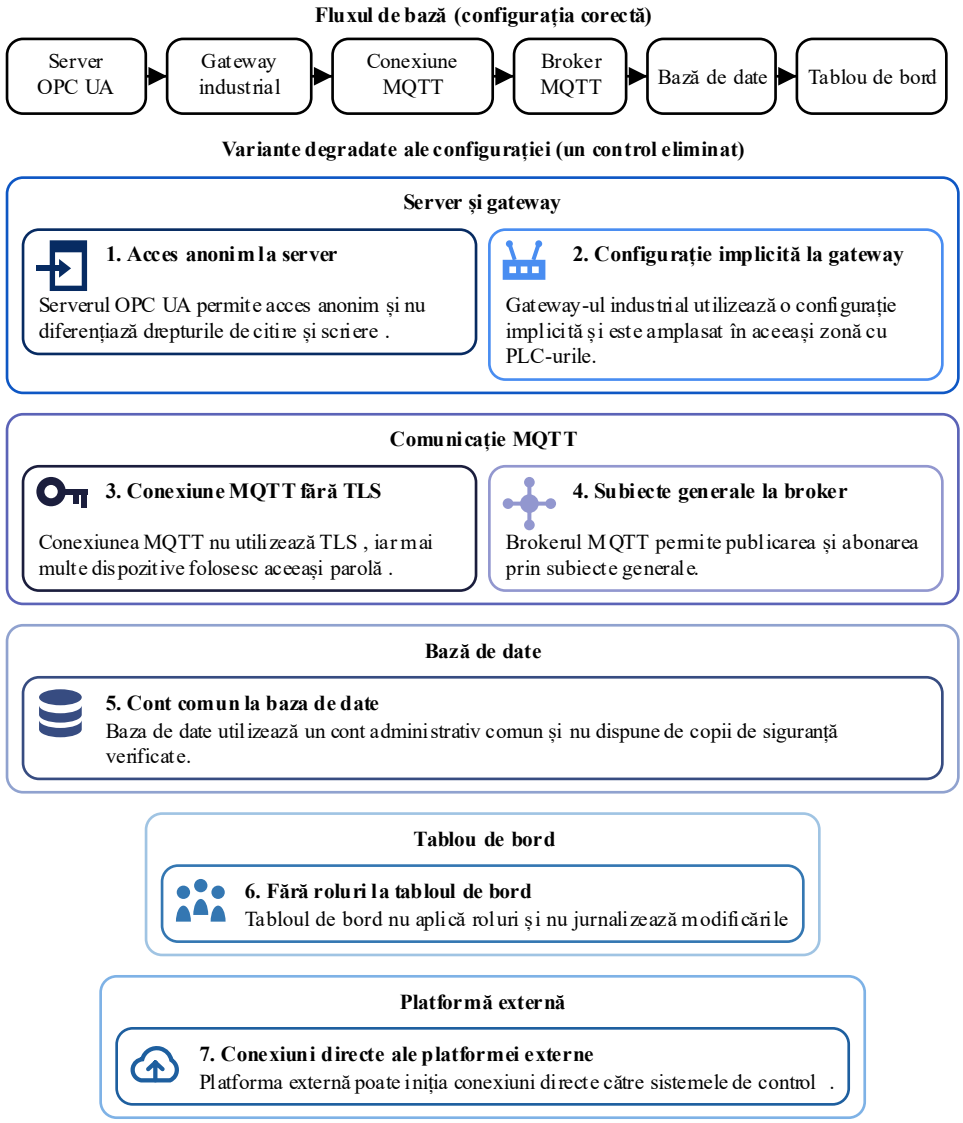


Figura 8.10 – Analiza de securitate a fluxului OPC UA–marginea rețelei–MQTT–servicii de calcul în cloud

Mesajul publicat și varianta lui falsificată

Analiza variantei 4 devine concretă numai dacă se lucrează cu structura reală a mesajului. Un mesaj corect, publicat de gateway în subiectul fabrica/sit01/linie01/umplere/telemetrie, are următorul conținut:

```
{
  "id_mesaj": "b7f3c2a1-4e8d-4f6b-9a12-7c5e0d3f8a41",
  "sursa": "gw-linie01",
  "echipament": "umplere",
  "variabila": "presiune_circuit",
  "valoare": 4.82,
  "unitate": "bar",
  "calitate": "buna",
  "marca_temporala_masurare": "2026-03-17T09:41:12.480Z",
  "marca_temporala_publicare": "2026-03-17T09:41:12.612Z",
  "nod_opcua": "ns=3;s=Linie01.Umplere.PresiuneCircuit",
  "versiune_schema": "1.0"
}
```

Câmpurile nu sunt opționale. Identificatorul mesajului permite eliminarea dublurilor la retransmitere; sursa și nodul OPC UA permit reconstituirea proveniență; unitatea de măsură previne interpretarea greșită a valorii; indicatorul de calitate transmite starea declarată de server, cu cele trei valori posibile buna, incerta și eronata; cele două mărci temporale, a măsurării și a publicării, nu se substituie una alteia, conform regulii stabilite în secțiunea 6.3. Denumirile câmpurilor se scriu fără diacritice și fără spații, pentru compatibilitate cu instrumentele de prelucrare. În formă compactă, fără spații de aliniere, mesajul ocupă aproximativ 370 de octeți; împreună cu subiectul și antetul MQTT, pachetul publicat are aproximativ 420 de octeți – valoare utilizată în exercițiul următor.

Un atacator care obține dreptul de publicare în acest subiect nu are nevoie să modifice structura mesajului. Este suficient să publice:

```
{
  "id_mesaj": "e1a9d4c7-2b60-4a31-8f77-19b4c6e2d05a",
  "sursa": "gw-linie01",
  "echipament": "umplere",
  "variabila": "presiune_circuit",
  "valoare": 4.35,
  "unitate": "bar",
  "calitate": "buna",
  "marca_temporala_masurare": "2026-03-17T09:41:14.480Z",
  "marca_temporala_publicare": "2026-03-17T09:41:14.590Z",
  "nod_opcua": "ns=3;s=Linie01.Umplere.PresiuneCircuit",
  "versiune_schema": "1.0"
}
```

De ce trece de verificările uzuale și ce anume îl poate opri

Mesajul este valid din punct de vedere sintactic, deci validarea de schemă îl acceptă. Valoarea de 4,35 bar se află în domeniul de măsurare 0–10 bar și peste

pragul de alarmă de 4,20 bar, deci verificarea de domeniu şi cea de alarmă îl acceptă. Mărcile temporale sunt coerente între ele şi ulterioare mesajului precedent, deci verificarea de ordonare îl acceptă.

Rămân trei verificări care îl pot identifica, iar exerciţiul trebuie să determine care dintre ele sunt implementate efectiv:

- Abaterea faţă de incertitudinea de măsurare. Diferenţa de 0,47 bar faţă de valoarea reală reprezintă de aproximativ nouă ori incertitudinea traductorului (±0,05 bar). Ea nu poate fi explicată prin zgomot de măsurare şi devine vizibilă imediat ce fluxul falsificat este comparat cu cel legitim, care continuă să circule.
- Viteza de variaţie. Între cele două mesaje au trecut 2,0 s, deci rata implicită este 0,47 / 2,0 = 0,235 bar/s, de aproximativ 4,7 ori peste valoarea maximă declarată în regim stabilizat (0,05 bar/s). Un detector de rată configurat cu pragul declarat respinge mesajul; unul configurat „generos", la 0,5 bar/s, nu îl respinge.
- Numărul de mesaje. Dacă gateway-ul publică o valoare pe secundă, iar în baza de date apar două mesaje în aceeaşi secundă, cu identificatori diferiţi şi aceeaşi sursă declarată, discrepanţa este detectabilă prin simpla comparare a numărului de mesaje primite cu cel raportat de gateway.

Limita analizei – toate cele trei verificări sunt statistice şi pot fi ocolite de un atacator care îşi reduce ambiţia: o abatere de 0,08 bar aplicată treptat rămâne sub pragul de rată, se află la marginea incertitudinii de măsurare şi totuşi deplasează media unui raport de schimb. Concluzia exerciţiului este că detecţia pe conţinut întârzie sau ratează atacul, în timp ce identitatea autentificată prin certificat şi politica pe subiecte îl împiedică din start. Detecţia nu înlocuieşte controlul accesului; ea acoperă intervalul dintre compromitere şi reacţie.

Analiza trebuie să răspundă şi următoarelor întrebări:

- Ce se întâmplă dacă dispozitivele nu utilizează certificate individuale?
- Ce consecinţe produce absenţa segmentării dintre platformă şi sistemul de control?
- De ce utilizarea TLS nu înlocuieşte politicile aplicate subiectelor MQTT?
- De ce identificatorul clientului MQTT nu este suficient pentru autentificare?
- Ce funcţii trebuie să continue la pierderea conexiunii cu platforma?
- Cum trebuie să reacţioneze sistemul la expirarea sau revocarea unui certificat?
- Ce informaţii sunt necesare în jurnale pentru reconstruirea unui incident?

Rezultatul va evidenţia faptul că securitatea traseului nu depinde de un singur mecanism. Protecţia este obţinută prin asocierea autentificării, autorizării, segmentării, criptării, monitorizării şi recuperării.

8.4.3. Exercițiul 3. Validarea controlată a măsurilor de securitate

Obiectiv: verificarea comportamentului arhitecturii în cazul conexiunilor neautorizate, al configuraţiilor incorecte şi al indisponibilităţii unor servicii.

Mediul de testare va conţine un server OPC UA de simulare, un gateway industrial, un broker MQTT izolat, o bază de date de test şi un tablou de bord. Datele utilizate vor fi simulate şi nu va exista nicio conexiune cu echipamentele aflate în exploatare. Înaintea începerii testelor se consemnează configuraţia de referinţă a fiecărei componente, astfel încât abaterile observate să poată fi atribuite testului, nu unei diferenţe iniţiale. Rostul acestei etape este ca fiecare cerinţă formulată să fie verificată printr-un test cu rezultat observabil, nu prin declaraţia că măsura a fost implementată [68].

Tabelul 8.6 – Criterii pentru validarea măsurilor implementate

Test	Comportament aşteptat	Dovadă necesară
Client OPC UA neautorizat	Conexiune refuzată la stabilirea sesiunii, fără mesaj care să dezvăluie motivul exact solicitantului	Eveniment în jurnalul serverului, cu identitatea prezentată și momentul respingerii
Operație de scriere nepermisă	Operație blocată, citirile autorizate ale aceluiași client continuă neafectate	Identitatea, nodul și operația înregistrate
Certificat MQTT nevalid	Conexiune refuzată, fără reîncercare automată cu o metodă mai slabă de autentificare	Cauza verificării eșuate și momentul evenimentului
Certificat expirat sau revocat	Conexiune refuzată, alertă generată către responsabilul desemnat	Înregistrarea verificării stării de revocare
Publicare într-un subiect neautorizat	Mesaj respins, conexiunea clientului menținută sau închisă conform politicii declarate	Identificatorul clientului, subiectul și politica aplicată
Abonare la datele altei linii	Abonare refuzată, fără livrarea niciunui mesaj	Cererea de abonare și decizia brokerului
Pierderea conexiunii cloud	Controlul local continuă fără întrerupere, datele sunt păstrate temporar în gateway	Starea procesului și evidența mesajelor stocate, cu numărul lor
Restabilirea conexiunii	Datele sunt retransmise în ordine, fără dublare necontrolată	Succesiunea temporală, confirmarea recepției și verificarea unicității identificatorilor
Restaurarea configurației	Serviciul revine la configurația aprobată, fără intervenții manuale nedocumentate	Raportul restaurării și verificarea funcțională

Testele vor verifica ce se întâmplă atunci când un client OPC UA neînregistrat încearcă să se conecteze sau să scrie într-un nod care permite numai citirea. Pentru MQTT, se vor testa conectarea cu un certificat emis de o autoritate neacceptată, utilizarea unui certificat expirat sau revocat, publicarea într-un subiect care nu este atribuit dispozitivului şi abonarea la datele unei alte linii. Se va întrerupe temporar conexiunea dintre gateway şi platformă, apoi se vor verifica reluarea comunicaţiei şi retransmiterea datelor păstrate temporar. Totodată, se va testa restaurarea configuraţiei gateway-ului şi a datelor dintr-o copie de siguranţă.

Testul 4 merită o precizare: expirarea și revocarea nu se verifică prin același mecanism. Expirarea rezultă din citirea certificatului, în timp ce revocarea presupune consultarea unei liste distribuite sau interogarea unui serviciu de stare [236]. Un sistem care refuză corect certificatul expirat, dar acceptă certificatul revocat, a trecut numai jumătate din test – iar cazul revocării este cel care apare atunci când o cheie privată a fost compromisă. Criteriile de acceptare pentru fiecare test sunt prezentate în Tabelul 8.6.

Verificarea cantitativă a comportamentului la întrerupere

Testele 7 și 8 permit o verificare numerică, cu rezultat previzibil înainte de execuție. Se măsoară durata întreruperii, numărul de mesaje generate în acest interval și numărul de mesaje regăsite în baza de date după restabilire. Dacă gateway-ul publică o valoare la fiecare secundă, iar întreruperea durează 180 de secunde, în baza de date trebuie să apară exact 180 de mesaje suplimentare, cu identificatori unici și cu mărcile temporale ale măsurării păstrate, nu înlocuite cu momentul retransmiterii. Orice abatere de la acest număr indică fie o pierdere de date, fie o dublare, fie o suprascriere a mărcii temporale – trei defecte cu efecte diferite asupra rapoartelor și care trebuie diferențiate.

Aceeași verificare permite și dimensionarea memoriei tampon, adică stabilirea duratei maxime de întrerupere pe care arhitectura o suportă fără pierderi. Se consideră șapte variabile publicate la 1 Hz, cu pachete de aproximativ 420 de octeți fiecare, conform structurii din exercițiul anterior:

$$D = 7 \times 420 = 2\,940 \text{ octeți/s} \approx 2{,}9 \text{ kB/s}$$

Pe durata întreruperii de 180 s rezultă aproximativ 530 kB de date păstrate temporar – o valoare neglijabilă. Pentru o memorie tampon de 100 MB alocată acestei funcții, orizontul de acoperire este:

$$T(\max) = 100 \times 10^{6} / 2\,940 \approx 34\,000 \text{ s} \approx 9{,}4 \text{ ore}$$

Interpretare și limite: rezultatul transformă o afirmație calitativă – „gateway-ul păstrează temporar datele" – într-o cerință verificabilă: arhitectura tolerează o întrerupere de cel mult aproximativ nouă ore la această configurație. Dincolo de acest prag, comportamentul trebuie declarat explicit în proiect: fie se suprascriu datele cele mai vechi, fie publicarea se oprește, fie se comută pe o stocare secundară. Alegerea este o decizie de securitate, nu una de implementare, pentru că determină ce anume se pierde dintr-un istoric care poate fi ulterior necesar pentru reconstituirea unui incident. Calculul are trei limite: nu include supraîncărcarea protocoalelor de transport și a stratului TLS, care poate adăuga între 5 și 15 % în funcție de dimensiunea pachetelor; presupune o rată de publicare constantă, în timp ce mesajele de eveniment apar în rafale; și ignoră eventuala compresie aplicată la stocarea locală, care poate extinde semnificativ orizontul pentru date repetitive. Toate cele trei

componente se măsoară pe configuraţia reală, iar valoarea obţinută se consemnează ca parametru de proiect.

Validarea nu se încheie prin constatarea faptului că o conexiune a fost refuzată. Trebuie verificat dacă evenimentul a fost înregistrat, dacă alerta a ajuns la responsabilul desemnat, dacă funcţia industrială a rămas într-o stare sigură şi dacă revenirea la funcţionarea normală poate fi realizată printr-o procedură documentată. Ultimele două verificări corespund funcţiilor de răspuns şi de recuperare, care sunt tratate distinct tocmai pentru că trebuie exersate înaintea incidentului [239].

Documentaţia finală va include configuraţia mediului de testare, condiţiile iniţiale, rezultatul fiecărui test, jurnalele relevante, abaterile observate şi acţiunile corective propuse.

8.5. Concluzii

Conectarea sistemelor de automatizare la gateway-uri industriale, platforme IIoT şi servicii externe transformă securitatea cibernetică într-o cerinţă de arhitectură, nu într-un strat adăugat ulterior. În mediul OT, compromiterea datelor sau a comunicaţiilor poate afecta direct disponibilitatea procesului, calitatea producţiei, integritatea echipamentelor şi siguranţa personalului, motiv pentru care priorităţile diferă de cele ale sistemelor informatice de birou şi impun soluţii adaptate duratelor lungi de exploatare, ferestrelor scurte de oprire şi protocoalelor moştenite.

Analiza riscului precedă alegerea măsurilor. Delimitarea activelor, ameninţărilor, vulnerabilităţilor, vectorilor de atac şi consecinţelor permite construirea unor scenarii verificabile, iar exemplul dezvoltat în capitol arată că aceeaşi vulnerabilitate produce riscuri diferite în funcţie de amplasarea activului, de drepturile acordate şi de măsurile compensatorii existente. Rezultatele unei astfel de evaluări ordonează intervenţiile; ele nu constituie estimări ale pierderii şi nu pot fi agregate într-un indicator unic de securitate al instalaţiei.

Protecţia eficientă rezultă din asocierea măsurilor tehnice şi organizatorice pe întregul ciclu de viaţă. Identităţile individuale, autorizarea explicită a operaţiilor, certificatele administrate pe tot parcursul ciclului lor de viaţă, criptarea corect configurată, segmentarea, DMZ-ul industrial, controlul accesului la distanţă, consolidarea configuraţiilor, monitorizarea şi verificarea recuperării formează un lanţ în care veriga cea mai slabă determină nivelul real de protecţie. O politică prea permisivă aplicată subiectelor unui broker sau o cheie privată păstrată neprotejat anulează efectul celorlalte controale. Granularitatea drepturilor depinde de decizii aparent minore, precum convenţia de denumire a subiectelor, care trebuie stabilită înaintea configurării, nu după.

Capitolul a arătat, prin trei calcule elementare, că deciziile de securitate sunt şi decizii de dimensionare. O politică de valabilitate a certificatelor este administrabilă sau nu în funcţie de numărul de identităţi şi de distribuţia momentelor de

emitere; nivelul de securitate al unei zone se exprimă corect printr-un vector asociat celor șapte cerințe fundamentale, iar aplatizarea lui la un singur număr ascunde tocmai diferențele care justifică arhitectura; durata de întrerupere pe care sistemul o suportă fără pierderi rezultă din debitul de date și din memoria disponibilă, nu dintr-o afirmație de principiu. Valorile obținute sunt orientative și trebuie refăcute pentru fiecare instalație, dar forma raționamentului se păstrează: o cerință de securitate devine verificabilă numai atunci când este exprimată printr-un număr, un prag sau un criteriu observabil.

Controlul procesului trebuie să rămână local și să poată continua într-o stare sigură atunci când comunicația cu serviciile externe devine indisponibilă. Regula complementară este că o defecțiune a mecanismelor de securitate – un certificat expirat, un serviciu de autentificare indisponibil – trebuie să conducă la refuzul accesului și la generarea unei alerte, nu la suspendarea protecției.

ISA/IEC 62443, NIST CSF 2.0, ISO/IEC 27001 și MITRE ATT&CK for ICS oferă perspective complementare pentru proiectarea, administrarea și validarea acestor măsuri, cu roluri distincte: cerințe tehnice structurate pe zone și conducte, organizarea rezultatelor urmărite, sistemul de management și, respectiv, comportamentele observabile ale atacatorilor. Conformitatea declarată sau utilizarea unor componente certificate nu demonstrează securitatea întregului sistem; nivelul realizat depinde de configurație, de infrastructura de rețea, de procesele de mentenanță și trebuie confirmat prin proceduri aplicabile, jurnalizare și teste efectuate într-un mediu izolat, cu criterii de reușită stabilite în prealabil.

Pe această bază, Capitolul 9 urmărește integrarea conceptelor tehnologice, arhitecturale și de securitate în aplicații industriale și mini-proiecte ghidate, în care soluția IIoT este analizată ca sistem complet, de la achiziția datelor până la utilizarea lor în deciziile operaționale.

8.6. Întrebări de verificare

1. *Care este diferența dintre o vulnerabilitate și un vector de atac, conform vocabularului folosit în capitol?*

a) cei doi termeni sunt sinonimi și pot fi folosiți interschimbabil;
b) vulnerabilitatea este o slăbiciune de proiectare, configurare, implementare sau exploatare; vectorul de atac este calea prin care amenințarea poate exploata acea slăbiciune;
c) vulnerabilitatea este cauza potențială a incidentului; vectorul de atac este efectul asupra procesului;
d) vulnerabilitatea este echipamentul protejat; vectorul de atac este probabilitatea incidentului.

2. *De ce nu pot fi transferate mecanic în mediul OT practicile de securitate din sistemele IT?*

a) deoarece în OT nu există nicio cerinţă de confidenţialitate;
b) deoarece echipamentele OT nu pot fi conectate în rețea;
c) deoarece actualizările nu trebuie testate niciodată în producţie;
d) deoarece echipamentele OT au durate lungi de exploatare, posibilităţi limitate de actualizare, intervale scurte de oprire, iar măsurile trebuie corelate cu performanţa, fiabilitatea şi siguranţa procesului.

3. *Care este diferența dintre pierderea controlului şi pierderea vizibilităţii asupra procesului?*

a) pierderea vizibilităţii opreşte automat procesul, iar pierderea controlului nu are efect;
b) sunt acelaşi fenomen, descris prin termeni diferiţi;
c) în cazul pierderii vizibilităţii procesul poate continua să funcţioneze fără ca operatorul să-i cunoască starea; în cazul pierderii controlului funcţia de control este degradată sau lipseşte;
d) pierderea controlului afectează doar baza de date istorică.

4. *De ce nu este suficientă verificarea domeniului numeric al unei valori pentru a detecta un mesaj fals?*

a) deoarece valorile false pot fi menţinute în limite plauzibile; trebuie analizate şi ritmul variaţiei, relaţia cu alte mărimi şi starea procesului;
b) deoarece un mesaj fals are întotdeauna o valoare imposibilă, deci verificarea domeniului nu este necesară;
c) deoarece domeniul numeric este stabilit doar de brokerul MQTT;
d) deoarece mesajele false pot fi detectate numai prin criptare.

5. *Acelaşi gateway vulnerabil este evaluat pe o scară ordinală 1–3 (R = P × I). În bancul de testare P = 2 şi I = 1, în instalaţia în funcţiune P = 2 şi I = 3, iar după tratare P = 1 şi I = 2. Care sunt valorile riscului?*

a) 3, 5, 3;
b) 2, 6, 4;
c) 2 (bancul de testare), 6 (instalaţia în funcţiune), 2 (după tratare);
d) 1, 6, 2.

6. *Cum diferă identificarea, autentificarea şi autorizarea?*

a) cele trei operaţii sunt echivalente şi se realizează printr-o singură parolă comună;
b) identificarea declară cine este entitatea, autentificarea verifică identitatea, autorizarea stabileşte ce operaţii îi sunt permise
c) identificarea stabileşte drepturile, autentificarea declară numele, autorizarea criptează traficul;
d) autentificarea declară identitatea, iar identificarea o verifică.

7. *O instalație are 180 de identități cu certificate valabile 24 de luni, reînnoite după consumarea a două treimi din perioadă. Câte reînnoiri pe lună rezultă în medie?*

a) 180 / 16 = 11,25 reînnoiri pe lună, deoarece ciclul efectiv de reînnoire este de 16 luni;
b) 180 / 8 = 22,5 reînnoiri pe lună;
c) 180 / 24 = 7,5 reînnoiri pe lună;
d) 180 × 16 = 2 880 reînnoiri pe lună.

8. *Ce verificare este cel mai des omisă la autentificarea mutuală cu certificate?*

a) existența unei chei publice în certificat;
b) starea de revocare a certificatului;
c) numele aplicației din certificat;
d) perioada de valabilitate a certificatului.

9. *De ce ierarhia subiectelor MQTT trebuie să conțină situl și linia, nu doar echipamentul?*

a) pentru că brokerul nu poate stoca mesaje fără numele liniei;
b) pentru că standardul MQTT interzice subiectele fără sit;
c) pentru a elimina necesitatea certificatelor individuale;
d) pentru ca politica de acces să poată separa liniile între ele fără enumerarea individuală a fiecărui echipament.

10. *Ce este DMZ-ul industrial („nivelul 3.5”) și ce regulă se aplică transferului de date către platformă?*

a) un segment intermediar între nivelurile 3 și 4; gateway-ul inițiază conexiunea securizată către un serviciu intermediar, fără acces direct din exterior spre rețeaua OT;
b) un echipament cu două interfețe care ocolește firewall-ul pentru a accelera transferul;
c) un nivel al ERP, în care platforma cloud se conectează direct la PLC;
d) un segment între nivelurile 0 și 1, în care sunt amplasați senzorii.

9. APLICAȚII INDUSTRIALE ȘI MINI-PROIECTE GHIDATE

Capitolele anterioare au construit, pas cu pas, elementele unei soluții IIoT: contextul digitalizării industriale și rolul datelor, organizarea companiei și fluxul comenzii, tipurile de producție și corespondența lor arhitecturală, sistemele flexibile și reconfigurabile, dispozitivele de măsurare și acționare împreună cu automatele programabile, protocoalele de comunicație, arhitectura integrată și măsurile de securitate. Fiecare capitol a tratat un segment. Capitolul de față le reunește în aplicații care rezolvă probleme industriale concrete și care pot fi realizate, măsurate și verificate.

Reunirea nu este o simplă însumare. O soluție IIoT devine utilă abia atunci când datele produc o decizie, iar decizia produce o modificare măsurabilă a procesului fizic. Numărul dispozitivelor conectate, volumul înregistrărilor și numărul graficelor dintr-un tablou de bord nu sunt indicatori de succes; ele descriu efortul, nu rezultatul. Din acest motiv, proiectarea pornește de la problema industrială și de la efectul urmărit, iar alegerea tehnologiei este ultima etapă, nu prima.

Prima parte a capitolului analizează trei familii de aplicații – mentenanța predictivă, monitorizarea consumului energetic și automatizarea agroindustrială. Pentru fiecare sunt urmărite problema industrială, mărimile necesare, arhitectura funcțională, regula de decizie, integrarea cu sistemele existente, indicatorii de evaluare, limitele și criteriile de validare. Cele trei au fost alese pentru că acoperă regimuri de date fundamental diferite: semnale rapide care se prelucrează local, contoare lente care capătă sens numai prin normalizare și mărimi de mediu cu variabilitate naturală mare și comunicație intermitentă. O secțiune distinctă tratează regimul juridic al datelor generate de produsele conectate, devenit o cerință de proiectare de la intrarea în aplicare a reglementării europene în domeniu.

A doua parte este dedicată mini-proiectelor ghidate. Spre deosebire de exercițiile din capitolele anterioare, fiecare dintre acestea urmărind câte un segment – interfața de operare în 5.6, integrarea unui senzor în 5.7, validarea comunicațiilor în 6.5, proiectarea arhitecturii în 7.5 și analiza securității în 8.4, mini-proiectele cer parcurgerea și verificarea întregului lanț informațional, de la semnalul electric până la indicatorul afișat. Ele pot fi realizate cu echipamente reale, prin simulare sau într-o configurație mixtă.

Capitolul aplică numeric metodele de dimensionare introduse anterior. Calculul lățimii de bandă din secțiunea 5.4.5 este folosit pentru a decide între transmiterea unui semnal de vibrație și transmiterea caracteristicilor extrase din el; bugetul de latență din secțiunile 5.4.5 și 7.1.4 este extins până la ecranul operatorului și

transformat într-o procedură de măsurare; indicatorul de eficacitate globală a echipamentelor, definit în secțiunea 7.2.3, este aplicat unei linii pentru a arăta unde se ascund pierderile care nu apar în jurnalul opririlor. În toate cele trei cazuri, concluzia are aceeași formă: o mărime necalculată nu poate fi administrată.

Regula care traversează întregul capitol rămâne cea enunțată încă din secțiunea 1.2.2. Funcțiile de control, interblocările și siguranța se realizează local, prin componente dedicate. Serviciile externe colectează, stochează, analizează și afișează. Această delimitare are, așa cum se arată în secțiunea 9.2.3, o justificare cantitativă, nu una de prudență.

Obiectivele capitolului

La finalul capitolului, cititorul trebuie să poată:

- să identifice problemele industriale pentru care o soluție IIoT este justificată și să stabilească mărimile necesare, punctele de măsurare, frecvența de achiziție și indicatorul prin care efectul va fi verificat;
- să descrie traseul complet al datelor, de la senzor și automat programabil (PLC) până la aplicația de analiză, și să coreleze fiecare segment cu decizia operațională pe care o susține;
- să analizeze aplicații de mentenanță predictivă, monitorizare energetică și automatizare agroindustrială, diferențiind datele, regulile de decizie, indicatorii și limitele specifice fiecăreia;
- să diferențieze funcțiile de control local de funcțiile de monitorizare și analiză și să argumenteze cantitativ de ce primele nu pot fi transferate serviciilor externe;
- să proiecteze mini-aplicații care integrează automate programabile, interfețe HMI, sisteme SCADA, OPC UA, MQTT, baze de date și tablouri de bord, pornind de la un contract de date explicit;
- să calculeze lățimea de bandă necesară unui flux de măsurări, bugetul de latență până la afișare și eficacitatea globală a echipamentelor, interpretând rezultatul, repartizarea pierderilor și limitele calculului;
- să proiecteze o celulă robotizată conectată IIoT, să delimiteze responsabilitățile componentelor și să valideze progresiv fiecare segment al fluxului informațional;
- să evalueze o aplicație IIoT prin criterii de reușită verificabile, să stabilească cerințele privind accesul la datele generate de produsele conectate și să documenteze configurația, rezultatele și limitele astfel încât soluția să poată fi reprodusă, verificată și extinsă.

9.1. Exemple de aplicații IIoT

Utilizarea IIoT este justificată atunci când datele colectate pot fi transformate în decizii şi acţiuni care îmbunătăţesc funcţionarea procesului. Simpla conectare a echipamentelor sau afişarea valorilor într-un tablou de bord nu reprezintă, în sine, o aplicaţie industrială completă.

Proiectarea trebuie să pornească de la problema urmărită şi să stabilească:

- activele şi procesele monitorizate;
- mărimile necesare şi punctele de măsurare;
- frecvenţa, precizia şi calitatea datelor;
- modul de contextualizare şi prelucrare;
- pragurile, regulile sau modelele utilizate;
- persoanele ori sistemele care primesc rezultatul;
- acţiunea operaţională declanşată;
- indicatorul prin care este verificat efectul obţinut.

Ultimul element este cel mai frecvent omis, iar omiterea lui are o consecinţă previzibilă: proiectul nu poate fi nici confirmat, nici infirmat. Un indicator este utilizabil numai dacă are o definiţie operaţională stabilă – aceeaşi formulă, acelaşi interval de referinţă, aceleaşi reguli de clasificare a opririlor şi aceeaşi unitate de măsură. Seria ISO 22400 oferă un cadru neutru pentru definirea şi schimbul indicatorilor din gestionarea operaţiunilor de fabricaţie şi este utilă tocmai pentru că impune această disciplină înaintea calculului [50], [51].

Nivelurile funcţionale între care circulă aceste date, de la procesul fizic până la planificarea întreprinderii, sunt cele definite de modelul ierarhic al integrării sistemelor de întreprindere şi control [49], iar poziţionarea componentelor IIoT faţă de ele a fost stabilită în secţiunea 7.1.5; arhitecturile de referinţă pentru internetul lucrurilor tratează separat nivelurile funcţionale de cele de implementare, tocmai pentru a evita confuzia dintre ele [193].

Locul prelucrării rezultă din cerinţele aplicaţiei, nu dintr-o preferinţă tehnologică. Prelucrarea poate fi realizată local, prin procesare edge sau într-o platformă externă, în funcţie de volumul datelor, de timpul de răspuns admisibil, de disponibilitatea comunicaţiei şi de sensibilitatea informaţiei; apropierea prelucrării de sursă răspunde simultan problemelor de latenţă, de volum transmis şi de confidenţialitate, care nu pot fi rezolvate prin creşterea capacităţii de calcul centralizate [111]. Criteriile detaliate de repartizare a funcţiilor sunt cele din secţiunea 7.3.3. Regula practică este următoarea: o funcţie se plasează cât mai aproape de proces atunci când întârzierea influenţează rezultatul sau când indisponibilitatea reţelei ar face funcţia inoperantă.

Funcţiile critice de control şi siguranţă rămân, în toate cazurile, locale, astfel încât procesul să poată continua într-o stare controlată dacă serviciile externe devin indisponibile. Această delimitare nu este o precauţie suplimentară, ci o cerinţă de

proiectare a sistemelor de automatizare conectate, derivată din faptul că mediile de control industrial sunt supuse unor constrângeri de disponibilitate, de timp de răspuns și de consecință fizică a defectării diferite de cele ale sistemelor informatice de birou [25].

9.1.1. Mentenanță predictivă

Mentenanța predictivă urmărește estimarea evoluției stării unui echipament și identificarea momentului în care este necesară o intervenție. Delimitarea față de mentenanța preventivă, efectuată la intervale prestabilite, și față de mentenanța bazată pe stare, declanșată la depășirea unui prag măsurat, a fost stabilită în secțiunea 1.3.1: cele trei nu diferă prin tehnologie, ci prin datele pe care le presupun, iar trecerea la ultima nu poate ocoli constituirea istoricului cerut de prima [60], [61]. Literatura de mentenanță industrială insistă asupra aceleiași ordini, arătând că un program de monitorizare a stării presupune stabilizarea prealabilă a evidenței intervențiilor și a regimurilor de funcționare [59].

Motoarele, pompele, reductoarele, ventilatoarele, rulmenții și alte echipamente rotative pot fi monitorizate prin senzori de vibrații, temperatură, curent, presiune sau debit. Aceste date trebuie corelate cu regimul de funcționare, sarcina, viteza, numărul de cicluri, comenzile de producție și intervențiile efectuate. O creștere a vibrațiilor poate indica degradarea unui rulment, dar poate fi produsă și de modificarea sarcinii, de dezechilibru sau de o fixare mecanică necorespunzătoare.

Ordinea etapelor de proiectare

Un program de monitorizare a stării nu începe cu alegerea senzorilor, ci cu analiza echipamentului: funcția pe care o îndeplinește, regimurile în care lucrează, criticitatea sa în fluxul de producție și modurile de defectare pe care monitorizarea urmează să le detecteze. Abia după această etapă se stabilesc parametrii măsurați, punctele de măsurare, criteriile de alarmare și acțiunile asociate fiecărui nivel de abatere, iar rezultatul intervențiilor este reintrodus în istoricul echipamentului. Aceeași sursă tratează programul de monitorizare ca proces ciclic, în care revizuirea periodică a parametrilor urmăriți face parte din program, nu din corectarea lui [42]. Ordinea este importantă din motive practice: senzorii montați fără o ipoteză privind modul de defectare produc date care nu pot fi interpretate.

Traseul funcțional al aplicației este prezentat în Figura 9.1. Succesiunea corespunde blocurilor funcționale definite pentru prelucrarea, comunicarea și prezentarea informațiilor de monitorizare a stării mașinilor, care separă explicit achiziția și manipularea datelor de detectarea stării, de evaluarea stării tehnice, de prognoză și de generarea recomandărilor [42]. Separarea are o consecință de proiectare directă: fiecare bloc poate fi verificat independent, iar o eroare de interpretare poate fi localizată fără a pune sub semnul întrebării întregul lanț. Ea are și o consecință de responsabilitate: o valoare agregată poate fi verificată de oricine reface calculul,

în timp ce o estimare produsă de un model necesită cunoaşterea datelor de instruire, a ipotezelor şi a condiţiilor în care estimarea încetează să fie validă [42].

La nivelul echipamentului sau al gateway-ului industrial (*industrial gateway*) pot fi calculate valori precum media, valoarea efectivă, valoarea de vârf, factorul de creastă ori indicatorii obţinuţi din analiza spectrală. Transmiterea acestor caracteristici reduce volumul comunicaţiei şi permite detectarea rapidă a abaterilor, iar datele detaliate pot fi păstrate pentru intervalele în care apare o anomalie; deplasarea prelucrării către sursă răspunde simultan cerinţelor de volum, de întârziere şi de confidenţialitate [111]. Raportul dintre volumul semnalului brut şi cel al caracteristicilor extrase este cuantificat în secţiunea 9.2.1.

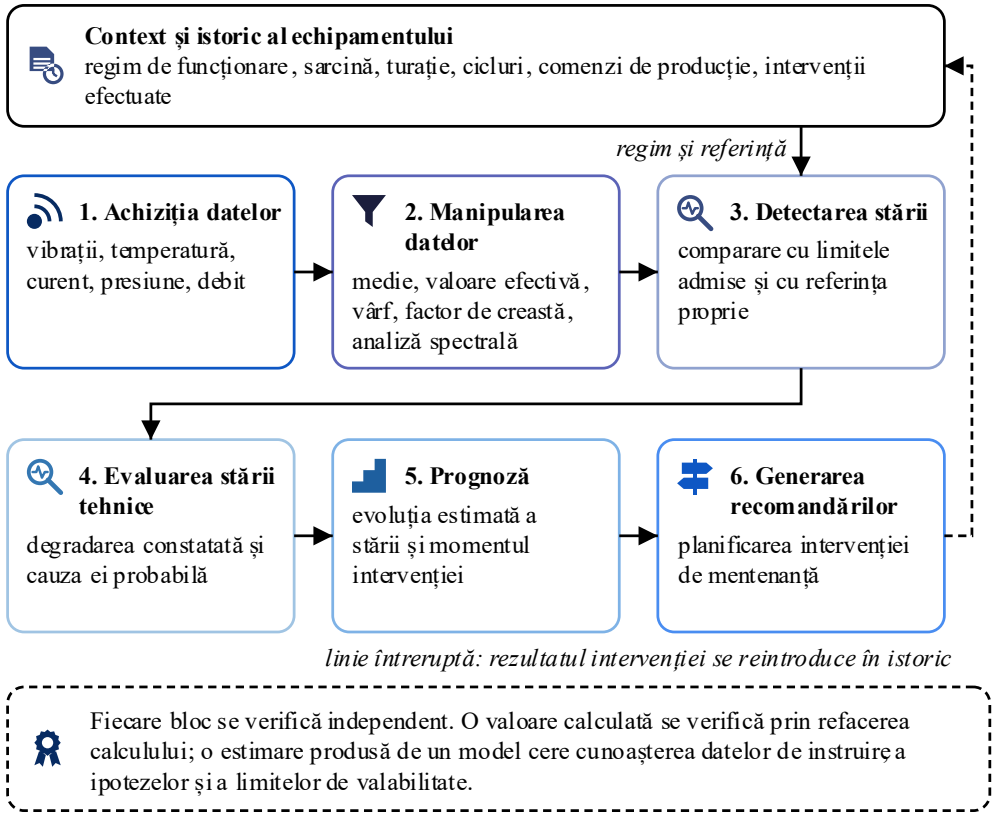


Figura 9.1 – Lanțul funcțional al mentenanței predictive

Stabilirea pragurilor

Stabilirea pragurilor este etapa în care majoritatea aplicaţiilor eşuează. Evaluarea vibraţiilor se realizează prin două criterii complementare: mărimea absolută a vibraţiei, raportată la limitele admisibile pentru clasa de maşini respectivă, şi variaţia faţă de o valoare de referinţă stabilită pentru echipamentul concret, în regim normal de funcţionare [41]. Pentru maşinile industriale uzuale, domeniile de

evaluare sunt precizate pe clase de putere și pe tipuri de fundație, ceea ce permite raportarea unei valori măsurate la o limită justificată, nu la una aleasă intern [246].

Al doilea criteriu este adesea mai sensibil decât primul, deoarece o creștere semnificativă față de referința proprie poate semnala o degradare cu mult înainte ca valoarea absolută să depășească o limită generală [41]. Pentru ca acest criteriu să fie utilizabil, condițiile de măsurare – punctul, orientarea, fixarea senzorului, turația și sarcina – trebuie menținute constante între măsurări succesive. Este motivul pentru care câmpul care descrie regimul de funcționare devine obligatoriu în structura mesajului, așa cum se arată în secțiunea 9.2.1: fără el, două valori nu sunt comparabile, oricât de precis ar fi fost măsurate.

Metoda este generală, pragurile nu. Succesiunea descrisă mai sus – analiza modurilor de defectare, alegerea mărimilor, stabilirea referinței proprii, compararea cu limitele clasei – se aplică oricărui echipament rotativ. Valorile numerice nu se transferă. Un prag stabilit pentru un ventilator montat pe fundație elastică nu este valabil pentru o pompă montată rigid, chiar la aceeași putere instalată, deoarece criteriul de evaluare depinde de clasa mașinii, de tipul fundației și de regimul de funcționare. Orice valoare orientativă preluată dintr-o sursă externă, inclusiv din acest capitol, trebuie tratată ca punct de plecare pentru observarea echipamentului propriu, nu ca limită de alarmare.

Modelele utilizate pot porni de la praguri și tendințe și pot evolua către metode statistice sau algoritmi de învățare automată. Complexitatea modelului trebuie justificată prin calitatea și cantitatea datelor disponibile. Atunci când nu există suficiente exemple de defectare, un model simplu, verificabil și corelat cu experiența personalului de mentenanță poate fi mai util decât un algoritm complex, insuficient validat. Sintezele metodelor de diagnostic și prognoză arată că factorul limitativ nu este disponibilitatea algoritmilor, ci calitatea și reprezentativitatea datelor de instruire [60].

De la alertă la intervenție

Monitorizarea unui motor care acționează un transportor poate utiliza vibrația, temperatura lagărelor, curentul absorbit, turația și sarcina estimată. Gateway-ul industrial calculează indicatorii necesari și îi transmite către sistemul de analiză. Dacă abaterea persistă în mai multe regimuri comparabile, este generată o alertă care trebuie verificată înainte de emiterea unui ordin de lucru în sistemul de management al mentenanței (CMMS).

Alerta nu trebuie să conducă automat la oprirea echipamentului decât dacă această acțiune a fost proiectată și validată ca funcție de control sau de protecție. Sistemul IIoT oferă informații pentru planificare, în timp ce funcțiile de oprire sigură rămân în sarcina controlerelor și a dispozitivelor locale, proiectate și validate după cerințele aplicabile părților de comandă cu rol de siguranță [45], [142]. Confuzia dintre cele două roluri produce fie opriri nejustificate, fie, mai grav,

dependenţa siguranţei de disponibilitatea unei conexiuni. Argumentul cantitativ pentru această delimitare este dat de bugetul de latenţă din secţiunea 9.2.3.

Un element frecvent omis este starea aparatului de măsură însuşi. Un traductor poate funcţiona în afara domeniului specificat, poate necesita verificare sau poate fi în curs de calibrare, fără ca valoarea transmisă să fie evident greşită. Practica industrială consacrată reduce diagnosticarea internă a dispozitivelor de teren la un număr mic de stări comunicate uniform – defect, verificare în curs, în afara specificaţiei, necesită întreţinere, astfel încât operatorul să primească o indicaţie acţionabilă în locul unui cod de eroare specific producătorului. Recomandarea cere, în plus, ca modificarea stării să fie semnalată imediat, iar confirmarea ei să fie tratată de sistemele superioare, nu la nivelul dispozitivului [247]. Aceste stări trebuie transportate până la aplicaţia de analiză, deoarece o valoare corectă provenită de la un senzor semnalat ca fiind în afara specificaţiei nu poate fi folosită pentru actualizarea referinţei.

Evaluare şi limite

Eficienţa aplicaţiei poate fi evaluată prin timpul de detectare a degradării, numărul alertelor false, durata opririlor neplanificate, proporţia intervenţiilor planificate, disponibilitatea echipamentelor şi costul total al mentenanţei. Rezultatele trebuie comparate cu o perioadă de referinţă şi analizate împreună cu personalul de exploatare, după metoda de evaluare economică din secţiunea 1.3.3, iar definiţiile mărimilor utilizate trebuie să rămână neschimbate pe tot intervalul comparat [51]. O rată ridicată a alertelor false este cel mai frecvent motiv pentru care un sistem corect din punct de vedere tehnic este abandonat în exploatare: după un număr mic de intervenţii inutile, alertele încetează să fie luate în considerare.

Principalele limitări sunt amplasarea necorespunzătoare a senzorilor, lipsa sincronizării temporale, modificarea regimurilor de lucru, deriva măsurărilor şi absenţa datelor etichetate privind defectările. Modelul trebuie verificat periodic, deoarece schimbarea echipamentului, a produsului sau a parametrilor procesului poate modifica relaţia dintre date şi starea tehnică.

9.1.2. Monitorizarea consumului energetic

Monitorizarea energetică urmăreşte identificarea modului în care energia şi celelalte utilităţi sunt consumate de clădiri, secţii, linii şi echipamente. Datele agregate din factura de utilităţi nu permit localizarea pierderilor şi nici corelarea consumului cu producţia. Din acest motiv, măsurarea trebuie organizată ierarhic, de la punctul general de alimentare până la consumatorii semnificativi, aşa cum se arată în Figura 9.2.

Ierarhia nu se construieşte uniform, ci pornind de la consumatorii cu pondere mare în consumul total sau cu potenţial semnificativ de îmbunătăţire. Aceştia determină ce se măsoară, cu ce frecvenţă şi cu ce precizie, iar planul de colectare a

datelor devine parte a sistemului de management al energiei, nu o activitate separată de instrumentare. Identificarea utilizărilor semnificative de energie precedă, în acest cadru, orice decizie de instrumentare [63]. Rezultatul practic este că numărul contoarelor rămâne rezonabil, iar fiecare punct de măsurare are o justificare.

Pot fi urmărite energia activă şi reactivă, puterea instantanee, curentul, tensiunea, factorul de putere şi valorile maxime ale sarcinii. Pentru aer comprimat, apă, gaz sau abur sunt necesare măsurări de debit, presiune şi temperatură. Datele trebuie înregistrate împreună cu starea utilajului, produsul fabricat, cantitatea realizată şi intervalele de funcţionare, aşteptare sau oprire; fără aceste elemente de context, indicatorul energetic nu poate fi compus corect şi nici comparat între perioade [50].

Datele pot circula de la contoare şi senzori, printr-un automat programabil sau un gateway industrial, către SCADA ori un server de date istorice. După prelucrare şi normalizare, acestea sunt afişate într-un tablou de bord energetic şi utilizate pentru decizia operaţională.

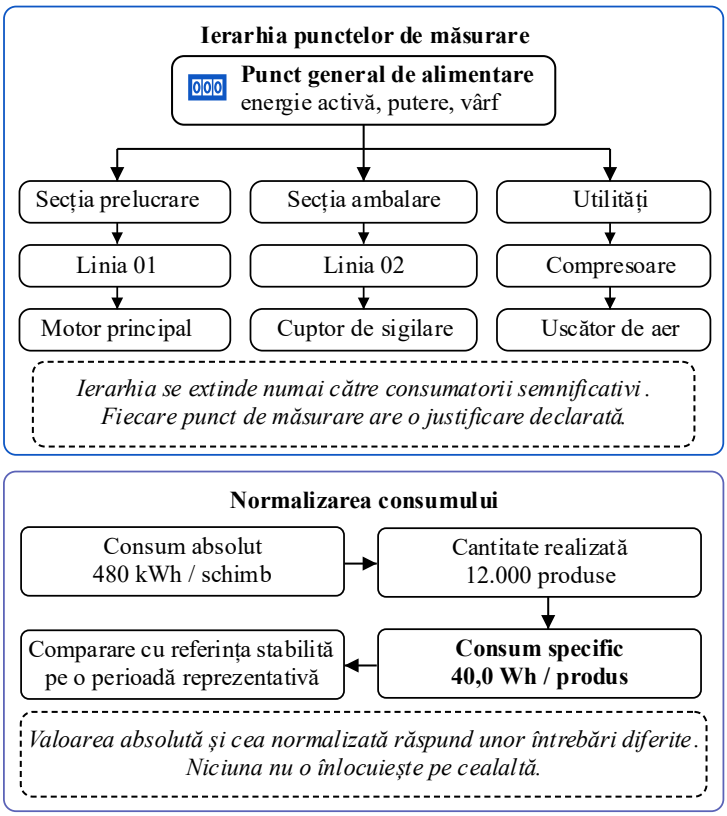


Figura 9.2 – Ierarhia măsurării energetice și normalizarea consumului în raport cu producția

Protocoalele Modbus, OPC UA sau MQTT pot fi utilizate pe segmente diferite ale arhitecturii, în funcție de echipamente și de cerințele sistemului; criteriile de alegere sunt cele din secțiunea 6.4.2. Prelucrarea locală poate detecta depășirea puterii contractate, funcționarea unui consumator în perioadele de oprire sau o pierdere de presiune. Platforma de analiză poate compara schimburile, produsele, liniile și perioadele de funcționare.

Valoare absolută și indicator normalizat

Consumul trebuie raportat atât ca valoare absolută, cât și prin indicatori normalizați, precum energia consumată pe produs, lot, oră de funcționare sau unitate de masă. Evaluarea performanței energetice presupune, în plus, o valoare de referință stabilită pentru o perioadă reprezentativă și normalizarea în raport cu variabilele care influențează consumul – volumul producției, mixul de produse sau temperatura exterioară [64]. Fără această contextualizare, o creștere a consumului poate fi interpretată greșit dacă volumul producției s-a modificat în aceeași perioadă.

Diferența este ușor de arătat printr-un exemplu numeric ilustrativ. Valorile de mai jos constituie un scenariu didactic construit pentru demonstrarea metodei, nu o măsurătoare industrială.

Date de intrare. Înainte de modificare: 480 kWh pe schimb pentru 12.000 de produse. După modificarea programului de producție: 505 kWh pentru 14.000 de produse.

Calcul. Consum specific inițial: 480.000 Wh / 12.000 = 40,0 Wh/produs. Consum specific final: 505.000 Wh / 14.000 = 36,1 Wh/produs. Variația consumului absolut: (505 − 480) / 480 = +5,2 %. Variația consumului specific: (36,1 − 40,0) / 40,0 = −9,8 %.

Interpretare. Consumul absolut a crescut, iar consumul specific a scăzut. Cele două mărimi răspund unor întrebări diferite și niciuna nu o înlocuiește pe cealaltă [64]. Raportarea exclusivă a valorii absolute ar fi indicat o înrăutățire, iar raportarea exclusivă a indicatorului normalizat ar fi ascuns creșterea sarcinii pe rețeaua electrică – relevantă pentru puterea contractată și pentru dimensionarea instalației. Ambele valori sunt necesare, iar interpretarea lor trebuie făcută împreună.

Limite. Comparația este validă numai dacă mixul de produse, condițiile de mediu și configurația liniei au rămas comparabile între cele două intervale. Dacă produsul s-a modificat, indicatorul specific compară două lucruri diferite; dacă temperatura exterioară a variat semnificativ, o parte din diferență aparține instalațiilor de climatizare, nu procesului. Normalizarea corectă presupune identificarea variabilelor relevante și verificarea faptului că relația dintre ele și consum este stabilă pe intervalul analizat [64].

Ce se transferă și ce nu. Metoda – ierarhizarea punctelor de măsurare, stabilirea unei referințe, normalizarea în raport cu variabilele care influențează consumul –

este independentă de instalaţie. Valoarea consumului specific nu este. Un indicator de 36,1 Wh/produs nu poate fi comparat cu al altei linii decât dacă produsul, tehnologia şi frontiera de măsurare sunt aceleaşi; în caz contrar, comparaţia măsoară diferenţa dintre produse, nu dintre performanţe. Din acelaşi motiv, ţinta de reducere se stabileşte faţă de referinţa proprie a instalaţiei, nu faţă de o valoare publicată.

Corelarea cu starea procesului

O linie de ambalare poate prezenta un consum redus în timpul producţiei, dar un consum semnificativ cumulat în perioadele de aşteptare. Corelarea datelor contoarelor cu stările automatului programabil permite separarea consumului productiv de cel asociat funcţionării în gol. În funcţie de rezultat, pot fi ajustate secvenţele de oprire, programul de producţie sau parametrii echipamentelor auxiliare.

Această corelare impune o cerinţă tehnică precisă: contorul şi automatul programabil trebuie să raporteze pe aceeaşi bază de timp, cu o incertitudine de sincronizare mult mai mică decât durata intervalelor analizate. Dacă intervalele de interes sunt de ordinul minutelor, o sincronizare prin protocol de reţea este suficientă; dacă analiza urmăreşte vârfuri de putere la pornirea unui motor, este necesar un mecanism cu precizie superioară, de tipul celui utilizat pentru sincronizarea echipamentelor de măsurare şi control [35]. Alegerea nu este o opţiune de configurare, ci determină ce întrebări pot primi răspuns din datele colectate.

Datele pot evidenţia şi degradări tehnice. Creşterea treptată a curentului absorbit de un motor, a consumului de aer comprimat sau a duratei unui ciclu poate indica uzură, pierderi sau reglaje necorespunzătoare. Monitorizarea energetică se corelează astfel cu mentenanţa, controlul calităţii şi analiza performanţei procesului.

Validarea instalării

Validarea aplicaţiei presupune verificarea acoperirii punctelor de măsurare, a preciziei contoarelor, a sincronizării temporale şi a concordanţei dintre consumurile parţiale şi consumul general. Diferenţa dintre suma consumurilor măsurate pe ramuri şi consumul înregistrat la punctul general este cel mai util indicator de calitate a instalării: o abatere care depăşeşte incertitudinea combinată a contoarelor indică fie un consumator nemăsurat, fie o eroare de configurare a raportului de transformare. Efectele măsurilor adoptate trebuie evaluate în condiţii comparabile, folosind indicatori normalizaţi şi o perioadă de referinţă suficientă.

9.1.3. Automatizări agroindustriale

Tehnologiile IIoT pot fi aplicate în sere, ferme, spaţii de depozitare şi instalaţii pentru prelucrarea produselor agricole. Aceste medii combină procese biologice, variaţii climatice, suprafeţe extinse şi echipamente distribuite, ceea ce impune adaptarea arhitecturii la condiţiile de amplasare şi la disponibilitatea comunicaţiei.

Volumul şi diversitatea datelor din agricultură au condus la arhitecturi în care colectarea, integrarea şi analiza sunt organizate distinct de sistemele de execuţie, iar dependenţa de furnizorii de platforme devine ea însăşi o problemă de proiectare [248].

Pot fi monitorizate umiditatea solului, temperatura şi umiditatea aerului, intensitatea luminoasă, concentraţia de dioxid de carbon, nivelul rezervoarelor, debitul, presiunea, pH-ul şi conductivitatea electrică. Actuatoarele pot include pompe, electrovalve, ventilatoare, sisteme de încălzire, ferestre motorizate şi instalaţii de iluminat.

Constrângerea impusă de tehnologia radio

În funcţie de distanţă, consumul energetic şi infrastructura disponibilă, senzorii pot comunica prin reţele cablate, Wi-Fi, LoRaWAN sau tehnologii celulare. Datele sunt concentrate într-un controler local sau într-un gateway industrial, unde pot fi verificate şi prelucrate înainte de transmiterea către platforma de supraveghere.

Alegerea tehnologiei radio impune însă o restricţie care trebuie asumată din faza de proiectare. Reţelele de consum redus, optimizate pentru autonomie şi acoperire, transmit mesaje scurte, rare şi fără garanţia livrării la un moment determinat, aşa cum s-a arătat în secţiunea 6.2.6. Restricţiile de acces la mediul radio şi dimensiunea redusă a cadrelor sunt proprietăţi ale specificaţiei, nu limitări de implementare [183]. Ele sunt potrivite pentru observarea unei tendinţe, dar nu pentru închiderea unei bucle de reglare. Consecinţa arhitecturală este prezentată în Figura 9.3: bucla de reglare se închide integral în controlerul local, iar legătura radio deserveşte exclusiv observarea şi configurarea controlată.

Irigarea, ventilaţia sau protecţia împotriva temperaturilor extreme nu trebuie să depindă de disponibilitatea unei conexiuni externe. Controlerul local aplică regulile şi interblocările necesare, iar platforma IIoT asigură analiza istorică, configurarea controlată, notificarea şi compararea zonelor sau culturilor.

Verificarea prin efect

Într-o seră, decizia de irigare poate utiliza umiditatea substratului, temperatura, ora, starea rezervorului şi disponibilitatea pompei. Comanda electrovalvei trebuie să includă limite de durată, histerezis şi verificarea debitului. Dacă valva este comandată, dar debitul nu apare în intervalul stabilit, sistemul trebuie să semnaleze o posibilă blocare, o lipsă de apă sau o defecţiune a pompei.

Verificarea prin efect – confruntarea comenzii cu o mărime independentă care confirmă executarea ei – este principiul care deosebeşte o instalaţie automatizată de una doar comandată de la distanţă. Ea se aplică identic ventilaţiei, încălzirii şi dozării, iar în cazul celulei robotizate din secţiunea 9.2.4 apare sub forma confirmării bidirecţionale dintre robot şi automatul programabil. Absenţa ei produce un tip

de defect deosebit de dificil de diagnosticat: sistemul raportează corect că a executat comanda, iar procesul nu se modifică. Problema aparţine categoriei în care controlul asupra procesului fizic devine incert, iar sistemele de automatizare conectate sunt evaluate tocmai după consecinţa fizică a unei asemenea incertitudini [25].

Limitele transferului. Regulile de decizie prezentate – histerezis, limitare a duratei, verificare prin efect – se aplică oricărei instalaţii de acest tip. Pragurile de umiditate, temperatură şi durată de irigare depind de cultură, substrat, fază de dezvoltare, sistem de irigare şi condiţii climatice locale. Ele se stabilesc împreună cu specialistul în tehnologia culturii şi se revizuiesc sezonier; niciun set de valori nu poate fi preluat ca atare dintr-o altă instalaţie.

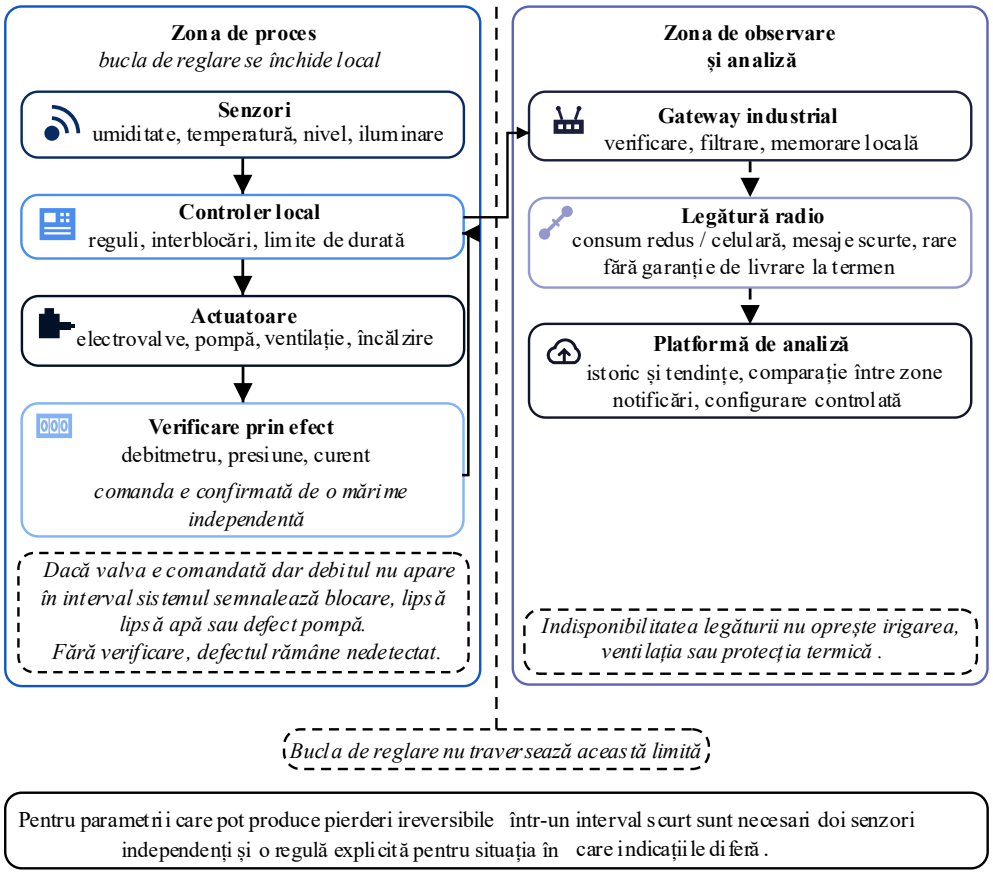


Figura 9.3 – Bucla de reglare locală şi fluxul IIoT de observare

Trasabilitate şi conformitate

Înregistrarea datelor permite asocierea condiţiilor de mediu şi a acţiunilor executate cu zona, cultura şi intervalul de producţie. Pentru operatorii din lanţul alimentar, această înregistrare are şi o dimensiune de conformitate: legislaţia

europeană impune capacitatea de a identifica furnizorul imediat și clientul imediat pentru fiecare produs, în toate etapele producției, prelucrării și distribuției [198]. Datele de proces colectate automat nu înlocuiesc aceste evidențe, dar le pot completa cu informații verificabile privind condițiile în care a fost obținut un lot. Genealogia produsului și mecanismele prin care aceasta este construită la nivelul sistemului de execuție a fabricației au fost tratate în secțiunea 7.2.3 și nu sunt reluate aici.

Fiabilitatea măsurărilor

Eficiența aplicației poate fi evaluată prin consumul de apă și energie raportat la producție, stabilitatea parametrilor de mediu, timpul de reacție la abateri, disponibilitatea sistemului și numărul intervențiilor manuale. Evaluarea trebuie să țină cont de variațiile sezoniere și de diferențele dintre culturi, deoarece rezultatele obținute într-un anumit interval nu pot fi generalizate automat.

Fiabilitatea măsurărilor reprezintă o condiție esențială. Senzorii pot fi afectați de umiditate, praf, coroziune, depuneri, amplasare necorespunzătoare sau descărcarea bateriilor. Sunt necesare verificări periodice, mecanisme de detectare a valorilor imposibile, protecție mecanică și posibilitatea operării manuale controlate. Pentru parametrii care pot produce pierderi ireversibile într-un interval scurt, precum temperatura într-o seră sau într-un depozit frigorific, o singură măsurare nu este suficientă: sunt necesari doi senzori independenți și o regulă explicită pentru situația în care indicațiile lor diferă. Regula trebuie să precizeze care valoare se folosește pentru reglare, ce se întâmplă la depășirea diferenței admise și cine este notificat – o divergență netratată este echivalentă cu absența măsurării.

9.1.4. Regimul juridic al datelor generate de produsele conectate

Datele produse de echipamentele conectate au încetat să fie exclusiv o problemă tehnică. Reglementarea europeană privind accesul echitabil la date și utilizarea acestora stabilește reguli armonizate pentru datele generate prin utilizarea produselor conectate și a serviciilor asociate, inclusiv dreptul utilizatorului de a accesa aceste date și de a le pune la dispoziția unui terț ales de el. Regulamentul a intrat în vigoare la 11 ianuarie 2024 și se aplică începând cu 12 septembrie 2025, iar obligațiile privind proiectarea produselor astfel încât datele să fie accesibile în mod implicit se aplică produselor introduse pe piață începând cu 12 septembrie 2026 [245].

Pentru proiectarea unei aplicații IIoT, consecințele sunt concrete și apar înaintea implementării, nu după.

Cine este utilizatorul datelor. Într-o instalație industrială, echipamentul poate fi deținut de fabrică, întreținut de furnizor și monitorizat de un integrator. Distincția dintre deținătorul datelor și utilizator este definită normativ și trebuie stabilită

contractual înainte de configurarea fluxului, deoarece ea determină cine poate solicita accesul, în ce format și cu ce frecvență [245].

Accesibilitatea impune export structurat. Stocarea exclusiv proprietară, fără export, compromite reutilizarea istoricului la schimbarea furnizorului, distinct de problema juridică. Seriile temporale se extrag cu identificatorul activului, unitatea de măsură, marca temporală a sursei și indicatorul de calitate. Cerința corespunde contractului de date definit în secțiunea 9.2.3.

Ce nu se transmite. Datele de proces pot conține informații care identifică persoane: identificatorul operatorului asociat unei opriri, durata intervenției unui tehnician, numărul de corecții manuale pe schimb. Aceste elemente intră sub incidența regulilor de protecție a datelor cu caracter personal și trebuie tratate conform politicii stabilite în secțiunea 1.2.4. Pseudonimizarea aplicată la nivelul gateway-ului, înainte de transmitere, este de regulă mai simplă decât filtrarea ulterioară în platformă.

Ce rămâne protejat. Regulamentul păstrează protecția secretelor comerciale, fără a exclude automat accesul la toate datele care au acest caracter. Pentru datele aflate sub incidența obligațiilor de acces, părțile trebuie să convină măsurile tehnice și organizatorice necesare păstrării confidențialității. Suspendarea sau refuzul partajării sunt permise numai în condițiile prevăzute de regulament, nu prin simpla declarare a informațiilor drept confidențiale. Rețetele, parametrii de proces și algoritmii de control nu formează o categorie exceptată în bloc: trebuie analizat ce informații sunt solicitate, dacă acestea intră în domeniul obligației de acces și ce măsuri de protecție sunt aplicabile. În specificația fluxului se documentează datele vizate, destinatarii autorizați și condițiile de utilizare și protejare a acestora [245].

Domeniul și limitele acestei prezentări. Regulamentul se aplică produselor conectate introduse pe piața Uniunii Europene și serviciilor asociate acestora, precum și datelor generate prin utilizarea lor. Prezentarea de față se limitează la consecințele asupra proiectării fluxului de date și a fost verificată în textul oficial publicat în Jurnalul Oficial, la data de referință a acestei revizuiri. Ea nu constituie o interpretare juridică: încadrarea unui echipament concret, obligațiile contractuale dintre părți și raportul cu celelalte acte aplicabile – inclusiv cele privind protecția datelor cu caracter personal și securitatea rețelelor – se stabilesc cu asistență de specialitate.

Aceste cerințe nu modifică arhitectura tehnică prezentată în capitolele anterioare, dar modifică lista elementelor care trebuie decise înaintea implementării. Un flux proiectat fără ele funcționează corect și poate deveni, ulterior, imposibil de adus în conformitate fără reconfigurare.

9.1.5. Elemente comune şi criterii de selecție a aplicației

Cele trei familii de aplicații urmează aceeaşi logică: definirea problemei, colectarea datelor relevante, contextualizarea acestora, formularea deciziei, executarea acțiunii şi verificarea rezultatului. Diferențele apar în regimul datelor, în locul prelucrării şi în natura limitărilor, aspecte sintetizate în Tabelul 9.1.

Ordinea de abordare într-o organizație

Atunci când mai multe aplicații sunt posibile simultan, ordinea nu este indiferentă. Criteriile utile pentru stabilirea priorității sunt cele din metoda prezentată în secțiunea 3.3.6, aplicate aici la nivel de aplicație, nu de fabrică:

1. Existența datelor. O aplicație care se poate realiza cu date deja disponibile în automatul programabil sau în sistemul SCADA are un cost de pornire mult mai mic decât una care impune instrumentare nouă. Inventarul mărimilor deja expuse la nivelul operațiunilor de fabricație este, din acest motiv, prima verificare [49]. Monitorizarea energetică porneşte frecvent de la contoare existente; mentenanța predictivă porneşte aproape întotdeauna de la senzori noi.

Tabelul 9.1 – Sinteza comparativă a celor trei familii de aplicații IIoT

Element	**Mentenanță predictivă**	**Monitorizare energetică**	**Automatizare agroindustrială**
Problema industrială	Opriri neplanificate și intervenții efectuate prea devreme sau prea târziu	Pierderi nelocalizate și consum necorelat cu producția	Variabilitatea condițiilor de mediu și distribuția spațială a echipamentelor
Mărimi măsurate	Vibrație, temperatură, curent, turație, sarcină	Energie activă și reactivă, putere, debit, presiune	Umiditate, temperatură, iluminare, CO_2, debit, nivel, pH
Regimul datelor	Semnal rapid, prelucrat local; caracteristici la interval fix	Contoare lente, cumulate pe intervale	Mărimi lente, cu variabilitate naturală mare
Context obligatoriu	Regim de funcționare, sarcină, istoricul intervențiilor	Stare utilaj, produs, cantitate realizată, interval	Zonă, cultură, fază de producție, acțiuni executate
Locul prelucrării	Extragerea caracteristicilor la edge; evaluarea tendinței în platformă	Detectarea depășirilor local; comparațiile în platformă	Reglarea și interblocările local; analiza istorică în platformă
Decizia sprijinită	Planificarea intervenției de mentenanță	Ajustarea programului, a secvențelor de oprire și a reglajelor	Comanda irigării, ventilației, încălzirii și iluminatului
Indicatori de evaluare	Timp de detectare, alerte false, opriri neplanificate, disponibilitate	Consum specific, abatere față de referință, consum în afara producției	Consum de apă și energie pe unitate de producție, stabilitatea parametrilor, intervenții manuale
Limitări principale	Amplasarea senzorilor, deriva, lipsa datelor de defectare	Sincronizarea temporală, acoperirea punctelor de măsurare	Condiții de mediu agresive, comunicație intermitentă, autonomia bateriilor

2. Durata până la primul rezultat verificabil. O aplicație care produce o valoare interpretabilă în câteva săptămâni permite corectarea ipotezelor. Una care necesită un an de istoric înainte de a produce orice concluzie consumă credit organizațional fără a-l reface.
3. Reversibilitatea deciziei. Modificarea unui program de producție pe baza unui indicator energetic poate fi anulată. Înlocuirea unui rulment pe baza unei alerte false costă o oprire.
4. Numărul de persoane care trebuie să își schimbe modul de lucru. O aplicație care produce o informație utilizată de o singură echipă se implementează; una care presupune coordonarea a trei departamente se negociază.

Aceste criterii nu ierarhizează aplicațiile în abstract, ci în raport cu o organizație concretă. Aceeași aplicație poate fi prima alegere într-o fabrică cu instrumentare bogată și ultima într-una în care fluxul de date nu a fost încă stabilizat.

Secțiunea următoare transpune această logică în mini-proiecte ghidate care pot fi realizate cu echipamente fizice, prin simulare sau într-o configurație mixtă.

9.2. Mini-proiecte ghidate

Mini-proiectele propuse urmăresc aplicarea progresivă a conceptelor prezentate în capitolele anterioare. Acestea pot fi realizate cu echipamente fizice, prin simulare sau într-o configurație mixtă. Alegerea componentelor și a platformelor poate fi adaptată infrastructurii disponibile, fără modificarea obiectivelor funcționale și a criteriilor de validare.

Cele patru proiecte formează o progresie deliberată, reprezentată în Figura 9.4. Primul urmărește o singură mărime fizică, de la senzor până la înregistrarea în baza de date, și decide ce anume se transmite. Al doilea adaugă logica secvențială, comanda actuatoarelor și calculul indicatorilor de producție. Al treilea se concentrează asupra fluxului informațional complet și asupra comportamentului acestuia la defect. Al patrulea le reunește într-o aplicație robotizată în care controlul, supravegherea, schimbul de date și securitatea coexistă. Fiecare proiect presupune validat ceea ce a fost verificat în cel anterior.

Implementarea trebuie realizată gradual. Mai întâi se validează separat achiziția datelor, comunicația și fiecare interfață, după care se construiește fluxul complet. Metoda comună de validare etapizată, cu ordinea verificărilor și cu situațiile de eroare care trebuie provocate deliberat, este cea din secțiunea 6.5.4. Aceeași logică – niveluri succesive, fiecare verificabil separat – guvernează și măsurile de securitate aplicate configurației rezultate, tratate în secțiunea 8.2. Ea permite localizarea erorilor și evită situația în care mai multe componente sunt configurate simultan fără a putea identifica segmentul care nu funcționează.

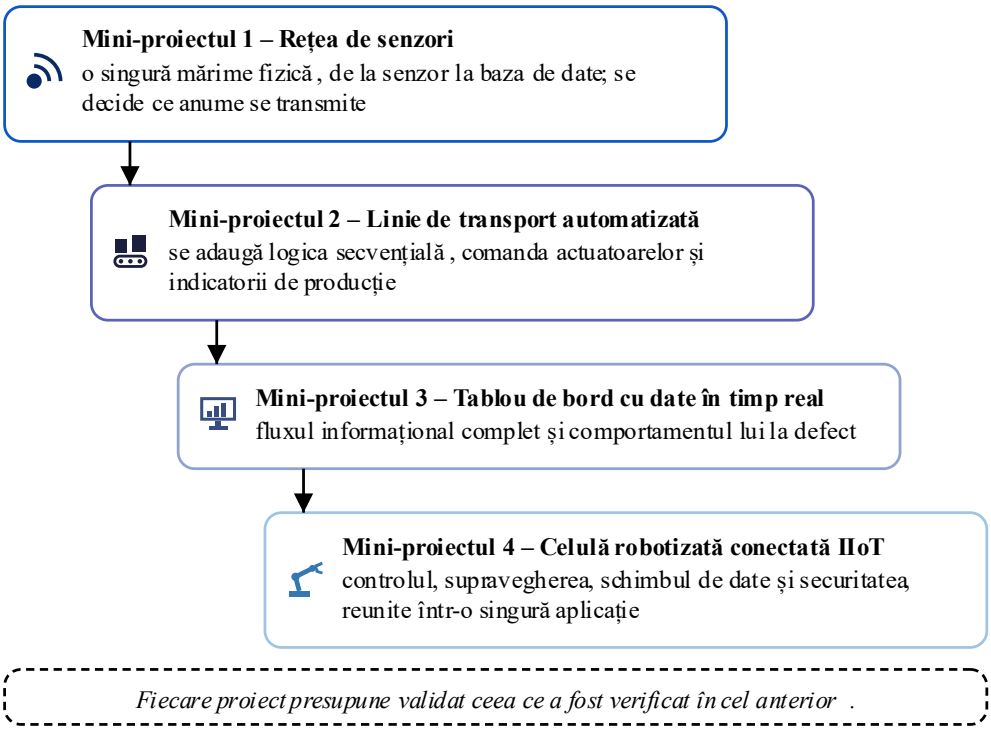


Figura 9.4 – Progresia celor patru mini-proiecte ghidate

Pentru fiecare mini-proiect, documentaţia trebuie să cuprindă descrierea procesului şi a rezultatului urmărit, arhitectura funcţională, precum şi lista intrărilor, ieşirilor şi variabilelor monitorizate. Aceasta trebuie să prezinte traseul datelor, protocoalele utilizate şi structura mesajelor, să definească condiţiile de alarmare şi regulile de prelucrare şi să includă planul de testare, rezultatele obţinute şi limitele soluţiei.

Aceste elemente nu sunt cerinţe formale de documentare. Ele reprezintă condiţia minimă pentru ca rezultatul să poată fi reprodus de altcineva, verificat după o modificare şi extins fără reproiectare. O configuraţie care funcţionează, dar nu poate fi descrisă în aceşti termeni, nu poate fi nici întreţinută.

Configuraţia materială şi versiunile software pe care au fost verificate exemplele din acest capitol sunt prezentate în Tabelul 9.2. Lista este organizată pe categorii de echipamente, nu pe produse impuse: fiecare poziţie precizează cerinţa funcţională minimă, referinţa utilizată efectiv şi alternativa acceptabilă.

Versiunile din coloana a doua sunt cele pe care au fost verificate exemplele din acest capitol. Ele nu constituie o cerinţă: orice versiune care păstrează interfeţele descrise este acceptabilă, cu condiţia ca versiunea utilizată efectiv să fie consemnată în documentaţia mini-proiectului. Fără această consemnare, un rezultat care nu se reproduce nu poate fi atribuit configuraţiei.

Tabelul 9.2 – Categorii de echipamente și versiuni software pentru cele patru mini-proiecte

Element	Categorie sau versiune de referință	Alternativă acceptabilă	Observație
Automat programabil	Controler compact cu module analogice, minimum 8 intrări digitale, 4 ieșiri digitale, 2 intrări analogice	Orice controler care acceptă programare conform IEC 61131-3	Mediul de inginerie trebuie să permită exportul programului în format text
Mediu de inginerie	TIA Portal V19 sau ulterior	CODESYS 3.5 SP20, Studio 5000 v35	Versiunea se consemnează în documentația proiectului
Simulator de proces	Factory I/O 2.5	Model propriu în mediul de inginerie	Necesar dacă echipamentele fizice nu sunt disponibile
Traductor de temperatură	Pt100 clasa A, montaj cu trei conductoare, domeniu −50…+250 °C	Traductor cu ieșire 4–20 mA, două fire	Domeniul se alege după procesul monitorizat, nu după disponibilitate
Accelerometru	Piezoelectric IEPE, ±50 g, bandă 10–2.500 Hz, montaj filetat	Accelerometru MEMS cu ieșire digitală și bandă declarată	Banda utilă a montajului limitează banda utilă a traductorului
Modul de achiziție vibrații	Intrare IEPE, eșantionare minimum 5.120 Hz pe canal, 16 biți	Modul dedicat cu extragere locală a caracteristicilor	Extragerea locală reduce cerințele de comunicație
Senzori de prezență	Optic difuz, distanță 0…40 cm, ieșire PNP	Inductiv sau capacitiv, după material	Se alege după proprietatea fizică a produsului
Gateway industrial	Node-RED 4.x pe calculator industrial fără piese în mișcare	Gateway comercial cu client OPC UA și publicare MQTT	Trebuie să permită memorarea locală a datelor
Server OPC UA	Server de simulare conform IEC 62541, cu autentificare	Serverul integrat al automatului programabil	Contul de achiziție are exclusiv drept de citire
Broker MQTT	Eclipse Mosquitto 2.0.x, TLS activat, autentificare pe client	Broker comercial cu liste de control al accesului	Nu se utilizează configurația implicită, fără autentificare
Bază de date	InfluxDB 2.7 sau ulterior	TimescaleDB 2.x	Rezoluția mărcii temporale se declară explicit
Vizualizare	Grafana 11.x	Tabloul de bord al platformei IIoT utilizate	Intervalul de reîmprospătare se consemnează, fiind dominant în bugetul de latență
Robot	Robot articulat cu șase axe, sarcină utilă minimum 3 kg, sau simulatorul producătorului	Celulă virtuală în mediul de simulare	Modul de operare cu viteză redusă este obligatoriu la punerea în funcțiune

Funcţiile critice de control, interblocare şi siguranţă trebuie să rămână locale. Gateway-ul industrial, brokerul MQTT (MQTT broker), baza de date şi tabloul de bord completează sistemul prin monitorizare şi analiză, dar indisponibilitatea lor nu trebuie să conducă la pierderea controlului procesului. Funcţiile de siguranţă propriu-zise – oprirea de urgenţă, supravegherea protecţiilor mobile, limitarea vitezei – nu se realizează în programul standard al automatului programabil şi nu fac

obiectul acestor mini-proiecte; ele se proiectează separat, pe baza unei evaluări a riscului şi a unui nivel de performanţă impus [45], [142].

9.2.1. Mini-proiectul 1: Rețea de senzori pentru monitorizarea temperaturii și vibrațiilor

Scop şi configuraţie

Realizarea unei aplicaţii pentru monitorizarea stării unui motor, a unui rulment sau a unui alt echipament rotativ prin măsurarea temperaturii şi a vibraţiilor.

Configuraţia minimă include senzori de temperatură şi vibraţii, un modul de achiziţie sau un automat programabil, o interfaţă locală şi un gateway industrial. În funcţie de infrastructura disponibilă, valorile pot proveni şi dintr-un simulator.

Traseul principal al datelor porneşte de la senzori şi include condiţionarea semnalelor, urmată de preluarea acestora printr-un modul de achiziţie sau un automat programabil. Datele ajung apoi la HMI ori SCADA şi sunt transmise, printr-un gateway industrial, către baza de date şi tabloul de bord.

Cerinţele de achiziţie

Cele două mărimi impun regimuri de achiziţie complet diferite, iar confundarea lor este eroarea tipică a acestui proiect. Temperatura evoluează lent şi poate fi citită o dată pe secundă sau mai rar, cu un traductor Pt100 sau Pt1000 în montaj cu trei conductoare ori cu un traductor cu ieşire în curent 4–20 mA, conform principiilor din secţiunea 5.1.1 şi cu semnalizarea defectului prin ieşirea în afara domeniului util [131]. Vibraţia conţine informaţia utilă în domeniul de frecvenţe de la câţiva hertzi până la câţiva kilohertzi, ceea ce impune un accelerometru cu bandă corespunzătoare şi o frecvenţă de eşantionare de cel puţin dublul frecvenţei maxime de interes. În mini-proiect, frecvenţa de 5.120 Hz pentru banda de 10–2.500 Hz dă un raport de aproximativ 2,05, suficient numai dacă lanţul de achiziţie conţine un filtru anti-aliasing analogic înaintea convertorului; pentru o marjă mai comodă s-ar alege 6.400 Hz, cu efect proporţional asupra debitului din varianta A.

Valorile de referinţă adoptate pentru exemplul dezvoltat în continuare sunt prezentate în Tabelul 9.3. Ele constituie un scenariu didactic: sunt realiste şi coerente între ele, astfel încât calculele să poată fi refăcute, dar nu descriu un echipament anume.

Rezoluţia în frecvenţă de 1,25 Hz determină dacă frecvenţele caracteristice de defect ale unui rulment pot fi separate între ele şi de armonicile turaţiei. Dacă nu pot, creşterea numărului de senzori nu ajută; trebuie mărită fereastra de analiză, ceea ce înseamnă mai multe eşantioane la aceeaşi frecvenţă de eşantionare, deci un timp de observare mai lung.

Tabelul 9.3 – Parametrii de achiziție adoptați pentru mini-proiectul 1

Parametru	Valoare adoptată	Mărime derivată	Consecința de proiectare
Domeniu de măsurare accelerometru	±50 g, triaxial	–	Acoperă șocurile de pornire fără saturare
Bandă utilă a traductorului	10–2.500 Hz	–	Limitează frecvențele de defect detectabile
Frecvență de eșantionare	5.120 Hz pe canal	$f_{max} = f_s / 2$ = 2.560 Hz	Frecvența maximă analizabilă
Rezoluția convertorului	16 biți	–	Determină debitul semnalului brut
Fereastră de analiză	4.096 de eșantioane	$\Delta f = f_s / N$ = 1,25 Hz	Rezoluția în frecvență
–	–	$T = N / f_s$ = 0,8 s	Durata unei ferestre de analiză
Traductor de temperatură	Pt100, trei conductoare	–	Compensarea rezistenței conductorilor
Interval de citire a temperaturii	1 s	–	Suficient pentru o constantă termică de ordinul minutelor

Etapele de realizare

Definirea echipamentului monitorizat. Se precizează tipul echipamentului, regimurile sale de funcţionare, punctele de măsurare şi defectările care ar putea influenţa temperatura sau vibraţiile.

*Selectarea şi amplasarea senzorilor***.** Se stabilesc domeniul de măsurare, precizia, frecvenţa de eşantionare şi modul de montare. Pentru vibraţii, orientarea şi fixarea senzorului trebuie menţinute constante pentru ca măsurările succesive să poată fi comparate. Modul de fixare influenţează direct banda utilă: o fixare rigidă păstrează componentele de frecvenţă înaltă, în timp ce o fixare magnetică sau prin adeziv le atenuează progresiv.

Configurarea achiziției. Canalele analogice sau digitale sunt configurate în automatul programabil ori în modulul de achiziție. Valorile brute sunt convertite în unități inginerești și sunt asociate cu o marcă temporală, identificatorul echipamentului și indicatorul de calitate.

Validarea măsurărilor locale. Valorile sunt comparate cu un instrument de referință sau cu datele furnizate de simulator. Trebuie verificate domeniul, rezoluția, stabilitatea și comportamentul în cazul întreruperii senzorului. Un traductor cu ieșire 4–20 mA permite deosebirea unei valori nule legitime de un circuit întrerupt, deoarece intervalul util este rezervat informației de măsurare, iar valorile din afara lui semnalează defectul [131]; mecanismul este cel implementat în secțiunea 5.7.2.

Stabilirea referinței și a pragurilor. Echipamentul este observat în regim normal, pe un interval care acoperă toate stările uzuale de funcționare, iar valorile obținute constituie referința proprie. Pragul de avertizare se raportează la această referință, iar pragul de alarmă la limitele admisibile pentru clasa de mașini respectivă [41], [246], conform criteriilor din secțiunea 9.1.1. Pragurile alese arbitrar produc fie alerte permanente, fie tăcere completă.

Configurarea supravegherii. Interfața HMI sau sistemul SCADA afișează valorile curente, tendințele și starea senzorilor, conform principiilor din secțiunea 5.5.5.

Trebuie afișată explicit și vechimea ultimei valori recepționate, pentru ca o valoare înghețată să nu fie interpretată drept valoare stabilă.

Extragerea caracteristicilor și transmiterea datelor. Din semnalul brut se calculează local valoarea efectivă, valoarea de vârf, factorul de creastă și, dacă instrumentele o permit, amplitudinile în benzile de frecvență de interes. Variabilele sunt expuse prin OPC UA sau sunt preluate de gateway-ul industrial și publicate prin MQTT [177]. Setul de caracteristici transmise trebuie să corespundă modurilor de defectare urmărite, stabilite la punctul 1 [43].

Stocarea și analiza. Datele sunt salvate într-o bază de date și reprezentate într-un tablou de bord. Se urmăresc tendințele, depășirile persistente și relația dintre temperatură, vibrații și regimul de funcționare. Evaluarea tendinței și estimarea evoluției aparțin blocurilor funcționale distincte de cel de achiziție, iar rezultatele lor nu trebuie confundate [42].

Testarea aplicației. Se introduc valori simulate sau variații controlate pentru a verifica detectarea abaterilor, generarea alertelor și păstrarea istoricului. Setul minim de date de test cuprinde: o serie de o oră în regim normal, care constituie referința; o creștere lentă a valorii efective, de 0,05 mm/s pe oră, pentru verificarea detectării tendinței; un salt brusc peste pragul de alarmă, pentru verificarea alertei; o întrerupere a traductorului; și o valoare corectă însoțită de starea „în afara specificației", pentru verificarea faptului că referința nu este actualizată din date marcate ca nesigure. Încercările de defect aplicabile sunt cele din Tabelul 9.10.

Dimensionarea fluxului de date

Decizia de a transmite caracteristici în locul semnalului brut este cea mai importantă din acest proiect și poate fi justificată numeric. Metoda de calcul, ipotezele privind antetele și supraîncărcarea protocoalelor sunt cele stabilite în secțiunea 5.4.5; aici se aplică unui caz în care raportul dintre variante este neobișnuit de mare.

Varianta A – transmiterea continuă a semnalului brut. Cu valorile din Tabelul 9.3:

$D_A = f_s \times n_{canale} \times b_{eșantion} = 5.120 \times 3 \times 16 = 245.760$ bit/s ≈ 245,8 kbit/s

Volumul zilnic pentru un singur echipament este 245.760 / 8 × 86.400 ≈ 2,65 GB, iar pentru douăzeci de echipamente monitorizate simultan aproximativ 4,92 Mbit/s și 53 GB pe zi.

Varianta B – transmiterea caracteristicilor extrase la edge. Se publică un mesaj la fiecare 10 secunde, conținând cele trei valori efective, valorile de vârf, factorii de creastă, două temperaturi, turația și câmpurile de context. Un asemenea mesaj în format JSON ocupă aproximativ 380 de octeți, iar împreună cu antetele MQTT, TCP/IP și cu supraîncărcarea introdusă de TLS se poate considera un total de circa 500 de octeți transmiși efectiv:

$$D_B = 500 \times 8 / 10 = 400 \text{ bit/s} = 0{,}40 \text{ kbit/s}$$

Volumul zilnic este 8.640 × 500 ≈ 4,32 MB pentru un echipament și circa 86 MB pentru douăzeci.

Interpretare. Raportul dintre cele două variante este de aproximativ 610:1. Diferența nu este de comoditate: la 4,92 Mbit/s susținut, monitorizarea devine un

consumator de resurse comparabil cu procesul supravegheat, iar prima măsură luată la apariţia unei probleme de reţea va fi oprirea ei. Semnalul brut rămâne totuşi necesar pentru diagnostic, motiv pentru care se transmite episodic: o secundă de semnal pe toate cele trei axe înseamnă aproximativ 30 KB, astfel încât zece asemenea capturi pe zi adaugă sub 8 % la volumul variantei B.

Limite ale calculului. Estimarea nu include retransmisiile, confirmările corespunzătoare nivelurilor superioare de calitate a serviciului, traficul de menţinere a conexiunii, restabilirea sesiunilor TLS şi nici retransmiterea datelor memorate local după o întrerupere, care produce vârfuri de trafic mult peste media calculată. În plus, reducerea este validă numai dacă setul de caracteristici extrase este suficient pentru modurile de defectare urmărite; un mod de defectare identificat ulterior poate impune revizuirea listei, iar datele deja transmise nu îl vor conţine. Aceasta este pierderea reală a variantei B şi motivul pentru care capturile episodice de semnal brut nu sunt opţionale.

Structura mesajului

Subiectele MQTT ale mini-proiectelor folosesc o formă simplificată, proprie acestui capitol, a convenţiei de referinţă din secţiunea 6.2.8: <sit>/<linie>/<echipament>/<tip_mesaj>. Pentru acest proiect rezultă fabricaA/linia01/motor01/stare, iar pentru capturile episodice fabricaA/linia01/motor01/semnal_brut. Payloadul, adică ansamblul câmpurilor transmise în corpul mesajului, are următoarea formă:

```
{
  "versiune_schema": "1.0",
  "identificator_activ": "linia01/motor01",
  "marca_temporala_sursa": "2026-08-05T09:41:20.000Z",
  "regim": "sarcina_nominala",
  "turatie_rpm": 1478,
  "temperatura_lagar_liber_c": 62.4,
  "temperatura_lagar_cuplat_c": 58.1,
  "vibratie_ef_x_mm_s": 3.42,
  "vibratie_ef_y_mm_s": 2.87,
  "vibratie_ef_z_mm_s": 1.95,
  "factor_creasta_x": 4.1,
  "fereastra_s": 0.8,
  "stare_senzor": "buna",
  "calitate_date": "buna"
}
```

Câmpul `regim` este obligatoriu: fără el, o valoare efectivă de 3,42 mm/s nu poate fi comparată cu istoricul, deoarece nu se ştie dacă a fost obţinută în gol sau la sarcină nominală. Câmpul `stare_senzor` transportă diagnosticul propriu al traductorului, în forma redusă a celor patru stări consacrate [247], şi este distinct de `calitate_date`, care se referă la validitatea valorii transmise. Un senzor semnalat ca necesitând întreţinere poate furniza încă valori valide, iar deosebirea determină dacă valoarea poate fi folosită pentru actualizarea referinţei. Contractul de date aplicat mesajelor din mini-proiecte este definit în secţiunea 9.2.3. Exemplul este

prescurtat: mesajul complet conține și valorile de vârf și factorii de creastă pe celelalte axe, iar câmpurile de identificare și unitățile cerute de contract se adaugă în același mod. Dimensiunea de aproximativ 380 de octeți folosită în calculul variantei B este, de aceea, un ordin de mărime, care se verifică pe forma finală a mesajului.

Criterii de reușită

Mini-proiectul este considerat funcțional dacă valorile afișate corespund mărimilor măsurate, iar unitățile de măsură și mărcile temporale sunt corecte. Funcționalitatea presupune detectarea pierderii sau defectării unui senzor și diferențierea acestei situații de o valoare validă, precum și generarea alertelor numai după îndeplinirea condițiilor stabilite, într-un regim de funcționare identificat. De asemenea, trebuie asigurată trasabilitatea datelor de la senzor până la înregistrarea în baza de date, concordanța dintre debitul măsurat pe interfața gateway-ului și valoarea calculată, cu o abatere explicabilă, precum și continuitatea monitorizării locale în cazul indisponibilității serviciilor externe.

Aplicația poate fi extinsă prin calcularea unor caracteristici spectrale suplimentare, prin memorarea locală a datelor pe durata întreruperilor de comunicație sau prin transmiterea alertei validate către un sistem de management al mentenanței, fără a transforma automat alerta într-un ordin de oprire a echipamentului.

9.2.2. Mini-proiectul 2: Linie de transport automatizată

Scop și configurație

Implementarea unei benzi transportoare care detectează, deplasează și numără produse, utilizând un automat programabil, senzori de prezență, un motor și, opțional, actuatoare pentru oprire, deviere sau sortare.

Spre deosebire de exercițiul de proiectare din secțiunea 7.5, care se oprea la nivelul arhitecturii și al modelului de date, acest mini-proiect presupune implementarea și testarea efectivă a secvenței, a interfeței operatorului și a fluxului de date.

Configurația poate include senzori optici, inductivi sau capacitivi; motor electric și echipament de acționare; cilindru pneumatic sau mecanism de deviere; automat programabil; interfață HMI; sistem SCADA sau gateway industrial; simulator pentru proces și semnale, dacă echipamentele fizice nu sunt disponibile.

Etapele de realizare

Definirea secvenței. Se descriu stările procesului: oprit, pregătit, pornire, transport, detectare, sortare, evacuare și defect. Pentru fiecare stare se precizează condițiile de intrare și de ieșire, iar tranzițiile se formulează astfel încât să fie mutual exclusive. De exemplu, trecerea din „transport" în „detectare" are loc pe frontul crescător al senzorului de prezență, cu condiția ca produsul anterior să fi părăsit zona; formularea „senzorul este activ" este insuficientă, deoarece nu deosebește un

produs nou de unul oprit în dreptul senzorului. Descrierea prin stări şi tranziţii poate fi transpusă direct în limbajul de programare corespunzător, ediţia în vigoare a standardului de programare punând la dispoziţie inclusiv reprezentarea grafică a secvenţelor prin diagrama funcţională secvenţială [123].

Realizarea listei de intrări şi ieşiri. Fiecare senzor, comandă şi actuator primeşte o denumire unică. Se stabilesc stările normale, condiţiile de defect şi comportamentul la revenirea alimentării. Lista rezultată este prezentată în Tabelul 9.4.

Implementarea controlului local. Programul automatului programabil comandă motorul şi actuatoarele, numără produsele şi detectează situaţiile de blocare. Temporizările şi interblocările trebuie justificate prin cerinţele procesului. Organizarea programului pe unităţi cu interfeţe declarate explicit permite testarea separată a fiecărei secvenţe [123].

Tabelul 9.4 – Lista intrărilor și ieșirilor pentru linia de transport automatizată

Denumire simbolică	**Tip**	**Element fizic**	**Stare în repaus**	**Rol și observații**
B1_Prezenta_Intrare	Intrare digitală	Senzor optic difuz, intrarea benzii	0 – fără produs	Frontul crescător incrementează contorul
B2_Prezenta_Deviere	Intrare digitală	Senzor optic, punctul de deviere	0 – fără produs	Declanșează comanda de sortare
B3_Cilindru_Retras	Intrare digitală	Senzor inductiv de capăt de cursă	1 – retras	Condiție de permisiune pentru transport
B4_Cilindru_Extins	Intrare digitală	Senzor inductiv de capăt de cursă	0	Confirmă executarea devierii
S1_Pornire	Intrare digitală	Buton, contact normal deschis	0	Activ numai în starea „pregătit"
S2_Oprire	Intrare digitală	Buton, contact normal închis	1	Cablat astfel încât întreruperea firului oprește linia
S3_Oprire_Urgenta	Intrare digitală	Buton cu reținere, două canale	1	Evaluat de circuitul de siguranță, nu de programul standard
K1_Retur_Contactor	Intrare digitală	Contact auxiliar oglindă	0	Detectează contactorul lipit
T1_Gata_Convertizor	Intrare digitală	Semnal de disponibilitate	1	Condiție de pornire a motorului
T1_Turatie_Reala	Intrare analogică	0–10 V de la convertizor	0 V	Verificarea concordanței cu referința
K1_Comanda_Motor	Ieșire digitală	Contactor sau validare convertizor	0	Blocată dacă lipsește retur sau permisiune
Y1_Comanda_Cilindru	Ieșire digitală	Distribuitor monostabil	0 – retras	La lipsa tensiunii revine în poziția sigură
H1_Semnalizare_Defect	Ieșire digitală	Lampă de semnalizare	0	Activă în starea de defect
T1_Referinta_Turatie	Ieșire analogică	0–10 V către convertizor	0 V	Limitată prin program la domeniul admis

Configurarea interfeței HMI. Operatorul trebuie să poată selecta modul de funcționare, să pornească și să oprească procesul, să observe stările senzorilor și să consulte mesajele de alarmă. Comenzile manuale trebuie limitate astfel încât să nu eludeze interblocările. Clasificarea cauzei unei opriri se introduce tot aici; fără această intervenție, opririle rămân neexplicate, iar indicatorii calculați ulterior nu pot fi interpretați.

Integrarea supravegherii. Sistemul SCADA sau gateway-ul industrial preia variabile precum starea liniei, numărul de produse, timpul ciclului, durata opririlor și codurile de defect – exact mărimile din care se compun ulterior indicatorii operaționali [51].

Calcularea indicatorilor. Pot fi determinați numărul de produse realizate, durata medie a ciclului, timpul de funcționare, timpul de oprire și numărul blocajelor, precum și eficacitatea globală a echipamentelor, tratată mai jos.

Testarea secvenței. Se verifică funcționarea normală, absența produsului, detectarea repetată a aceleiași piese, blocarea senzorului, defectarea actuatorului și oprirea comunicației cu sistemele externe.

Detectarea blocajului prin supravegherea duratei

Detectarea blocajului se realizează prin supravegherea duratei dintre două evenimente așteptate: dacă un produs a intrat în zona de deviere și confirmarea evacuării nu apare în intervalul stabilit, se trece în starea de defect. Mecanismul este exemplificat mai jos în text structurat, unul dintre limbajele suitei definite normativ [123]:

```
// Supravegherea executării devierii
IF Cerere_Deviere AND NOT B4_Cilindru_Extins THEN
    Tmr_Deviere(IN := TRUE, PT := T#1s500ms);
ELSE
    Tmr_Deviere(IN := FALSE);
END_IF;

IF Tmr_Deviere.Q THEN
    Stare := STARE_DEFECT;
    Cod_Defect := 21;            // devierea nu s-a executat
    Y1_Comanda_Cilindru := FALSE;
    K1_Comanda_Motor := FALSE;
END_IF;

// Numărarea pe front, cu blocarea repetării pe același produs
IF B1_Prezenta_Intrare AND NOT B1_Memorie THEN
    Contor_Produse := Contor_Produse + 1;
    Ts_Produs := Ceas_Sistem;
END_IF;
B1_Memorie := B1_Prezenta_Intrare;
```

Valoarea temporizării nu este arbitrară: ea trebuie să depășească durata maximă normală a cursei cilindrului, majorată cu o marjă care acoperă variația

presiunii de alimentare, dar să rămână suficient de mică pentru ca produsul următor să nu ajungă în zonă. Dacă cele două condiţii nu pot fi îndeplinite simultan, problema nu este de programare, ci de dimensionare a distanţei dintre produse.

Memorarea stării senzorului la ciclul anterior, exemplificată în ultimele rânduri, este mecanismul care împiedică numărarea repetată a unui produs oprit în dreptul senzorului. Fără el, o oprire a benzii cu o piesă în faţa barierei optice produce o creştere a contorului la fiecare ciclu de scanare, adică mii de produse inexistente pe minut – o eroare care se propagă direct în indicatorii calculaţi ulterior.

Limitele realizării prin simulare

Un mediu de simulare reproduce logica secvenţială, nu comportamentul fizic al instalaţiei. Un program validat în simulator poate eşua pe echipamentul real din cauze care nu sunt reprezentate în model: dispersia duratelor cursei cilindrului la variaţia presiunii, alunecarea produsului pe bandă, zgomotul electric pe intrările digitale, timpul de răspuns al contactorului, oscilaţia barierei optice la trecerea unui produs transparent. Consecinţa practică este că temporizările stabilite în simulator sunt valori de pornire care se reverifică pe instalaţie, iar detectarea blocajului trebuie retestată cu produsul real, nu cu modelul lui.

Simularea nu poate valida în niciun caz funcţiile de siguranţă. Oprirea de urgenţă, supravegherea protecţiilor mobile şi comportamentul la revenirea alimentării se verifică exclusiv pe instalaţia fizică, prin procedurile impuse de evaluarea riscului [45], [142].

Calculul eficacităţii globale a echipamentelor

Indicatorul a fost definit în secţiunea 7.2.3, împreună cu formula de compunere, cu originea sa în mentenanţa productivă totală [65] şi cu cerinţele privind consecvenţa datelor [51]. Aici este aplicat numeric unei linii cu alte date decât cele din capitolul 7, pentru a arăta ce anume trebuie colectat efectiv de la automatul programabil şi cum se interpretează repartizarea pierderilor. Valorile de mai jos constituie un scenariu didactic, nu o măsurare industrială.

Date de intrare, pentru un schimb:

- durata schimbului: 480 min, din care 30 min pauze planificate, rezultând un timp planificat pentru producţie de 450 min;
- opriri neplanificate înregistrate: 38 min, formate din 22 min blocaje, 9 min defectarea unui actuator şi 7 min lipsă de material;
- timp de ciclu de referinţă: 2,0 s/produs, echivalent cu 30 produse/min;
- cantitate totală realizată: 11.100 produse;
- cantitate neconformă: 240 de produse, deci 10.860 conforme.

Înlocuire numerică:

Disponibilitate: $D = (450 - 38) / 450 = 412 / 450 = 0{,}9156$, adică 91,6 %.

Performanță: $P = (11.100 \times 2{,}0) / (412 \times 60) = 22.200 / 24.720 = 0{,}8981$, adică 89,8 %.

Calitate: $C = 10.860 / 11.100 = 0{,}9784$, adică 97,8 %.

OEE = $D \times P \times C = 0{,}9156 \times 0{,}8981 \times 0{,}9784 = 0{,}8044$, adică **80,4 %**.

Verificare: aceeași valoare se obține direct din relația echivalentă OEE = (cantitate conformă × timp de ciclu de referință) / timp planificat = (10.860 × 2,0) / (450 × 60) = 21.720 / 27.000 = 0,8044. Concordanța celor două căi de calcul este un test util: dacă rezultatele diferă cu mai mult decât eroarea de rotunjire, una dintre mărimile colectate este definită diferit față de cum este utilizată.

Repartizarea pierderilor. Valoarea globală spune mai puțin decât distribuția ei, prezentată în Tabelul 9.5.

Tabelul 9.5 – Repartizarea pierderilor pe componentele indicatorului, exprimată în minute echivalente

Componentă	Valoare	Pierdere echivalentă	Vizibilă în jurnalul opririlor	Sursa datelor
Timp planificat	450 min	—	—	Program de lucru
Disponibilitate	91,6 %	38 min	Da, cu cauză atribuită	Contor de stare al automatului programabil
Performanță	89,8 %	42 min	Nu	Diferența dintre producția teoretică și cea realizată
Calitate	97,8 %	8 min	Parțial	Contor de produse neconforme
Total pierderi	—	88 min	—	—
Timp productiv efectiv	362 min	—	—	Rezultat

Interpretare. Cea mai mare pierdere nu este cea vizibilă. Opririle înregistrate au costat 38 de minute, dar componenta de performanță arată o pierdere mai mare: în cele 412 minute de funcționare, linia ar fi trebuit să realizeze 412 × 30 = 12.360 de produse, iar diferența de 1.260 de produse corespunde unei pierderi echivalente cu 42 de minute. Aceste minute nu apar nicăieri ca oprire, deoarece sunt formate din micro-opriri și funcționare sub viteza de referință, sub pragul de înregistrare al sistemului. Concluzia practică este că o linie nu poate fi îmbunătățită pornind exclusiv de la jurnalul de opriri, iar pragul de detectare a opririlor trebuie ales suficient de mic pentru ca micro-opririle să devină vizibile. Un prag de 60 de secunde, uzual în configurațiile implicite, ascunde integral această componentă. Clasificarea intervalelor de timp și regulile după care o oprire devine înregistrabilă fac parte din definiția indicatorului, nu din configurarea sistemului de colectare [50], [51].

Limite. Rezultatul depinde de definițiile adoptate. Includerea sau excluderea pauzelor planificate din timpul de referință modifică valoarea cu câteva puncte procentuale, iar utilizarea timpului de ciclu proiectat în locul celui realizabil pentru produsul curent deplasează pierderea între componentele de disponibilitate și performanță. Din acest motiv, compararea valorilor între linii, schimburi sau

organizaţii este validă numai dacă regulile de clasificare a timpului şi cantităţilor sunt identice [51]. Indicatorul nu conţine, în plus, nicio informaţie despre necesarul de producţie: o valoare ridicată obţinută fabricând produse care nu sunt cerute reprezintă o pierdere, nu o performanţă.

Criterii de reuşită

Aplicaţia trebuie să execute secvenţa în ordinea stabilită, să numere fiecare produs o singură dată, inclusiv când acesta staţionează în dreptul senzorului, şi să blocheze comenzile incompatibile. Oprirea procesului trebuie să conducă la o stare controlată, iar informaţiile din HMI şi SCADA trebuie să corespundă stării automatului programabil. Fiecare oprire trebuie să aibă o durată înregistrată şi o cauză atribuită. Valorile componentelor indicatorului trebuie să poată fi reconstituite din datele brute stocate, iar rapoartele trebuie generate din date validate. Linia trebuie să funcţioneze în continuare local la pierderea conexiunii cu platforma de analiză.

Mini-proiectul poate fi extins prin introducerea identificării produsului, a sortării pe categorii, a urmăririi lotului sau a corelării consumului energetic cu numărul de produse realizate, folosind indicatorii normalizaţi discutaţi în secţiunea 9.1.2.

9.2.3. Mini-proiectul 3: Tablou de bord industrial cu date în timp real

Scop şi stivă tehnologică

Realizarea unui flux complet prin care datele provenite de la un simulator, un automat programabil sau un server OPC UA sunt preluate de un gateway industrial, publicate prin MQTT, stocate şi reprezentate într-un tablou de bord.

Arhitectura generală porneşte de la o sursă de date şi include un gateway industrial care organizează datele într-un mesaj structurat şi îl transmite către un broker MQTT. Mesajul este apoi procesat conform unei reguli de prelucrare, iar datele sunt stocate într-o bază de date şi prezentate într-un tablou de bord.

Configuraţia de referinţă utilizată în continuare cuprinde un server OPC UA de simulare ca sursă, Node-RED pentru integrare şi pentru regulile de prelucrare, un broker Mosquitto în reţeaua locală, o bază de date pentru serii temporale de tip InfluxDB şi Grafana pentru vizualizare. Alegerea produselor nu modifică logica proiectului: fiecare componentă poate fi înlocuită cu un echivalent, cu condiţia păstrării rolurilor şi a interfeţelor. Figura 9.5 prezintă componentele şi interfeţele dintre ele.

Etapele de realizare

Definirea contractului de date – se stabilesc variabilele transmise, tipurile lor, unităţile, frecvenţa actualizării şi denumirile câmpurilor. Contractul este documentul de referinţă al proiectului: orice modificare ulterioară a unui câmp înseamnă o versiune nouă, nu o corecţie tăcută.

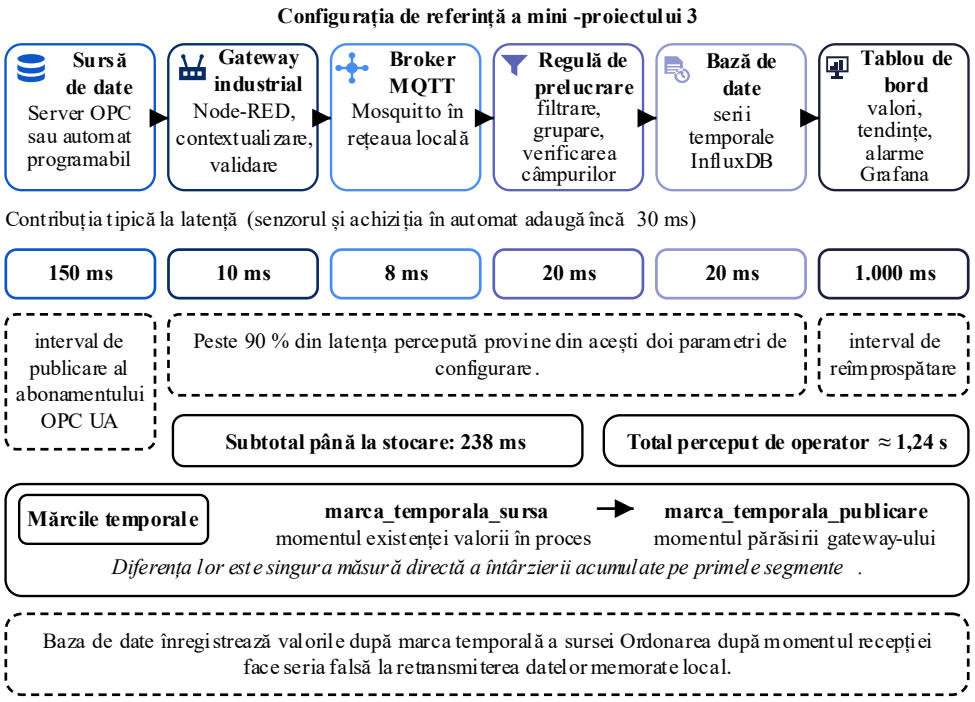


Figura 9.5 – Arhitectura tabloului de bord industrial cu date în timp real

Validarea sursei – se confirmă că valorile sunt citite corect din simulator, din automatul programabil sau din serverul OPC UA şi că modificările sunt observabile local.

Testarea comunicaţiei MQTT – înaintea conectării sursei industriale se publică un mesaj simplu şi se verifică recepţia lui printr-un client abonat la acelaşi subiect [177]. Astfel sunt validate separat adresa brokerului, portul, autentificarea, TLS şi politicile aplicate subiectului. Procedura detaliată şi situaţiile de eroare care trebuie provocate sunt cele din secţiunea 6.5.1.

Construirea mesajului complet – după validarea comunicaţiei, valorile industriale sunt grupate şi contextualizate. Mesajul este publicat numai după verificarea existenţei câmpurilor obligatorii.

Configurarea stocării – baza de date trebuie să permită identificarea sursei şi ordonarea temporală a înregistrărilor.

Realizarea tabloului de bord – sunt configurate valori curente, grafice temporale, stări, alarme şi indicatori sintetici. Fiecare element vizual trebuie să răspundă unei nevoi de monitorizare şi nu doar să reproducă toate câmpurile disponibile.

Validarea traseului complet – se compară valoarea de la sursă cu mesajul transmis, înregistrarea din baza de date şi valoarea afişată. Se verifică inclusiv marca temporală şi unitatea de măsură.

Testarea situațiilor anormale – se analizează pierderea conexiunii, mesajele incomplete, valorile nevalide, duplicatele și recepția în altă ordine decât cea în care datele au fost generate.

Identificarea variabilelor în serverul OPC UA

Fiecare variabilă expusă de server este identificată printr-un identificator de nod format din indicele spațiului de nume și un identificator, care poate fi numeric sau de tip șir de caractere:

```
ns=3;i=1042
ns=3;s="DB_Linie01"."Ambalare"."TimpCiclu"
```

Standardul definește spațiul de adrese și regulile identificării nodurilor [66]. Prima formă este compactă și eficientă, dar greu de interpretat; a doua reflectă lizibil blocurile de date ale automatului. Indicele ns indică poziția URI-ului în tabloul spațiilor de nume, poziție care se poate schimba după reconfigurare sau actualizare. Un client care păstrează ns=3 poate ajunge să citească altă variabilă fără eroare de comunicație [66]. De aceea, aplicația memorează URI-ul spațiului de nume și identifică indicele la fiecare conectare sau caută variabila parcurgând structura de nume.

La configurarea achiziției se stabilesc, pentru fiecare variabilă monitorizată, intervalul de eșantionare pe server, intervalul de publicare al abonamentului, dimensiunea cozii de valori și, acolo unde este util, banda moartă sub care modificările nu sunt raportate [174]. Pentru acest proiect se adoptă un interval de eșantionare de 100 ms și un interval de publicare de 200 ms, cu o coadă de zece valori, astfel încât o întârziere scurtă a clientului să nu producă pierderea eșantioanelor intermediare [174].

Tabelul 9.6 – Contractul de date: câmpuri obligatorii, rol și consecința absenței

Câmp	Tip	Rol	Ce se pierde în absența lui
versiune_schema	șir	Identifică structura mesajului	Modificările de format devin indistinctibile de erori
identificator_mesaj	șir	Identifică unic mesajul	Duplicatele nu pot fi eliminate după retransmitere
identificator_dispozitiv	șir	Identifică sursa transmisiei	Publicarea greșită nu poate fi atribuită
identificator_activ	șir	Identifică echipamentul măsurat	Valoarea nu poate fi asociată unui activ
marca_temporala_sursa	ISO 8601, UTC	Momentul existenței valorii în proces	Seria temporală devine falsă după o retransmitere
marca_temporala_publicare	ISO 8601, UTC	Momentul părăsirii gateway-ului	Întârzierea acumulată nu poate fi măsurată
stare	șir	Regimul de funcționare	Valorile nu sunt comparabile între ele
valori de proces	numeric	Mărimile măsurate	—
unitate	șir	Unitatea de măsură	Conversiile devin implicite și nedocumentate
calitate_date	șir	Validitatea valorii	O valoare nevalidă este tratată ca validă

Contractul de date

Mesajul trebuie să conțină cel puțin identificatorul dispozitivului, marca temporală, valorile procesului și informația privind calitatea acestora. Protocolul de transport nu impune niciunul dintre aceste câmpuri, ceea ce face ca stabilirea lor să fie o responsabilitate a proiectantului aplicației, nu o proprietate a tehnologiei [177]. Câmpurile obligatorii și rolul fiecăruia sunt prezentate în Tabelul 9.6; structura urmează principiile contractului de referință din secțiunea 6.2.8, cu denumiri de câmpuri explicite, în limba română, alese pentru lizibilitate în mini-proiecte.

Un mesaj construit după acest contract are forma:

```
{
  "versiune_schema": "1.0",
  "identificator_mesaj": "mesaj_000841",
  "identificator_dispozitiv": "gw_linia01",
  "identificator_activ": "linia01/ambalare01",
  "marca_temporala_sursa": "2026-08-05T11:02:14.400Z",
  "marca_temporala_publicare": "2026-08-05T11:02:14.612Z",
  "stare": "productie",
  "timp_ciclu_s": 2.06,
  "produse_conforme": 10860,
  "produse_neconforme": 240,
  "temperatura_sigilare_c": 176.4,
  "calitate_date": "buna"
}
```

Subiectul pe care este publicat mesajul respectă convenția <sit>/<linie>/<echipament>/<tip_mesaj>, deci fabricaA/linia01/ambalare01/stare. Convenția trebuie documentată și aplicată consecvent, deoarece structura subiectelor determină ulterior drepturile de acces, filtrele abonaților și regulile de arhivare; modificarea ei după punerea în funcțiune afectează toate aceste elemente simultan [177]. În acest mesaj, unitatea de măsură este inclusă în numele câmpurilor (timp_ciclu_s, temperatura_sigilare_c), formă acceptabilă a câmpului unitate din Tabelul 9.6 pentru mesajele cu mai multe valori, cu condiția ca regula să fie scrisă în contract. Contractul corespunde variantelor folosite în capitolele anterioare, cu denumiri diferite: marca temporală a sursei apare ca ts în secțiunea 6.2.8 și ca marca_temporala_masurare în secțiunea 8.4.2, calitatea ca q, respectiv calitate, iar identificatorul mesajului ca id_mesaj în secțiunea 8.4.2. Diferențele sunt intenționate, fiecare capitol ilustrând o variantă locală a aceluiași contract; într-o instalație reală se adoptă o singură variantă, documentată.

Marca sursei arată când valoarea a existat în proces, iar marca publicării, când a părăsit gateway-ul. Diferența indică întârzierea acumulată până atunci. Dacă baza de date folosește momentul recepției, valorile retransmise după o întrerupere apar drept date curente, falsificând istoricul fără vreo eroare semnalată. De aceea, modelul de date trebuie să distingă momentul măsurării de cel al recepției [42].

Formatul JSON este potrivit pentru un proiect didactic, fiind lizibil și ușor de depanat. Pentru instalații cu multe echipamente, unde volumul mesajelor și

gestionarea stării devin importante, specificația dedicată prezentată în secțiunea 6.2.3 fixează structura subiectelor, codificarea binară a datelor și mecanismele de anunțare a intrării și ieșirii din sesiune ale nodurilor, astfel încât aplicația receptoare să știe în orice moment care surse sunt active; specificația a fost transpusă ca standard internațional [206]. Ea fixează inclusiv numerotarea secvențială a mesajelor și marcarea informațiilor drept neactualizate la pierderea legăturii cu un nod [110]. Adoptarea ei elimină decizii de proiectare care altfel trebuie luate individual, dar impune o disciplină mai strictă asupra modelului de date și reduce lizibilitatea directă a mesajelor.

De la sursă la ecran: bugetul de latență și măsurarea lui

Un tablou de bord industrial nu afișează starea prezentă a procesului, ci o stare anterioară. Diferența trebuie cunoscută înainte de a atribui tabloului de bord funcții pe care nu le poate îndeplini.

Valorile reprezintă ipoteze pentru configurația analizată, nu limite garantate. Pentru afișare, contribuția include așteptarea actualizării și timpul necesar interogării și redării. Intervalul configurat de reîmprospătare nu este identic cu întârzierea fiecărei înregistrări, deoarece aceasta depinde și de momentul în care datele devin disponibile.

Tabelul 9.7 – Bugetul de latență până la afișare, pentru configurația de referință a mini-proiectului

Segment	Estimare tipică	Estimare superioară	Parametrul determinant
Senzor și condiționarea semnalului	10 ms	20 ms	Constanta de timp a traductorului
Achiziție în automatul programabil	20 ms	30 ms	Perioada de scanare, timpul de conversie
Publicare OPC UA	150 ms	300 ms	Intervalul de eșantionare și cel de publicare
Prelucrare în gateway	10 ms	20 ms	Contextualizarea și serializarea
Rețea locală și TLS către broker	3 ms	80 ms	Amplasarea brokerului: local sau extern
Broker MQTT	5 ms	10 ms	Numărul abonaților, nivelul de calitate a serviciului
Regulă de prelucrare și inserare	20 ms	50 ms	Complexitatea regulii, gruparea înregistrărilor
Scriere în baza de date	20 ms	50 ms	Confirmarea scrierii, indexarea
Subtotal până la stocare	**238 ms**	**560 ms**	—
Reîmprospătarea tabloului de bord	1.000 ms	5.000 ms	Intervalul configurat în aplicația de vizualizare
Total perceput de operator	**≈ 1,24 s**	**≈ 5,6 s**	—

Metoda de construire a bugetului, cu descompunerea pe segmente și cu ipotezele fiecăruia, a fost stabilită în secțiunile 5.4.5 și 7.1.4. Elementul adăugat aici este ultimul segment, absent din ambele: intervalul de reîmprospătare al aplicației de

vizualizare, care nu aparţine lanţului de date, dar determină singur ceea ce percepe operatorul. Tabelul 9.7 prezintă bugetul complet, până la ecran.

Interpretare. Ierarhia contribuţiilor contrazice intuiţia comună. Segmentele de reţea şi brokerul, asupra cărora se concentrează de regulă atenţia, însumează sub 4 % din latenţa tipică. Peste 90 % provine din două intervale configurabile: intervalul de publicare al abonamentului OPC UA şi intervalul de reîmprospătare al tabloului de bord. În configuraţia analizată, reducerea întârzierilor mici ale reţelei are un efect limitat asupra timpului total până la afişare. Intervenţia prioritară priveşte contribuţiile dominante, în special publicarea OPC UA şi actualizarea tabloului de bord, cu verificarea încărcării suplimentare produse de reducerea intervalelor.

Consecinţa pentru arhitectură. O buclă de reglare a unui transportor lucrează cu perioade de ordinul a 10 ms, iar o interblocare trebuie să acţioneze într-un interval comparabil. Latenţa tipică a lanţului IIoT, până la stocare, este de peste douăzeci de ori mai mare decât perioada de scanare a automatului programabil (238 ms faţă de 10 ms), iar până la afişare, în scenariul superior considerat, de peste cinci sute de ori mai mare (≈ 5,6 s). Aceasta este justificarea cantitativă a regulii repetate în întreaga carte: funcţiile de control şi interblocare rămân locale nu din prudenţă, ci pentru că lanţul de monitorizare nu poate îndeplini cerinţele lor de timp.

Procedura de măsurare. Bugetul estimat se verifică urmărind aceeaşi modificare de-a lungul traseului. Pentru fiecare încercare se identifică înregistrarea şi se consemnează patru momente: achiziţia la sursă, publicarea din gateway, disponibilitatea în baza de date şi afişarea efectivă pe ecran. Ceasurile utilizate trebuie sincronizate, iar incertitudinea sincronizării trebuie să fie suficient de mică în raport cu întârzierile urmărite.

Sursă – publicare din gateway. Se scade marca_temporala_sursa din marca_temporala_publicare pentru aceeaşi înregistrare. Dacă marca sursei este atribuită la achiziţia valorii în automatul programabil, diferenţa acoperă transferul prin OPC UA şi prelucrarea în gateway. Pentru ipotezele din Tabelul 9.7, contribuţiile estimate sunt de 160 ms în situaţia tipică şi de 320 ms în scenariul superior considerat. Acest interval nu include răspunsul senzorului şi achiziţia anterioară atribuirii mărcii temporale.

Publicare din gateway – disponibilitate în baza de date. Se măsoară intervalul dintre publicarea înregistrării şi momentul în care aceasta devine disponibilă pentru interogare. Momentul disponibilităţii se consemnează separat, prin instrumentarea aplicaţiei sau a serviciului de stocare; el nu se confundă cu marca temporală a măsurării, păstrată în serie. Dacă disponibilitatea este verificată prin interogări periodice, perioada acestora introduce o incertitudine suplimentară, care trebuie declarată. Segmentul include transportul, prelucrarea mesajului şi stocarea.

Disponibilitate în baza de date – afişare. Se măsoară intervalul dintre disponibilitatea înregistrării şi prima afişare efectivă a aceleiaşi înregistrări. Momentul final

trebuie observat sau înregistrat la nivelul interfeței, nu dedus numai din încheierea unei cereri de date. Segmentul include așteptarea următoarei actualizări, interogarea, transferul rezultatului și redarea pe ecran. Pornirea cronometrării la modificarea sursei ar măsura întregul traseu, nu acest segment.

Măsurarea se repetă de cel puțin zece ori, în momente diferite față de ciclul de reîmprospătare, atât în regim obișnuit, cât și la încărcare ridicată. Se raportează numărul încercărilor, condițiile, media și maximul observat. Maximul observat caracterizează încercările efectuate; el nu reprezintă o limită garantată pentru orice situație de funcționare.

Pentru fiecare încercare, suma celor trei intervale trebuie să corespundă diferenței dintre momentul afișării și momentul achiziției la sursă, în limitele incertitudinii de măsurare. Nu se însumează maxime provenite din încercări diferite pentru a le prezenta drept o latență totală măsurată.

Bugetul complet din Tabelul 9.7 include și răspunsul senzorului, respectiv achiziția în automat. Dacă marca temporală a sursei este atribuită după aceste etape, verificarea lor necesită identificarea separată a momentului modificării fizice. În absența acestei măsurări, rezultatul se raportează explicit de la achiziția în automat până la afișare. Pentru configurația din tabel, acest traseu corespunde subtotalului până la stocare din Tabelul 9.7, diminuat cu răspunsul senzorului și achiziția (238 − 10 − 20 = 208 ms în situația tipică), la care se adaugă întârzierea afișării.

Diferențele față de buget se analizează pe segmente. O depășire poate proveni din configurare, încărcare, retransmisii sau din metoda de măsurare și nu indică automat un singur parametru configurat greșit.

Limite ale calculului. Valorile din tabel sunt estimări orientative și trebuie verificate în instalația concretă. Întârzierile pot depăși scenariul superior considerat atunci când apar retransmisii, restabiliri de sesiune sau vârfuri de încărcare. Bugetul descrie funcționarea curentă și nu include recuperarea datelor memorate local după o întrerupere. În această situație, vechimea măsurării și durata transferului la retransmitere se analizează separat, iar ordinea sosirii nu trebuie confundată cu ordinea producerii datelor.

Stocarea datelor

Pentru o bază de date de serii temporale, structura înregistrării separă etichetele, folosite pentru identificare și filtrare, de câmpurile care conțin valorile măsurate:

```
  stare_linie,sit=fabricaA,linie=linia01,echipament=ambalare01,schimb=S2
timp_ciclu_s=2.06,produse_conforme=10860i,produse_neconforme=240i,tempera-
tura_sigilare_c=176.4,stare="productie",calitate_date="buna"
1785927734400000000

  // Ultimul element este marca temporală a sursei, în nanosecunde
  // de la epoca Unix. Corespunde momentului
```

```
// 2026-08-05T11:02:14.400Z din mesajul JSON.
// Sufixul „i” declară contoarele ca numere întregi cu semn.
// Câmpul calitate_date păstrează validitatea valorilor.
```

Conectarea

În acest exemplu, calitate_date se aplică întregului grup de valori, presupuse achiziţionate în acelaşi context. Dacă semnalele au stări de calitate diferite, indicatorul se păstrează separat pentru fiecare semnal. Înregistrările cu valori numerice invalide rămân disponibile pentru diagnostic, dar nu intră în agregatele numerice destinate analizei procesului. O valoare lipsă sau invalidă nu se înlocuieşte cu zero.

Etichetele sunt indexate, ceea ce face interogările rapide, dar impune o restricţie importantă: numărul combinaţiilor distincte de etichete determină dimensiunea indexului. Utilizarea ca etichetă a unui câmp cu valori unice – identificatorul mesajului, marca temporală sau un număr de serie – produce o creştere necontrolată a acestui număr şi degradează progresiv performanţa, fără un mesaj de eroare care să indice cauza. Asemenea valori se păstrează ca simple câmpuri. Consecinţele alegerii modelului de stocare pentru datele industriale sunt tratate pe larg în secţiunea 7.4.4, iar structura interogărilor ulterioare depinde direct de această alegere [193].

Marca temporală a înregistrării trebuie să fie cea a sursei, nu momentul scrierii, iar rezoluţia aleasă trebuie să fie compatibilă cu frecvenţa datelor. Acolo unde mai multe echipamente contribuie la aceeaşi serie, sursele trebuie sincronizate între ele cu o incertitudine mult mai mică decât intervalul analizat [35]; altfel, ordonarea temporală a evenimentelor provenite de la surse diferite nu este semnificativă.

Criterii de reuşită

Fluxul este validat dacă mesajul simplu este publicat şi recepţionat înaintea integrării sursei industriale, iar mesajul complet include toate câmpurile obligatorii din Tabelul 9.6 . Mesajele cu câmpuri obligatorii lipsă sunt respinse şi consemnate, fără stocare parţială. Înregistrările din baza de date corespund mesajelor publicate, tabloul de bord afişează valorile şi momentele corecte, iar seria temporală este ordonată după marca temporală a sursei. Latenţa măsurată pe cele trei segmente se încadrează în bugetul estimat, cu abateri explicabile. Întreruperea comunicaţiei este detectată şi indicată, inclusiv prin vechimea ultimei valori, iar reconectarea nu produce dublări necontrolate. Identităţile şi permisiunile sunt diferenţiate, fiecare client având acces numai la subiectele necesare, conform principiului privilegiului minim [233]. Cheile private şi datele de autentificare nu sunt incluse în fluxuri, capturi sau documentaţia publică.

Proiectul poate fi extins prin adăugarea notificărilor, a indicatorilor calculaţi conform secţiunii 9.2.2, a comparaţiei între mai multe echipamente sau a stocării temporare locale pentru intervalele în care conexiunea externă nu este disponibilă. Ultima extindere impune însă tratarea explicită a datelor retransmise: fără o marcă a provenienţei lor, acestea nu pot fi deosebite de datele produse în timp real.

9.2.4. Mini-proiectul 4: Celulă robotizată conectată IIoT

Scop și arhitectură

Proiectarea și implementarea unei celule robotizate care execută procesul local și transmite către sistemele de supraveghere și analiză datele necesare pentru monitorizarea producției, a stării tehnice și a calității.

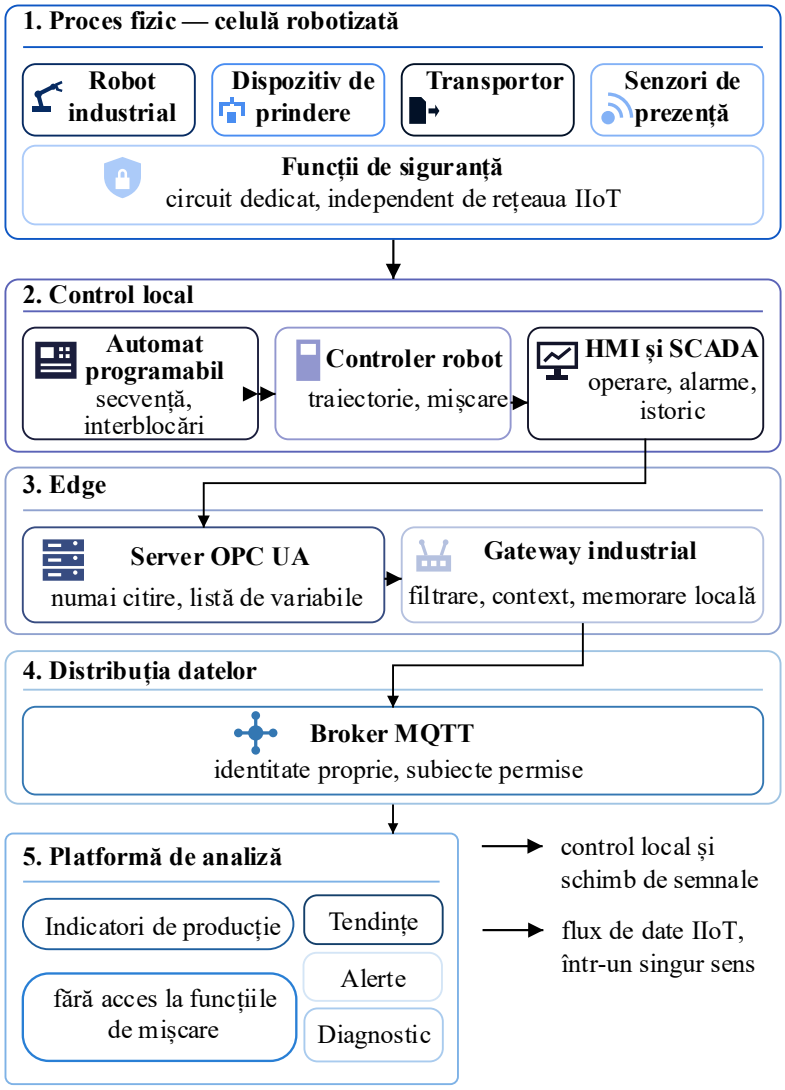


Figura 9.6 – Arhitectura celulei robotizate conectate IIoT

Celula poate include un robot industrial sau un simulator, un automat programabil, o bandă transportoare, senzori de prezență, un dispozitiv de prindere, o interfață HMI, un sistem SCADA, un gateway industrial și o platformă de analiză. Integrarea unei celule robotizate în rețeaua IIoT, cu datele disponibile la nivelul

controlerului de robot, a fost tratată în secțiunea 4.3.2; mini-proiectul de față o implementează și o validează.

Arhitectura funcțională pornește de la procesul robotizat și cuprinde robotul și automatul programabil, urmate de sistemele HMI și SCADA și de serverul OPC UA. Datele sunt apoi preluate de gateway-ul industrial și transmise prin MQTT către baza de date și tabloul de bord.

Componentele și interfețele dintre ele sunt prezentate în Figura 9.6. Controlul mișcărilor robotului, coordonarea cu automatul programabil și funcțiile de siguranță rămân locale. Platforma externă nu transmite direct comenzi de mișcare și nu poate modifica programul robotului.

Delimitarea rolurilor și tratarea siguranței

Mini-proiectul se referă exclusiv la fluxul informațional al celulei. Protecția persoanelor – delimitarea spațiului de lucru, dispozitivele de supraveghere a accesului, oprirea de urgență, modurile de operare cu viteză redusă și validarea acestora – aparține integrării celulei și se proiectează pe baza unei evaluări a riscului. Cadrul normativ tratează robotul ca mașină incompletă, ale cărei cerințe se completează la nivelul aplicației [150], în timp ce cerințele pentru integrarea aplicațiilor robotizate și a celulelor, incluzând punerea în funcțiune, exploatarea, mentenanța și verificarea măsurilor de protecție, fac obiectul unei părți distincte a seriei [128]. Evaluarea riscului precedă, în ambele cazuri, alegerea măsurilor de protecție, iar rezultatul ei determină nivelul de performanță cerut părților de comandă relevante pentru siguranță [45], [142].

Tabelul 9.8 – Repartizarea responsabilităților în celula robotizată conectată

Funcție	Componenta responsabilă	Poate fi transferată extern	Comportament la pierderea legăturii externe
Traiectoria și mișcarea robotului	Controlerul de robot	Nu	Neafectat
Secvența celulei și interblocările	Automat programabil	Nu	Neafectat
Oprirea de urgență și supravegherea accesului	Circuit de siguranță dedicat	Nu	Neafectat
Operarea și confirmarea alarmelor	HMI local	Nu	Neafectat
Supravegherea și istoricul pe termen scurt	SCADA	Parțial	Funcționează local
Contextualizarea și filtrarea datelor	Gateway industrial	Nu	Memorează local
Distribuirea mesajelor	Broker MQTT	Da	Gateway-ul acumulează
Stocarea pe termen lung	Bază de date	Da	Lacună, recuperată la reconectare
Calculul indicatorilor și analiza	Platformă externă	Da	Indisponibil temporar
Modificarea programului robotului	Stație de inginerie, local	Nu	Indisponibil, fără efect asupra producției

Aceste funcţii nu se realizează prin reţeaua IIoT, nu se supraveghează prin tabloul de bord şi nu sunt condiţionate de disponibilitatea vreunui serviciu extern. Sistemul de monitorizare poate afişa faptul că o protecţie a fost declanşată, dar nu participă în niciun fel la declanşarea sau anularea ei.

Separarea trebuie să se regăsească şi în arhitectura de reţea. Celula, gateway-ul industrial şi serviciile externe aparţin unor zone distincte, iar traficul dintre ele trece prin puncte de trecere controlate, cu reguli explicite privind sensul iniţierii conexiunii; principiul zonelor şi al conductelor, împreună cu cerinţele asociate nivelurilor de securitate, a fost tratat în secţiunile 8.2.5 şi 8.3.2. În configuraţia uzuală, gateway-ul iniţiază conexiunea către broker, iar serviciile externe nu deschid conexiuni către zona de automatizare [68].

Rezultatul acestei delimitări se consemnează în tabelul de responsabilităţi prezentat în Tabelul 9.8. O delimitare păstrată numai în memoria proiectantului se pierde la prima modificare.

Datele urmărite şi cele două regimuri de publicare

Aplicaţia poate colecta starea celulei şi modul de funcţionare; starea robotului şi programul executat; numărul ciclului şi identificatorul produsului; momentul începerii şi finalizării ciclului; durata ciclului; rezultatul operaţiei; starea dispozitivului de prindere; codurile de alarmă şi defect, cu momentul apariţiei şi al confirmării; numărul şi durata opririlor; consumul energetic sau al altor utilităţi, dacă există instrumentaţia necesară.

Aceste date se transmit prin două tipuri de mesaje, cu regimuri diferite:

- *Mesajul de stare* se publică periodic, la o secundă, pe subiectul fabricaA/celula01/robot01/stare, şi descrie situaţia curentă.
- *Mesajul de ciclu* se publică la eveniment, la finalizarea fiecărui ciclu, pe subiectul fabricaA/celula01/robot01/ciclu, şi conţine identificatorul produsului, momentele de început şi de sfârşit, durata şi rezultatul.

Confuzia dintre cele două regimuri este o eroare frecventă şi are consecinţe asimetrice. Eşantionarea periodică a unui contor de cicluri pierde ciclurile mai scurte decât perioada de eşantionare, iar pierderea este tăcută: seria arată coerent, dar subestimează producţia. Publicarea la eveniment a unei mărimi continue produce fie mesaje inutile, fie lacune în serie, iar lacuna este vizibilă. Prima eroare este mai gravă tocmai pentru că nu se observă.

Etapele de realizare

Definirea procesului. Se descrie operaţia realizată de robot, succesiunea mişcărilor, transferul piesei, criteriul de finalizare şi situaţiile de defect.

Delimitarea responsabilităţilor. Se completează tabelul de responsabilităţi din Tabelul 9.8 pentru configuraţia concretă. Nicio funcţie critică nu trebuie repartizată exclusiv serviciilor externe.

Implementarea sincronizării locale. Schimbul de semnale dintre robot şi automatul programabil trebuie să includă stări precum pregătit, cerere de pornire, ciclu activ, operaţie finalizată şi defect. Confirmarea trebuie realizată în ambele sensuri: emiţătorul menţine cererea până la primirea confirmării, iar receptorul menţine confirmarea până la retragerea cererii. Structurarea acestui schimb pe stări explicite, cu tranziţii verificabile, corespunde reprezentării secvenţiale definite normativ [123]. Fiecare aşteptare trebuie limitată în timp, astfel încât o confirmare care nu sosește să conducă la starea de defect, nu la blocarea nedeterminată a secvenţei.

Configurarea HMI şi SCADA. Operatorul trebuie să poată observa starea celulei, etapele ciclului, alarmele şi valorile procesului. Istoricul trebuie să permită reconstruirea succesiunii evenimentelor, ceea ce impune înregistrarea momentului apariţiei, al confirmării şi al dispariţiei fiecărei alarme, nu doar a stării curente.

Expunerea datelor. Variabilele selectate sunt puse la dispoziţia gateway-ului prin OPC UA sau printr-o altă interfaţă industrială adecvată. Drepturile de citire şi scriere trebuie stabilite explicit, iar contul utilizat de gateway trebuie să dispună exclusiv de drept de citire asupra variabilelor din listă. Expunerea întregii memorii a automatului programabil „pentru orice eventualitate" transformă o interfaţă de monitorizare într-o cale de acces la proces, iar cerinţele tehnice aplicabile componentelor de acest tip impun explicit restrângerea funcţiilor la cele necesare [156].

Contextualizarea edge. Gateway-ul filtrează datele, adaugă identificatorul celulei şi marca temporală, verifică existenţa valorilor obligatorii şi construieşte mesajul transmis către platformă, conform contractului de date din Tabelul 9.6.

Transmiterea şi stocarea. Mesajele sunt publicate prin MQTT, utilizând o identitate individuală şi permisiuni limitate la subiectele necesare. O identitate comună mai multor celule face imposibilă atât atribuirea unei publicări greşite, cât şi revocarea accesului unei singure surse [156].

Configurarea indicatorilor. Pot fi calculaţi numărul de cicluri, durata medie a ciclului, dispersia duratelor, disponibilitatea, numărul opririlor şi proporţia operaţiilor finalizate fără eroare. Dispersia duratelor este adesea mai informativă decât media: o creştere a împrăştierii, la medie constantă, semnalează de regulă o problemă de alimentare cu piese sau de prindere, înainte ca aceasta să producă opriri.

Validarea progresivă. Se testează separat controlul local, schimbul robot–automat programabil, achiziţia OPC UA, publicarea MQTT, stocarea şi vizualizarea. Numai după validarea fiecărui segment se verifică fluxul complet.

Testarea rezilienţei. Se întrerupe controlat conexiunea cu gateway-ul, brokerul MQTT sau baza de date. Celula trebuie să continue ori să ajungă într-o stare sigură, iar pierderea monitorizării trebuie semnalată fără a afecta logica locală. Se verifică, de asemenea, comportamentul la restabilirea conexiunii: datele memorate local

trebuie retransmise fără a fi confundate cu date curente şi fără a produce înregistrări duplicate. Identificatorul de mesaj şi numerotarea secvenţială sunt mecanismele care fac posibilă eliminarea duplicatelor [25].

Dimensionarea memoriei tampon locale

Cerinţa de la punctul 10 nu se rezolvă prin configurare implicită. Capacitatea de memorare locală determină durata întreruperii pe care sistemul o poate acoperi fără pierdere de date, iar calculul este simplu şi rareori efectuat.

Date de intrare. Mesajul de stare: 1 mesaj/s, aproximativ 380 de octeţi stocaţi local, în formă comprimată. Mesajul de ciclu: 1 mesaj la 24 s, aproximativ 300 de octeţi. Memorie disponibilă alocată pentru tampon: 64 MB.

Calcul. Volumul acumulat într-o oră este:

$$V = (3.600 \times 380) + (150 \times 300) = 1.413.000 \text{ octeţi/h} = 1{,}413 \text{ MB/h}$$

Se utilizează unităţi zecimale: 1 MB = 1.000.000 de octeţi. Durata teoretică acoperită de memoria alocată este:

$$t = 64 / 1{,}413 \approx 45{,}3 \text{ h}$$

Interpretare. Capacitatea calculată nu acoperă integral o întrerupere de 48 de ore. Pentru această durată, mesajele ar ocupa cel puţin 1,413 × 48 = 67,824 MB, înaintea spaţiului suplimentar necesar administrării stocării şi a rezervei de capacitate. Dacă cerinţa este păstrarea tuturor datelor timp de 48 de ore, se măreşte memoria disponibilă sau se reduce justificat volumul înregistrat. În toate cazurile se declară comportamentul la umplere: oprirea înregistrărilor noi, suprascrierea celor mai vechi sau reducerea frecvenţei de memorare, cu prioritizarea evenimentelor importante. Alegerea depinde de informaţia care trebuie conservată.

Limite. Calculul presupune un debit constant şi dimensiunile medii declarate ale mesajelor stocate. Durata efectivă poate fi mai mică din cauza metadatelor, a administrării memoriei şi a variaţiilor de trafic. La reconectare, retransmiterea datelor acumulate încarcă suplimentar comunicaţia şi baza de date; debitul recuperării se limitează astfel încât să permită şi prelucrarea datelor curente.

Limitele realizării prin simulare

Simulatorul producătorului reproduce cinematica, ciclul şi schimbul de semnale, dar nu reproduce toleranţele de poziţionare a piesei, forţa de prindere, uzura dispozitivului de prindere, deformarea elastică a braţului la sarcină şi nici timpii reali de comutare ai perifericelor. O traiectorie fără coliziuni în model poate produce contact în celula reală dacă geometria, poziţia piesei sau starea dispozitivelor de protecţie diferă de reprezentare.

Din acest motiv, trecerea de la model la instalaţie se face progresiv: verificare în model, apoi funcţionare în regim controlat, cu viteză redusă şi spaţiu de lucru restrâns, apoi în condiţii reale de producţie. Validarea măsurilor de protecţie se

realizează exclusiv pe celula fizică, indiferent de fidelitatea reprezentării digitale [128]. Un model nu poate prelua funcţiile echipamentelor de siguranţă şi nu poate constitui dovadă a conformităţii aplicaţiei.

Criterii de reuşită

Mini-proiectul integrator trebuie să demonstreze că:

- robotul şi automatul programabil execută corect şi repetabil secvenţa locală;
- funcţiile de siguranţă sunt independente de sistemele IIoT şi rămân operante la indisponibilitatea acestora;
- fiecare ciclu poate fi asociat cu un moment, un rezultat şi o stare a celulei;
- datele afişate corespund stărilor reale;
- o alarmă poate fi urmărită de la sursă până la înregistrarea din baza de date, cu momentele apariţiei şi confirmării;
- pierderea serviciilor externe nu conduce la pierderea controlului local, iar durata acoperită de memoria tampon este cunoscută şi declarată;
- platforma externă nu dispune de acces direct la funcţiile de mişcare, iar contul utilizat pentru achiziţie nu are drept de scriere;
- configuraţiile, rezultatele testelor şi limitele sistemului sunt documentate.

Proiectul poate fi extins prin monitorizarea uzurii dispozitivului de prindere, integrarea unui sistem de vedere artificială, calcularea indicatorilor de eficienţă, realizarea unui geamăn digital conform delimitărilor din secţiunea 7.3.4 sau coordonarea mai multor roboţi. Extensiile trebuie introduse numai după validarea configuraţiei de bază şi fără modificarea principiului potrivit căruia controlul critic rămâne local.

9.2.5. Evaluarea şi documentarea mini-proiectelor

Cele patru mini-proiecte formează o progresie de la achiziţia unei mărimi fizice la integrarea unei aplicaţii robotizate complete. Sinteza lor, cu competenţa centrală şi criteriul de acceptare decisiv al fiecăruia, este prezentată în Tabelul 9.9.

Încercările de defect obligatorii

Un mini-proiect nu este validat prin funcţionarea în regim normal. Regimul normal demonstrează că soluţia poate funcţiona; comportamentul la defect demonstrează că poate fi exploatată. Încercările din Tabelul 9.10 se execută deliberat, în ordinea indicată, iar rezultatul fiecăreia se consemnează.

Cele două încercări separă actualitatea unei măsurări de modificarea valorii sale. O temperatură poate rămâne constantă în timp ce senzorul şi achiziţia funcţionează corect. Invers, o conexiune activă poate transmite repetat ultima valoare disponibilă, fără ca sursa să mai efectueze măsurări. Actualitatea se verifică prin marca temporală a ultimei achiziţii sau printr-un indicator explicit al actualizării, nu prin diferenţa dintre valorile numerice succesive.

Tabelul 9.9 – Sinteza celor patru mini-proiecte ghidate

Mini-proiect	Competența centrală dobândită	Componente minime	Date produse	Criteriul de acceptare decisiv
9.2.1 Rețea de senzori	Achiziția corectă a unei mărimi fizice și dimensionarea fluxului de date	Senzori, modul de achiziție sau automat programabil, HMI, gateway	Caracteristici extrase, la interval fix	Valoarea măsurată se regăsește identic în baza de date, iar debitul corespunde calculului
9.2.2 Linie de transport	Logica secvențială, comanda actuatoarelor și indicatorii de producție	Automat programabil, senzori de prezență, motor, actuator de deviere, HMI	Contoare, durate de ciclu, opriri clasificate	Componentele indicatorului pot fi reconstituite din datele brute stocate
9.2.3 Tablou de bord	Contractul de date, traseul informațional complet și comportamentul la defect	Sursă OPC UA, gateway, broker, bază de date, aplicație de vizualizare	Mesaje contextualizate, serii temporale	Traseul unei valori este demonstrabil de la sursă la afișare, cu latență măsurată
9.2.4 Celulă robotizată	Integrarea controlului, supravegherii, schimbului de date și securității	Robot sau simulator, automat programabil, HMI, SCADA, gateway, platformă	Cicluri, rezultate, alarme, indicatori	Pierderea serviciilor externe nu afectează controlul local sau siguranța

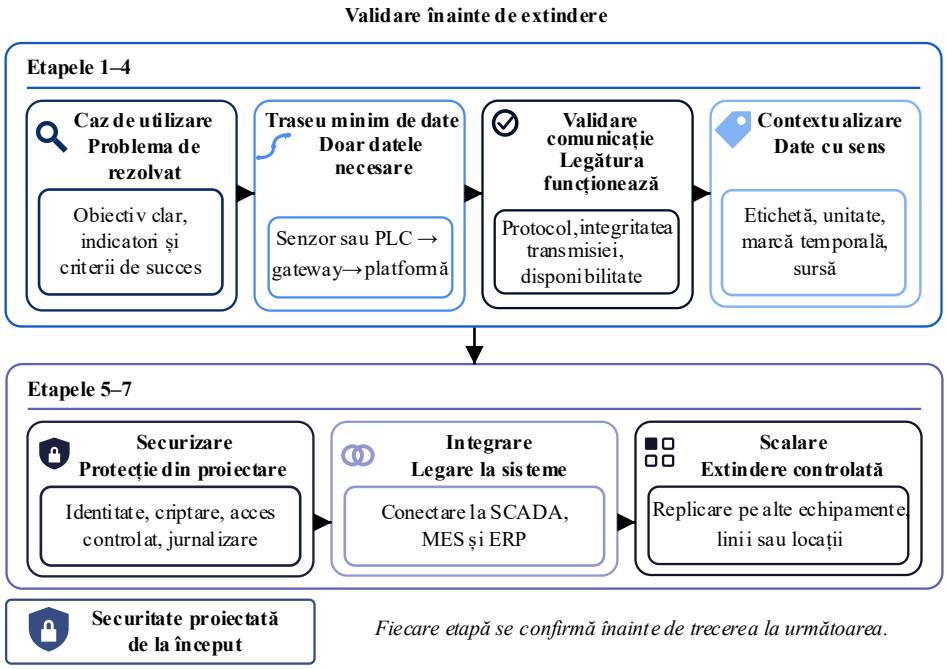


Figura 9.7 – Etapele de validare a unui mini-proiect înaintea extinderii

Pentru semnalele periodice, pragul de vechime se stabilește în raport cu perioada de achiziție, intervalul de raportare și întârzierile admise. Dacă raportarea utilizează o bandă moartă sau transmite numai schimbările, trebuie prevăzută o confirmare periodică a actualizării achiziției, independentă de variația valorii. Un

mesaj care confirmă doar funcţionarea gateway-ului nu demonstrează că senzorul continuă să furnizeze măsurări.

Pentru înregistrările generate la eveniment, precum rezultatul unei cântăriri, absenţa unei înregistrări noi nu indică singură un defect: este posibil să nu fi fost procesat un produs. Verificarea se raportează la evenimentul aşteptat şi la starea procesului. La retransmiterea unei măsurări memorate, momentul achiziţiei rămâne neschimbat; momentul recepţiei nu o transformă într-o măsurare nouă.

Tabelul 9.10 – Încercări de defect obligatorii pentru fiecare mini-proiect

Încercare	Cum se provoacă	Comportamentul aşteptat	Se aplică la
Întreruperea unui traductor	Se deconectează un fir al buclei de curent	Valoarea este marcată nevalidă, distinct de o valoare mică legitimă	9.2.1, 9.2.2
Oprirea actualizării măsurării	Se oprește achiziția unui semnal periodic, menținând comunicația activă și ultima valoare disponibilă	Marca temporală a măsurării nu avansează; după depășirea pragului de vechime, valoarea este marcată ca neactualizată	9.2.1, 9.2.3
Valoare constantă, actualizată	Se menține constantă mărimea simulată, iar achiziția periodică și actualizarea mărcii temporale continuă	Valoarea rămâne validă și actuală; constanța numerică nu declanșează semnalarea lipsei actualizării	9.2.1, 9.2.3
Produs oprit în dreptul senzorului	Se oprește banda cu o piesă în fața barierei	Contorul nu crește; numărarea rămâne pe front	9.2.2
Actuator care nu confirmă	Se blochează mecanic cursa cilindrului	Trecere în starea de defect după temporizarea stabilită, cu cod atribuit	9.2.2, 9.2.4
Câmp obligatoriu lipsă	Se publică un mesaj fără marca temporală a sursei	Mesajul este respins și consemnat, nu stocat parțial	9.2.3
Pierderea legăturii cu brokerul	Se oprește serviciul brokerului	Gateway-ul memorează local; procesul continuă neafectat	9.2.3, 9.2.4
Reconectare cu date acumulate	Se repornește brokerul după 15 minute	Retransmitere fără duplicate, cu marca temporală a sursei păstrată	9.2.3, 9.2.4
Umplerea memoriei tampon	Se reduce spațiul alocat și se întrerupe legătura	Comportamentul la umplere este cel declarat în documentație	9.2.4
Confirmare care nu sosește	Se suprimă semnalul de răspuns al robotului	Secvența trece în defect după temporizare, nu se blochează	9.2.4
Cont fără drepturi	Se încearcă publicarea pe un subiect nepermis	Publicarea este respinsă și înregistrată	9.2.3, 9.2.4

Grila de evaluare

Evaluarea unui mini-proiect nu poate consta în constatarea că aplicaţia funcţionează. Un sistem care afişează valori plauzibile, dar al cărui traseu informaţional nu poate fi verificat, nu îndeplineşte condiţiile unei soluţii industriale. Grila din Tabelul 9.11 separă criteriile pe cinci dimensiuni, fiecare verificabilă independent. Ordinea

în care se confirmă etapele unui mini-proiect, de la cazul de utilizare până la extindere, este sintetizată în Figura 9.7.

Tabelul 9.11 – Grilă de evaluare a unui mini-proiect IIoT

Dimensiune	Ponderе	Ce se verifică	Cum se verifică	Rezultat acceptabil
Corectitudinea datelor	25 %	Concordanța valorii de la sursă cu cea afișată, unitatea și marca temporală	Comparare pe cinci valori, în trei regimuri de funcționare	Abatere numai din rotunjire; unități și mărci temporale identice
Trasabilitatea	20 %	Posibilitatea urmăririi unei valori înapoi până la sursă	Se alege o înregistrare din baza de date și se reconstituie traseul complet	Toate segmentele identificabile, fiecare cu marcă temporală
Comportamentul la defect	30 %	Reacția la fiecare încercare din Tabelul 9.10	Se execută toate încercările aplicabile mini-proiectului	Fiecare încercare produce comportamentul așteptat, consemnat
Dimensionarea justificată	10 %	Existența bugetelor calculate și concordanța lor cu măsurarea	Se compară valoarea calculată cu cea măsurată pentru bandă, latență și memorie tampon	Abatere explicabilă între calcul și măsurare
Reproductibilitatea	15 %	Posibilitatea refacerii configurației de altcineva	Documentația este dată unei persoane neimplicate în realizare	Configurația poate fi refăcută fără întrebări suplimentare

Ponderile însumează 100 %, iar fiecare criteriu este observabil: verificarea produce un rezultat consemnabil, nu o apreciere. Un mini-proiect se consideră acceptat la minimum 80 % din total, cu condiția ca dimensiunea „comportamentul la defect" să obțină cel puțin jumătate din ponderea proprie; un sistem care funcţionează impecabil în regim normal şi cedează necontrolat la prima întrerupere nu poate fi acceptat, indiferent de punctajul obţinut la celelalte dimensiuni.

Ultima dimensiune este cea mai frecvent ignorată şi cea mai costisitoare pe termen lung. Un proiect care nu poate fi refăcut din documentaţia proprie nu este un rezultat, ci o demonstraţie. Cerinţa de reproductibilitate coincide, în cazul datelor industriale, cu cerinţa de a putea extrage seriile împreună cu contextul lor [245].

Documentaţia minimă

Pentru fiecare mini-proiect trebuie păstrate: lista intrărilor şi ieşirilor cu denumirile simbolice; contractul de date, cu versiunea sa; convenţia de denumire a subiectelor; parametrii de achiziţie adoptaţi şi justificarea lor; valorile de referinţă şi pragurile, cu perioada în care au fost stabilite; rezultatele testelor de defect; bugetele calculate – bandă, latenţă, memorie tampon – împreună cu valorile măsurate; limitele cunoscute ale soluţiei.

Această listă corespunde elementelor cerute la începutul secţiunii 9.2 şi închide bucla: ceea ce a fost enunţat ca cerinţă de proiectare devine, la final, criteriu de acceptare.

9.3. Concluzii

Aplicaţiile prezentate în acest capitol arată că valoarea IIoT nu rezultă din conectarea echipamentelor, ci din transformarea datelor în informaţii relevante şi acţiuni verificabile. Mentenanţa predictivă, monitorizarea energetică şi automatizarea agroindustrială urmează aceeaşi logică: definirea problemei, selectarea datelor necesare, achiziţia şi contextualizarea acestora, prelucrarea, formularea deciziei şi evaluarea rezultatului. Ordinea acestor etape nu este negociabilă; inversarea ei, prin alegerea platformei înaintea definirii problemei, produce sisteme care funcţionează fără a fi utile.

Cele trei familii diferă însă prin regimul datelor, iar diferenţa determină arhitectura mai mult decât orice preferinţă tehnologică. Un semnal de vibraţie impune prelucrare locală, pentru că volumul brut face transmiterea nerezonabilă. Un contor de energie impune normalizare, pentru că valoarea absolută nu este interpretabilă singură. O măsurare de mediu impune redundanţă şi verificare prin efect, pentru că defectul aparatului şi absenţa fenomenului produc aceeaşi indicaţie. Recunoaşterea regimului de date este, practic, prima decizie de proiectare.

Mini-proiectele ghidate transpun această logică în configuraţii care integrează senzori, automate programabile, interfeţe HMI, sisteme SCADA, OPC UA, MQTT, baze de date şi tablouri de bord. Validarea progresivă a fiecărui segment permite identificarea erorilor, verificarea traseului informaţiei şi demonstrarea concordanţei dintre starea procesului, mesajele transmise şi datele utilizate în analiză. Elementul care deosebeşte o implementare matură de una improvizată nu este complexitatea componentelor, ci existenţa unui contract de date explicit şi a unei proceduri prin care orice valoare afişată poate fi urmărită înapoi până la sursa ei.

Tratările cantitative incluse în capitol au un rol care depăşeşte exemplificarea. Ele arată unde se află efectiv limitele unei soluţii IIoT şi, mai ales, unde nu se află. Volumul comunicaţiei este determinat de decizia privind ceea ce se transmite, nu de performanţa reţelei: raportul de 610:1 dintre semnalul brut şi caracteristicile extrase se obţine printr-o decizie de proiectare, nu printr-o investiţie. Întârzierea percepută de operator provine aproape integral din două intervale de configurare, nu din infrastructura de transport, ceea ce face ca optimizarea reţelei să fie, în cele mai multe cazuri, un efort fără efect vizibil. O pierdere de productivitate poate fi de aceeaşi mărime cu opririle înregistrate şi totuşi complet invizibilă în jurnalul acestora. Durata acoperită de o memorie tampon locală este un număr calculabil, iar comportamentul la umplerea ei este o decizie, nu o proprietate implicită. În toate cazurile, concluzia este identică: o mărime care nu a fost calculată nu poate fi administrată, iar aprecierile calitative privind „viteza" sau „volumul" conduc la decizii de proiectare greşite.

O soluţie IIoT industrială trebuie să păstreze o delimitare clară între controlul local şi serviciile de monitorizare sau analiză. Funcţiile critice, interblocările şi mecanismele de siguranţă rămân la nivelul robotului, al automatului programabil şi al

dispozitivelor locale. Sistemele externe completează aceste funcţii prin stocare, vizualizare, corelare şi sprijinirea deciziilor, fără a deveni o condiţie pentru menţinerea procesului într-o stare controlată. Această delimitare are, aşa cum s-a arătat prin bugetul de latenţă, o justificare măsurabilă, nu una de precauţie.

Arhitectura trebuie evaluată împreună cu securitatea, disponibilitatea, calitatea datelor şi posibilitatea de extindere. Identităţile individuale, drepturile limitate, comunicaţiile protejate, segmentarea reţelei, jurnalizarea şi comportamentul la pierderea conexiunii reprezintă cerinţe ale proiectării, nu intervenţii care pot fi adăugate după finalizarea implementării. La acestea se adaugă, de la intrarea în aplicare a reglementării europene privind accesul la date, cerinţe care privesc însuşi modul în care datele sunt structurate şi puse la dispoziţie – decizii care, luate târziu, impun reconfigurarea unui sistem altfel funcţional.

Parcursul cărţii a urmărit evoluţia de la digitalizarea proceselor industriale şi organizarea fabricii până la automatizare, comunicaţii, arhitecturi IIoT, securitate şi aplicaţii integrate. Firul comun îl reprezintă utilizarea controlată a datelor pentru îmbunătăţirea proceselor fizice, păstrând corectitudinea tehnică, responsabilităţile clar delimitate şi rolul deciziei umane.

Soluţiile prezentate nu constituie configuraţii rigide, ci repere pentru proiectarea unor sisteme adaptate procesului, infrastructurii şi obiectivelor fiecărei organizaţii. O implementare poate fi considerată matură atunci când problema industrială este clar definită, traseul datelor poate fi demonstrat, efectul asupra procesului poate fi măsurat, iar sistemul continuă să funcţioneze sigur şi controlat atât în condiţii normale, cât şi la apariţia unor defecte.

9.4. Întrebări de verificare

1. *Care este criteriul prin care se stabileşte dacă o aplicaţie IIoT este justificată?*

a) utilizarea unei platforme cloud, indiferent de rezultatul procesului;
b) numărul graficelor din tabloul de bord;
c) datele colectate trebuie să poată fi transformate în decizii şi acţiuni care îmbunătăţesc funcţionarea procesului, iar efectul trebuie verificat printr-un indicator definit;
d) numărul dispozitivelor conectate şi volumul înregistrărilor stocate.

2. *De ce se evaluează vibraţiile prin două criterii complementare, iar cel al variaţiei faţă de referinţa proprie este adesea mai sensibil?*

a) pentru că limita clasei de maşini este valabilă identic pentru orice montaj şi orice pompă;
b) pentru că referinţa proprie se stabileşte o singură dată, la achiziţia senzorului, indiferent de regim;

c) pentru că o creștere față de valoarea de referință a echipamentului concret, în regim normal, poate semnala degradarea cu mult înainte ca valoarea absolută să depășească limita generală a clasei de mașini;
d) pentru că valoarea absolută nu poate fi măsurată cu un accelerometru.

3. *Ce trebuie să se întâmple când o aplicație de mentenanță predictivă generează o alertă?*

a) alerta se ignoră până la depășirea limitei absolute a clasei de mașini;
b) alerta modifică direct programul PLC pentru a reduce sarcina;
c) echipamentul se oprește automat prin comandă transmisă de platforma cloud;
d) alerta se verifică și se folosește la planificarea intervenției; oprirea echipamentului este automată numai dacă a fost proiectată și validată ca funcție de control sau de protecție.

4. *Consumul unei linii a fost de 480 kWh pe schimb pentru 12 000 de produse, iar după modificarea programului de 505 kWh pentru 14 000 de produse. Ce concluzie este corectă?*

a) consumul absolut a crescut cu 5,2 %, iar consumul specific a scăzut de la 40,0 la 36,1 Wh/produs (−9,8 %); cei doi indicatori răspund unor întrebări diferite;
b) consumul specific a crescut de la 36,1 la 40,0 Wh/produs;
c) consumul s-a înrăutățit, deoarece consumul absolut a crescut;
d) indicatorul absolut este suficient și cel specific nu trebuie calculat.

5. *Care este cel mai util indicator de calitate a instalării unui sistem de monitorizare energetică?*

a) numărul graficelor din tabloul de bord energetic;
b) diferența dintre suma consumurilor măsurate pe ramuri și consumul înregistrat la punctul general;
c) frecvența cu care este actualizată factura de utilități;
d) numărul de protocoale utilizate de contoare.

6. *Ce înseamnă „verificarea prin efect” în automatizările agroindustriale (de exemplu la irigare)?*

a) verificarea efectului asupra facturii de apă la sfârșitul lunii;
b) verificarea efectului numai de către platforma cloud;
c) confruntarea comenzii cu o mărime independentă care confirmă executarea ei, de exemplu debitul după comanda electrovalvei;
d) verificarea doar a faptului că PLC-ul a emis comanda.

7. *De ce irigarea sau ventilația dintr-o seră nu trebuie să depindă de disponibilitatea unei conexiuni externe?*

a) deoarece rețelele LoRaWAN sunt mai rapide decât orice rețea locală;
b) deoarece regulile și interblocările sunt aplicate de controlerul local, iar platforma asigură analiza istorică, configurarea controlată, notificarea și compararea zonelor;

c) deoarece platforma IIoT nu poate stoca date agricole;
d) deoarece senzorii agricoli nu pot comunica prin rețele radio.

8. Un senzor de vibrații eșantionează la 5 120 Hz pe 3 canale, cu 16 biți pe eșantion. Ce debit are semnalul brut transmis continuu și cum se compară cu transmiterea caracteristicilor (circa 500 de octeți la 10 s)?

a) 245 760 bit/s (≈ 2,65 GB/zi pe echipament), față de ≈ 4,32 MB/zi pentru caracteristici; raportul este de aproximativ 610:1;
b) 2 457 600 bit/s; transmiterea semnalului brut este mai eficientă;
c) 24 576 bit/s; raportul față de caracteristici este de aproximativ 6:1;
d) 245 760 bit/s; raportul față de caracteristici este de aproximativ 2:1.

9. Ce două momente trebuie păstrate în mesaj și de ce nu se folosește momentul recepției în baza de date?

a) doar marca temporală a brokerului; deoarece sursa nu are ceas;
b) marca temporală a sursei și marca temporală a publicării; folosirea momentului recepției ar face ca valorile retransmise după o întrerupere să apară drept date curente;
c) marca temporală a recepției și numărul mesajului; deoarece marca sursei nu poate fi citită;
d) nu este nevoie de nicio marcă temporală, ordinea fiind dată de QoS.

10. Care este diferența dintre mesajul de stare și mesajul de ciclu al unei celule robotizate și ce se întâmplă dacă sunt confundate?

a) starea se publică la eveniment, iar ciclul periodic; nu există consecințe;
b) ambele se publică la o secundă și transportă aceleași date;
c) mesajul de ciclu este transmis exclusiv de platforma cloud, către robot;
d) starea se publică periodic (la o secundă), iar ciclul la eveniment; eșantionarea periodică a unui contor de cicluri pierde în mod tăcut ciclurile mai scurte decât perioada de eșantionare.

ANEXĂ – RĂSPUNSURI LA ÎNTREBĂRILE DE VERIFICARE

Cap.	1	2	3	4	5	6	7	8	9
1	c	d	d	b	c	c	c	b	c
2	d	c	b	d	b	d	a	d	c
3	d	c	b	a	a	a	d	c	d
4	c	b	d	a	c	a	c	a	a
5	a	a	c	c	d	d	a	c	b
6	b	d	a	a	c	c	b	b	c
7	b	d	a	b	b	b	a	a	b
8	c	b	a	d	b	b	d	b	a
9	a	a	d	b	d	c	b	d	b
10	b	c	c	c	a	d	d	a	d

BIBLIOGRAFIE

[1] Groover, M. P. (2019). *Automation, production systems, and computer-integrated manufacturing* (5th ed.). Pearson.

[2] Bolton, W. (2015). *Programmable logic controllers* (6th ed.). Newnes/Elsevier.

[3] Lasi, H., Fettke, P., Kemper, H.-G., Feld, T., & Hoffmann, M. (2014). Industry 4.0. *Business & Information Systems Engineering, 6*(4), 239–242. https://doi.org/10.1007/s12599-014-0334-4

[4] Kagermann, H., Wahlster, W., & Helbig, J. (2013). *Recommendations for implementing the strategic initiative INDUSTRIE 4.0: Final report of the Industrie 4.0 Working Group*. acatech — National Academy of Science and Engineering.

[5] Hermann, M., Pentek, T., & Otto, B. (2016). Design principles for Industrie 4.0 scenarios. *Proceedings of the 49th Hawaii International Conference on System Sciences*, 3928–3937. https://doi.org/10.1109/HICSS.2016.488

[6] Deutsches Institut für Normung. (2016). *Referenzarchitekturmodell Industrie 4.0 (RAMI4.0)* (DIN SPEC 91345:2016-04). Beuth. https://doi.org/10.31030/2436156

[7] International Electrotechnical Commission. (2017). *Smart manufacturing — Reference architecture model Industry 4.0 (RAMI4.0)* (IEC PAS 63088:2017).

[8] Baheti, R., & Gill, H. (2011). Cyber-physical systems. În T. Samad & A. M. Annaswamy (Eds.), *The impact of control technology* (pp. 161–166). IEEE Control Systems Society.

[9] Monostori, L., Kádár, B., Bauernhansl, T., Kondoh, S., Kumara, S., Reinhart, G., Sauer, O., Schuh, G., Sihn, W., & Ueda, K. (2016). Cyber-physical systems in manufacturing. *CIRP Annals, 65*(2), 621–641. https://doi.org/10.1016/j.cirp.2016.06.005

[10] Lee, J., Bagheri, B., & Kao, H.-A. (2015). A cyber-physical systems architecture for Industry 4.0-based manufacturing systems. *Manufacturing Letters, 3*, 18–23. https://doi.org/10.1016/j.mfglet.2014.12.001

[11] Breque, M., De Nul, L., & Petridis, A. (2021). *Industry 5.0: Towards a sustainable, human-centric and resilient European industry*. European Commission, Directorate-General for Research and Innovation. https://doi.org/10.2777/308407

[12] Xu, X., Lu, Y., Vogel-Heuser, B., & Wang, L. (2021). Industry 4.0 and Industry 5.0 — Inception, conception and perception. *Journal of Manufacturing Systems, 61*, 530–535. https://doi.org/10.1016/j.jmsy.2021.10.006

[13] Nahavandi, S. (2019). Industry 5.0 — A human-centric solution. *Sustainability, 11*(16), 4371. https://doi.org/10.3390/su11164371

[14] Brennen, J. S., & Kreiss, D. (2016). Digitalization. In *The international encyclopedia of communication theory and philosophy*. Wiley. https://doi.org/10.1002/9781118766804.wbiect111

[15] Verhoef, P. C., Broekhuizen, T., Bart, Y., Bhattacharya, A., Dong, J. Q., Fabian, N., & Haenlein, M. (2021). Digital transformation: A multidisciplinary reflection and research agenda. *Journal of Business Research, 122*, 889–901. https://doi.org/10.1016/j.jbusres.2019.09.022

[16] Vial, G. (2019). Understanding digital transformation: A review and a research agenda. *The Journal of Strategic Information Systems, 28*(2), 118–144. https://doi.org/10.1016/j.jsis.2019.01.003

[17] Frank, A. G., Dalenogare, L. S., & Ayala, N. F. (2019). Industry 4.0 technologies: Implementation patterns in manufacturing companies. *International Journal of Production Economics, 210*, 15–26. https://doi.org/10.1016/j.ijpe.2019.01.004

[18] Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks, 54*(15), 2787–2805. https://doi.org/10.1016/j.comnet.2010.05.010

[19] International Telecommunication Union. (2012). *Overview of the Internet of things* (Recommendation ITU-T Y.2060). https://www.itu.int/rec/T-REC-Y.2060-201206-I

[20] International Organization for Standardization & International Electrotechnical Commission. (2021). *Internet of Things (IoT) — Vocabulary* (ISO/IEC 20924:2021). https://www.iso.org/standard/82771.html

[21] Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems, 29*(7), 1645–1660. https://doi.org/10.1016/j.future.2013.01.010

[22] Sisinni, E., Saifullah, A., Han, S., Jennehag, U., & Gidlund, M. (2018). Industrial Internet of Things: Challenges, opportunities, and directions. *IEEE Transactions on Industrial Informatics, 14*(11), 4724–4734. https://doi.org/10.1109/TII.2018.2852491

[23] Boyes, H., Hallaq, B., Cunningham, J., & Watson, T. (2018). The industrial internet of things (IIoT): An analysis framework. *Computers in Industry, 101*, 1–12. https://doi.org/10.1016/j.compind.2018.04.015

[24] International Electrotechnical Commission. (2019). *Industrial communication networks — Profiles — Part 2: Additional fieldbus profiles for real-time networks based on ISO/IEC/IEEE 8802-3* (IEC 61784-2:2019, ed. 4.0). https://webstore.iec.ch/en/publication/59888

[25] Stouffer, K., Pease, M., Tang, C., Zimmerman, T., Pillitteri, V., Lightman, S., Hahn, A., Saravia, S., Sherule, A., & Thompson, M. (2023). *Guide to operational technology (OT) security* (NIST Special Publication 800-82, Revision 3). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-82r3

[26] Wollschlaeger, M., Sauter, T., & Jasperneite, J. (2017). The future of industrial communication: Automation networks in the era of the Internet of Things and Industry 4.0. *IEEE Industrial Electronics Magazine, 11*(1), 17–27. https://doi.org/10.1109/MIE.2017.2649104

[27] Industrial Internet Consortium. (2019). *The Industrial Internet of Things Volume G1: Reference architecture* (version 1.9).

[28] Kang, H. S., Lee, J. Y., Choi, S., Kim, H., Park, J. H., Son, J. Y., Kim, B. H., & Noh, S. D. (2016). Smart manufacturing: Past research, present findings, and future directions. *International Journal of Precision Engineering and Manufacturing-Green Technology, 3*(1), 111–128. https://doi.org/10.1007/s40684-016-0015-5

[29] Kusiak, A. (2018). Smart manufacturing. *International Journal of Production Research, 56*(1–2), 508–517. https://doi.org/10.1080/00207543.2017.1351644

[30] Lu, Y., Morris, K. C., & Frechette, S. (2016). *Current standards landscape for smart manufacturing systems* (NISTIR 8107). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8107

[31] Zhong, R. Y., Xu, X., Klotz, E., & Newman, S. T. (2017). Intelligent manufacturing in the context of Industry 4.0: A review. *Engineering, 3*(5), 616–630. https://doi.org/10.1016/j.eng.2017.05.015

[32] Tao, F., Qi, Q., Liu, A., & Kusiak, A. (2018). Data-driven smart manufacturing. *Journal of Manufacturing Systems, 48*, 157–169. https://doi.org/10.1016/j.jmsy.2018.01.006

[33] Redman, T. C. (1998). The impact of poor data quality on the typical enterprise. *Communications of the ACM, 41*(2), 79–82. https://doi.org/10.1145/269012.269025

[34] International Electrotechnical Commission. (2020). *OPC Unified Architecture — Part 4: Services* (IEC 62541-4:2020).

[35] Institute of Electrical and Electronics Engineers. (2020). *IEEE standard for a precision clock synchronization protocol for networked measurement and control systems* (IEEE Std 1588-2019). https://doi.org/10.1109/IEEESTD.2020.9120376

[36] Joint Committee for Guides in Metrology. (2008). *Evaluation of measurement data — Guide to the expression of uncertainty in measurement* (JCGM 100:2008). BIPM. https://www.bipm.org/en/committees/jc/jcgm/publications

[37] Wang, R. Y., & Strong, D. M. (1996). Beyond accuracy: What data quality means to data consumers. *Journal of Management Information Systems, 12*(4), 5–33. https://doi.org/10.1080/07421222.1996.11518099

[38] International Organization for Standardization. (2015). *Data quality — Part 8: Information and data quality: Concepts and measuring* (ISO 8000-8:2015).

[39] Ackoff, R. L. (1989). From data to wisdom. *Journal of Applied Systems Analysis, 16*, 3–9.

[40] Rowley, J. (2007). The wisdom hierarchy: Representations of the DIKW hierarchy. *Journal of Information Science, 33*(2), 163–180. https://doi.org/10.1177/0165551506070706

[41] International Organization for Standardization. (2016). *Mechanical vibration — Measurement and evaluation of machine vibration — Part 1: General guidelines* (ISO 20816-1:2016). https://www.iso.org/standard/63180.html

[42] International Organization for Standardization. (2003). *Condition monitoring and diagnostics of machines — Data processing, communication and presentation — Part 1: General guidelines* (ISO 13374-1:2003). https://www.iso.org/standard/21832.html

[43] International Organization for Standardization. (2018). *Condition monitoring and diagnostics of machines — General guidelines* (ISO 17359:2018). https://www.iso.org/standard/71194.html

[44] International Electrotechnical Commission. (2010). *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 1: General requirements* (IEC 61508-1:2010, ed. 2.0). https://webstore.iec.ch/en/publication/5515

[45] International Organization for Standardization. (2023). *Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design* (ISO 13849-1:2023). https://www.iso.org/standard/73481.html

[46] International Society of Automation. (2016). *Management of alarm systems for the process industries* (ANSI/ISA-18.2-2016). https://www.isa.org/products/ansi-isa-18-2-2016-management-of-alarm-systems-fo

[47] Hollifield, B., Oliver, D., Nimmo, I., & Habibi, E. (2008). *The high performance HMI handbook*. PAS.

[48] Porter, M. E. (1985). *Competitive advantage: Creating and sustaining superior performance*. Free Press.

[49] International Electrotechnical Commission. (2013). *Enterprise-control system integration — Part 1: Models and terminology* (IEC 62264-1:2013).

[50] International Organization for Standardization. (2014). *Automation systems and integration — Key performance indicators (KPIs) for manufacturing operations management — Part 1: Overview, concepts and terminology* (ISO 22400-1:2014).

[51] International Organization for Standardization. (2014). *Automation systems and integration — Key performance indicators (KPIs) for manufacturing operations management — Part 2: Definitions and descriptions* (ISO 22400-2:2014).

[52] GS1. (2026). *GS1 General Specifications* (Release 26.0). https://www.gs1.org/standards/barcodes-epcrfid-id-keys/gs1-general-specifications

[53] International Organization for Standardization & International Electrotechnical Commission. (2017). *Information technology — Cloud computing — Interoperability and portability* (ISO/IEC 19941:2017). https://www.iso.org/standard/66639.html

[54] Khatri, V., & Brown, C. V. (2010). Designing data governance. *Communications of the ACM, 53*(1), 148–152. https://doi.org/10.1145/1629175.1629210

[55] DAMA International. (2017). *DAMA-DMBOK: Data management body of knowledge* (2nd ed.). Technics Publications.

[56] Parlamentul European & Consiliul Uniunii Europene. (2016). *Regulamentul (UE) 2016/679 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date*. Jurnalul Oficial al Uniunii Europene, L 119, 1–88. https://eur-lex.europa.eu/eli/reg/2016/679/oj

[57] International Organization for Standardization. (2016). *Information and documentation — Records management — Part 1: Concepts and principles* (ISO 15489-1:2016). https://www.iso.org/standard/62542.html

[58] Müller, J. M., Kiel, D., & Voigt, K.-I. (2018). What drives the implementation of Industry 4.0? The role of opportunities and challenges in the context of sustainability. *Sustainability, 10*(1), 247. https://doi.org/10.3390/su10010247

[59] Mobley, R. K. (2002). *An introduction to predictive maintenance* (2nd ed.). Butterworth-Heinemann.

[60] Jardine, A. K. S., Lin, D., & Banjevic, D. (2006). A review on machinery diagnostics and prognostics implementing condition-based maintenance. *Mechanical Systems and Signal Processing, 20*(7), 1483–1510. https://doi.org/10.1016/j.ymssp.2005.09.012

[61] Lee, J., Kao, H.-A., & Yang, S. (2014). Service innovation and smart analytics for Industry 4.0 and big data environment. *Procedia CIRP, 16*, 3–8. https://doi.org/10.1016/j.procir.2014.02.001

[62] International Organization for Standardization. (2015). *Condition monitoring and diagnostics of machines — Prognostics — Part 1: General guidelines* (ISO 13381-1:2015). https://www.iso.org/standard/51436.html

[63] International Organization for Standardization. (2018). *Energy management systems — Requirements with guidance for use* (ISO 50001:2018). https://www.iso.org/standard/69426.html

[64] International Organization for Standardization. (2023). *Energy management systems — Evaluating energy performance using energy performance indicators and energy baselines* (ISO 50006:2023, ed. 2.0). https://www.iso.org/standard/81622.html

[65] Nakajima, S. (1988). *Introduction to TPM: Total productive maintenance*. Productivity Press.

[66] International Electrotechnical Commission. (2025). *OPC Unified Architecture — Part 3: Address space model* (IEC 62541-3:2025, ed. 4.0).

[67] International Electrotechnical Commission. (2016). *Electromagnetic compatibility (EMC) — Part 6-2: Generic standards — Immunity standard for industrial environments* (IEC 61000-6-2:2016, ed. 3.0). https://webstore.iec.ch/en/publication/25628

[68] International Electrotechnical Commission. (2013). *Industrial communication networks — Network and system security — Part 3-3: System security requirements and security levels* (IEC 62443-3-3:2013). https://webstore.iec.ch/en/publication/7033

[69] Parlamentul European & Consiliul Uniunii Europene. (2024). *Regulamentul (UE) 2024/2847 privind cerințele orizontale de securitate cibernetică pentru produsele cu elemente digitale*. Jurnalul Oficial al Uniunii Europene. https://eur-lex.europa.eu/eli/reg/2024/2847/oj

[70] Horváth, D., & Szabó, R. Z. (2019). *Driving forces and barriers of Industry 4.0: Do multinational and small and medium-sized companies have equal opportunities? Technological Forecasting and Social Change, 146, 119–132*. https://doi.org/10.1016/j.techfore.2019.05.021

[71] Kamble, S. S., Gunasekaran, A., & Sharma, R. (2018). Analysis of the driving and dependence power of barriers to adopt Industry 4.0 in Indian manufacturing industry. *Computers in Industry, 101*, 107–119. https://doi.org/10.1016/j.compind.2018.06.004

[72] Blank, L., & Tarquin, A. (2018). *Engineering economy* (8th ed.). McGraw-Hill Education.

[73] International Electrotechnical Commission. (2017). *Dependability management — Part 3-3: Application guide — Life cycle costing* (IEC 60300-3-3:2017). https://webstore.iec.ch/publication/28536

[74] Galbraith, J. R. (1974). Organization design: An information processing view. *Interfaces, 4*(3), 28–36.

[75] International Society of Automation. (2025). *Enterprise-control system integration — Part 1: Models and terminology* (ANSI/ISA-95.00.01-2025, IEC 62264-1 Mod). https://www.isa.org/products/ansi-isa-95-00-01-2025-iec-62264-1-mod-enterprise

[76] Hopp, W. J., & Spearman, M. L. (2011). *Factory physics* (3rd ed.). Waveland Press.

[77] Mintzberg, H. (1979). *The structuring of organizations: A synthesis of the research*. Prentice-Hall.

[78] Jacobs, F. R., Berry, W. L., Whybark, D. C., & Vollmann, T. E. (2018). *Manufacturing planning and control for supply chain management* (2nd ed.). McGraw-Hill Education.

[79] Chopra, S., & Meindl, P. (2016). *Supply chain management: Strategy, planning, and operation* (6th ed.). Pearson.

[80] International Organization for Standardization. (2015). *Quality management systems — Requirements* (ISO 9001:2015). https://www.iso.org/standard/62085.html

[81] Tompkins, J. A., White, J. A., Bozer, Y. A., & Tanchoco, J. M. A. (2010). *Facilities planning* (4th ed.). John Wiley & Sons.

[82] Muther, R. (1973). *Systematic layout planning* (2nd ed.). Cahners Books.

[83] Rother, M., & Shook, J. (2003). *Learning to see: Value stream mapping to create value and eliminate muda* (Version 1.4). Lean Enterprise Institute.

[84] GS1. (2022). *EPC Information Services (EPCIS) Standard* (Release 2.0). https://ref.gs1.org/standards/epcis/

[85] International Electrotechnical Commission. (2020). *Security for industrial automation and control systems — Part 3-2: Security risk assessment for system design* (IEC 62443-3-2:2020). https://webstore.iec.ch/en/publication/30727

[86] International Electrotechnical Commission. (2013). *Degrees of protection provided by enclosures (IP code)* (IEC 60529:1989+AMD1:1999+AMD2:2013 CSV). https://webstore.iec.ch/en/publication/2452

[87] International Electrotechnical Commission. (2016). *Enterprise-control system integration — Part 3: Activity models of manufacturing operations management* (IEC 62264-3:2016, ed. 2.0).

[88] Olhager, J. (2003). Strategic positioning of the order penetration point. *International Journal of Production Economics, 85*(3), 319–329. https://doi.org/10.1016/S0925-5273(03)00119-1

[89] Little, J. D. C. (1961). A proof for the queuing formula: L = λW. *Operations Research, 9*(3), 383–387. https://doi.org/10.1287/opre.9.3.383

[90] Lee, H. L., Padmanabhan, V., & Whang, S. (1997). Information distortion in a supply chain: The bullwhip effect. *Management Science, 43*(4), 546–558. https://doi.org/10.1287/mnsc.43.4.546

[91] International Electrotechnical Commission. (2023). *Security for industrial automation and control systems — Part 2-4: Security program requirements for IACS service providers* (IEC 62443-2-4:2023).

[92] Parlamentul European & Consiliul Uniunii Europene. (2024). *Regulamentul (UE) 2024/1781 de instituire a unui cadru pentru stabilirea cerințelor în materie de proiectare ecologică pentru produsele durabile*. Jurnalul Oficial al Uniunii Europene, L 2024/1781. https://eur-lex.europa.eu/eli/reg/2024/1781/oj

[93] Comisia Europeană. (2025). *Ecodesign for Sustainable Products and Energy Labelling Working Plan 2025–2030*. https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1071

[94] Hayes, R. H., & Wheelwright, S. C. (1979). Link manufacturing process and product life cycles. *Harvard Business Review, 57*(1), 133–140.

[95] International Electrotechnical Commission. (2026). *Batch control — Part 1: Models and terminology* (IEC 61512-1:2026, ed. 2.0). https://webstore.iec.ch/en/publication/75287

[96] Shingo, S. (1985). *A revolution in manufacturing: The SMED system*. Productivity Press.

[97] Seborg, D. E., Edgar, T. F., Mellichamp, D. A., & Doyle, F. J. (2016). *Process dynamics and control* (4th ed.). Wiley.

[98] Womack, J. P., Jones, D. T., & Roos, D. (1990). *The machine that changed the world*. Rawson Associates.

[99] Sugimori, Y., Kusunoki, K., Cho, F., & Uchikawa, S. (1977). Toyota production system and Kanban system: Materialization of just-in-time and respect-for-human system. *International Journal of Production Research, 15*(6), 553–564.

[100] Ohno, T. (1988). *Toyota production system: Beyond large-scale production*. Productivity Press.

[101] Womack, J. P., & Jones, D. T. (1996). *Lean thinking: Banish waste and create wealth in your corporation*. Simon & Schuster.

[102] Liker, J. K. (2004). *The Toyota way: 14 management principles from the world's greatest manufacturer*. McGraw-Hill.

[103] Rother, M., & Shook, J. (1999). *Learning to see: Value stream mapping to add value and eliminate muda*. Lean Enterprise Institute.

[104] Nagel, R. N., & Dove, R. (1991). *21st century manufacturing enterprise strategy: An industry-led view*. Iacocca Institute, Lehigh University.

[105] Gunasekaran, A. (1999). Agile manufacturing: A framework for research and development. *International Journal of Production Economics, 62*(1–2), 87–105.

[106] Koren, Y., Heisel, U., Jovane, F., Moriwaki, T., Pritschow, G., Ulsoy, G., & Van Brussel, H. (1999). Reconfigurable manufacturing systems. *CIRP Annals, 48*(2), 527–540. https://doi.org/10.1016/S0007-8506(07)63232-6

[107] Tao, F., Zhang, H., Liu, A., & Nee, A. Y. C. (2019). Digital twin in industry: State-of-the-art. *IEEE Transactions on Industrial Informatics, 15*(4), 2405–2415. https://doi.org/10.1109/TII.2018.2873186

[108] Pine, B. J. (1993). *Mass customization: The new frontier in business competition*. Harvard Business School Press.

[109] Salvador, F., de Holan, P. M., & Piller, F. (2009). Cracking the code of mass customization. *MIT Sloan Management Review, 50*(3), 71–78.

[110] Eclipse Sparkplug Contributors. (2022). *Sparkplug specification 3.0.0*. https://sparkplug.eclipse.org/specification/version/3.0/documents/sparkplug-specification-3.0.0.pdf

[111] Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L. (2016). Edge computing: Vision and challenges. *IEEE Internet of Things Journal, 3*(5), 637–646. https://doi.org/10.1109/JIOT.2016.2579198

[112] ElMaraghy, H. A. (2005). Flexible and reconfigurable manufacturing systems paradigms. *International Journal of Flexible Manufacturing Systems, 17*(4), 261–276. https://doi.org/10.1007/s10696-006-9028-7

[113] Mehrabi, M. G., Ulsoy, A. G., & Koren, Y. (2000). Reconfigurable manufacturing systems: Key to future manufacturing. *Journal of Intelligent Manufacturing, 11*(4), 403–419. https://doi.org/10.1023/A:1008930403506

[114] Bi, Z. M., Lang, S. Y. T., Shen, W., & Wang, L. (2008). Reconfigurable manufacturing systems: The state of the art. *International Journal of Production Research, 46*(4), 967–992. https://doi.org/10.1080/00207540600905646

[115] Koren, Y., Gu, X., & Guo, W. (2018). Reconfigurable manufacturing systems: Principles, design, and future trends. *Frontiers of Mechanical Engineering, 13*(2), 121–136. https://doi.org/10.1007/s11465-018-0483-0

[116] Koren, Y., & Shpitalni, M. (2010). Design of reconfigurable manufacturing systems. *Journal of Manufacturing Systems, 29*(4), 130–141. https://doi.org/10.1016/j.jmsy.2011.01.001

[117] Browne, J., Dubois, D., Rathmill, K., Sethi, S. P., & Stecke, K. E. (1984). Classification of flexible manufacturing systems. *The FMS Magazine, 2*(2), 114–117.

[118] Terwiesch, C., & Bohn, R. E. (2001). Learning and process improvement during production ramp-up. *International Journal of Production Economics, 70*(1), 1–19. https://doi.org/10.1016/S0925-5273(00)00045-1

[119] Wiendahl, H.-P., ElMaraghy, H. A., Nyhuis, P., Zäh, M. F., Wiendahl, H.-H., Duffie, N., & Brieke, M. (2007). Changeable manufacturing — Classification, design

and operation. *CIRP Annals, 56*(2), 783–809. https://doi.org/10.1016/j.cirp.2007.10.003

[120] International Electrotechnical Commission. (2023). *Asset Administration Shell for industrial applications — Part 1: Asset Administration Shell structure* (IEC 63278-1:2023, ed. 1.0).

[121] Sethi, A. K., & Sethi, S. P. (1990). Flexibility in manufacturing: A survey. *International Journal of Flexible Manufacturing Systems, 2*(4), 289–328. https://doi.org/10.1007/BF00186471

[122] Ulrich, K. T. (1995). The role of product architecture in the manufacturing firm. *Research Policy, 24*(3), 419–440. https://doi.org/10.1016/0048-7333(94)00775-3

[123] International Electrotechnical Commission. (2025). *Programmable controllers — Part 3: Programming languages* (IEC 61131-3:2025, ed. 4.0). https://webstore.iec.ch/en/publication/68533

[124] International Electrotechnical Commission. (2012). *Function blocks — Part 1: Architecture* (IEC 61499-1:2012, ed. 2.0).

[125] Arai, T., Aiyama, Y., Maeda, Y., Sugi, M., & Ota, J. (2000). Agile assembly system by “plug and produce”. *CIRP Annals, 49*(1), 1–4. https://doi.org/10.1016/S0007-8506(07)62883-2

[126] Chen, D., Doumeingts, G., & Vernadat, F. (2008). Architectures for enterprise integration and interoperability: Past, present and future. *Computers in Industry, 59*(7), 647–659. https://doi.org/10.1016/j.compind.2007.12.016

[127] OPC Foundation. (2025). *OPC Unified Architecture — Part 1: Overview and concepts* (OPC 10000-1, Release 1.05.06). https://reference.opcfoundation.org/Core/Part1/v105/docs/

[128] International Organization for Standardization. (2025). *Robotics — Safety requirements — Part 2: Industrial robot applications and robot cells* (ISO 10218-2:2025). https://www.iso.org/standard/73934.html

[129] Lipták, B. G. (Ed.). (2003). *Instrument engineers’ handbook, Volume 1: Process measurement and analysis* (4th ed.). CRC Press.

[130] International Electrotechnical Commission. (1982). *Analogue signals for process control systems — Part 1: Direct current signals* (IEC 60381-1:1982, ed. 2.0). https://webstore.iec.ch/en/publication/1948

[131] NAMUR. (2021). *NE 43: Standardization of the signal level for the failure information of digital transmitters* (Ed. 2021-07-26). https://www.namur.net/

[132] International Electrotechnical Commission. (2022). *Programmable controllers — Part 9: Single-drop digital communication interface for small sensors and actuators (SDCI)* (IEC 61131-9:2022, ed. 2.0). https://webstore.iec.ch/en/publication/68534

[133] Joint Committee for Guides in Metrology. (2012). *International vocabulary of metrology — Basic and general concepts and associated terms (VIM)* (JCGM 200:2012, 3rd ed.). BIPM. https://doi.org/10.59161/JCGM200-2012

[134] Wilson, J. S. (Ed.). (2005). *Sensor technology handbook*. Newnes/Elsevier.

[135] International Electrotechnical Commission. (2022). *Industrial platinum resistance thermometers and platinum temperature sensors* (IEC 60751:2022, ed. 3.0). https://webstore.iec.ch/en/publication/63753

[136] Fraden, J. (2016). *Handbook of modern sensors: Physics, designs, and applications* (5th ed.). Springer. https://doi.org/10.1007/978-3-319-19303-8

[137] International Electrotechnical Commission. (2019). *Low-voltage switchgear and controlgear — Part 5-2: Control circuit devices and switching elements — Proximity switches* (IEC 60947-5-2:2019, ed. 4.0). https://webstore.iec.ch/en/publication/32517

[138] International Electrotechnical Commission. (2005). *Industrial-process control valves — Part 1: Control valve terminology and general considerations* (IEC 60534-1:2005, ed. 3.0). https://webstore.iec.ch/en/publication/2459

[139] International Electrotechnical Commission. (2016). *Safety of machinery — Electrical equipment of machines — Part 1: General requirements* (IEC 60204-1:2016, ed. 6.0). https://webstore.iec.ch/en/publication/26037

[140] International Organization for Standardization. (2010). *Hydraulic fluid power — General rules and safety requirements for systems and their components* (ISO 4413:2010). https://www.iso.org/standard/44796.html

[141] International Organization for Standardization. (2010). *Pneumatic fluid power — General rules and safety requirements for systems and their components* (ISO 4414:2010). https://www.iso.org/standard/44790.html

[142] International Electrotechnical Commission. (2021). *Safety of machinery — Functional safety of safety-related control systems* (IEC 62061:2021, ed. 2.0). https://webstore.iec.ch/en/publication/59927

[143] International Electrotechnical Commission. (2011). *Industrial-process control valves — Part 2-1: Flow capacity — Sizing equations for fluid flow under installed conditions* (IEC 60534-2-1:2011, ed. 2.0). https://webstore.iec.ch/en/publication/2461

[144] Lipták, B. G. (Ed.). (2005). *Instrument engineers' handbook, Volume 2: Process control and optimization* (4th ed.). CRC Press.

[145] Siciliano, B., Sciavicco, L., Villani, L., & Oriolo, G. (2009). *Robotics: Modelling, planning and control*. Springer. https://doi.org/10.1007/978-1-84628-642-1

[146] International Electrotechnical Commission. (2016). *Adjustable speed electrical power drive systems — Part 5-2: Safety requirements — Functional* (IEC 61800-5-2:2016, ed. 2.0). https://webstore.iec.ch/en/publication/24556

[147] International Organization for Standardization. (2018). *Pneumatic fluid power — Cylinders with detachable mountings, 1 000 kPa (10 bar) series, bores from 32 mm to 320 mm — Basic, mounting and accessories dimensions* (ISO 15552:2018). https://www.iso.org/standard/66921.html

[148] Beater, P. (2007). *Pneumatic drives: System design, modelling and control*. Springer. https://doi.org/10.1007/978-3-540-69471-7

[149] International Organization for Standardization. (2021). *Robotics — Vocabulary* (ISO 8373:2021). https://www.iso.org/standard/75539.html

[150] International Organization for Standardization. (2025). *Robotics — Safety requirements — Part 1: Industrial robots* (ISO 10218-1:2025, ed. 3.0). https://www.iso.org/standard/73933.html

[151] International Electrotechnical Commission. (2003). *Programmable controllers — Part 1: General information* (IEC 61131-1:2003, ed. 2.0). https://webstore.iec.ch/en/publication/4550

[152] International Electrotechnical Commission. (2017). *Programmable controllers — Part 2: Equipment requirements and tests* (IEC 61131-2:2017, ed. 4.0). https://webstore.iec.ch/en/publication/29154

[153] Galloway, B., & Hancke, G. P. (2013). Introduction to industrial control networks. *IEEE Communications Surveys & Tutorials, 15*(2), 860–880. https://doi.org/10.1109/SURV.2012.071812.00124

[154] International Electrotechnical Commission. (2016). *Functional safety — Safety instrumented systems for the process industry sector — Part 1: Framework, definitions, system, hardware and application programming requirements* (IEC 61511-1:2016, ed. 2.0). https://webstore.iec.ch/en/publication/24241

[155] Modbus Organization. (2012). *MODBUS application protocol specification* (V1.1b3). https://www.modbus.org/docs/Modbus_Application_Protocol_V1_1b3.pdf

[156] International Electrotechnical Commission. (2019). *Security for industrial automation and control systems — Part 4-2: Technical security requirements for IACS components* (IEC 62443-4-2:2019). https://webstore.iec.ch/en/publication/34421

[157] Mills, D., Martin, J. (Ed.), Burbank, J., & Kasch, W. (2010). *Network Time Protocol version 4: Protocol and algorithms specification* (RFC 5905). Internet Engineering Task Force. https://doi.org/10.17487/RFC5905

[158] Bonomi, F., Milito, R., Zhu, J., & Addepalli, S. (2012). Fog computing and its role in the Internet of Things. In *Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing* (pp. 13–16). ACM. https://doi.org/10.1145/2342509.2342513

[159] Mell, P., & Grance, T. (2011). *The NIST definition of cloud computing* (NIST Special Publication 800-145). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-145

[160] Endsley, M. R. (1995). Toward a theory of situation awareness in dynamic systems. *Human Factors, 37*(1), 32–64. https://doi.org/10.1518/001872095779049543

[161] Bailey, D., & Wright, E. (2003). *Practical SCADA for industry*. Newnes/Elsevier.

[162] International Society of Automation. (2015). *Human machine interfaces for process automation systems* (ANSI/ISA-101.01-2015). https://www.isa.org/products/ansi-isa-101-01-2015-human-machine-interfaces-for

[163] International Electrotechnical Commission. (2002). *Basic and safety principles for man-machine interface, marking and identification — Coding principles for indicators and actuators* (IEC 60073:2002, ed. 5.0). https://webstore.iec.ch/en/publication/1055

[164] Siemens. (2024). *SIMATIC S7-1200 programmable controller: System manual, ediția 11/2024. Secțiunile „SM 1231 analog input module specifications” și „Sample time and update times for the analog inputs”, din capitolul „Analog signal modules (SMs)”. Documentație tehnică online Siemens.*

[165] International Organization for Standardization. (2024). *Road vehicles — Controller area network (CAN) — Part 1: Data link layer and physical coding sublayer* (ISO 11898-1:2024, ed. 3). https://www.iso.org/standard/86384.html

[166] CAN in Automation. (2011). *CiA 301: CANopen application layer and communication profile* (Version 4.2.0). https://www.can-cia.org/

[167] Modbus Organization. (2006). *MODBUS messaging on TCP/IP implementation guide* (V1.0b). https://modbus.org/docs/Modbus_Messaging_Implementation_Guide_V1_0b.pdf

[168] Modbus Organization. (2021). *MODBUS/TCP security protocol specification* (V36). https://modbus.org/docs/MB-TCP-Security-v36_2021-07-30.pdf

[169] PROFIBUS & PROFINET International. (2018). *PROFINET system description: Technology and application*. https://www.profibus.com/

[170] ODVA. (2026). *Specifications: The CIP Networks Library*. https://www.odva.org/subscriptions-services/specifications/

[171] EtherCAT Technology Group. (f.a.). *ETG.1000: EtherCAT specification*. Consultat la 12 august 2026, de la https://www.ethercat.org/en/downloads/

[172] OPC Foundation. (f.a.). *OPC Classic*. Consultat la 12 august 2026, de la https://opcfoundation.org/about/opc-technologies/opc-classic/

[173] OPC Foundation. (2025). *OPC Unified Architecture — Part 3: Address space model* (OPC 10000-3). https://reference.opcfoundation.org/Core/Part3/

[174] OPC Foundation. (2026). *OPC Unified Architecture — Part 4: Services* (OPC 10000-4, Release 1.05.07). https://reference.opcfoundation.org/specs/OPC-10000-4

[175] OPC Foundation. (2025). *OPC Unified Architecture — Part 2: Security model* (OPC 10000-2). https://reference.opcfoundation.org/Core/Part2/

[176] OPC Foundation. (2025). *OPC Unified Architecture — Part 14: PubSub* (OPC 10000-14). https://reference.opcfoundation.org/Core/Part14/

[177] OASIS Open. (2019). *MQTT version 5.0* (A. Banks, E. Briggs, K. Borgendale, & R. Gupta, Eds.). OASIS Standard. https://docs.oasis-open.org/mqtt/mqtt/v5.0/os/mqtt-v5.0-os.html

[178] Shelby, Z., Hartke, K., & Bormann, C. (2014). *The Constrained Application Protocol (CoAP)* (RFC 7252). RFC Editor. https://doi.org/10.17487/RFC7252

[179] Bormann, C., & Shelby, Z. (Ed.). (2016). *Block-wise transfers in the Constrained Application Protocol (CoAP)* (RFC 7959). RFC Editor. https://doi.org/10.17487/RFC7959

[180] Bormann, C., Lemay, S., Tschofenig, H., Hartke, K., Silverajan, B., & Raymor, B. (Ed.). (2018). *CoAP (Constrained Application Protocol) over TCP, TLS, and WebSockets* (RFC 8323). RFC Editor. https://doi.org/10.17487/RFC8323

[181] Fielding, R., Nottingham, M., & Reschke, J. (Eds.). (2022). *HTTP semantics* (RFC 9110). Internet Engineering Task Force. https://doi.org/10.17487/RFC9110

[182] OASIS Open. (2012). *OASIS Advanced Message Queuing Protocol (AMQP) version 1.0* (OASIS Standard). https://docs.oasis-open.org/amqp/core/v1.0/amqp-core-complete-v1.0.pdf

[183] LoRa Alliance. (2020). *TS001-1.0.4: LoRaWAN L2 1.0.4 specification*. https://lora-alliance.org/resource_hub/ts001-1-0-4-lorawan-l2-1-0-4-specification/

[184] OPC Foundation. (2025). *OPC Unified Architecture — Part 6: Mappings* (OPC 10000-6). https://reference.opcfoundation.org/Core/Part6/

[185] International Organization for Standardization & International Electrotechnical Commission. (1994). *Information technology — Open Systems Interconnection — Basic reference model: The basic model* (ISO/IEC 7498-1:1994).

[186] Eddy, W. (Ed.). (2022). *Transmission Control Protocol (TCP)* (RFC 9293). RFC Editor. https://doi.org/10.17487/RFC9293

[187] Postel, J. (1980). *User Datagram Protocol* (RFC 768). RFC Editor. https://doi.org/10.17487/RFC0768

[188] Bray, T. (Ed.). (2017). *The JavaScript Object Notation (JSON) data interchange format* (RFC 8259). RFC Editor. https://doi.org/10.17487/RFC8259

[189] Rescorla, E. (2026). *The Transport Layer Security (TLS) protocol version 1.3* (RFC 9846). Internet Engineering Task Force. https://doi.org/10.17487/RFC9846

[190] Postel, J. (1981). *Internet Protocol* (RFC 791). RFC Editor. https://doi.org/10.17487/RFC0791

[191] Institute of Electrical and Electronics Engineers. (2022). *IEEE standard for Ethernet* (IEEE Std 802.3-2022). https://standards.ieee.org/ieee/802.3/10422/

[192] Williams, T. J. (1994). The Purdue enterprise reference architecture. *Computers in Industry, 24*(2–3), 141–158. https://doi.org/10.1016/0166-3615(94)90017-5

[193] International Organization for Standardization & International Electrotechnical Commission. (2024). *Internet of Things (IoT) — Reference architecture* (ISO/IEC 30141:2024, ed. 2.0). https://www.iso.org/standard/88800.html

[194] International Electrotechnical Commission. (2016). *Enterprise-control system integration — Part 5: Business to manufacturing transactions* (IEC 62264-5:2016).

[195] Kopetz, H., & Steiner, W. (2022). *Real-time systems: Design principles for distributed embedded applications* (3rd ed.). Springer. https://doi.org/10.1007/978-3-031-11992-7

[196] Felser, M. (2005). Real-time Ethernet — industry prospective. *Proceedings of the IEEE, 93*(6), 1118–1129. https://doi.org/10.1109/JPROC.2005.849720

[197] International Electrotechnical Commission & Institute of Electrical and Electronics Engineers. (2026). *Time-sensitive networking profile for industrial automation* (IEC/IEEE 60802:2026).

[198] Parlamentul European & Consiliul Uniunii Europene. (2002). *Regulamentul (CE) nr. 178/2002 de stabilire a principiilor și a cerințelor generale ale legislației alimentare, de instituire a Autorității Europene pentru Siguranța Alimentară și de stabilire a procedurilor în domeniul siguranței produselor alimentare*. Jurnalul Oficial al Uniunii Europene, L 31, 1–24. https://eur-lex.europa.eu/eli/reg/2002/178/oj

[199] Iorga, M., Feldman, L., Barton, R., Martin, M. J., Goren, N., & Mahmoudi, C. (2018). *Fog computing conceptual model* (NIST Special Publication 500-325). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.500-325

[200] Kritzinger, W., Karner, M., Traar, G., Henjes, J., & Sihn, W. (2018). Digital twin in manufacturing: A categorical literature review and classification. *IFAC-PapersOnLine, 51*(11), 1016–1022. https://doi.org/10.1016/j.ifacol.2018.08.474

[201] Malik, A. A., Shao, G., & Tarakhovsky, J. (2024). Digital twins for robot systems in manufacturing. În M. Grieves & E. Y. Hua (Ed.), *Digital twins, simulation, and the metaverse*. Springer. https://doi.org/10.1007/978-3-031-69107-2_13

[202] Veneri, G., & Capasso, A. (2018). *Hands-on Industrial Internet of Things: Create a powerful Industrial IoT infrastructure using Industry 4.0*. Packt Publishing.

[203] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., & Polk, W. (2008). *Internet X.509 public key infrastructure certificate and certificate revocation list (CRL) profile* (RFC 5280). Internet Engineering Task Force. https://doi.org/10.17487/RFC5280

[204] Amazon Web Services. (f.a.). *How AWS IoT works*. AWS IoT Core Developer Guide. Consultat la 17 august 2026, de la https://docs.aws.amazon.com/iot/latest/developerguide/aws-iot-how-it-works.html

[205] International Electrotechnical Commission. (2024). *Security for industrial automation and control systems — Part 2-1: Security program requirements for IACS asset owners* (IEC 62443-2-1:2024, ed. 2.0).

[206] International Organization for Standardization & International Electrotechnical Commission. (2023). *Information technology — Sparkplug® version 3.0* (ISO/IEC 20237:2023). https://www.iso.org/standard/86204.html

[207] Amazon Web Services. (f.a.). *AWS IoT rule actions*. AWS IoT Core Developer Guide. Consultat la 17 august 2026, de la https://docs.aws.amazon.com/iot/latest/developerguide/iot-rule-actions.html

[208] Microsoft. (f.a.). *Big data architectures*. Azure Architecture Center. Consultat la 17 august 2026, de la https://learn.microsoft.com/en-us/azure/architecture/databases/guide/big-data-architectures

[209] Amazon Web Services. (f.a.). *Core components of Amazon DynamoDB*. Amazon DynamoDB Developer Guide. Consultat la 17 august 2026, de la https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/HowItWorks.CoreComponents.html

[210] Siemens. (f.a.). *Insights Hub industrial IoT*. Siemens Digital Industries Software. Consultat la 17 august 2026, de la https://www.siemens.com/en-us/products/insights-hub/

[211] AVEVA. (f.a.). *CONNECT: The industrial intelligence platform*. Consultat la 17 august 2026, de la https://connect.aveva.com/

[212] PTC. (f.a.). *ThingWorx: Industrial IoT software*. Consultat la 17 august 2026, de la https://www.ptc.com/en/products/thingworx

[213] International Electrotechnical Commission. (2018). *Security for industrial automation and control systems — Part 4-1: Secure product development lifecycle requirements* (IEC 62443-4-1:2018).

[214] Asghar, M. R., Hu, Q., & Zeadally, S. (2019). Cybersecurity in industrial control systems: Issues, technologies, and challenges. *Computer Networks, 165*, 106946. https://doi.org/10.1016/j.comnet.2019.106946

[215] Industrial Control Systems Cyber Emergency Response Team. (2016). *Recommended practice: Improving industrial control system cybersecurity with defense-in-depth strategies*. U.S. Department of Homeland Security.

[216] International Electrotechnical Commission. (2009). *Industrial communication networks — Network and system security — Part 1-1: Terminology, concepts and models* (IEC/TS 62443-1-1:2009).

[217] Alladi, T., Chamola, V., & Zeadally, S. (2020). Industrial control systems: Cyberattack trends and countermeasures. *Computer Communications, 155*, 1–8. https://doi.org/10.1016/j.comcom.2020.03.007

[218] International Electrotechnical Commission. (2015). *Security for industrial automation and control systems — Part 2-3: Patch management in the IACS environment* (IEC TR 62443-2-3:2015).

[219] Knapp, E. D., & Langill, J. T. (2015). *Industrial network security: Securing critical infrastructure networks for smart grid, SCADA, and other industrial control systems* (2nd ed.). Syngress.

[220] MITRE Corporation. (f.a.). *ATT&CK for ICS*. Consultat la 15 august 2026, de la https://attack.mitre.org/matrices/ics/

[221] Industrial Control Systems Cyber Emergency Response Team. (2010). *Primary Stuxnet advisory* (ICSA-10-272-01). https://www.cisa.gov/news-events/ics-advisories/icsa-10-272-01

[222] Langner, R. (2011). Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Security & Privacy, 9*(3), 49–51. https://doi.org/10.1109/MSP.2011.67

[223] International Electrotechnical Commission. (2020). *OPC Unified Architecture — Part 2: Security model* (IEC TR 62541-2:2020, ed. 3.0).

[224] Boyens, J., Smith, A., Bartol, N., Winkler, K., Holbrook, A., & Fallon, M. (2024). *Cybersecurity supply chain risk management practices for systems and organizations* (NIST Special Publication 800-161r1-upd1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-161r1-upd1

[225] Lee, R. M., Assante, M. J., & Conway, T. (2016). *Analysis of the cyber attack on the Ukrainian power grid: Defense use case*. Electricity Information Sharing and Analysis Center & SANS Industrial Control Systems.

[226] Cybersecurity and Infrastructure Security Agency. (2017). *CrashOverride malware* (Alert TA17-163A). https://www.cisa.gov/news-events/alerts/2017/06/12/crashoverride-malware

[227] Cybersecurity and Infrastructure Security Agency. (2018). *HatMan — Safety system targeted malware* (Malware Analysis Report MAR-17-352-01, Update A).

[228] Cybersecurity and Infrastructure Security Agency. (2021). *DarkSide ransomware: Best practices for preventing business disruption from ransomware attacks* (Cybersecurity Advisory AA21-131A). https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-131a

[229] Cybersecurity and Infrastructure Security Agency. (2022). *APT cyber tools targeting ICS/SCADA devices* (Cybersecurity Advisory AA22-103A). https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-103a

[230] Dragos. (2024). *FrostyGoop ICS malware* (Intel Brief). https://hub.dragos.com/hubfs/Reports/Dragos-FrostyGoop-ICS-Malware-Intel-Brief-0724_.pdf

[231] Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero trust architecture* (NIST Special Publication 800-207). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207

[232] Temoshok, D., Choong, Y.-Y., Regenscheid, A., Galluzzo, R., Fenton, J., Richer, J., & Lefkovitz, N. (2025). *Digital identity guidelines: Authentication and authenticator management* (NIST Special Publication 800-63B-4). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-63B-4

[233] Sandhu, R. S., Coyne, E. J., Feinstein, H. L., & Youman, C. E. (1996). Role-based access control models. *Computer, 29*(2), 38–47. https://doi.org/10.1109/2.485845

[234] International Organization for Standardization & International Electrotechnical Commission. (2022). *Information security, cybersecurity and privacy protection — Information security management systems — Requirements* (ISO/IEC 27001:2022).

[235] Barker, E. (2020). *Recommendation for key management: Part 1 — General* (NIST Special Publication 800-57 Part 1, Rev. 5). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-57pt1r5

[236] Santesson, S., Myers, M., Ankney, R., Malpani, A., Galperin, S., & Adams, C. (2013). *X.509 Internet public key infrastructure Online Certificate Status Protocol*

— *OCSP* (RFC 6960). Internet Engineering Task Force. https://doi.org/10.17487/RFC6960

[237] Moriarty, K., & Farrell, S. (2021). *Deprecating TLS 1.0 and TLS 1.1* (RFC 8996, BCP 195). Internet Engineering Task Force. https://doi.org/10.17487/RFC8996

[238] OPC Foundation. (2022). *OPC Unified Architecture — Part 7: Profiles* (OPC 10000-7, Release 1.04). https://reference.opcfoundation.org/Core/Part7/v104/docs/

[239] Pascoe, C., Quinn, S., & Scarfone, K. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST CSWP 29). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29

[240] Industrial Internet Consortium. (2016). *Industrial Internet of Things, Volume G4: Security framework* (IIC:PUB:G4:V1.0:PB:20160926).

[241] International Organization for Standardization & International Electrotechnical Commission. (2024). *Information security, cybersecurity and privacy protection — Information security management systems — Requirements — Amendment 1: Climate action changes* (ISO/IEC 27001:2022/Amd 1:2024).

[242] International Organization for Standardization & International Electrotechnical Commission. (2022). *Information security, cybersecurity and privacy protection — Information security controls* (ISO/IEC 27002:2022).

[243] Parlamentul European & Consiliul Uniunii Europene. (2022). *Directiva (UE) 2022/2555 din 14 decembrie 2022 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune (Directiva NIS 2)*. Jurnalul Oficial al Uniunii Europene, L 333, 27.12.2022. https://eur-lex.europa.eu/eli/dir/2022/2555/oj

[244] Parlamentul European & Consiliul Uniunii Europene. (2023). *Regulamentul (UE) 2023/1230 din 14 iunie 2023 privind mașinile*. Jurnalul Oficial al Uniunii Europene, L 165, 29.6.2023. https://eur-lex.europa.eu/eli/reg/2023/1230/oj

[245] Parlamentul European & Consiliul Uniunii Europene. (2023). *Regulamentul (UE) 2023/2854 din 13 decembrie 2023 privind normele armonizate pentru un acces echitabil la date și o utilizare corectă a acestora și de modificare a Regulamentului (UE) 2017/2394 și a Directivei (UE) 2020/1828 (Regulamentul privind datele)*. Jurnalul Oficial al Uniunii Europene, L, 2023/2854, 22.12.2023. https://eur-lex.europa.eu/eli/reg/2023/2854/oj

[246] International Organization for Standardization. (2022). *Mechanical vibration — Measurement and evaluation of machine vibration — Part 3: Industrial machinery with a power rating above 15 kW and operating speeds between 120 r/min and 30 000 r/min* (ISO 20816-3:2022).

[247] NAMUR. (2017). *NE 107: Self-monitoring and diagnosis of field devices* (Ed. 2017-04-10).

[248] Wolfert, S., Ge, L., Verdouw, C., & Bogaardt, M.-J. (2017). Big data in smart farming — A review. *Agricultural Systems, 153*, 69–80. https://doi.org/10.1016/j.agsy.2017.01.023

DESPRE CARTE

Cum devine o fabrică inteligentă: de la senzorul din hală la decizia de management.

Fabrica modernă nu mai este doar un ansamblu de utilaje, ci un sistem în care datele leagă procesul fizic de deciziile de conducere. Cartea urmărește acest drum, de la senzori, actuatori și echipamente de automatizare până la sistemele de supraveghere și execuție a producției, la planificarea resurselor întreprinderii și la platformele cloud.

În nouă capitole sunt tratate transformarea digitală a industriei, organizarea producției, sistemele de fabricație flexibile și reconfigurabile, componentele și protocoalele de comunicație, arhitecturile de integrare, securitatea cibernetică și aplicațiile industriale, cu studii de caz, exerciții și mini-proiecte.

Lucrarea se adresează studenților și specialiștilor din automatică, robotică, informatică industrială și inginerie industrială.

TEME ABORDATE

Transformare digitală · Organizarea producției · Sisteme de fabricație flexibile · Senzori, actuatori și PLC · Protocoale industriale · SCADA – MES – ERP · Cloud și edge · Securitate cibernetică · Aplicații și mini-proiecte

U.T.PRESS
Cluj-Napoca, 2026
ISBN 978-606-737-870-2