

DOCUMENT PROFESIONAL M-02

METODOLOGIE INTEGRATĂ ARES

Metodologia ARES–SIGMA

S.I.G.M.A. – Sisteme Integrate de Gestiune și Monitorizare a Alarimei: metodologie integrată pentru fundamentarea, proiectarea, verificarea, recepția și exploatarea sistemelor de securitate fizică.

S · I · G · M · A

Metodologia ARES–SIGMA

S.I.G.M.A. – Sisteme Integrate de Gestiune și Monitorizare a Alarimei: metodologie integrată pentru fundamentarea, proiectarea, verificarea, recepția și exploatarea sistemelor de securitate fizică.

08 CAPITOLE	29.888 CUVINTE	≈ 136 MINUTE DE LECTURĂ	2026 EDIȚIE PROFESIONALĂ
-----------------------	--------------------------	-----------------------------------	------------------------------------

NOTĂ PROFESIONALĂ

Documentul nu are natura unui act normativ și se aplică în completarea legislației în vigoare, fără a înlocui ori modifica obligațiile legale aplicabile.

CUPRINS

CAPITOLUL 1

Fundamentele metodologiei S.I.G.M.A.

CAPITOLUL 3

Procesul integrat de proiectare S.I.G.M.A.

CAPITOLUL 5

Proiectarea subsistemelor

CAPITOLUL 7

Verificare, punere în funcțiune și recepție

ANEXE

Fluxuri, matrici, registre și liste de verificare

CAPITOLUL 2

Cadrul normativ, responsabilități și conformitate

CAPITOLUL 4

Context, cerințe și riscuri

CAPITOLUL 6

Integrare, reziliență și securitatea informațiilor

CAPITOLUL 8

Exploatare, mentenanță și managementul schimbării

S.I.G.M.A. – Sisteme Integrate de Gestiune și Monitorizare a Alarimei

Metodologie integrată pentru proiectarea sistemelor de securitate fizică

VERSIUNE SINTETICĂ OFICIALĂ ARES

Proiect pentru consultare profesională • Ediția 1 • Revizia 0

Asociația pentru Reziliență, Evaluare și Securitate

Fișa documentului

Identificare, statut, control și utilizare

Statutul și limitele documentului

Prezenta metodologie formulează un cadru profesional unitar pentru fundamentarea, elaborarea, verificarea și predarea proiectelor sistemelor de securitate fizică. Ea organizează procesul de proiectare, explicitează relația dintre risc, cerințe și soluții tehnice și stabilește rezultate documentabile pentru fiecare etapă.

Metodologia nu înlocuiește actele normative obligatorii, standardele aplicabile, cerințele autorităților competente, documentațiile producătorilor sau obligațiile contractuale. Aplicarea ei presupune verificarea edițiilor în vigoare ale tuturor referințelor folosite. În caz de conflict, cerința cu forță juridică superioară sau cerința tehnică mai severă, după caz, trebuie identificată, analizată și documentată.

Istoricul reviziilor

Reguli de redactare și interpretare

„trebuie” indică o cerință considerată obligatorie în cadrul metodologiei sau reproduce sensul unei obligații externe identificate explicit;

„se recomandă” indică o practică preferată, de la care abaterea este posibilă dacă este justificată și documentată;

„poate” indică o opțiune permisă, dependentă de contextul proiectului;

- citatele din surse externe vor fi marcate distinct și vor avea indicată sursa; parafrazele nu vor fi prezentate drept citate;

- deciziile bazate pe ipoteze trebuie identificate ca atare și confirmate înainte de emiterea proiectului pentru execuție.

Cuvânt înainte

De la conformitatea formală la eficacitatea demonstrabilă

Securitatea fizică nu rezultă din simpla prezență a unor echipamente. Ea rezultă din concordanța dintre riscurile reale ale obiectivului, funcțiile de securitate necesare, arhitectura tehnică aleasă, modul de exploatare și capacitatea sistemului de a funcționa previzibil inclusiv în condiții de defect, incident sau schimbare.

În practică, numeroase neajunsuri apar nu din lipsa tehnologiei, ci din fragmentarea deciziilor: analiza riscului este tratată separat de proiectare, proiectarea separat de execuție, iar recepția separat de exploatare. În această succesiune, informația se pierde, cerințele se diluează, iar sistemul ajunge să fie evaluat prin inventarul de echipamente, nu prin performanța pe care o asigură.

ARES S.I.G.M.A. propune un limbaj profesional comun și o disciplină a trasabilității. Fiecare măsură trebuie să răspundă unui risc sau unei cerințe identificabile; fiecare funcție trebuie să poată fi verificată; fiecare abatere trebuie să fie justificată; fiecare rezultat trebuie să poată fi urmărit de la nevoie până la testul de acceptanță.

Versiunea sintetică este concepută ca instrument de lucru. Ea concentrează regulile esențiale ale metodologiei extinse și le organizează într-un proces aplicabil proiectelor de dimensiuni și complexități diferite.

Proportionalitatea nu înseamnă reducerea arbitrară a exigenței, ci adaptarea controlată a profunzimii analizei și a volumului documentației.

Metodologia se adresează specialiștilor care doresc să depășească abordarea minimală și să construiască soluții coerente, explicabile și verificabile. Ea oferă beneficiarului o bază mai bună pentru decizie, proiectantului un cadru pentru judecată profesională, instalatorului o documentație executabilă, iar utilizatorului un sistem care poate fi exploatat și întreținut în condiții controlate.

Introducere

Obiectul, necesitatea și logica versiunii sintetice

Necesitatea unui cadru metodologic unitar

Proiectarea sistemelor de securitate fizică se desfășoară la intersecția dintre cerințe juridice, analiză de risc, inginerie electrică și de comunicații, arhitectură, securitate operațională, protecția datelor și managementul ciclului de viață. Fără un cadru integrator, proiectul riscă să devină o colecție de planșe și fișe tehnice care nu demonstrează de ce soluția este necesară și dacă aceasta este suficientă.

S.I.G.M.A. tratează proiectul ca pe un lanț de argumentare tehnică. Punctul de plecare îl constituie contextul și riscurile; acestea sunt transformate în cerințe măsurabile; cerințele sunt transpuse în funcții și arhitecturi; soluțiile sunt dimensionate și documentate; rezultatul este verificat, testat, predat și menținut.

Obiectivele versiunii sintetice

- să ofere un proces comun, suficient de riguros pentru proiectele curente;
- să definească minimumul de informații și rezultate necesare unei decizii tehnice trasabile;
- să armonizeze comunicarea dintre beneficiar, evaluator, proiectant, instalator și utilizator;
- să reducă soluțiile standardizate nejustificate și dependența de preferințe comerciale;
- să lege verificarea și recepția de cerințele stabilite la începutul proiectului;
- să permită extinderea controlată către volumele detaliate și anexele specializate S.I.G.M.A.

Modelul logic al metodologiei

CAPITOLUL 1

Fundamentele metodologiei S.I.G.M.A.

1.1 Scopul și necesitatea metodologiei

Scopul metodologiei S.I.G.M.A. este de a institui un proces coerent prin care nevoia de securitate este transformată într-o soluție tehnică justificată, documentată și verificabilă. Metodologia urmărește calitatea raționamentului profesional, nu uniformizarea artificială a soluțiilor. Două obiective similare pot necesita soluții diferite atunci când contextul, modul de utilizare, amenințările, consecințele sau constrângerile diferă.

Necesitatea sa derivă din caracterul multidisciplinar al proiectării și din efectele pe care deciziile inițiale le produc asupra întregului ciclu de viață. O cerință formulată ambiguu conduce la o alegere tehnică dificil de verificat; o alegere fără criteriu de performanță conduce la teste formale; o recepție fără scenarii conduce la acceptarea unui sistem care poate funcționa tehnic, dar nu își îndeplinește scopul operațional.

1.1.1 Problemele profesionale adresate

- lipsa unei legături explicite între evaluarea riscului și cerințele proiectului;
- confundarea proiectării cu selectarea și amplasarea echipamentelor;
- utilizarea unor soluții-tip fără verificarea adecvării la obiectiv;
- cerințe imposibil de testat sau formulate exclusiv prin denumiri comerciale;
- tratarea separată a subsistemelor, fără analiza interacțiunilor și a modurilor degradate;
- documentarea insuficientă a ipotezelor, calculelor și deciziilor;
- recepția limitată la existența echipamentelor, fără verificarea performanței operaționale;
- absența unui mecanism clar de gestionare a modificărilor ulterioare.

1.1.2 Rezultatul urmărit

Aplicarea metodologiei trebuie să conducă la un proiect pentru care un terț competent poate răspunde, pe baza documentației, la cinci întrebări: ce risc sau ce obligație justifică măsura; ce funcție trebuie realizată; ce performanță este cerută; prin ce soluție este obținută; prin ce verificare se demonstrează îndeplinirea cerinței.

1.2 Filosofia metodologiei S.I.G.M.A.

1.2.1 Fundamentul conceptual al metodologiei

S.I.G.M.A. pornește de la ideea că securitatea este o proprietate emergentă a unui ansamblu socio-tehnic. Echipamentele, oamenii, procedurile, infrastructura, informațiile și mediul funcționează împreună. Performanța ansamblului nu poate fi dedusă numai din performanța nominală a componentelor sale.

În consecință, proiectarea trebuie să considere atât lanțul normal de funcționare, cât și condițiile de eroare: pierderea alimentării, indisponibilitatea comunicației, defectarea unui element, acțiunea greșită a operatorului, schimbarea configurației sau apariția unei amenințări neanticipate. Robustă este soluția care își păstrează funcțiile esențiale sau trece într-o stare degradată cunoscută și gestionabilă.

1.2.2 Proiectarea ca proces ingineresc

Proiectarea este un proces iterativ de definire a problemei, modelare a cerințelor, explorare a alternativelor, dimensionare, verificare și control al modificărilor. Planșele și schemele sunt rezultate ale acestui proces, nu procesul însuși. Calitatea grafică nu poate compensa absența ipotezelor, a calculelor ori a criteriilor de acceptanță.

Proiectantul trebuie să distingă între date confirmate, date estimate, ipoteze și decizii. Această clasificare permite identificarea incertitudinii și previne transformarea unei presupunerii într-o cerință aparent certă. Ipotezele cu impact semnificativ trebuie validate înaintea înghețării soluției.

1.2.3 Orientarea către risc

Riscul oferă logica prioritizării. Metodologia nu presupune eliminarea absolută a riscului, ci tratarea lui până la un nivel acceptat în mod informat și documentat. Măsurile se aleg în raport cu scenariile relevante, cu efectele posibile și cu capacitatea organizației de a preveni, detecta, întârzia, răspunde și recupera.

1.2.4 Orientarea către performanță

Cerințele trebuie formulate, pe cât posibil, prin rezultate observabile și criterii măsurabile: aria acoperită, probabilitatea de detectare, calitatea imaginii, timpul de transmitere, autonomia, disponibilitatea, capacitatea de stocare, timpul de răspuns sau comportarea la defect. Descrierea exclusivă prin tipuri de echipamente limitează verificarea și poate introduce dependențe comerciale nejustificate.

1.2.5 Abordarea sistemică și integrată

Subsistemele sunt proiectate în contextul sistemului general de securitate și al operațiunilor obiectivului. O alarmă trebuie analizată până la acțiunea pe care o declanșează; un flux video, până la utilizatorul și decizia pe care le sprijină; o ușă controlată, până la efectele sale asupra circulației, evacuării și continuității activității.

1.2.6 Proportionalitatea soluției

Profundimea analizei, redundanța, nivelul documentării și severitatea testelor trebuie corelate cu riscul, complexitatea și consecințele unei funcționări necorespunzătoare. Proportionalitatea nu autorizează omisiunea cerințelor obligatorii și nu justifică reducerea nedocumentată a performanței.

1.2.7 Trasabilitatea deciziilor

Trasabilitatea reprezintă capacitatea de a urmări o cerință de la sursa sa până la soluția implementată și la dovada de verificare. Ea trebuie menținută bidirecțional: de la cerință către elementele proiectului și de la fiecare element relevant al proiectului către cerința care îl justifică.

1.2.8 Responsabilitatea profesională

Metodologia sprijină judecata profesională, dar nu o înlocuiește. Proiectantul răspunde pentru coerența soluției în limitele rolului, competenței și informațiilor disponibile. Atunci când datele sunt insuficiente, conflictuale sau depășesc competența sa, acesta trebuie să solicite clarificări, validări ori contribuția unui specialist competent.

1.2.9 Îmbunătățirea continuă

Incidentele, alarmele false, defecțiunile, schimbările de utilizare, rezultatele mentenanței și feedbackul operatorilor constituie informații pentru îmbunătățire. Proiectarea trebuie să permită colectarea și valorificarea acestor informații, iar metodologia trebuie revizuită pe baza experienței profesionale și a evoluției cadrului aplicabil.

1.3 Domeniul de aplicare

Metodologia se aplică proiectării sistemelor tehnice destinate protecției persoanelor, bunurilor, informațiilor, proceselor și continuității activităților împotriva amenințărilor relevante de securitate fizică. Ea acoperă proiectele noi, extinderile, modernizările, înlocuirile și integrarea sistemelor existente.

1.3.1 Sisteme și interfețe vizate

- sisteme de detecție și alarmare la efracție și agresiune;
- sisteme de supraveghere video pentru aplicații de securitate;
- sisteme electronice de control al accesului;
- interfonie, comunicații de securitate și transmiterea alarmelor;
- infrastructuri de alimentare, comunicații, sincronizare și stocare aferente;
- interfețe cu sisteme de incendiu, management al clădirii, IT, iluminat și procese operaționale, în limitele competențelor și reglementărilor aplicabile.

1.3.2 Limite de aplicare

Metodologia nu substituie proiectarea specializată a instalațiilor de detectare, semnalizare și alarmare la incendiu, a instalațiilor electrice, a rețelilor de date, a construcțiilor sau a altor specialități reglementate. Atunci când soluția de securitate depinde de acestea, proiectul trebuie să definească interfețele, responsabilitățile și criteriile de coordonare interdisciplinară.

1.3.3 Aplicare proporțională

Pentru proiectele cu risc și complexitate reduse, unele rezultate pot fi reunite într-un document unic, dacă informația rămâne completă și verificabilă. Pentru proiectele complexe, rezultatele pot fi dezvoltate în volume, memorii, calcule și registre distincte. Reducerea numărului de documente nu trebuie confundată cu eliminarea etapelor de raționament.

1.4 Terminologia fundamentală

Termenii de mai jos sunt utilizați în sens metodologic. Atunci când un act normativ, un standard sau un contract impune o definiție specifică, aceasta trebuie identificată și aplicată în domeniul său. Diferențele de terminologie trebuie consemnate în registrul cerințelor sau în glosarul proiectului.

1.4.1 Relația dintre termenii fundamentali

Un activ are valoare și este expus unor amenințări. Vulnerabilitățile permit materializarea amenințărilor în scenarii, iar consecințele afectează obiectivele organizației. Riscul este evaluat pentru aceste scenarii. Măsurile de securitate modifică probabilitatea, consecința sau ambele, rezultând un risc rezidual care trebuie comparat cu criteriile de acceptare.

1.5 Arhitectura metodologiei

S.I.G.M.A. este organizată pe niveluri complementare. Nivelul strategic definește contextul, obiectivele și criteriile de acceptare. Nivelul funcțional transformă riscurile în funcții și cerințe. Nivelul tehnic dezvoltă arhitectura, calculele, selecțiile și documentația. Nivelul de asigurare verifică, validează și păstrează dovezile. Nivelul ciclului de viață menține configurația și adecvarea soluției.

1.5.1 Caracterul iterativ

Etaplele nu sunt strict liniare. O constrângere descoperită la dimensionare poate impune revizuirea arhitecturii; un test poate evidenția o cerință ambiguă; o schimbare operațională poate necesita reevaluarea riscului. Iterația este controlată prin versiuni, aprobări și menținerea trasabilității, nu prin modificări informale.

1.6 Principiile fundamentale S.I.G.M.A.

1.6.1 Ierarhizarea principiilor în decizie

Principiile se aplică împreună. Proportionalitatea nu poate prevala asupra legalității; neutralitatea tehnologică nu poate exclude o caracteristică necesară performanței; apărarea în profunzime nu justifică redundanțe fără valoare; reziliența trebuie corelată cu scenariile și cu resursele de exploatare. Conflictele aparente se soluționează prin revenirea la cerințe, risc și criteriile de acceptare.

1.7 Rezultatele procesului metodologic

Rezultatele S.I.G.M.A. sunt dovezi ale procesului de proiectare și suport pentru execuție, verificare și exploatare. Conținutul lor se adaptează proiectului, însă funcțiile informaționale trebuie păstrate.

1.7.1 Criteriile de calitate ale rezultatelor

- completitudine — informațiile necesare deciziei și utilizării sunt prezente;
- corectitudine — datele, calculele și referințele sunt verificabile;
- coerență — documentele nu conțin cerințe sau soluții contradictorii;
- trasabilitate — sursa, implementarea și verificarea pot fi urmărite;
- actualitate — versiunea și starea informației sunt controlate;
- lizibilitate — documentele pot fi înțelese de destinatarii lor fără interpretări arbitrare;
- executabilitate — soluția poate fi implementată în condițiile definite;
- verificabilitate — criteriile de acceptanță și metodele de testare sunt explicite.

1.7.2 Punctul de control la încheierea Capitolului 1

Înainte de inițierea cadrului normativ și a procesului detaliat de proiectare, organizația sau echipa de proiect trebuie să confirme domeniul, statutul documentelor, vocabularul utilizat, principiile aplicabile, responsabilitățile și rezultatele care vor fi produse. Orice derogare de la rezultatele minimale trebuie justificată prin complexitatea și riscul proiectului și consemnată în fișa de inițiere.

CAPITOLUL 2

Cadrul normativ, responsabilități și conformitate

Prezentul capitol stabilește modul în care cerințele juridice, normative, contractuale și profesionale sunt identificate, ierarhizate, transpuse în proiect și păstrate ca dovezi de conformitate. În metodologia S.I.G.M.A., conformitatea nu este o verificare efectuată numai la final, ci o proprietate controlată pe întregul proces de proiectare.

Cadrul aplicabil unui proiect nu este alcătuit dintr-o listă fixă. El depinde de natura unității, activele protejate, destinația construcției, subsistemele incluse, amplasament, cerințele autorităților, regimul datelor, sursele de finanțare și obligațiile contractuale. Din acest motiv, fiecare proiect trebuie să dețină propriul registru al documentelor aplicabile, cu ediții și stări verificate la data emiterii.

2.1 Ierarhia cerințelor aplicabile

Cerințele sunt ordonate după forța juridică și după sursa lor. Ierarhia nu trebuie confundată cu severitatea tehnică: o cerință contractuală poate fi mai exigentă decât minimul legal, însă nu poate autoriza încălcarea unei obligații legale și nu poate transfera unui participant competențe pe care acesta nu le deține.

2.1.1 Caracterul standardelor

Ca regulă generală a standardizării naționale, aplicarea unui standard are caracter voluntar. Standardul devine însă o cerință efectivă a proiectului atunci când un act normativ îl face aplicabil, când este introdus în contract ori în documentația de atribuire, când este necesar pentru certificarea solicitată sau când proiectantul îl adoptă explicit drept bază de proiectare. În aceste situații trebuie stabilite referința completă, ediția și eventualele amendamente.

2.1.2 Regula cerinței controlate

Fiecare cerință relevantă trebuie înregistrată cu sursă, autoritate, domeniu, caracter obligatoriu sau recomandat, responsabil de implementare și metodă de verificare. Formulările generale precum „conform standardelor în vigoare” nu sunt suficiente pentru cerințele critice, deoarece nu indică documentul, ediția ori partea aplicabilă.

- cerința obligatorie se aplică integral în domeniul său, cu excepția derogărilor permise și aprobate potrivit legii;
- cerința contractuală suplimentară se aplică dacă este compatibilă cu legea și a fost inclusă valid în domeniul proiectului;
- recomandarea tehnică poate fi înlocuită printr-o soluție echivalentă numai după documentarea performanței și a riscului;
- cerința neclară, conflictuală sau imposibil de verificat se clarifică înainte de înghețarea soluției.

2.2 Legislația privind securitatea fizică

La data verificării prezentei versiuni — 10 august 2026 — actul principal este Legea nr. 333/2003 privind paza obiectivelor, bunurilor, valorilor și protecția persoanelor, în forma consolidată care include modificările introduse prin O.U.G. nr. 37/2026. Normele metodologice sunt aprobate prin H.G. nr. 301/2012, cu modificările ulterioare, iar normele tehnice din anexa nr. 7 reglementează proiectarea, instalarea, modificarea, monitorizarea, întreținerea și utilizarea sistemelor de alarmare împotriva efracției.

2.2.1 Regimul proiectului după O.U.G. nr. 37/2026

Modificarea art. 27 din Legea nr. 333/2003 schimbă mecanismul aplicabil proiectelor sistemelor de alarmare împotriva efracției. Proiectele se întocmesc cu respectarea cerințelor minimale și a normelor tehnice stabilite prin normele metodologice; proiectul, analiza de risc ori fișa de securitate, după caz, precum și modificările acestora se transmit electronic de conducătorul unității beneficiare către unitatea de poliție competentă. Instalarea sau modificarea se realizează conform proiectului și rămâne supusă controlului organelor de poliție cu atribuții în domeniu.

Prin urmare, proiectul nu își pierde caracterul obligatoriu și nici funcția de control tehnic prin eliminarea mecanismului anterior de avizare. Dimpotrivă, răspunderea pentru corectitudinea proiectului, transmiterea documentelor și executarea conform proiectului trebuie delimitată mai clar între beneficiar, proiectant și instalator.

2.2.2 Perioada de necorelare normativă

La aceeași dată de referință, forma publicată a normelor aprobate prin H.G. nr. 301/2012 păstrează dispoziții redactate pentru vechiul mecanism de avizare. O normă metodologică nu poate prevala asupra legii modificate ulterior. Totuși, necorelarea trebuie consemnată în registrul legislativ al proiectului, iar procedurile administrative curente trebuie verificate în sursele oficiale ale autorității competente. Metodologia nu transformă o pagină administrativă neactualizată într-un temei juridic și nu autorizează ignorarea unei obligații aflate în vigoare.

2.2.3 Legislația complementară

În funcție de obiectiv și de soluție, proiectul poate intra și sub incidența unor acte complementare. Aplicabilitatea acestora nu se presupune automat, ci se stabilește în fișa proiectului.

Regulamentul (UE) 2016/679 și Legea nr. 190/2018, pentru prelucrarea datelor personale prin supraveghere video, control al accesului, jurnale și identificatori;

O.U.G. nr. 155/2024, aprobată prin Legea nr. 124/2025, pentru entitățile și sistemele care intră în cadrul național de securitate cibernetică;

Legea nr. 10/1995 și reglementările privind calitatea în construcții, atunci când lucrările și specialitatea proiectată intră în domeniul acestora;

Legea nr. 50/1991 și regimul autorizării lucrărilor, după natura intervenției asupra construcției;

Legea nr. 307/2006 și reglementările de securitate la incendiu, pentru interfețe, alimentări, căi de evacuare, uși controlate și condiții de funcționare la incendiu;

Normativul I 7/2011, cu modificările din 2023, și celelalte reglementări electrice aplicabile alimentării, protecțiilor, cablării și verificării instalațiilor;

Legea nr. 98/2016, pentru proiectele realizate în cadrul achizițiilor publice, inclusiv regulile privind specificațiile tehnice și acceptarea soluțiilor echivalente.

2.3 Standarde și documente tehnice de referință

Standardele oferă vocabular comun, clasificări, cerințe de produs și sistem, metode de proiectare și criterii de încercare. Ele trebuie utilizate ca ansamblu coerent: selectarea numai a unor valori favorabile dintr-un standard, fără condițiile și metodele sale de verificare, nu reprezintă aplicare conformă.

2.3.1 Controlul edițiilor

Denumirile de familie din această metodologie nu substituie verificarea catalogului ASRO. Pentru fiecare proiect se identifică standardul național adoptat, ediția, amendamentele, corecturile, data anulării sau înlocuirii și perioada de tranziție, dacă există. O ediție nouă nu se aplică retroactiv în mod automat unui proiect contractat pe o ediție anterioară, dar impactul ei asupra siguranței, conformității și acceptării trebuie evaluat.

Evoluția standardului IEC 62676-4 este un exemplu relevant: ediția 2025 înlocuiește ediția 2014 la nivel IEC și actualizează cadrul pentru planificarea, proiectarea, instalarea, testarea, punerea în funcțiune și mentenanța sistemelor video. Înainte de utilizarea indicativului SR EN IEC, proiectantul trebuie să confirme adoptarea națională și starea exactă în catalogul ASRO.

2.3.2 Documentațiile producătorilor

Fișele tehnice, manualele, certificatele și declarațiile producătorilor demonstrează caracteristicile produsului și condițiile sale de utilizare, dar nu demonstrează singure performanța sistemului proiectat. Proiectantul trebuie să verifice limitele de mediu, alimentarea, compatibilitatea, versiunile software și firmware, licențele, capacitatea, interfețele și condițiile care pot invalida performanța declarată.

2.4 Cerințe contractuale și cerințe ale beneficiarului

Contractul și tema de proiectare transformă obiectivele beneficiarului în obligații concrete ale proiectului. Cerințele contractuale trebuie să fie legale, realizabile, verificabile și corelate cu responsabilitățile atribuite. O solicitare verbală ori o preferință comercială nu trebuie introdusă ca cerință obligatorie fără confirmarea autorității care o formulează.

2.4.1 Clasificarea cerințelor

2.4.2 Controlul cerințelor comerciale

Cerințele formulate prin marcă, model sau ecosistem închis trebuie justificate prin compatibilitate, continuitatea configurației, performanță ori alte motive verificabile. În achizițiile publice se aplică regulile specifice privind specificațiile tehnice și mențiunea „sau echivalent”, după caz. Neutralitatea tehnologică nu exclude o cerință tehnică necesară, dar exclude limitarea comercială fără justificare.

Orice reducere de buget sau termen care afectează o cerință de securitate se tratează ca modificare a proiectului, nu ca simplă optimizare comercială. Impactul asupra riscului, performanței, conformității și testării trebuie prezentat decidentului competent înainte de aprobare.

2.5 Rolurile participanților

Responsabilitățile trebuie stabilite printr-o matrice de tip RACI sau printr-un instrument echivalent. Existența mai multor participanți nu diluează răspunderea fiecăruia, iar cumularea legal permisă a unor roluri nu elimină nevoia de verificare independentă pentru deciziile critice.

2.5.1 Separarea deciziilor

Evaluatorul propune și fundamentează tratarea riscului; proiectantul definește soluția tehnică; instalatorul o implementează; beneficiarul acceptă riscul rezidual și recepționează rezultatul pe baza dovezilor. Aceste funcții trebuie distinse chiar dacă, în limitele legii și ale incompatibilităților aplicabile, aceeași organizație participă la mai multe etape.

Autoritatea competentă controlează respectarea cadrului legal în limitele atribuțiilor sale. Transmiterea, controlul sau verificarea administrativă a proiectului nu exonerează proiectantul, instalatorul ori beneficiarul de responsabilitățile proprii și nu reprezintă o garanție generală a eficacității operaționale.

2.6 Responsabilitatea proiectantului

Proiectantul răspunde pentru procesul și rezultatele aflate în sfera mandatului său. Responsabilitatea se raportează la competența profesională, datele disponibile, cerințele confirmate și nivelul de diligență rezonabil pentru riscul și complexitatea proiectului. Lipsa unei cerințe explicite nu justifică omisiunea unei condiții obligatorii sau a unei incompatibilități tehnice evidente.

2.6.1 Obligații metodologice minime

- să verifice mandatul, competența, limitele și datele de intrare înainte de elaborarea soluției;
- să identifice cadrul aplicabil și să mențină registrul legislativ, normativ și contractual;
- să distingă datele confirmate de ipoteze și să solicite validarea ipotezelor cu impact semnificativ;
- să transforme riscurile și obiectivele în cerințe verificabile, fără supradimensionare arbitrară;
- să compare alternativele relevante și să documenteze criteriile deciziilor critice;
- să dimensioneze, coordoneze și specifice soluția până la un nivel executabil;
- să prevadă numai produse adecvate, cu dovezi de conformitate și compatibilitate corespunzătoare;
- să definească metodele și criteriile de verificare înainte de emiterea proiectului pentru execuție;
- să controleze codificarea, versiunile, distribuția și confidențialitatea documentației;

- să analizeze modificările și să actualizeze proiectul și trasabilitatea înainte de implementare.

2.6.2 Limitele datelor și rezervele profesionale

Dacă informațiile esențiale lipsesc, proiectantul trebuie să precizeze efectul, să solicite completarea și să evite emiterea ca proiect pentru execuție a unei soluții a cărei adecvare nu poate fi demonstrată. O rezervă generică de tipul „beneficiarul răspunde” nu transferă răspunderea pentru o decizie tehnică luată de proiectant.

Atunci când beneficiarul solicită o soluție neconformă sau insuficientă, proiectantul formulează în scris neconformitatea, temeiul, consecința și opțiunile conforme. Dacă abaterea afectează o obligație legală ori o funcție critică și nu este remediată, proiectul nu trebuie emis într-o formă care ar prezenta soluția drept conformă.

2.6.3 Confidențialitatea și integritatea proiectului

Proiectele conțin amplasări, trasee, zone, coduri, capacități și vulnerabilități care pot deveni informații sensibile. Accesul trebuie limitat la persoanele autorizate, transmiterea trebuie protejată, iar copiile și versiunile trebuie controlate. Documentația predată beneficiarului și cea păstrată de proiectant se codifică și se gestionează potrivit cerințelor legale și contractuale aplicabile.

2.7 Gestionarea conflictelor dintre cerințe

Un conflict există atunci când două cerințe nu pot fi îndeplinite simultan, când una este ambiguă sau când aplicarea ei într-un domeniu produce neconformitate în altul. Conflictul nu se rezolvă prin alegerea informală a cerinței convenabile și nici prin aplicarea automată a celei aparent mai severe.

2.7.1 Procesul de soluționare

Identificarea exactă a celor două cerințe, a surselor, edițiilor și domeniilor lor de aplicare.

Clasificarea conflictului: juridic, tehnic, contractual, operațional, de securitate la incendiu, de protecția datelor ori de competență.

Aplicarea ierarhiei juridice și eliminarea interpretărilor care depășesc domeniul sursei.

Evaluarea consecințelor asupra riscului, performanței, costului, termenului și posibilității de verificare.

Solicitarea clarificării de la autoritatea sau partea competentă și formularea alternativelor conforme.

Înregistrarea deciziei, justificării, aprobării și efectului în registrul cerințelor și în documentele afectate.

2.7.2 Situații tipice

2.8 Prezumția de conformitate și justificarea abatelor

Conformitatea cu un standard relevant poate constitui o dovadă tehnică puternică și, în anumite regimuri, poate conferi prezumție de conformitate pentru cerințele acoperite. Ea nu dovedește însă automat respectarea tuturor cerințelor legale, adecvarea la risc sau performanța instalației realizate. Domeniul prezumției trebuie identificat exact.

2.8.1 Tipuri de abatere

- abaterea de la o cerință legală obligatorie nu este admisibilă decât dacă actul permite expres o derogare și aceasta este obținută în forma cerută;
- abaterea de la o cerință contractuală necesită acordul părții competente și actualizarea controlată a documentelor;
- abaterea de la o recomandare de standard poate fi acceptată dacă soluția alternativă oferă performanță cel puțin echivalentă și nu produce alte neconformități;
- abaterea de la instrucțiunea producătorului este admisibilă numai dacă este susținută de o confirmare tehnică validă ori dacă produsul este înlocuit cu unul adecvat.

2.8.2 Dosarul soluției alternative

Atunci când proiectantul propune o soluție diferită de referința tehnică uzuală, dosarul de justificare trebuie să conțină minimum: cerința și sursa; motivul abaterii; descrierea alternativei; comparația de performanță; riscurile și ipotezele; calculele, certificatele sau încercările; interfețele afectate; metoda de verificare; responsabilul și aprobările necesare.

2.8.3 Declarația de conformitate a proiectului

Înainte de emiterii pentru execuție, proiectantul întocmește o declarație sau o matrice de conformitate adecvată complexității proiectului. Aceasta identifică documentele aplicate, cerințele majore, locul implementării lor în proiect, abaterile aprobate și verificările necesare. Declarația nu este o formulă generală de exonerare, ci o sinteză trasabilă a dovezilor.

2.9 Evidența documentelor normative utilizate

Registrul documentelor aplicabile este un document controlat al proiectului. El se inițiază odată cu tema de proiectare și se actualizează la fiecare etapă care poate schimba baza de conformitate. Pentru proiectele de durată, simpla dată a contractului nu este suficientă; trebuie stabilită data de referință normativă și regula contractuală pentru modificările ulterioare.

2.9.1 Momentele de reverificare

- la inițierea proiectului și înainte de aprobarea temei;

- la înghețarea conceptului și a arhitecturii;
- înaintea emiterii proiectului pentru execuție;
- la aprobarea unei modificări cu impact asupra cerințelor;
- înaintea recepției și predării dosarului final;
- la reevaluarea riscului, modernizare sau schimbarea destinației obiectivului.

2.9.2 Punctul de control al Capitolului 2

Capitolul 2 este închis numai dacă proiectul deține: registrul documentelor aplicabile; registrul cerințelor derivat din acestea; matricea rolurilor; lista conflictelor și clarificărilor; evidența abaterilor; regula de control al edițiilor; precum și o cale de verificare pentru fiecare cerință critică. În lipsa acestor rezultate, trecerea la proiectarea detaliată introduce un risc necontrolat de neconformitate și refacere.

Referințe citate în Capitolul 2

Referințele de mai jos au fost verificate în surse oficiale la 10.08.2026. Lista nu este exhaustivă și nu substituie registrul aplicabil fiecărui proiect.

[N1] O.U.G. nr. 37/2026 pentru modificarea și completarea Legii nr. 333/2003 — sursa oficială (Portal Legislativ)

[N2] Legea nr. 333/2003, forma publicată în Portalul Legislativ — sursa oficială (se verifică forma consolidată la data utilizării)

[N3] H.G. nr. 301/2012 și normele metodologice de aplicare — sursa oficială (inclusiv anexele tehnice)

[N4] O.G. nr. 39/1998 privind activitatea de standardizare națională în România — sursa oficială (caracterul voluntar al standardelor)

[N5] Instrucțiunile M.A.I. nr. 9/2013 privind efectuarea analizelor de risc la securitatea fizică — sursa oficială (aplicabilitate de verificat în contextul O.U.G. nr. 37/2026)

[N6] Regulamentul (UE) 2016/679 privind protecția datelor cu caracter personal — sursa oficială (EUR-Lex)

[N7] Ghidul EDPB 3/2019 privind prelucrarea datelor prin dispozitive video — sursa oficială (versiune finală)

[N8] O.U.G. nr. 155/2024 privind cadrul de securitate cibernetică — sursa oficială (aprobată prin Legea nr. 124/2025)

[N9] IEC 62676-4:2025 — Video surveillance systems — Application guidelines — sursa oficială (adoptarea națională se verifică la ASRO)

[N10] IEC 60839-11-1:2013 — Electronic access control systems — sursa oficială (cerințe de sistem și componente)

[N11] IEC 60839-11-2:2014 — Electronic access control systems — Application guidelines — sursa oficială (planificare, instalare, punere în funcțiune și operare)

[N12] ASRO — Întrebări frecvente privind utilizarea standardelor — sursa oficială (verificarea statutului și a adoptării naționale)

CAPITOLUL 3

Procesul integrat de proiectare S.I.G.M.A.

Procesul integrat de proiectare S.I.G.M.A. reprezintă mecanismul prin care contextul obiectivului, riscurile, obligațiile aplicabile și nevoile operaționale sunt transformate într-o soluție tehnică justificată, executabilă și verificabilă. Procesul nu este o succesiune administrativă de documente și nici o selecție progresivă de echipamente. El este un lanț controlat de decizii ingineresti, în care fiecare rezultat devine intrare pentru etapa următoare și păstrează legătura cu sursa sa.

Cele zece etape descrise în prezentul capitol formează fluxul de referință al metodologiei. În funcție de amploarea, noutatea și riscul proiectului, activitățile pot fi parcurse predictiv, iterativ sau într-o combinație a celor două. Adaptarea procesului este permisă, însă eliminarea unei etape trebuie justificată prin absența reală a nevoii, nu prin lipsa timpului, a datelor ori a bugetului. Pentru proiectele mici se poate reduce volumul documentelor, dar nu se elimină raționamentul, responsabilitatea sau dovada deciziei.

Fluxul de referință și porțile de control

Fiecărei etape îi corespunde o poartă de control, notată G1–G10. O poartă nu este o formalitate și nu presupune în mod obligatoriu o ședință distinctă; ea reprezintă verificarea criteriilor de ieșire înainte ca proiectul să consume resurse semnificative în etapa următoare. Rezultatul porții poate fi: aprobat; aprobat cu acțiuni controlate; returnat pentru completare; sau suspendat până la eliminarea unui impediment.

Reguli transversale ale procesului

- trasabilitatea se menține bidirecțional: de la sursă și risc către cerință, soluție și test, precum și invers, de la elementul proiectat către justificarea sa;
- ipotezele, incertitudinile și datele provizorii se înregistrează împreună cu responsabilul, termenul de confirmare și consecința neconfirmării;
- modificările se analizează înainte de implementare pentru efectele asupra cerințelor, riscului, interfețelor, calculelor, costului, termenului și criteriilor de verificare;
- deciziile critice se bazează pe dovezi proporționale cu riscul: măsurători, calcule, standarde, încercări, declarații de performanță, modele sau judecată profesională documentată;
- independența revizuirii crește odată cu riscul, complexitatea și caracterul inovator al soluției; autorul nu trebuie să fie singurul control al propriilor ipoteze critice;
- confidențialitatea documentelor, integritatea fișierelor și controlul distribuției se aplică pe întregul proces, nu numai la predarea proiectului;
- fiecare etapă include analiza efectului asupra întregului ciclu de viață: instalare, punere în funcțiune, exploatare, mentenanță, modificare și scoatere din funcțiune;

- proiectul rămâne deschis iterării controlate: o constatare nouă poate impune revenirea la o etapă anterioară, cu actualizarea tuturor rezultatelor afectate.

3.1 Inițierea proiectului

Inițierea stabilește dacă proiectul poate începe în condiții profesionale controlate. În această etapă se clarifică mandatul, obiectivul intervenției, limitele preliminare, rolurile, accesul la informații și resursele necesare. O inițiere incompletă transferă incertitudinea către etapele tehnice, unde corectarea devine mai costisitoare și poate genera soluții care răspund unei probleme formulate greșit.

3.1.1 Activități și criterii de decizie

Proiectantul identifică entitatea care comandă lucrarea, persoana competentă să aprobe cerințele și riscul rezidual, obiectivul protejat, amplasamentele incluse, sistemele existente și faza de proiectare solicitată. Se delimitează proiectarea de evaluarea riscului, execuție, consultanță, ofertare, verificare și asistență tehnică. Dacă mandatul combină aceste activități, responsabilitățile și livrabilele se separă explicit.

Acceptarea proiectului presupune confirmarea competenței profesionale și organizaționale, a accesului rezonabil la obiectiv, a posibilității de a obține informațiile necesare și a unui calendar compatibil cu profunzimea analizei. Conflictele de interese, incompatibilitățile, cererile nelegitime și restricțiile care împiedică respectarea obligațiilor se declară înainte de începerea proiectării.

- identificarea beneficiarului, utilizatorului, proprietarului infrastructurii și a celorlalte părți cu putere de decizie;
- stabilirea scopului de securitate declarat și a evenimentului care a generat proiectul: obiectiv nou, conformare, modernizare, incident, extindere sau integrare;
- definirea limitelor fizice, funcționale, organizaționale și informaționale preliminare;
- stabilirea clasificării informațiilor, regulilor de acces, canalelor de transmitere și păstrare;
- identificarea etapelor contractuale, a dependențelor, a punctelor de aprobare și a resurselor specializate necesare;
- deschiderea registrului problemelor, ipotezelor, deciziilor și modificărilor.

3.1.2 Responsabilități și coordonare

Beneficiarul confirmă mandatul și desemnează reprezentantul cu autoritate de decizie. Proiectantul propune procesul, precizează datele necesare și declară limitele competenței. Evaluatorul de risc, utilizatorul, responsabilul IT, specialistul de securitate la incendiu și alte discipline sunt implicați de la început atunci când deciziile lor condiționează soluția. Responsabilitatea pentru coordonare trebuie atribuită nominal, nu presupusă.

3.1.3 Rezultate și control

Fișa de inițiere trebuie să permită unei persoane care nu a participat la discuțiile inițiale să înțeleagă cine a solicitat proiectul, ce se urmărește, ce este inclus, ce este exclus, cine aprobă și care sunt condițiile de continuare. Domeniul preliminar se menține distinct de soluția tehnică; la această dată nu se îngheață amplasări, produse ori cantități.

3.1.4 Erori frecvente

- acceptarea unei solicitări verbale fără desemnarea persoanei care aprobă cerințele;
- confundarea bugetului estimat cu domeniul tehnic deja decis;
- omiterea sistemelor existente și a interfețelor din limitele proiectului;
- presupunerea că toate datele vor fi disponibile ulterior, fără responsabil și termen;
- inițierea selecției de echipamente înaintea clarificării problemei de securitate.

3.2 Definirea temei de proiectare

Tema de proiectare transformă intenția inițială într-un mandat tehnic controlabil. Ea descrie problema, rezultatele urmărite, domeniul, constrângerile și criteriile după care proiectul va fi acceptat. Tema nu trebuie să anticipeze nejustificat soluția și nici să transfere proiectantului decizii care aparțin beneficiarului, evaluatorului sau autorităților competente.

3.2.1 Conținut și formulare

Tema trebuie să includă scopul de securitate, obiectivele protejate, utilizatorii, zonele, programul de funcționare, scenariile cunoscute, cerințele legale și contractuale, nivelurile de performanță deja stabilite, interfețele, condițiile de mediu, cerințele privind protecția datelor și securitatea cibernetică, restricțiile de patrimoniu sau arhitectură, livrabilele, fazele, aprobările și criteriile de acceptanță. Formulările de tip „sistem complet”, „cea mai bună tehnologie” sau „acoperire totală” nu sunt suficiente fără definirea rezultatului observabil.

Bugetul și termenul se tratează ca restricții de proiect, nu ca justificări automate pentru reducerea cerințelor. Atunci când resursele sunt incompatibile cu rezultatul solicitat, proiectantul prezintă diferența, riscul și alternativele: etapizare, modificarea domeniului, soluție echivalentă ori revizuirea cerinței de către rolul competent.

3.2.2 Controlul ipotezelor și al limitelor

- fiecare ipoteză cu impact se identifică prin cod, sursă, responsabil pentru confirmare, termen și efectul neconfirmării;
- excluderile se descriu concret și se verifică dacă nu separă artificial o interfață necesară funcționării sistemului;

- datele furnizate de beneficiar sunt confirmate ca informație de intrare, fără a fi preluate necritic atunci când există contradicții evidente;
- cerințele incompatibile se introduc în registrul conflictelor și nu se maschează prin formulări ambigue;
- orice schimbare a temei după aprobare urmează procesul de management al modificării.

3.2.3 Validarea temei cu părțile interesate

Tema este parcursă cu persoanele care cunosc exploatarea reală: conducerea, securitatea, personalul tehnic, IT, protecția datelor, utilizatorii zonelor și intervenția. Validarea urmărește nu doar acordul formal, ci detectarea diferențelor dintre procedurile declarate și practicile reale. Aprobarea se documentează împreună cu rezervele, acțiunile rămase și persoanele autorizate să modifice tema.

3.2.4 Erori frecvente

- copierea unei teme dintr-un proiect similar fără analiza contextului;
- introducerea unor mărci și modele înainte de definirea performanței;
- omiterea criteriilor de acceptanță și a interfețelor;
- aprobarea unei teme cu contradicții nerezolvate;
- lipsa delimitării între cerință, preferință și ipoteză.

3.3 Colectarea informațiilor

Colectarea informațiilor formează baza de evidență a proiectului. Calitatea soluției nu poate depăși în mod rezonabil calitatea datelor pe care se sprijină. Activitatea urmărește nu acumularea nediferențiată de documente, ci identificarea informațiilor necesare, verificarea sursei, actualității și coerenței lor, precum și semnalarea golurilor care influențează proiectarea.

3.3.1 Categoriile de informații

- documente juridice și administrative relevante pentru regimul obiectivului, destinație, proprietate și obligații;
- analize de risc, istoricul incidentelor, rapoarte de intervenție, alarme false, pierderi și neconformități;
- planuri de arhitectură, structură, instalații electrice, comunicații, incendiu, evacuare și alte discipline;
- inventare de active, clasificări, valori, procese critice și dependențe operaționale;
- organigrame, roluri, fluxuri de persoane, bunuri, vehicule și informații, inclusiv variațiile temporale;
- documentația sistemelor existente: scheme, licențe, capacități, parole gestionate, versiuni, mentenanță, defecte și integrare;

- infrastructura IT și energetică, politicile de rețea, identitate, jurnalizare, timp, backup și securitate cibernetică;
- condiții de mediu și exploatare: iluminare, temperatură, umiditate, praf, vibrații, interferențe, coroziune și acces pentru mentenanță.

3.3.2 Calitatea și trasabilitatea datelor

Fiecărei informații relevante i se asociază sursa, data, proprietarul, versiunea, gradul de încredere și domeniul în care poate fi utilizată. O planșă fără revizie, un inventar neverificat sau o declarație informală pot constitui indicii, dar nu trebuie tratate automat ca date confirmate. Contradicțiile dintre surse se păstrează vizibile până la clarificare; alegerea unei variante se justifică.

Datele sensibile se colectează proporțional cu nevoia, se păstrează în medii aprobate și se distribuie controlat. Colectarea de imagini, jurnale, liste de personal sau configurații nu se extinde dincolo de scopul proiectului. Atunci când se folosesc exporturi din sisteme, integritatea și perioada reprezentativă trebuie consemnate.

3.3.3 Gestionarea lipsurilor

Lipsa unei informații nu se rezolvă prin completare tacită. Proiectantul evaluează impactul și decide dacă: solicită date suplimentare; planifică o măsurare; folosește o ipoteză conservatoare; propune o etapă de investigație; limitează domeniul; sau suspendă decizia. Ipoteza conservatoare nu trebuie confundată cu supradimensionarea arbitrară și trebuie înlocuită atunci când apar date confirmate.

3.3.4 Erori frecvente

- folosirea exclusivă a planurilor existente fără verificarea situației reale;
- preluarea listelor de echipamente ca dovadă a funcționării sistemului;
- ignorarea incidentelor și alarmelor false deoarece nu sunt documentate uniform;
- păstrarea datelor fără versiune, autor sau dată;
- colectarea excesivă de informații sensibile fără necesitate și control.

3.4 Investigarea amplasamentului

Investigarea amplasamentului confirmă realitatea fizică și operațională în care va funcționa soluția. Ea nu se reduce la o vizită de orientare sau la fotografierea spațiilor. Investigația este planificată pe baza temei și a lacunelor identificate, urmărește ipotezele critice și produce măsurători, observații și dovezi suficient de precise pentru proiectare.

3.4.1 Planificarea și desfășurarea

Planul investigației precizează zonele, traseul, persoanele necesare, intervalele reprezentative, instrumentele, condițiile de securitate a muncii și informațiile care trebuie confirmate. Pentru sisteme video pot fi necesare măsurări de iluminare și probe de câmp vizual; pentru comunicații, verificări ale traseelor, capacităților și

interferențelor; pentru alimentare, identificarea circuitelor, protecțiilor, spațiilor și surselor de rezervă; pentru control acces, analiza ușilor, feroneriei, evacuării și modurilor de defect.

Investigația trebuie să observe și funcționarea obiectivului: fluxuri, perioade aglomerate, accesul furnizorilor, operațiunile de închidere, intervenția, mentenanța și situațiile excepționale. O condiție verificată numai în intervalul cel mai favorabil poate conduce la concluzii greșite. Când variația zi/noapte, sezonieră sau operațională este relevantă, se planifică vizite suplimentare, măsurări reprezentative sau monitorizare temporară.

3.4.2 Înregistrarea dovezilor

- pozițiile și orientările se raportează la un sistem de referință identificabil în planuri;
- fotografiile primesc cod, dată, locație, direcție și nivel de acces; imaginile sensibile se protejează;
- instrumentele și condițiile de măsurare se consemnează atunci când rezultatul influențează dimensionarea;
- diferențele față de documentația primită se marchează explicit și se transmit disciplinelor afectate;
- zonele neaccesibile și informațiile neverificabile se înregistrează ca limitări, nu ca spații presupus conforme;
- constatările privind defecte, pericole sau neconformități urgente se escaladează fără a aștepta raportul final.

3.4.3 Coordonarea interdisciplinară

Investigația se coordonează cu arhitectura, structura, instalațiile electrice, comunicațiile, securitatea la incendiu și cerințele de exploatare. Proiectantul de securitate nu validează în locul specialistului competent aspecte care depășesc domeniul său, dar trebuie să le identifice și să solicite confirmarea. Interfețele critice — de exemplu deblocarea la incendiu, alimentarea de siguranță, spațiile tehnice și rețelele partajate — se verifică împreună cu proprietarii lor.

3.4.4 Erori frecvente

- vizita efectuată fără plan și fără lista ipotezelor de confirmat;
- măsurători fără unitate, instrument, poziție sau condiții;
- fotografii care nu pot fi corelate cu planurile;
- omiterea condițiilor nocturne, sezoniere ori de vârf;
- confirmarea verbală a unor interfețe critice fără responsabil și dovadă.

3.5 Stabilirea cerințelor de securitate

În această etapă, riscurile, obligațiile, nevoile utilizatorilor și constrângerile sunt transformate în cerințe care pot ghida proiectarea și verificarea. Cerința descrie rezultatul necesar, nu doar mijlocul preferat. Ea trebuie să fie suficient de clară pentru a putea fi alocată, proiectată, testată și urmărită pe întregul ciclu de viață.

3.5.1 Formularea cerințelor

O cerință bine formulată identifică subiectul, funcția sau performanța, condiția de aplicare și criteriul observabil. Expresia trebuie să evite adjectivele nedeterminate precum „rapid”, „adecvat”, „inteligent” ori „înaltă calitate”, dacă acestea nu sunt definite. Când o valoare nu poate fi stabilită încă, cerința se marchează provizorie și primește termen de închidere; nu se ascunde incertitudinea într-o formulare vagă.

3.5.2 Analiza calității și a conflictelor

Cerințele se verifică individual și ca ansamblu pentru necesitate, unicitate, claritate, completitudine, fezabilitate, consecvență, verificabilitate și trasabilitate. Cerințele compuse se separă atunci când părțile lor pot avea metode sau stări diferite. Conflictele dintre securitate, evacuare, protecția datelor, operare, patrimoniu, rețea și buget se soluționează prin procesul din Capitolul 2 și se reflectă în registru.

3.5.3 Alocarea și trasabilitatea

Cerințele nu se alocă automat unui echipament. Unele sunt realizate prin combinația dintre tehnologie, procedură și răspuns uman. Matricea de trasabilitate trebuie să arate lanțul: sursă sau scenariu — cerință — funcție — element de arhitectură — specificație — dovadă de verificare. Orice componentă fără cerință asociată este analizată ca posibilă supradimensionare; orice cerință fără soluție și metodă de test este o lacună.

3.5.4 Erori frecvente

- formularea cerințelor ca listă de produse sau cantități;
- cerințe fără condiții de mediu, exploatare ori defect;
- amestecarea mai multor rezultate într-o singură frază imposibil de testat unitar;
- prioritizare exclusiv comercială, fără raportare la risc și conformitate;
- modificarea cerințelor în planșe fără actualizarea registrului.

3.6 Definirea conceptului de securitate

Conceptul de securitate descrie modul în care măsurile fizice, tehnice, organizaționale și umane vor coopera pentru prevenirea, detectarea, evaluarea, întârzierea și tratarea scenariilor relevante. El face legătura dintre cerințe și arhitectură și trebuie stabilit înaintea dimensionării detaliate. Conceptul răspunde la întrebarea „cum va funcționa protecția?”, fără a coborî prematur la nivelul fiecărui produs.

3.6.1 Construirea conceptului operațional

Pentru fiecare scenariu prioritar se descriu starea inițială, actorul sau evenimentul declanșator, barierele preventive, punctul de detectare, informația necesară evaluării, modul de alarmare, responsabilul pentru decizie, acțiunea de răspuns, continuitatea în caz de defect și condiția de revenire. Se precizează ce realizează sistemul automat, ce confirmă operatorul și ce depinde de intervenția externă.

Conceptul include zonarea de securitate, nivelurile de acces, straturile de protecție, relația dintre perimetru, anvelopă, spațiu și activ, precum și principiile pentru ore normale, program redus, evacuare, avarie, mentenanță și incident. Funcțiile care pot produce efecte nedorite — blocarea unei uși, urmărirea video, transmiterea datelor sau acționarea automată — primesc condiții și autorizări explicite.

3.6.2 Analiza alternativelor

- se definesc cel puțin alternativele rezonabile, inclusiv măsuri procedurale sau fizice care pot reduce dependența de tehnologie;
- criteriile se stabilesc înaintea clasamentului: reducerea riscului, conformitate, performanță, operabilitate, reziliență, mentenabilitate, protecția datelor, cost și adaptabilitate;
- compararea se bazează pe ipoteze comune și pe costul total al ciclului de viață, nu numai pe investiția inițială;
- avantajele și limitele se prezintă separat; un scor total nu trebuie să ascundă neîndeplinirea unei cerințe obligatorii;
- alternativa selectată și motivele respingerii celorlalte se păstrează în registrul deciziilor.

3.6.3 Validarea cu utilizatorii

Conceptul se parcurge prin scenarii cu utilizatorii și responsabili de intervenție. Validarea urmărește dacă fluxurile sunt realizabile, dacă volumul alarmelor poate fi gestionat, dacă rolurile sunt disponibile în intervalele necesare și dacă măsurile nu creează practici de ocolire. Un concept tehnic performant, dar imposibil de operat, nu este valid.

3.6.4 Erori frecvente

- echivalarea conceptului cu o schemă de echipamente;
- ignorarea timpului și capacității reale de răspuns;
- proiectarea numai pentru regimul normal, fără avarie sau mentenanță;
- selectarea alternativei exclusiv după costul inițial;
- validarea fără operatorii și disciplinele care vor utiliza interfețele.

3.7 Elaborarea arhitecturii sistemului

Arhitectura transformă conceptul în structuri funcționale și tehnice. Ea definește subsistemele, componentele majore, zonele, fluxurile de informație și energie, interfețele, limitele de încredere, dependențele și modurile de funcționare. Arhitectura trebuie să fie suficient de stabilă înaintea selecției detaliate, deoarece incompatibilitățile identificate târziu generează reproiectare, costuri și vulnerabilități.

3.7.1 Dezvoltarea arhitecturii

Proiectantul descompune funcțiile fără a pierde legătura cu cerințele și stabilește ce element detectează, decide, transmite, înregistrează, afișează, alimentează și permite acțiunea. Se definesc zonele de securitate fizică și logică, punctele de concentrare, căile principale și de rezervă, sursele de timp, identitatea, administrarea, jurnalizarea și limitele dintre sistemele proprii și serviciile externe.

Interfețele se descriu prin părți, direcția fluxului, informația sau energia transferată, protocol, stare normală, timp, prioritate, condiții de defect, responsabilitate și metodă de test. Formularea generică „se integrează” este insuficientă. Pentru fiecare integrare trebuie stabilit cine inițiază evenimentul, cine confirmă, ce se întâmplă la pierderea comunicației și cum se evită comenzi contradictorii.

3.7.2 Reziliență și moduri degradate

- identificarea punctelor unice de defect și evaluarea necesității redundanței, diversității ori degradării controlate;
- separarea alimentărilor și comunicațiilor atunci când o cauză comună poate anula mai multe funcții critice;
- definirea comportamentului la lipsă de energie, rețea, timp sincronizat, server, stocare, licență, comunicație sau operator;
- prioritizarea alarmelor și limitarea efectelor în cascadă;
- protejarea funcțiilor administrative și a configurațiilor prin roluri, autentificare, jurnalizare și copii de siguranță;
- rezervarea capacității pentru vârf, extindere și actualizare, fără a accepta resurse nominale insuficiente.

3.7.3 Controlul interdependențelor

Arhitectura se coordonează cu rețeaua, energia, construcția, HVAC, iluminatul, detecția incendiului, evacuarea și procesele organizației. Dependențele externe se introduc în registru împreună cu proprietarul, nivelul de serviciu, ipotezele și planul de verificare. Un serviciu partajat nu se consideră disponibil sau sigur numai pentru că există; capacitatea, continuitatea și administrarea lui trebuie confirmate.

3.7.4 Erori frecvente

- desenarea unei topologii fără fluxuri și stări definite;
- dependențe față de rețele sau surse externe neconfirmate;

- integrare bazată pe promisiuni comerciale fără interfață și test;
- redundanță aparentă cu elemente care au aceeași cauză comună de defect;
- omiterea administrării, jurnalizării și actualizării din arhitectură.

3.8 Dimensionarea și alegerea echipamentelor

Dimensionarea demonstrează că arhitectura poate furniza performanța cerută în condițiile reale, iar alegerea echipamentelor stabilește produse și configurații adecvate acestei demonstrații. Procesul pornește de la calcule și criterii, nu de la catalog. O caracteristică declarată a produsului devine relevantă numai dacă este valabilă pentru configurația, mediul și modul de utilizare proiectate.

3.8.1 Domenii de dimensionare

- acoperire, câmp de detecție, zone moarte și condiții care influențează detectarea;
- câmp vizual, densitate de pixeli, rezoluție efectivă, iluminare, mișcare, compresie și scop operațional pentru video;
- capacitate de utilizatori, credențiale, evenimente, uși, reguli, tranzacții și timpi pentru control acces;
- bandă, latență, pierderi, disponibilitate, adresare, segmentare și sincronizare pentru comunicații;
- stocare utilă, perioadă, redundanță, rată de înregistrare, evenimente și rezervă de creștere;
- puteri, curenți, căderi de tensiune, protecții, selectivitate, autonomie, încărcare și temperatură pentru alimentare;
- capacități de procesare, licențiere, sesiuni, operatori, afișare și performanță în regim de vârf;
- spații, disipare termică, masă, fixare, acces de service, mediu și compatibilitate electromagnetică.

3.8.2 Alegerea și echivalența produselor

Fișa de selecție corelează fiecare produs cu cerințele alocate, standardele relevante, declarațiile de conformitate, clasele de mediu, limitările, interfețele, versiunile software, accesoriile obligatorii și condițiile de mentenanță. Compatibilitatea nu se deduce doar din utilizarea aceluiași protocol sau producător; se confirmă pentru funcțiile, versiunile și configurațiile proiectate.

Specificarea prin performanță rămâne regula. Marca sau modelul se poate utiliza atunci când este necesar pentru compatibilitatea justificată, continuitatea unei configurații ori alt temei permis, cu respectarea cadrului aplicabil. Soluțiile echivalente sunt evaluate pe toate criteriile relevante, inclusiv funcțiile ascunse în licențe, securitatea actualizărilor, disponibilitatea pieselor și costul de exploatare.

3.8.3 Controlul calculelor și rezervelor

Fiecare calcul trebuie să indice formula sau metoda, datele de intrare, unitățile, sursa parametrilor, ipotezele, coeficienții, rezultatul, limita admisă și rezerva. Fișierele de calcul se versionează și se revizuiesc independent pentru funcțiile critice. Rotunjirile, valori tipice și condițiile favorabile nu se folosesc pentru a crea o rezervă aparentă. Sensibilitatea la parametri incerti se analizează acolo unde o variație rezonabilă poate schimba selecția.

3.8.4 Erori frecvente

- preluarea valorilor maxime din fișa de produs ca valori garantate în instalație;
- calcularea unei medii care ascunde condiția cea mai defavorabilă;
- ignorarea accesoriilor, licențelor și versiunilor necesare funcției;
- acceptarea compatibilității numai pe baza mărcii sau a protocolului declarat;
- supradimensionarea fără justificare, care crește complexitatea și suprafața de defect.

3.9 Elaborarea documentației tehnice

Documentația tehnică transformă soluția proiectată într-un ansamblu univoc de instrucțiuni și dovezi care poate fi contractat, executat, verificat, pus în funcțiune și menținut. Un proiect nu este complet dacă intenția autorului poate fi înțeleasă numai prin explicații verbale. Nivelul de detaliu se adaptează fazei, dar fiecare document trebuie să aibă un scop, o stare și o relație controlată cu celelalte piese.

3.9.1 Conținutul pachetului de proiect

- foaia de titlu, identificarea proiectului, semnăturile, starea emiterii și borderoul documentelor;
- memoriul tehnic cu scop, bază de proiectare, descriere funcțională, criterii, limite, ipoteze și coordonări;
- planurile de amplasare, zonare, acoperire, trasee, alimentare și interfețe, la scări și niveluri de detaliu adecvate;
- schemele bloc, funcționale, de conexiuni, alimentare, rețea și integrare;
- detaliile de montaj relevante pentru performanță, mediu, acces, protecție și mentenanță;
- specificațiile tehnice și listele de cantități corelate cu cerințele și desenele;
- memoriile de calcul, fișele de selecție și dovezile de conformitate ori echivalență;
- matricea cauză—efect, lista punctelor, nomenclatorul, planul de adresare și convențiile de identificare;
- planul de inspecții, încercări și testare, cu criterii de acceptanță derivate din cerințe;
- cerințele de predare, instruire, documentație finală, backup, licențe, parole administrate și date de configurare.

3.9.2 Coerența documentelor

O singură informație trebuie să aibă o sursă controlată. Cantitățile, codurile, denumirile, zonele, adresele și interfețele se verifică între planuri, scheme, liste, specificații și calcule. În caz de contradicție, documentația trebuie să stabilească ordinea de prevalență și mecanismul de clarificare; această regulă nu justifică menținerea intenționată a contradicțiilor.

Desenele trebuie să permită localizarea și execuția, fără aglomerare care ascunde informația. Simbolurile, culorile, straturile și codurile se definesc în legendă. Notele generale nu înlocuiesc detaliile specifice, iar sintagma „conform situației din teren” nu transferă instalatorului o decizie de proiectare care trebuia fundamentată înainte de execuție.

3.9.3 Controlul documentelor și al securității

Fiecare piesă primește cod, titlu, revizie, dată, autor, verifikator, stare și paginare. Emiterea pentru informare, coordonare, avizare, ofertare sau execuție trebuie distinsă. Reviziile indică modificările și documentele înlocuite; copiile retrase nu rămân disponibile ca versiuni valide. Fișierele editabile, modelele, parolele, configurațiile și planurile cu vulnerabilități se predau și se arhivează prin canale și drepturi adecvate sensibilității lor.

3.9.4 Erori frecvente

- planuri, scheme și liste cu revizii sau coduri necorelate;
- specificații copiate din catalog, fără condițiile aplicației;
- cantități care nu pot fi urmărite la planuri și calcule;
- note generale care lasă instalatorului alegeri critice;
- emiterea fișierelor sensibile fără controlul accesului și al distribuției.

3.10 Verificarea și validarea proiectului

Verificarea și validarea reprezintă controlul final al proiectării înaintea emiterii pentru execuție. Verificarea răspunde întrebării dacă proiectul a fost elaborat corect în raport cu cerințele, regulile, calculele și propriile sale specificații. Validarea răspunde întrebării dacă soluția proiectată este potrivită pentru nevoia reală, scenariile, utilizatorii și condițiile obiectivului. Cele două activități se completează și nu se substituie.

3.10.1 Planul de verificare

Planul stabilește obiectul, criteriile, metodele, responsabilitățile, nivelul de independență și înregistrările. Metodele pot include analiza documentară, recalcularea, inspecția, modelarea, simularea, compararea cu standarde, revizuirea interdisciplinară, demonstrația unui prototip sau parcurgerea scenariilor. Intensitatea verificării se adaptează criticității; elementele cu consecințe mari, ipoteze sensibile ori soluții neuzuale primesc control suplimentar.

Verificatorul trebuie să aibă acces la cerințe și justificări, nu numai la planșele finale. Observațiile se clasifică după severitate și se leagă de piesa, cerința și riscul afectat. Închiderea unei observații necesită dovada corecției și, după caz, reverificarea documentelor dependente. Răspunsul „se va rezolva în execuție” nu este acceptabil pentru o decizie care aparține proiectării.

3.10.2 Domeniile minime de control

- completitudinea și actualitatea bazei legale, normative și contractuale;
- acoperirea tuturor cerințelor și trasabilitatea către soluții și teste;
- corectitudinea calculelor, unităților, ipotezelor, coeficienților și rezervelor;
- compatibilitatea componentelor, versiunilor, licențelor, mediilor și interfețelor;
- coordonarea dintre subsisteme și discipline, inclusiv prevenirea conflictelor cu evacuarea și siguranța vieții;
- funcționarea normală, la vârf, în mentenanță, la defect și după restabilire;
- protecția datelor, securitatea cibernetică, administrarea și jurnalizarea;
- executabilitatea, accesibilitatea pentru mentenanță, testabilitatea și posibilitatea de recepție;
- coerența codurilor, cantităților, reviziilor și specificațiilor în toate documentele;
- închiderea ipotezelor, abaterilor, clarificărilor și neconformităților cu impact critic.

3.10.3 Validarea soluției

Validarea se realizează cu beneficiarul, utilizatorii și specialiștii relevanți prin parcurgerea scenariilor aprobate. Se verifică dacă informația furnizată de sistem permite decizia operațională, dacă timpii și rolurile sunt realiste, dacă modurile degradate sunt acceptabile și dacă soluția nu generează efecte care determină ocolirea ei. Pentru elemente cu incertitudine tehnică ridicată se pot solicita demonstrații, probe de concept, mostre, mock-up-uri sau teste de amplasament înainte de înghețării definitive.

Aprobarea beneficiarului nu înlocuiește verificarea tehnică, iar verificarea tehnică nu transferă beneficiarului responsabilitatea proiectantului. Acceptarea informată trebuie să indice cerințele îndeplinite, limitările, riscurile reziduale relevante pentru soluție, acțiunile rămase și condițiile care trebuie menținute în execuție și exploatare.

3.10.4 Erori frecvente

- verificarea limitată la ortografie, format și existența planșelor;
- revizuirea fără registrul cerințelor și fără calcule;
- validarea exclusiv de către persoana care a solicitat achiziția, fără utilizatori;
- închiderea observațiilor prin răspuns, fără dovada corecției;
- confundarea validării proiectului cu recepția instalației executate, tratată distinct în Capitolul 7.

Închiderea procesului de proiectare

Închiderea Capitolului 3 nu înseamnă încetarea responsabilității de proiectare. După emiterea pentru execuție, clarificările, propunerile de echivalență și modificările din teren se supun aceluiași lanț de trasabilitate și control. Orice schimbare care alterează o cerință, o interfață, un calcul sau un criteriu de test trebuie analizată și aprobată înainte de implementare, iar documentația se actualizează la starea corespunzătoare.

Referințe metodologice pentru Capitolul 3

Referințele următoare fundamentează principiile de ciclu de viață, management al cerințelor, risc, arhitectură și ghidurile de aplicație. Ele nu devin automat obligatorii; statutul și ediția aplicabile fiecărui proiect se stabilesc conform Capitolului 2. Referințele au fost verificate în sursele oficiale la 10.08.2026.

[P1] ISO/IEC/IEEE 15288:2023 — Systems and software engineering — System life cycle processes — sursa oficială (cadru pentru procesele ciclului de viață al sistemelor)

[P2] ISO/IEC/IEEE 29148:2018 — Systems and software engineering — Life cycle processes — Requirements engineering — sursa oficială (procese și elemente informaționale pentru cerințe)

[P3] ISO/IEC/IEEE 24748-2:2024 — Guidelines for the application of ISO/IEC/IEEE 15288 — sursa oficială (adaptarea și aplicarea proceselor de ciclu de viață)

[P4] ISO 31000:2018 — Risk management — Guidelines — sursa oficială (principii, cadru și proces pentru managementul riscului)

[P5] ISO 21502:2020 — Project, programme and portfolio management — Guidance on project management — sursa oficială (practici de management aplicabile proiectelor)

[P6] ISO/IEC/IEEE 42010:2011 — Systems and software engineering — Architecture description — sursa oficială (descrierea și controlul arhitecturilor)

[P7] IEC 62676-4:2025 — Video surveillance systems for use in security applications — Part 4: Application guidelines — sursa oficială (planificare, proiectare, instalare, testare, punere în funcțiune și mentenanță)

[P8] IEC 60839-11-2:2014 — Electronic access control systems — Application guidelines — sursa oficială (planificare, instalare, punere în funcțiune, mentenanță și documentare)

CAPITOLUL 4

Context, cerințe și riscuri

Prezentul capitol definește conținutul analitic prin care realitatea obiectivului este transformată într-o bază de cerințe controlată. Capitolul 3 a stabilit când și prin ce porți de control se desfășoară proiectarea; Capitolul 4 precizează ce trebuie înțeles despre obiectiv, cum se utilizează informația privind riscul și cum se formulează cerințe tehnice suficient de clare pentru proiectare, verificare și recepție.

În sensul S.I.G.M.A., contextul, riscul și cerințele nu sunt documente independente care se predau succesiv, ci trei reprezentări corelate ale aceleiași probleme. Contextul explică obiectivele, activele, procesele, persoanele și constrângerile. Analiza riscului explică evenimentele nedorite, cauzele, vulnerabilitățile și consecințele. Cerințele stabilesc rezultatele pe care ansamblul măsurilor trebuie să le realizeze în condiții definite. Orice ruptură între aceste reprezentări produce fie măsuri fără justificare, fie riscuri fără tratament, fie funcții care nu pot fi testate.

Modelul de lucru și delimitarea responsabilităților

Proiectantul nu reface, nu substituie și nu modifică unilateral analiza de risc la securitatea fizică întocmită de persoana competentă. El trebuie însă să îi verifice utilizabilitatea ca intrare de proiectare: identificarea obiectivului, data și starea documentului, domeniul acoperit, coerența cu situația constatată, claritatea măsurilor și existența informațiilor necesare dimensionării. O neconcordanță se înregistrează și se transmite pentru clarificare; nu se rezolvă prin modificarea tacită a scorului de risc sau prin alegerea unei soluții convenabile.

Analiza complementară realizată în proiectare privește fezabilitatea, interfețele, modurile de defect, riscurile introduse de soluție, protecția datelor, securitatea cibernetică și condițiile de exploatare. Ea nu dobândește prin denumire efectele juridice ale analizei de risc la securitatea fizică. Dacă documentul obligatoriu lipsește, are termenul de revizuire depășit ori nu mai corespunde obiectivului, proiectarea finală se suspendă sau se emite numai într-o stare condiționată, fără a prezenta ipotezele drept cerințe aprobate.

4.1 Contextul obiectivului

Analiza contextului stabilește cadrul în care trebuie să funcționeze securitatea. Obiectivul nu este redus la clădire și program; el include scopul organizației, procesele, persoanele, activele, relațiile cu exteriorul, infrastructurile de care depinde și condițiile în care o măsură poate fi operată. Aceeași configurație tehnică poate avea eficacități diferite în funcție de disciplină operațională, timp de intervenție, iluminat, nivelul de ocupare, competența operatorilor sau continuitatea comunicațiilor.

4.1.1 Domeniile contextului

4.1.2 Limite și interfețe

Limitele se definesc fizic, funcțional, organizațional, tehnologic și informațional. O limită fizică arată unde începe și se termină obiectivul; una funcțională, ce activități și funcții intră în proiect; una organizațională, cine deține decizia; una tehnologică, ce sisteme și servicii sunt incluse; iar una informațională, ce date pot fi colectate,

transmise și păstrate. Interfețele care traversează limitele se descriu împreună cu proprietarul, condițiile de disponibilitate și răspunderea pentru testare.

4.1.3 Validarea profilului contextual

Profilul contextual se validează prin documente, interviuri și constatări la amplasament. Diferența dintre practica declarată și practica observată se păstrează ca informație relevantă. Contextul nu este înghețat definitiv: modificarea programului, destinației, amenajării, valorilor deținute, fluxurilor ori infrastructurii poate schimba atât riscul, cât și cerințele. De aceea, registrul contextual trebuie să indice sursa, data, responsabilul și evenimentul care declanșează reverificarea.

4.2 Identificarea și clasificarea activelor

Un activ este orice element a cărui afectare poate compromite un obiectiv al organizației. Inventarul nu se limitează la bunuri cu valoare monetară. Persoanele, informațiile, reputația, serviciile, capacitatea de a continua activitatea, cheile, credențialele, configurațiile și infrastructurile suport pot avea o criticitate mai mare decât echipamentele sau mărfurile vizibile.

4.2.1 Categoriile și relații

- persoane: angajați, public, vizitatori, personal vulnerabil, operatori, intervenție și persoane cu responsabilități critice;
- bunuri și valori: numerar, mărfuri, colecții, medicamente, arme, documente, materii ori echipamente atractive sau periculoase;
- informații și mijloace de acces: date personale, secrete, imagini, jurnale, parole, chei, carduri, certificate și copii de siguranță;
- procese și servicii: activități care trebuie menținute, timpi maximi de întrerupere, obligații față de public și dependențe contractuale;
- infrastructuri: energie, comunicații, climatizare, rețele, spații tehnice, căi de acces și sisteme a căror pierdere produce efecte în cascadă;
- încredere și conformitate: reputație, autorizații, dovezi, trasabilitate și capacitatea de a demonstra îndeplinirea obligațiilor.

Activele se leagă de proprietari, utilizatori, locații, procese și dependențe. O clasificare izolată poate rata efectul în cascadă: o cameră tehnică de valoare modestă poate susține toate comunicațiile, iar un set de credențiale poate permite accesul la mai multe zone critice. Relațiile dintre active trebuie reprezentate acolo unde compromiterea unuia amplifică impactul asupra celorlalte.

4.2.2 Atributele registrului de active

4.2.3 Criticitate și consecințe

Criticitatea se stabilește în raport cu obiectivele și consecințele, nu numai prin prețul de înlocuire. Se analizează vătămarea persoanelor, pierderea sau degradarea bunurilor, întreruperea activității, compromiterea informațiilor, efectele juridice, reputaționale și asupra mediului. Scările și criteriile trebuie definite înaintea evaluării, cu praguri verificabile acolo unde există date. Valorile estimate și judecățile calitative se marchează distinct, împreună cu nivelul de încredere.

4.3 Caracterizarea amenințărilor

Amenințarea reprezintă sursa potențială a unui eveniment nedorit. Caracterizarea sa trebuie să fie suficient de concretă pentru a informa proiectarea, dar să evite certitudini pe care datele nu le susțin. Etichete generale precum „efracție”, „furt” sau „vandalism” nu descriu capacitatea, intenția, oportunitatea, ținta, modul de acțiune ori condițiile în care evenimentul devine plauzibil.

4.3.1 Surse și tipologii

Se consideră amenințări intenționate externe și interne, acțiuni oportuniste sau planificate, erori și utilizări necorespunzătoare, evenimente tehnice ori de mediu și combinații ale acestora. În domeniul securității fizice, o defecțiune sau o eroare umană poate crea fereastra folosită ulterior de un actor ostil; de aceea, separarea analitică nu trebuie să ascundă succesiunile cauzale.

- actorul sau sursa: profil, acces legitim ori nelegitim, cunoaștere, resurse, motivație și toleranță la risc;
- ținta și efectul urmărit: sustragere, agresiune, acces, sabotaj, observare, alterare, întrerupere sau distrugere;
- modul de operare: apropiere, recunoaștere, instrumente, manipulare socială, folosirea credențialelor și evitarea detecției;
- condițiile favorizante: perioadă, ocupare, vizibilitate, evenimente, lucrări, schimburi de personal, întreruperi și degradări;
- indicatorii și sursele: incidente proprii, informații oficiale, tendințe locale, experiență sectorială și observații documentate.

4.3.2 Relevanță și plauzibilitate

O amenințare se reține atunci când există o legătură rezonabilă cu activele, amplasamentul și modul de funcționare. Absența incidentelor raportate nu dovedește absența amenințării; la fel, un eveniment mediatizat nu justifică automat o probabilitate ridicată. Se separă frecvența observată, posibilitatea tehnică și atractivitatea țintei. Sursele se datează, iar incertitudinea se exprimă explicit pentru a evita transformarea impresiei în fapt.

4.3.3 Evoluție și indicatori de schimbare

Catalogul amenințărilor se leagă de indicatori care pot modifica proiectul: incidente noi, schimbarea valorilor, apariția unei metode de atac, variația criminalității, lucrări care deschid trasee, publicitate nedorită, modificarea personalului sau dependența de servicii noi. Monitorizarea acestor indicatori aparține exploatarei și poate declanșa revizuirea riscului și a cerințelor.

4.4 Identificarea vulnerabilităților

Vulnerabilitatea este o condiție care poate fi exploatată de o amenințare sau care poate amplifica probabilitatea ori consecința unui eveniment. Ea nu trebuie confundată cu absența unui anumit produs. Formularea „nu există cameră” descrie o soluție lipsă; vulnerabilitatea relevantă poate fi lipsa capacității de a observa și reconstrui un eveniment într-o zonă în care această funcție este necesară.

4.4.1 Domenii de examinare

4.4.2 Dovada și condiția de exploatare

Constatarea vulnerabilității trebuie susținută prin observație, măsurare, document, test, incident, comparație cu o cerință sau judecată profesională argumentată. Se notează locația, starea, perioada, configurația și sursa. Vulnerabilitățile temporare, precum lucrările ori defectele, se diferențiază de cele structurale. O măsură declarată existentă nu se consideră eficace fără confirmarea funcționării, configurării, utilizării și mentenanței sale.

4.4.3 Vulnerabilități create de soluție

Proiectul poate introduce vulnerabilități noi: o integrare extinde suprafața de atac; o ușă controlată poate afecta evacuarea; o cameră poate crea intruziuni disproporționate în viața privată; o automatizare poate elimina verificarea umană; o redundanță aparentă poate depinde de aceeași sursă. Aceste efecte se analizează înaintea selecției finale și se transformă în cerințe de arhitectură, configurare, testare sau operare.

4.5 Construirea scenariilor de securitate

Scenariul leagă activele, amenințările, vulnerabilitățile și consecințele într-o succesiune inteligibilă. El este unitatea de lucru prin care analiza devine proiectabilă: permite stabilirea momentului în care evenimentul trebuie prevenit sau detectat, a întârzierii necesare, a informației de care are nevoie operatorul, a răspunsului posibil și a rezultatului acceptabil.

4.5.1 Structura minimă a scenariului

4.5.2 Nivelul de detaliu

Scenariul trebuie să fie suficient de specific pentru a diferenția căile și condițiile care impun măsuri diferite. Nu este necesară descrierea cinematografică a fiecărui pas și nici inventarea unor detalii fără suport. Scenariile echivalente pot fi grupate dacă au aceleași active, vulnerabilități, consecințe și cerințe de tratare; gruparea nu trebuie să ascundă calea cea mai defavorabilă sau un mod de operare care schimbă performanța necesară.

4.5.3 Scenarii normale, degradate și combinate

Pe lângă acțiunea intenționată în regim normal, se examinează indisponibilitatea alimentării, pierderea comunicației, mentenanța, lipsa operatorului, alarma multiplă, defectul comun și restabilirea după incident. Se includ combinațiile rezonabile care pot invalida soluția: pătrundere în timpul lucrărilor, folosirea unei credențiale valide în afara profilului, întreruperea comunicației concomitent cu alarma sau evacuarea care modifică regulile de acces.

4.6 Estimarea și evaluarea riscurilor

Estimarea riscului analizează probabilitatea și consecințele scenariilor în condițiile măsurilor existente. Evaluarea compară rezultatele cu criteriile aprobate pentru a decide prioritatea și necesitatea tratării. Metoda utilizată trebuie să fie compatibilă cu cadrul legal aplicabil, cu natura datelor și cu scopul deciziei. S.I.G.M.A. nu impune o singură formulă și nu înlocuiește grilele obligatorii; impune transparența ipotezelor, consecvența aplicării și trasabilitatea rezultatului.

4.6.1 Probabilitate, consecință și expunere

Probabilitatea poate reflecta frecvența, plauzibilitatea ori șansa producerii într-un interval definit. Consecința se evaluează pe dimensiuni relevante: persoane, bunuri, activitate, informații, conformitate, reputație și mediu. Atunci când se folosesc scări ordinale, nivelurile trebuie descrise prin criterii, nu numai prin cifre. Operațiile aritmetice asupra scorurilor sunt permise numai dacă metoda definește sensul lor și nu creează o precizie aparentă.

- intervalul și unitatea de analiză sunt explicate: eveniment, an, program, transport, campanie sau altă perioadă relevantă;
- se evaluează situația existentă, fără a credita măsuri doar planificate ori nefuncționale;
- se separă probabilitatea inițierii de probabilitatea succesului atunci când această distincție schimbă decizia;
- consecința maximă credibilă nu este confundată cu cea mai gravă consecință imaginabilă;
- sursele cantitative, estimările și judecata profesională sunt marcate distinct;
- nivelul de încredere și sensibilitatea la ipotezele critice însoțesc rezultatul.

4.6.2 Tehnici și proporționalitate

Tehnica se selectează în funcție de complexitate, calitatea datelor și decizia urmărită. Listele structurate, interviurile, analiza scenariilor, matricele, analiza bow-tie, analiza modurilor de defect, arborii de evenimente sau alte tehnici pot fi utilizate separat ori combinat, conform ghidurilor relevante [R4]. Proiectele cu consecințe ridicate, interdependențe sau tehnologii noi necesită o analiză mai profundă decât o simplă încadrare într-o matrice.

4.6.3 Controlul părtinirilor și al incertitudinii

Echipa trebuie să controleze ancorarea în soluția existentă, supraevaluarea incidentelor recente, normalizarea abaterilor, optimismul privind răspunsul și tendința de a ajusta scorul pentru a se încadra în buget. Ipotezele se testează prin întrebări de sensibilitate: ce rezultat se schimbă dacă timpul de intervenție crește, iluminarea scade, un sistem devine indisponibil sau valoarea activului se modifică? Dacă o variație plauzibilă schimbă categoria de risc, se adoptă o abordare prudentă ori se solicită date suplimentare.

4.7 Criterii de acceptare și prioritzare

Criteriile de risc exprimă condițiile în care un nivel de risc este considerat acceptabil, tolerabil numai cu controale sau inacceptabil. Ele trebuie stabilite ori confirmate înaintea clasificării, pentru a evita adaptarea pragurilor la rezultatul dorit. Criteriile provin din obligații legale, politici, obiective, consecințe maxime admise, continuitate, protecția persoanelor și capacitatea de răspuns.

4.7.1 Autoritatea și limitele acceptării

Acceptarea riscului aparține rolului desemnat de organizație, în limitele legii și ale competenței. Proiectantul explică implicațiile tehnice și diferențele dintre alternative; evaluatorul formulează concluziile în cadrul atribuțiilor sale; conducătorul unității sau proprietarul riscului își asumă decizia. Nicio aprobare internă nu poate transforma într-o opțiune o obligație legală, o cerință de siguranță a vieții ori o condiție impusă de autoritatea competentă.

4.7.2 Reguli de prioritzare

- se tratează cu prioritate riscurile care pot produce vătămări grave, pierderi ireversibile sau încălcări obligatorii, chiar dacă frecvența estimată este redusă;
- se examinează riscurile agregate și cauzele comune, nu numai scorurile individuale;
- se consideră timpul disponibil pentru tratament și fereastra în care expunerea rămâne necontrolată;
- măsurile cu efect asupra mai multor scenarii pot primi prioritate, dacă nu creează dependențe sau consecințe disproporționate;
- incertitudinea ridicată nu justifică ignorarea; ea poate impune investigație, măsură provizorie ori rezervă de proiectare;
- prioritatea tehnică, ordinea de execuție și prioritatea bugetară se mențin distincte și se corelează documentat.

4.7.3 Decizii condiționate

Atunci când datele ori resursele nu permit închiderea imediată, decizia poate fi condiționată prin măsuri interimare, termen, responsabil și criteriu de revenire. Etapizarea este acceptabilă numai dacă starea intermediară este cunoscută și nu este prezentată drept conformitate finală. Registrul riscurilor păstrează motivele amânării, expunerea rămasă și evenimentul care impune escaladarea.

4.8 Selectarea măsurilor de tratare

Tratarea riscului urmărește modificarea probabilității, consecinței ori ambelor, printr-o combinație de măsuri fizice, tehnice, umane, procedurale și contractuale. Selectarea nu pornește de la subsistem, ci de la scenariu și obiectivul de tratament. O cameră, un detector sau un cititor de acces nu reprezintă singur o măsură completă dacă informația sa nu ajunge la un rol capabil să decidă și să acționeze.

4.8.1 Strategii și funcții

4.8.2 Evaluarea alternativelor

Alternativelor se compară prin reducerea estimată a riscului, acoperirea scenariilor, conformitate, fezabilitate, timp de implementare, interoperabilitate, securitate cibernetică, protecția datelor, ergonomie, mentenanță, disponibilitatea competențelor și costul total al ciclului de viață. Costul inițial este un criteriu legitim, dar nu poate fi singurul. O măsură care nu poate fi operată, testată sau menținută nu furnizează reducerea de risc presupusă.

4.8.3 Eficacitatea individuală și în ansamblu

Eficacitatea se estimează atât pe element, cât și pe lanțul prevenire–detectare–întârziere–răspuns–recuperare. Se verifică timpul: alarma trebuie generată, transmisă, verificată și tratată înainte ca actorul să atingă obiectivul ori consecința să devină inacceptabilă. Măsurile independente reduc riscul numai dacă nu au aceeași cauză comună de defect. Compensarea unei slăbiciuni se justifică prin performanță echivalentă demonstrabilă, nu prin numărul de echipamente adăugate.

4.8.4 Planul de tratare

Planul de tratare identifică scenariul și riscul vizat, măsura, proprietarul, cerințele derivate, resursele, termenul, dependențele, criteriul de finalizare, metoda de verificare și riscul rezidual anticipat. Pentru proiectare, planul devine sursă a cerințelor; pentru implementare, devine bază de etapizare și control. Schimbarea unei măsuri după aprobare necesită reevaluarea lanțului de scenarii și a cerințelor dependente.

4.9 Riscul rezidual, acceptarea și monitorizarea

Riscul rezidual este riscul rămas după luarea în considerare a măsurilor existente și planificate, evaluate la performanța realistă. El nu este sinonim cu riscul „zero” și nu se declară redus numai prin includerea unui echipament în proiect. Estimarea se actualizează după definirea soluției, după testarea instalației și ori de câte ori condițiile care susțin eficacitatea se modifică.

4.9.1 Condițiile acceptării

Documentul de acceptare trebuie să indice riscul, măsurile considerate, dovezile disponibile, limitările, incertitudinea, perioada de valabilitate și persoana autorizată. Riscurile care depășesc autoritatea, contravin unei obligații sau afectează alte părți fără consultare se escaladează. Acceptarea temporară include termen, măsură compensatorie și condiție de încetare.

4.9.2 Riscuri secundare și efecte adverse

Măsurile pot crea riscuri secundare: blocarea necorespunzătoare a unei căi, supraveghere disproporționată, stocarea excesivă a datelor, dependență de un serviciu extern, privilegii administrative concentrate ori complexitate care favorizează eroarea. Aceste riscuri se înregistrează separat, se evaluează și se tratează. Beneficiul de securitate nu elimină obligația de proporționalitate, protecție a datelor și coordonare cu siguranța vieții [R7][R8].

4.9.3 Indicatori și declanșatori de revizuire

- incident, tentativă, alarmă repetată, alarmă neconfirmată sau creșterea timpului de răspuns;
- modificarea activelor, valorilor, destinației, programului, fluxurilor ori limitelor obiectivului;
- schimbarea amenințărilor, vulnerabilităților, vecinătăților sau infrastructurilor externe;
- defecte, indisponibilități, rezultate de mentenanță și degradarea indicatorilor de performanță;
- modificări software, de rețea, integrare, furnizor, licențiere sau suport tehnic;
- schimbări legislative, normative, contractuale ori constatări ale autorităților și auditului.

Indicatorii se asociază cu praguri, proprietari și acțiuni. Monitorizarea fără regulă de escaladare produce informație, nu control. Datele din exploatare se utilizează pentru revizuirea ipotezelor și pentru calibrarea cerințelor, cu păstrarea legalității, integrității și perioadelor de retenție.

4.10 Transformarea riscurilor în cerințe tehnice

Transformarea riscurilor în cerințe este punctul în care analiza devine contractabilă și verificabilă. Cerința descrie o nevoie sau un rezultat necesar, nu preferința pentru o tehnologie. Ea păstrează legătura cu sursa — obligație, scenariu, măsură de tratament, utilizator, interfață ori condiție de exploatare — și include criteriul prin care îndeplinirea va fi demonstrată.

4.10.1 Surse și categorii de cerințe

Baza de cerințe include cerințe funcționale, de performanță, de interfață, de mediu, disponibilitate și reziliență, utilizabilitate, protecția informațiilor, conformitate și ciclu de viață. Clasificarea ajută la verificarea completitudinii, dar o cerință poate avea mai multe atribute; se păstrează un singur proprietar și o singură formulare controlată.

4.10.2 Reguli de formulare

O cerință de calitate este necesară, corectă, neechivocă, completă, fezabilă, singulară, verificabilă, compatibilă cu celelalte cerințe și trasabilă [R5]. Ea indică subiectul, acțiunea sau rezultatul, condițiile, criteriul de performanță și metoda ori nivelul de verificare. Termenii vagi — rapid, adecvat, suficient, modern, inteligent, acoperire completă — se înlocuiesc cu criterii observabile sau cu referințe controlate.

Exemplu metodologic: în loc de „se montează o cameră performantă la acces”, cerința trebuie să definească scopul operațional, zona, condițiile de iluminare și mișcare, informația care trebuie obținută, durata și metoda de verificare. Valorile concrete se stabilesc prin analiza proiectului și standardele aplicabile; ele nu se introduc arbitrar pentru a justifica un produs deja ales.

4.10.3 Atribute, prioritate și acceptanță

Prioritatea nu se confundă cu ordinea implementării. O cerință obligatorie poate fi executată într-o etapă ulterioară numai dacă starea intermediară rămâne legală și riscul este controlat. Cerințele critice primesc criterii de verificare mai stricte, independență adecvată și control sporit al modificărilor. Cerințele nefezabile sau contradictorii nu sunt eliminate tacit; se întorc proprietarului pentru decizie documentată.

4.10.4 Trasabilitate, bază aprobată și modificări

Matricea de trasabilitate leagă contextul și riscul de cerințe, funcții, elemente de arhitectură, documente și teste. Legătura trebuie să funcționeze în ambele sensuri: fiecare risc tratat conduce la cerințe și dovezi, iar fiecare element relevant al soluției are o justificare. Cerințele aprobate formează baza de referință; după înghețare, modificarea este analizată pentru efecte asupra riscului, interfețelor, calculelor, costului, termenului, protecției datelor și testelor.

Închiderea Capitolului 4

Rezultatele Capitolului 4 constituie baza tehnică pentru proiectarea subsistemelor din Capitolul 5. Ele trebuie să includă: profilul contextual validat; registrul activelor și dependențelor; catalogul amenințărilor și vulnerabilităților; scenariile; referința la evaluarea riscurilor; criteriile și prioritățile; planul de tratare; riscurile reziduale și autoritatea de acceptare; registrul cerințelor; precum și matricea de trasabilitate.

Dacă o informație critică rămâne necunoscută, aceasta se tratează ca ipoteză controlată, cu responsabil, termen și efectul neconfirmării. Nu se trece la dimensionare definitivă atunci când ipoteza poate schimba gradul, arhitectura, acoperirea, autonomia, interfața, capacitatea sau criteriul de testare. Disciplina suspendării unei decizii nefundamentate este parte a calității profesionale, nu o întârziere administrativă.

Referințe metodologice pentru Capitolul 4

Referințele următoare susțin delimitarea rolurilor, procesul de management al riscului, tehnicile de evaluare, ingineria cerințelor, continuitatea și protecția informațiilor. Statutul și ediția aplicabile fiecărui proiect se stabilesc conform Capitolului 2. Sursele au fost verificate la 10.08.2026.

- [R1] Instrucțiunile M.A.I. nr. 9/2013 privind efectuarea analizelor de risc la securitatea fizică — sursa oficială (Portal Legislativ; aplicabilitatea se verifică în contextul modificărilor din 2026)
- [R2] H.G. nr. 301/2012 și Normele metodologice de aplicare a Legii nr. 333/2003 — sursa oficială (inclusiv cerințele privind analiza și măsurile de securitate)
- [R3] ISO 31000:2018 — Risk management — Guidelines — sursa oficială (principii, cadru și proces; ediție confirmată și în curs de revizuire)

- [R4] IEC 31010:2019 — Risk management — Risk assessment techniques — sursa oficială (selectarea și aplicarea tehnicilor de evaluare)
- [R5] ISO/IEC/IEEE 29148:2018 — Requirements engineering — sursa oficială (proces și caracteristici ale cerințelor; o nouă ediție este în dezvoltare)
- [R6] ISO 31073:2022 — Risk management — Vocabulary — sursa oficială (terminologie generică pentru managementul riscului)
- [R7] Regulamentul (UE) 2016/679 privind protecția datelor cu caracter personal — sursa oficială (principii, legalitate și protecția datelor prin proiectare)
- [R8] EDPB, Guidelines 3/2019 on processing of personal data through video devices — sursa oficială (versiune finală, 30.01.2020)
- [R9] ISO/IEC 27005:2022 — Guidance on managing information security risks — sursa oficială (riscuri privind informația și componentele conectate)
- [R10] ISO 22301:2019 — Business continuity management systems — Requirements — sursa oficială (continuitate, reziliență și recuperare; include Amd 1:2024)

CAPITOLUL 5

Proiectarea subsistemelor

Capitolul stabilește modul în care cerințele de securitate aprobate sunt transformate în subsisteme tehnice coerente, dimensionate, verificabile și exploatabile. Proiectarea nu începe cu alegerea echipamentelor, ci cu funcțiile necesare pentru scenariile tratate, condițiile reale ale obiectivului și criteriile de acceptare. Soluția rezultată trebuie să poată fi urmărită de la risc la cerință, de la cerință la elementul de proiect și de la element la proba prin care conformitatea va fi demonstrată.

5.1 Principii comune de proiectare

Principiile comune se aplică tuturor subsistemelor și interfețelor, indiferent de tehnologie. Ele asigură compatibilitatea soluției cu arhitectura de securitate, cu mediul construit, cu activitatea beneficiarului și cu ciclul de viață previzibil.

5.1.1 Lanțul funcțional și apărarea în profunzime

Proiectantul examinează întregul lanț prevenire–descurajare–detectare–confirmare–întârziere–comunicare–răspuns–recuperare. Un subsistem poate contribui la mai multe funcții, însă existența lui nu dovedește automat eficacitatea lanțului. Pentru fiecare scenariu se verifică dacă evenimentul poate fi observat suficient de devreme, dacă informația ajunge la un operator competent și dacă timpul disponibil permite intervenția prevăzută.

5.1.2 Cerințe, performanță și criterii de acceptare

Specificația tehnică definește rezultate măsurabile: zona protejată, condițiile de mediu, probabilitatea ori calitatea detecției, informația vizuală necesară, timpul de procesare, disponibilitatea, autonomia, retenția, jurnalizarea, comportarea la defect și limitele de integrare. Formulările exclusiv comerciale sau expresii precum „performant”, „de ultimă generație” ori „compatibil” fără criteriu sunt insuficiente.

5.1.3 Zonare, criticitate și separare

Zonele tehnice se derivă din zonele de securitate și din fluxurile reale, nu numai din împărțirea arhitecturală. Se identifică limitele, punctele de trecere, activele critice, spațiile cu regim distinct, căile de atac și punctele unice de defect. Separarea fizică, logică și funcțională trebuie să împiedice propagarea necontrolată a unei defecțiuni sau compromiteri.

5.1.4 Selectarea și compatibilitatea echipamentelor

Selecția se face după funcție, grade sau clase aplicabile, condiții de mediu, compatibilitate electrică și protocolară, capacitate, securitate, mentenabilitate, suport și cost pe ciclul de viață. Declarațiile producătorului se confruntă cu documentația tehnică și cu certificările cerute. Compatibilitatea nu se deduce din existența aceluiași conector sau a aceleiași rețele.

5.1.5 Proiectarea pentru exploatare și mentenanță

Echipamentele trebuie să poată fi inspectate, testate, înlocuite și actualizate în siguranță. Proiectul prevede accesul pentru mentenanță, identificarea circuitelor, rezerve rezonabile, exportul configurației, sincronizarea timpului, jurnalizarea, copii de siguranță și restabilirea controlată. Elementele ascunse sau greu accesibile se justifică și se prevăd cu soluții de testare.

5.2 Detecția și alarmarea la efracție și atac

Subsistemul de detecție la efracție și atac urmărește detectarea oportună a pătrunderii neautorizate, a tentativei, a sabotajului și, când este cerut, a solicitării de ajutor. Proiectarea se corelează cu profilul de risc, timpul de răspuns, procedurile utilizatorilor și seria aplicabilă SR EN 50131/IEC 62642.

5.2.1 Gradul sistemului și clasele de mediu

Gradul se stabilește pentru sistem în raport cu capacitatea anticipată a intrusului și cu cerințele aplicabile. Componentele nu se aleg sub nivelul necesar funcției și nu se combină astfel încât performanța reală să fie inferioară nivelului declarat. Clasele de mediu se stabilesc pentru amplasarea efectivă: interior controlat, interior general, exterior protejat sau exterior sever, după documentele aplicabile.

5.2.2 Strategia de detecție și zonarea

Strategia combină, după caz, protecția perimetrală, periferică, volumetrică, punctuală și a traseelor de apropiere. Suprapunerea tehnologiilor trebuie să reducă vulnerabilitatea, nu să multiplice alarmele fără valoare. Fiecare zonă are denumire unică, limită inteligibilă, regim de armare, tip de eveniment și relație explicită cu aria fizică.

5.2.3 Amplasarea detectoarelor și controlul acoperirii

Amplasarea se justifică prin geometria reală, instrucțiunile producătorului, caracteristicile țintei și condițiile perturbatoare. Desenul indică orientarea, înălțimea, aria estimată și zonele excluse. Pentru tehnologiile cu diagramă de detecție, proiectantul verifică limitele la distanța maximă, unghiul de traversare, mascare, reflexii, încălzire, vibrații, vegetație și modificări previzibile ale amenajării.

5.2.4 Circuite, interconectare și protecția la sabotaj

Topologia circuitelor trebuie să permită localizarea evenimentului, supravegherea integrității și izolarea defectelor potrivit gradului cerut. Se proiectează protecția la deschiderea carcaselor, desprindere, scurtcircuit, întrerupere, substituie, interferență radio și acces neautorizat la programare. Cablurile expuse sau traseele comune vulnerabile impun protecție mecanică, separare ori măsuri compensatorii.

5.2.5 Control, indicare, armare și utilizare

Centrala și echipamentele de control se dimensionează pentru numărul de zone, ieșiri, utilizatori, partiții, memorii, comunicații și rezerve. Armarea trebuie să fie inteligibilă și compatibilă cu fluxurile. Se previn situațiile în care utilizatorul trebuie să ocolească frecvent protecții pentru a opera normal; ocolirile sunt autorizate, limitate, jurnalizate și semnalizate.

5.2.6 Alarmare locală, confirmare și transmitere

Semnalizarea locală, confirmarea și transmiterea se stabilesc după scenariu și procedura de răspuns. Proiectul definește tipurile de eveniment, prioritățile, timpii, căile de transmitere, supravegherea legăturii, destinațiile și mesajele. Confirmarea poate utiliza secvențe, tehnologii diferite, imagine sau verificare umană, fără a întârzia nejustificat intervenția.

5.2.7 Testarea proiectată

Pentru fiecare tip de detector se prevăd probe reprezentative ale țintei și mediului, inclusiv limitele acoperirii și condițiile de defect. Se testează traseul complet până la destinația alarmei, identificarea zonei, semnalizarea sabotajului, armarea parțială, pierderea comunicației, revenirea alimentării și menținerea configurației.

5.3 Supravegherea video

Proiectarea video pornește de la scopurile operaționale: observare, detectare, recunoaștere, identificare, inspecție ori obținerea unei dovezi definite. IEC 62676-4:2025 tratează planificarea, proiectarea, instalarea, testarea, punerea în funcțiune și mentenanța sistemelor video; proiectul trebuie să transforme aceste scopuri în condiții măsurabile pentru fiecare scenă.

5.3.1 Cerința operațională și fișa scenei

Fiecare cameră sau poziție planificată are o fișă de scenă: identificator, scop, țintă, direcție de deplasare, distanțe, câmp de vizualizare, densitate minimă de pixeli, înălțime și unghi, iluminare, contrast, timp, mascări, retenție, operator și probă de acceptare. Numărul de camere rezultă din acoperire și performanță, nu dintr-o densitate generică pe suprafață.

5.3.2 Geometria imaginii și densitatea de pixeli

Densitatea orizontală de pixeli se calculează prin raportul dintre numărul de pixeli utili pe orizontală și lățimea reală a scenei la planul țintei: $D = P / L$ [px/m]. Reciproc, lățimea maximă a scenei este $L = P / D$. Calculul se face pentru imaginea efectiv utilizabilă, după decupare, stabilizare ori corecții, și se verifică în teren cu o țintă de test adecvată.

5.3.3 Optica, poziționarea și câmpul de vizualizare

Distanța focală, dimensiunea senzorului și distanța până la țintă se aleg împreună. Poziția evită unghiuri excesiv de abrupte, contralumină necontrolată, reflexii, vegetație, reclame luminoase și obstacole mobile. Se prevăd zone de interes, limite de confidențialitate și, când este justificat, redundanță pentru puncte critice. Funcțiile PTZ nu substituie acoperirea permanentă a unei scene care trebuie înregistrată continuu.

5.3.4 Iluminarea, expunerea și redarea mișcării

Proiectul evaluează nivelul și uniformitatea iluminării, spectrul, alternanțele zi/noapte, pâlpâirea, farurile, umbrele și contrastul. Se specifică timpul maxim de expunere compatibil cu viteza țintei, controlul câștigului și gama dinamică. Iluminatorul se dimensionează după unghiul optic, distanță, reflectanță și limitele de expunere; iluminarea integrată nu este presupusă suficientă fără verificare.

5.3.5 Compresie, debit, latență și stocare

Debitul se estimează pentru rezoluție, frecvență de cadre, complexitatea scenei, codec, profil și calitatea cerută. Capacitatea brută de stocare se poate estima cu $C = \sum(B_i \times t_i) / 8$, la care se aplică rezerve pentru variația debitului, metadate, sistem de fișiere, redundanță și indisponibilitatea discurilor. Proiectul declară dacă înregistrarea este continuă, pe eveniment ori mixtă și cum este demonstrată retenția minimă în condiția cea mai defavorabilă.

5.3.6 Înregistrare, export și integritatea dovezii

Înregistrarea trebuie să păstreze data și ora corecte, asocierea cu sursa, calitatea necesară și urmele operațiunilor relevante. Exportul se verifică pe un sistem independent și include playerul ori formatul deschis necesar, metadatele și metoda de control al integrității. Accesul, căutarea, exportul și ștergerea sunt autorizate și jurnalizate.

5.3.7 Analitice video și limitările lor

O funcție analitică se tratează ca detector cu domeniu de aplicare, țintă, condiții, praguri, rată admisă de alarme nejustificate și metodă de test. Performanța declarată se validează în scena reală, zi/noapte și în condiții perturbatoare. Analitica nu se folosește ca unic control critic dacă degradarea ei nu este detectată sau compensată.

5.3.8 Protecția datelor prin proiectare

Se aplică necesitatea, proporționalitatea, minimizarea, limitarea scopului și a retenției. Câmpul vizual se restrânge la zonele justificate; mascarea, controlul rolurilor, autentificarea, criptarea și jurnalizarea se stabilesc din proiect. Funcțiile biometrice ori de identificare automată necesită o analiză juridică distinctă și nu sunt presupuse permise prin simpla existență tehnică.

5.4 Controlul electronic al accesului

Controlul accesului decide și aplică dreptul unei identități de a traversa un punct controlat, într-un interval și în anumite condiții. IEC 60839-11-1 definește funcții și cerințe de performanță pentru sisteme și componente, iar IEC 60839-11-2 oferă îndrumări pentru planificare, instalare, punere în funcțiune, mentenanță și documentare.

5.4.1 Modelul de autorizare și zonele de acces

Proiectul definește zonele, punctele de trecere, sensurile, grupurile, intervalele, excepțiile și autoritatea de aprobare. Drepturile se acordă după principiul necesității și sunt revocabile. Se tratează vizitatorii, contractorii, persoanele cu dizabilități, livrările, accesul în afara programului și situațiile de urgență.

5.4.2 Identificare, autentificare și credențiale

Metoda se selectează după risc: element deținut, cunoscut sau caracteristică biometrică, individual ori în combinație. Se analizează rezistența la copiere, împrumut, interceptare și substituție, precum și procesul de emitere, activare, suspendare, pierdere, expirare și distrugere. Identificatoarele nesupravegheate și protocoalele fără protecție se evită în punctele cu risc ridicat.

5.4.3 Ansamblul uşii controlate

Uşa se proiectează ca ansamblu: canat, toc, balamale, închidere, broască sau electromagnet, contact de stare, senzor de zăvor, dispozitiv de ieşire, buton, cititor, protecţie cabluri şi controler. Forţa de reţinere declarată nu compensează o tâmplărie vulnerabilă. Se verifică timpii de deblocare, reînchidere, uşă menţinută deschisă şi uşă forţată.

5.4.4 Comportarea la defect şi evacuarea

Pentru fiecare punct se stabileşte explicit starea la pierderea energiei, comunicaţiei, controlerului şi funcţiei centrale. Alegerea fail-safe ori fail-secure rezultă din evaluarea simultană a securităţii, evacuării, securităţii la incendiu şi cerinţelor speciale. Nicio comandă de securitate nu trebuie să împiedice evacuarea prevăzută de reglementările aplicabile. Deblocările de urgenţă sunt prioritare, monitorizate şi testabile.

5.4.5 Funcţii avansate şi interblocări

Anti-passback, numărarea persoanelor, escortarea, două persoane, interblocarea şi restricţiile temporale se folosesc numai cu reguli operaţionale clare. Proiectul defineşte stările excepţionale, resetarea, efectul pierderii comunicaţiei şi prevenirea blocării persoanelor. Interblocarea uşilor nu se confundă cu o soluţie de evacuare şi necesită analiză interdisciplinară.

5.4.6 Jurnalizare, timp şi administrare

Evenimentele trebuie să indice cine sau ce identitate, unde, când, ce decizie şi ce rezultat. Ceasurile se sincronizează cu sursă controlată. Rolurile de administrare se separă, acţiunile privilegiate se jurnalizează, iar exportul şi păstrarea datelor respectă scopul şi termenele aprobate. Funcţionarea offline are reguli pentru liste, evenimente, capacitate şi reconciliere.

5.5 Interfonie şi comunicaţii de securitate

Subsistemele de interfonie, apel de ajutor şi comunicaţii de securitate susţin verificarea identităţii, coordonarea răspunsului şi asistenţa. Ele se proiectează după seria IEC 62820 şi după cerinţa operaţională, fără a presupune că simpla audiţie ori imaginea de la post produce o verificare sigură.

5.5.1 Puncte de apel şi posturi de răspuns

Se stabilesc amplasarea, accesibilitatea, inteligibilitatea, câmpul vizual, iluminarea, protecţia la vandalism, indicarea stării şi redundanţa posturilor. Chemarea trebuie să ajungă la un rol disponibil, cu regulă de escaladare şi timp ţintă. În mediile zgomotoase se prevăd măsuri acustice ori mijloace alternative.

5.5.2 Comanda accesului şi verificarea

Comanda unei uşi din interfonie trebuie să indice fără ambiguitate punctul comandat şi să ofere suficiente date pentru decizie. Se evită deblocarea permanentă accidentală, comenzile nesupravegheate şi dependenţa de un singur flux video. Evenimentul, operatorul şi rezultatul pot fi jurnalizate proporţional cu scopul.

5.5.3 Prioritate, disponibilitate și confidențialitate

Apelurile de urgență primesc prioritate față de traficul curent. Proiectul tratează pierderea serverului, a rețelei ori a alimentării și definește ruta alternativă. Audio și video sunt accesibile numai rolurilor autorizate, iar înregistrarea lor se justifică separat.

5.6 Interfețe cu sistemele de detectare și alarmare la incendiu

Metodologia nu substituie proiectarea instalațiilor de detectare și alarmare la incendiu. Ea tratează exclusiv interfețele care afectează sistemele de securitate fizică: deblocări, eliberarea căilor, oprirea unor funcții, transmiterea stărilor și coordonarea mesajelor. Cerințele de securitate la incendiu și evacuare au prioritatea stabilită prin reglementările și scenariul aplicabile.

5.6.1 Principiul interfeței controlate

Orice interfață are sursă, destinație, condiție, logică, prioritate, stare sigură, supraveghere, întârziere admisă, resetare și probă. Semnalul „incendiu” nu se utilizează generic pentru acțiuni nedefinite. Se preferă contacte sau protocoale supravegheate și documentate, cu separare galvanică unde este necesară.

5.6.2 Uși, turnicheți și bariere

Proiectul identifică elementele care trebuie eliberate, modul de acționare și efectul pierderii alimentării. Comanda nu trebuie să creeze o reblocare prematură ori o stare nedeterminată. Starea fizică a ușii se verifică, deoarece existența comenzii nu dovedește deschiderea sau posibilitatea trecerii.

5.6.3 Matricea cauză–efect și testarea integrată

Toate acțiunile comune se înscriu într-o matrice cauză–efect aprobată de specialitățile implicate. Testele includ declanșarea reală sau simulată, propagarea, prioritatea față de alte comenzi, funcționarea la defect, resetarea și revenirea. Modificarea unei logici impune controlul versiunii și retestarea efectelor dependente.

5.7 Iluminat, protecții fizice și infrastructuri auxiliare

Performanța sistemelor electronice depinde de infrastructura fizică. Proiectantul coordonează iluminatul de securitate, tâmplăria, închiderile, împrejmuirile, canalizațiile, dulapurile, împământarea și protecția la supratensiuni. Aceste elemente se includ în interfețe și responsabilități chiar dacă aparțin altor specialități.

5.7.1 Iluminatul pentru supraveghere și operare

Nivelul, uniformitatea, redarea culorilor, direcția și regimul de comandă se corelează cu camerele, traseele și punctele de control. Se evită contrastele extreme și zonele orbitoare. Dacă performanța depinde de iluminatul unei alte instalații, condiția devine cerință de interfață verificabilă.

5.7.2 Carcase, dulapuri și protecție mecanică

Carcasele se aleg după mediu, impact, praf, apă, coroziune și acces. Dulapurile au spațiu pentru cablare, ventilație, baterii, rezervă, etichetare și mentenanță. Echipamentele critice nu se amplasează în zone publice ori ușor accesibile fără protecție și detectarea accesului neautorizat.

5.7.3 Coordonarea cu construcția

Golurile, consolele, traseele, penetrările, etanșările și sarcinile trebuie coordonate înainte de execuție. Proiectul identifică responsabilul pentru fiecare lucrare și cerințele de refacere a rezistenței la foc, etanșeității, finisajului și protecției structurale.

5.8 Alimentarea cu energie și autonomia

Alimentarea se proiectează pentru funcționarea normală, regimul de alarmă, defecte previzibile și durata necesară până la restabilire ori intervenție. Se inventariază toate sarcinile, inclusiv încălzitoare, iluminatoare, încuietori, switch-uri, convertoare, comunicații și pierderi.

5.8.1 Bilanțul de putere

Pentru fiecare sursă se calculează curentul în regim normal și maxim simultan, ținând seama de porniri, încărcarea bateriei, lungimea conductoarelor, căderea de tensiune și temperatura. Rezerva de capacitate trebuie declarată și nu poate compensa omiterea consumatorilor. Protecțiile sunt selective și împărțirea circuitelor limitează defectele comune.

5.8.2 Calculul autonomiei

Capacitatea necesară se estimează separat pentru regimul de veghe și regimul activ: $C = (I_v \times t_v + I_a \times t_a) \times K$, unde K include îmbătrânirea, temperatura, randamentul și rezerva cerută. Calculul se confruntă cu curentul disponibil al sursei, caracteristicile bateriei și tensiunea minimă admisă la consumator.

5.8.3 Distribuție, monitorizare și continuitate

Pierderea rețelei, defectul sursei, bateria descărcată și protecția declanșată se semnalizează la nivelul adecvat. Pentru sarcini IP se coordonează UPS-ul, PoE-ul, bugetul switch-ului și autonomia fiecărui segment. Un generator sau UPS central nu elimină necesitatea analizei căilor comune și a timpului de transfer.

5.9 Rețele de comunicații și cablare

Rețeaua de securitate este parte a sistemului, nu o utilitate presupusă. Proiectul definește topologia, mediile, capacitatea, latența, disponibilitatea, segregarea, adresarea, sincronizarea timpului, managementul și responsabilitățile. Cablarea se coordonează cu seriile aplicabile de cablare generică și instalare, precum și cu cerințele producătorilor.

5.9.1 Topologie și capacitate

Se reprezintă legăturile fizice și logice, nodurile, vitezele, redundanța și punctele de demarcație. Calculul include traficul permanent, vârfurile, multicast/unicast, managementul, actualizările și rezerva. Suprasubscrierea este acceptată numai dacă nu compromite fluxurile critice în condițiile prevăzute.

5.9.2 Trasee, separare și compatibilitate electromagnetică

Traseele respectă separarea față de energie și surse perturbatoare, raza de curbură, lungimea, ecranarea și legarea la pământ. Căile redundante nu sunt considerate independente dacă folosesc aceeași canalizație, același switch, aceeași sursă sau același spațiu vulnerabil.

5.9.3 Segregare și administrare

Segregarea prin rețele virtuale, filtre, zone și puncte de control limitează accesul și propagarea incidentelor. Interfețele de management nu sunt expuse inutil. Conturile implicite, serviciile neutilizate și accesul de la distanță se tratează prin cerințe explicite; detalierea măsurilor cibernetice este continuată în Capitolul 6.

5.9.4 Protocoale, interoperabilitate și timp

Protocolul se selectează după funcții demonstrate, securitate, supraveghere, versiune și suport. „ONVIF”, „IP” ori „API” nu constituie singure dovada interoperabilității; se declară profilul, funcțiile și testele. Toate sistemele corelate folosesc o referință temporală controlată și reguli pentru abatere, schimbarea orei și pierderea sursei.

5.10 Documentarea calculelor și a alegerilor tehnice

Documentația trebuie să permită unui profesionist competent să înțeleagă de ce a fost aleasă soluția, să o execute fără presupuneri critice și să verifice rezultatul. Conținutul se adaptează fazei, dar trasabilitatea și ipotezele nu se omit.

5.10.1 Setul minim de documente

- memoriul tehnic și baza de proiectare, cu scopuri, ipoteze, excluderi și cerințe aplicabile;
- planurile de amplasare, zonele, câmpurile de acoperire, traseele și detaliile de montaj;
- schemele bloc, funcționale, monofilare, de conexiuni și topologiile de rețea;
- listele de echipamente și materiale, cu caracteristici minime verificabile;
- calculele de acoperire, optică, bandă, stocare, alimentare, autonomie și cădere de tensiune;
- matricele de interfață și cauză—efect, registrele de adrese, zone, uși, camere și evenimente;
- planul de verificare, probele de acceptare și criteriile de rezultat;
- cerințele pentru configurare, securizare, copii de siguranță, instruire și documentația finală.

5.10.2 Note de calcul și controlul ipotezelor

Fiecare calcul indică formula sau instrumentul, unitățile, sursa datelor, cazul defavorabil, factorii de rezervă, rezultatul și criteriul de acceptare. Fișierele software relevante se arhivează în format editabil și export controlabil. Ipotezele care pot schimba soluția sunt înscrise în registru, cu proprietar și termen de confirmare.

5.10.3 Neutralitatea specificației și echivalența

Cerințele se exprimă prin performanță și interfețe, evitând restricțiile comerciale nejustificate. Dacă este necesar un produs ori ecosistem pentru compatibilitate, continuitate sau securitate, justificarea se documentează. Echivalența se evaluează pe ansamblul cerințelor, nu prin compararea selectivă a câtorva valori de catalog.

5.10.4 Revizuirea interdisciplinară și emiterea

Înainte de emitere se verifică interferențele cu arhitectura, structura, instalațiile electrice, rețelele, incendiul, evacuarea, protecția datelor și operarea. Observațiile se închid documentat. Documentele emise au cod, revizie, dată, statut și aprobare; versiunile retrase sunt identificate pentru a preveni utilizarea accidentală.

Închiderea Capitolului 5

Rezultatul Capitolului 5 este o soluție de subsisteme dimensionată și documentată, capabilă să răspundă cerințelor din Capitolul 4 și pregătită pentru integrarea tratată în Capitolul 6. Închiderea presupune existența cerințelor trasabile, a calculelor, a interfețelor, a criteriilor de acceptare, a limitelor și a responsabilităților.

Referințe tehnice pentru Capitolul 5

- [R1] IEC 62642-1:2010 — Alarm systems — Intrusion and hold-up systems — Part 1: System requirements (corespondent internațional al familiei europene pentru I&HAS).
- [R2] IEC 62642-3:2010 — Intrusion and hold-up systems — Control and indicating equipment.
- [R3] IEC 62599-1:2010 și IEC 62599-2:2010 — metode de încercare de mediu și cerințe de compatibilitate electromagnetică pentru componentele sistemelor de alarmă.
- [R4] IEC 62676-1-1:2013 — Video surveillance systems for use in security applications — General system requirements.
- [R5] IEC 62676-1-2:2013 — Video transmission performance requirements.
- [R6] IEC 62676-4:2025 — Video surveillance systems for use in security applications — Application guidelines.
- [R7] IEC 60839-11-1:2013 — Electronic access control systems — System and components requirements.
- [R8] IEC 60839-11-2:2014 — Electronic access control systems — Application guidelines.
- [R9] IEC 60839-11-5:2020 — Open supervised device protocol (OSDP) pentru sisteme de control electronic al accesului.

- [R10] IEC 62820-3-2:2018 — Building intercom systems — Application guidelines for advanced security building intercom systems.
- [R11] Regulamentul (UE) 2016/679 și EDPB Guidelines 3/2019 — protecția datelor în cazul dispozitivelor video.
- [R12] Seria SR EN 50174 și seria SR EN 50173 — instalarea și performanța infrastructurilor de cablare pentru tehnologia informației; ediția aplicabilă se verifică la data proiectului.

Notă de control normativ: standardele de mai sus sunt repere metodologice și tehnice. Proiectantul verifică ediția națională adoptată, amendamentele, corecțiile, statutul și aplicabilitatea contractuală la data fiecărui proiect. Referirea la un standard nu înlocuiește accesul la textul său integral.

CAPITOLUL 6

Integrare, reziliență și securitatea informațiilor

Capitolul stabilește condițiile prin care subsistemele proiectate individual devin un sistem integrat, capabil să furnizeze informații corecte, la timp și către rolul potrivit, inclusiv în situații de defect, degradare sau atac cibernetic. Integrarea trebuie tratată ca funcție inginerescă distinctă: cu arhitectură, interfețe, reguli de prioritate, stări, responsabilități, criterii de acceptare și dovezi de verificare.

6.1 Principiile integrării

Integrarea urmărește obținerea unei funcții operaționale mai coerente decât suma subsistemelor, fără a crea dependențe ascunse ori puncte unice de defect necontrolate. Proiectantul păstrează limitele de responsabilitate ale fiecărui subsistem, identifică funcțiile comune și stabilește autoritatea asupra comenzilor, configurațiilor și datelor.

6.1.1 Integrarea orientată către scenariu

Fiecare integrare se justifică printr-un scenariu și un rezultat: confirmarea unei alarme prin imagine, asocierea unei treceri cu un eveniment video, deblocarea controlată la urgență, transmiterea către dispecerat sau corelarea stărilor tehnice. Integrarea fără scop declarat mărește suprafața de atac și dificultatea exploatării fără a demonstra un beneficiu de securitate.

6.1.2 Cuplare minimă și autoritate clară

Funcțiile critice trebuie să rămână cât mai autonome. O platformă superioară poate coordona și prezenta evenimente, dar nu trebuie să anuleze nejustificat protecțiile locale ori să devină singura cale de operare. Pentru fiecare comandă se stabilește sistemul autoritar, dreptul de inițiere, confirmarea execuției și mecanismul de revenire.

6.1.3 Determinism, trasabilitate și timp comun

Aceeași cauză, în aceleași condiții, trebuie să producă același efect previzibil. Evenimentele sunt identificabile, jurnalizate și corelate temporal. Sistemele integrate folosesc o sursă de timp controlată, o abatere maximă admisă și reguli pentru pierderea sincronizării, schimbarea orei și reconcilierea jurnalelor.

6.2 Arhitectura funcțională și interfețele

Arhitectura funcțională descrie componentele, serviciile, zonele, fluxurile și relațiile de încredere. Ea completează schemele fizice: arată ce informație circulă, în ce sens, prin ce interfață, cu ce latență și ce se întâmplă dacă un element nu răspunde.

6.2.1 Niveluri și puncte de demarcație

Se disting cel puțin nivelul de câmp, controlul local, comunicațiile, serverele ori platformele și posturile de operare. Punctele de demarcație stabilesc proprietatea, configurarea, mentenanța și răspunderea. Serviciile externe, accesul la distanță și dependențele de cloud se reprezintă explicit, inclusiv condițiile în care sistemul continuă local.

6.2.2 Registrul interfețelor

Fiecare interfață primește un identificator unic și o fișă controlată. Fișa precizează sistemele conectate, protocolul și versiunea, suportul fizic, datele, comenzile, frecvența, latența, autentificarea, criptarea, monitorizarea, tratarea erorilor, proprietarul și testele. Formulări precum „integrare BMS”, „API disponibil” sau „compatibil ONVIF” sunt incomplete fără funcțiile și profilurile efectiv utilizate.

6.2.3 Controlul configurației și al versiunilor

Versiunile de firmware, software, protocol, schemă de date și configurație sunt compatibile și controlate. Modificarea unei interfețe declanșează analiza impactului asupra funcțiilor dependente și retestarea proporțională. Configurațiile aprobate se exportă și se păstrează împreună cu instrucțiunile de restaurare.

6.3 Matricea cauză–efect

Matricea cauză–efect este documentul central al logicii integrate. Ea transformă scenariile în comportamente verificabile și împiedică programarea pe baza unor presupuneri nescrise. Matricea include atât evenimente de securitate, cât și defecte, pierderi de comunicație, indisponibilități și comenzi manuale.

6.3.1 Structura unei reguli

O regulă conține cauza, condițiile, inhibările permise, întârzierea, efectele, ordinea lor, prioritatea, confirmarea, jurnalizarea, resetarea și comportarea la nereușită. Cauzele multiple și condițiile logice sunt exprimate fără ambiguitate. Temporizările sunt valori controlate, nu opțiuni rămase la instalator.

6.3.2 Conflicte și priorități

Dacă două reguli solicită stări incompatibile, proiectul stabilește prioritatea după securitatea persoanelor, cerințele legale, criticitatea activelor și starea operațională. Comenzile de urgență, evacuare și securitate la incendiu se coordonează cu specialitățile competente. Nicio automatizare nu trebuie să producă o stare periculoasă sau să ascundă un defect relevant.

6.3.3 Aprobarea și testarea matricei

Matricea este aprobată de proiectant, beneficiar și specialitățile afectate. Implementarea se confruntă cu versiunea aprobată, iar testul verifică efectul fizic, nu numai mesajul software. Rezultatele, excepțiile și neconformitățile sunt înregistrate; o schimbare de logică după test impune revalidarea funcțiilor afectate.

6.4 Managementul și prioritizarea alarmelor

Scopul managementului alarmelor este ca operatorul să identifice rapid ce s-a întâmplat, unde, cât de critic este și ce acțiune trebuie inițiată. Volumul mare, mesajele neclare și alarmele repetate pot transforma un sistem tehnic funcțional într-un control operațional ineficace.

6.4.1 Clasificare și prezentare

Evenimentele se clasifică cel puțin în alarmă de securitate, atac/panică, sabotaj, defect, avertizare și informație. Prioritatea rezultă din consecință și urgență, nu din ordinea sosirii. Mesajul include identificatorul, locul, tipul, ora, starea și instrucțiunea asociată, într-un limbaj stabil și inteligibil.

6.4.2 Confirmare, recunoaștere și escaladare

Recunoașterea de către operator nu echivalează cu rezolvarea. Fluxul distinge primirea, confirmarea, acțiunea, escaladarea și închiderea. Se definesc timpi-țintă, roluri de rezervă și condițiile de escaladare automată. Evenimentele critice nu pot fi șterse ori închise fără urmă.

6.4.3 Reducerea alarmelor nejustificate

Se urmăresc alarmele repetitive, sursele instabile, pragurile, condițiile de mediu și practicile utilizatorilor. Filtrarea, corelarea sau suprimarea se aplică numai controlat și reversibil; nu se maschează un defect de proiectare. Indicatorii minimi includ frecvența, distribuția pe surse, timpul de recunoaștere și procentul de evenimente fără valoare operațională.

6.5 Continuitatea funcționării și reziliența

Reziliența reprezintă capacitatea sistemului de a anticipa, absorbi, limita și recupera după o perturbare, menținând funcțiile prioritare la un nivel acceptat. Ea se proiectează pentru servicii și scenarii, nu prin dublarea nediferențiată a tuturor componentelor.

6.5.1 Funcții prioritare și obiective de recuperare

Beneficiarul și proiectantul clasifică funcțiile, stabilesc durata maximă tolerabilă a întreruperii, obiectivul de timp pentru restabilire și pierderea de date acceptabilă. Valorile se corelează cu timpul de intervenție, autonomia energetică, disponibilitatea pieselor, copiile de siguranță și competențele de restaurare.

6.5.2 Redundanță și diversitate

Redundanța este eficace numai dacă elementele nu împart aceeași cauză de defect. Se examinează alimentarea, traseele, switch-urile, serverele, licențele, stocarea, comunicațiile, răcirea, spațiul și furnizorul. Pentru funcții critice poate fi necesară diversitatea tehnologică sau procedurală, însă complexitatea suplimentară trebuie administrată.

6.5.3 Copii de siguranță și restaurare

Se păstrează configurațiile, bazele de date necesare, cheile și documentația, cu acces controlat și copii protejate față de compromiterea sistemului principal. Restaurarea se testează pe o bază aprobată. O copie existentă, dar nevalidată ori dependentă de un produs indisponibil, nu constituie capacitate demonstrată de recuperare.

6.6 Modurile degradate și gestionarea defectelor

Modul degradat este o stare proiectată în care anumite performanțe sunt reduse, dar funcțiile esențiale rămân controlate și utilizatorii cunosc limitările. El nu trebuie confundat cu funcționarea accidentală după defect.

6.6.1 Analiza defectelor și dependențelor

Pentru componentele și căile critice se examinează pierderea energiei, comunicației, timpului, stocării, autentificării, licenței, senzorului, actuatorului și serviciului extern. Se identifică efectele locale și propagate, detectabilitatea, timpul până la impact și măsurile de izolare sau compensare.

6.6.2 Starea sigură și starea securizată

Starea favorabilă securității persoanelor poate diferi de starea favorabilă protecției activelor. Proiectul rezolvă explicit conflictul, cu respectarea cerințelor de evacuare și incendiu. Pentru fiecare ieșire se precizează starea la pierderea alimentării, controlului și comunicației, precum și metoda de comandă manuală autorizată.

6.6.3 Alarmare, revenire și reconciliere

Defectul trebuie detectat la nivelul la care poate fi gestionat. Revenirea nu generează automat o stare nesigură, nu șterge evenimente și nu aplică o configurație neverificată. Datele acumulate local sunt reconciliate, iar diferențele ori golurile sunt semnalate. Procedura indică cine poate declara revenirea la regim normal.

6.7 Securitatea cibernetică

Subsistemele IP, serverele, controlerile, aplicațiile și serviciile asociate sunt rețele și sisteme informatice care pot afecta direct securitatea fizică. Măsurile se stabilesc proporțional cu riscul și cu obligațiile aplicabile beneficiarului. ISO/IEC 27001 și 27002 oferă cadrul organizațional, iar conceptele IEC 62443 privind sistemul analizat, zonele, conductele și cerințele de securitate pot fundamenta arhitectura tehnică.

6.7.1 Inventar, zone și fluxuri permise

Se inventariază activele hardware, software, firmware, conturile, certificatele, cheile, licențele și dependențele. Rețeaua se segmentează în zone de încredere, iar comunicațiile dintre ele se limitează la fluxurile justificate. Accesul din rețeaua generală, internet, wireless, cloud sau mentenanță este controlat prin puncte de trecere monitorizate.

6.7.2 Identitate, autentificare și privilegii

Conturile implicite se elimină ori se securizează înainte de punerea în funcțiune. Se folosesc identități individuale, privilegii minime, separarea rolurilor și autentificare adecvată riscului, inclusiv multifactor pentru acces administrativ sau la distanță când este fezabil. Conturile de serviciu, urgență și furnizor au proprietar, termen și jurnalizare.

6.7.3 Configurare sigură și reducerea suprafeței de atac

Serviciile, porturile, protocoalele și funcțiile neutilizate se dezactivează. Interfețele de administrare sunt separate și criptate; certificatele sunt validate și gestionate. Setările de securitate aprobate se documentează ca bază de configurație. Conectivitatea directă la internet și redirectionările necontrolate de porturi nu sunt acceptate ca soluție de mentenanță.

6.7.4 Vulnerabilități, actualizări și suport

Proiectul definește sursa informațiilor despre vulnerabilități, responsabilitatea evaluării, ferestrele de mentenanță, testarea și revenirea. Actualizarea nu se aplică automat fără analiza impactului funcțional, dar nici nu se amână indefinit. Produsele fără suport, cu credențiale fixe sau fără posibilitate rezonabilă de remediere se evită ori se tratează prin măsuri compensatorii aprobate.

6.7.5 Jurnalizare, monitorizare și răspuns

Se înregistrează autentificările, schimbările de configurație, acțiunile privilegiate, alarmele, defectele și evenimentele relevante de rețea. Jurnalurile au timp comun, integritate și retenție adecvate. Se definesc criteriile de incident, păstrarea dovezilor, izolarea, notificarea și restaurarea, corelate cu planurile beneficiarului și, unde este cazul, cu O.U.G. nr. 155/2024 aprobată prin Legea nr. 124/2025.

6.8 Protecția datelor și controlul informațiilor

Datele video, audio, de acces, identitățile, jurnalurile și configurațiile pot conține date cu caracter personal sau informații sensibile despre securitatea obiectivului. Protecția se aplică prin proiectare și implicit, de la colectare până la ștergere, export sau predare.

6.8.1 Clasificare, scop și minimizare

Pentru fiecare categorie se documentează scopul, temeiul stabilit de operator, destinatarii, retenția, necesitatea și nivelul de sensibilitate. Se colectează numai datele necesare funcției. Câmpurile video, audio, metadatele și rapoartele sunt limitate; utilizările ulterioare incompatibile nu se introduc implicit prin capabilități tehnice disponibile.

6.8.2 Acces, export și confidențialitate

Accesul este bazat pe rol și separă vizualizarea, căutarea, exportul, administrarea și ștergerea. Exporturile sunt controlate, urmărite și protejate în tranzit și stocare. Planurile, parolele, cheile și copiile de configurație se predau prin canale adecvate și nu se includ neprotejat în documente cu circulație largă.

6.8.3 Retenție, ștergere și drepturi

Termenele sunt implementate tehnic și verificate, inclusiv pentru copii și spații temporare, ținând seama de conservarea justificată a unui incident. Sistemul trebuie să permită operatorului să își îndeplinească obligațiile aplicabile privind informarea, accesul, restricționarea și ștergerea, fără a compromite integritatea dovezilor ori securitatea altor persoane.

6.9 Interoperabilitatea și evitarea dependenței nejustificate de furnizor

Interoperabilitatea înseamnă îndeplinirea demonstrată a funcțiilor între produse și versiuni determinate. Utilizarea unui protocol publicat sau a unei certificări de profil ajută, dar nu garantează toate funcțiile necesare. Proiectul definește explicit ce trebuie să fie interoperabil și cum se verifică.

6.9.1 Specificații deschise și portabilitate

Unde este rezonabil, se preferă protocoale documentate, formate exportabile și interfețe standardizate. Beneficiarul trebuie să poată obține configurațiile, jurnalele și datele în formate utilizabile și să restaureze sistemul fără dependență disproporționată de o singură persoană. Cheile, licențele și drepturile de administrare se predau controlat.

6.9.2 Dependențe comerciale justificate

O platformă proprietară poate fi justificată prin performanță, securitate, compatibilitate sau continuitate, dar decizia trebuie să includă costul ciclului de viață, suportul, migrarea, disponibilitatea pieselor, condițiile de licențiere și riscul încetării serviciului. Specificația nu prezintă dependența drept inevitabilă fără analiză.

6.9.3 Testul de interoperabilitate și predarea

Testul folosește produsele, versiunile, licențele și funcțiile reale. Se verifică evenimentele, comenzile, confirmările, timpul, pierderea legăturii, revenirea și securitatea. Dosarul final conține registrul interfețelor, matricea cauză–efect, versiunile, configurațiile, credențialele predate securizat, licențele și limitele cunoscute.

Închiderea Capitolului 6

Rezultatul Capitolului 6 este o arhitectură integrată controlată, rezilientă și securizată, în care funcțiile, interfețele, prioritățile, datele, defectele și responsabilitățile pot fi urmărite și testate. Capitolul pregătește verificarea, punerea în funcțiune și recepția tratate în Capitolul 7.

Referințe tehnice și normative pentru Capitolul 6

- [R1] ISO/IEC 27001:2022 și Amd 1:2024 — sisteme de management al securității informației; cerințe.
- [R2] ISO/IEC 27002:2022 — controale pentru securitatea informației, securitate cibernetică și protecția vieții private.
- [R3] IEC 62443-3-2:2020 — evaluarea riscului de securitate pentru proiectarea sistemului, inclusiv zone și conduite.

- [R4] IEC 62443-3-3:2013 și Corrigendum 1:2014 — cerințe de securitate ale sistemului și niveluri de securitate.
- [R5] IEC 62443-4-2:2019 — cerințe tehnice de securitate pentru componente IACS; utilizabil ca reper pentru capabilități.
- [R6] IEC 62443-2-1:2024 — cerințe de program de securitate pentru proprietarii de active IACS.
- [R7] ISO 22301:2019 și Amd 1:2024 — sisteme de management al continuității activității; cerințe.
- [R8] Directiva (UE) 2022/2555 (NIS 2), în versiunea aplicabilă — măsuri pentru un nivel comun ridicat de securitate cibernetică.
- [R9] O.U.G. nr. 155/2024, aprobată cu modificări prin Legea nr. 124/2025, cu modificările ulterioare — cadrul național pentru securitatea cibernetică a rețelelor și sistemelor informatice.
- [R10] Regulamentul (UE) 2016/679 — protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal.
- [R11] EDPB Guidelines 3/2019, versiunea 2.0 adoptată la 29 ianuarie 2020 — prelucrarea datelor cu caracter personal prin dispozitive video.
- [R12] IEC 62676-1-1:2013, IEC 62676-1-2:2013, IEC 62676-4:2025, IEC 60839-11-1:2013 și IEC 60839-11-2:2014 — cerințe și ghiduri relevante pentru integrarea video și control acces.

Notă de control normativ: aplicabilitatea NIS 2 și a cadrului național depinde de încadrarea beneficiarului și a serviciilor sale. Standardele sunt repere tehnice și metodologice; se verifică ediția națională adoptată, amendamentele, statutul și caracterul obligatoriu la data proiectului. Referirea la un standard nu înlocuiește consultarea textului integral.

CAPITOLUL 7

Verificare, punere în funcțiune și recepție

Capitolul stabilește procesul prin care conformitatea proiectului și a execuției este demonstrată prin examinare, inspecție, măsurare și încercare, iar sistemul este configurat, validat în condiții reprezentative și predat controlat beneficiarului. Acceptarea nu se bazează pe impresia că sistemul „funcționează”, ci pe cerințe identificabile, criterii prestabilite, rezultate reproductibile și dovezi păstrate în dosarul final.

7.1 Verificarea documentației

Verificarea documentației confirmă că proiectul emis pentru execuție este complet, coerent, aplicabil și controlat. Ea precedă lucrările și continuă pentru documentele de atelier, fișele tehnice, configurații și modificări. Verificarea nu transferă autorului răspunderea către verficator și nu înlocuiește aprobările cerute de lege sau contract.

7.1.1 Planul de verificare și matricea de conformitate

Planul identifică documentele, cerințele, metodele, responsabilii, nivelul de independență și înregistrările. Matricea de conformitate urmărește fiecare cerință până la soluție și probă. Cerințele fără criteriu măsurabil sunt clarificate înaintea testării; lipsa criteriului nu poate fi compensată printr-o apreciere informală la recepție.

7.1.2 Controlul coerenței și al emiterii

Se confruntă piesele scrise, desenate, listele, calculele, matricea cauză–efect și versiunile. Se verifică interfețele, alimentările, capacitățile, licențele, compatibilitatea, accesul pentru mentenanță și condițiile de mediu. Documentele aprobate poartă identificator, revizie, statut, dată și autoritate de emitere; exemplarele înlocuite sunt retrase din utilizare.

7.2 Controlul conformității execuției

Controlul execuției urmărește dacă instalația realizată corespunde proiectului aprobat, instrucțiunilor producătorului, cerințelor aplicabile și condițiilor reale din obiectiv. El se desfășoară pe parcurs, când traseele și lucrările ascunse sunt încă accesibile, nu numai la final.

7.2.1 Inspecția lucrărilor și materialelor

Se verifică identitatea și integritatea echipamentelor, amplasarea, orientarea, fixarea, protecția mecanică, traseele, separările, etichetarea, conexiunile, împământarea unde este aplicabilă, condițiile de mediu și accesibilitatea. Pentru lucrări ascunse se păstrează procese-verbale, fotografii controlate și măsurători înainte de acoperire.

7.2.2 Modificări și neconcordanțe de șantier

Nicio abatere cu efect asupra performanței, securității, evacuării, protecției datelor sau mentenanței nu este regularizată retrospectiv doar prin desen „as built”. Modificarea este identificată, analizată, aprobată de rolurile competente și introdusă în documentație înaintea acceptării. Echipamentele substituite sunt evaluate funcțional, nu numai comercial.

7.3 Inspecțiile și încercările

Inspecția observă caracteristici și condiții; încercarea aplică un stimul și compară răspunsul cu un criteriu. Programul combină inspecția integrală a elementelor critice cu eșantionarea justificată pentru elemente repetitive, dacă legea, standardul, contractul și riscul permit aceasta.

7.3.1 Planul de inspecții și încercări

Planul precizează obiectul, metoda, condițiile inițiale, instrumentele, toleranțele, eșantionul, ordinea, condițiile de oprire, responsabilul, martorii și formularul de rezultat. Sunt incluse atât cazurile pozitive, cât și cele negative: alarmă, sabotaj, acces refuzat, pierdere de alimentare, întrerupere de comunicație și revenire.

7.3.2 Instrumente, mediu și repetabilitate

Instrumentele adecvate au identificare și stare de verificare ori calibrare proporțională cu măsurarea. Se înregistrează condițiile relevante: iluminare, trafic, zgomot electromagnetic, temperatură, sarcină, stare rețea și versiuni. O încercare nereproductibilă sau efectuată într-o configurație necunoscută nu constituie dovadă suficientă.

7.4 Punerea în funcțiune

Punerea în funcțiune este procesul controlat prin care sistemul instalat este energizat, parametrizat, verificat și adus în configurația aprobată. Ea începe numai după confirmarea condițiilor de siguranță, a alimentărilor, a continuității circuitelor, a adresării și a pregătirii infrastructurii.

7.4.1 Configurarea controlată

Se stabilesc identificatorii, zonele, utilizatorii inițiali, drepturile, temporizările, pragurile, orarele, retenția, sincronizarea timpului, comunicațiile și logica integrată. Conturile implicite sunt eliminate ori securizate, accesul temporar este retras, iar configurația inițială aprobată este exportată și protejată.

7.4.2 Stabilizarea și baza de referință

După energizare se urmăresc defectele, temperaturile, comunicațiile, capacitatea, evenimentele repetitive și încărcarea. Se corectează cauzele, nu se suprimă nejustificat alarmele. Configurația stabilă, inventarul, versiunile și parametrii mășurați formează baza de referință pentru testele de acceptare și exploatarea ulterioară.

7.5 Testarea funcțională

Testarea funcțională demonstrează că fiecare subsistem și fiecare funcție locală îndeplinește cerințele sale în regim normal, de alarmă, de defect și de revenire. Testul verifică efectul observabil în teren și în punctul de operare, nu doar schimbarea unei variabile în aplicație.

7.5.1 Acoperirea funcțiilor

Pentru efracție se testează detectarea, armarea, alarma, sabotajul, transmiterea și autonomia; pentru video — câmpul, calitatea, iluminarea, înregistrarea, căutarea, exportul și pierderea fluxului; pentru control acces — autorizarea, refuzul, ușa forțată sau menținută deschisă, stările la defect și jurnalizarea. Interfonia și comunicațiile se verifică bidirecțional, inclusiv inteligibilitatea.

7.5.2 Rezultatul și dovada

Fișa consemnează identificatorul testului și al cerinței, data, configurația, stimulul, rezultatul așteptat și obținut, măsurarea, verdictul, operatorul, martorul și dovada anexată. „OK” fără criteriu și fără trasabilitate este insuficient. Rezultatele la limită sunt analizate, nu rotunjite administrativ.

7.6 Testarea integrată

Testarea integrată demonstrează comportarea cap-la-cap a funcțiilor care traversează subsisteme, rețele, platforme și proceduri. Scenariile derivă din Capitolul 4 și din matricea cauză–efect aprobată; sunt incluse conflictele de prioritate, modurile degradate și restaurarea după defect.

7.6.1 Scenarii și martori

Pentru fiecare scenariu se stabilesc condițiile, rolurile, succesiunea, punctele de observație, efectele, timpii și criteriul de închidere. Participă reprezentanții specialităților și ai beneficiarului afectați. Testarea interfețelor cu securitatea la incendiu se realizează numai în condiții coordonate și autorizate, fără a compromite siguranța persoanelor.

7.6.2 Defecte, revenire și regresie

Se simulează controlat pierderea energiei, comunicației, serverului, timpului sau unui element critic. Se verifică alarmarea, autonomia locală, starea sigură/securizată, reconcilierea și revenirea. Orice corecție de logică ori configurație impune retestarea funcției și a dependențelor afectate; testul inițial nu rămâne valabil după schimbare.

7.7 Tratarea neconformităților

Neconformitatea este abaterea demonstrată față de o cerință. Ea se înregistrează cu identificator, sursă, descriere factuală, cerință încălcată, impact, responsabil, termen și stare. Observațiile, rezervele și propunerile de optimizare se disting de neconformități pentru a nu dilua obligațiile.

7.7.1 Clasificare și dispoziție

Clasificarea ține seama de siguranță, securitate, funcție critică, legalitate, date, întindere și posibilitatea de verificare. Dispoziția poate fi corectare, înlocuire, refacere, acceptare justificată prin derogare aprobată sau respingere. Acceptarea unei abateri nu transformă automat produsul ori lucrarea în conformă și nu poate încălca cerințe imperative.

7.7.2 Închidere și prevenirea recurenței

Închiderea cere dovada corecției și reverificarea. Pentru neconformități sistemice se analizează cauza, extinderea la elemente similare și acțiunea preventivă. Lista deschisă este anexată procesului-verbal; elementele care afectează funcțiile critice, siguranța ori legalitatea blochează acceptarea până la rezolvare sau decizie formală competentă.

7.8 Recepția sistemului

Recepția este actul contractual și documentar prin care beneficiarul constată stadiul, examinează dovezile și acceptă, acceptă cu rezerve admisibile sau refuză lucrarea, potrivit cadrului aplicabil. Ea nu trebuie confundată cu punerea în funcțiune, avizarea, autorizarea, verificarea tehnică sau expirarea perioadei de probă.

7.8.1 Condiții de prezentare la recepție

Sistemul se prezintă în configurația finală, cu documentația actualizată, testele încheiate, neconformitățile critice închise, licențele active, copiile de siguranță verificate, instruirea programată și responsabilitățile de exploatare clarificate. Sunt consemnate limitările, excluderile, lucrările restante, condițiile de garanție și termenele.

7.8.2 Decizia și transferul controlat

Procesul-verbal identifică obiectul, documentele, participanții, testele, rezervele, termenul de remediere, data transferului și decizia. Predarea cheilor, conturilor privilegiate, certificatelor și configurațiilor se face separat și securizat, cu confirmarea beneficiarului. Recepția nu justifică păstrarea accesului nedeclarat de către furnizor.

7.9 Instruirea utilizatorilor

Instruirea este o condiție a utilizării corecte și a menținerii performanței. Ea se adaptează rolurilor: operator, administrator, responsabil de securitate, mentenanță și conducere. Demonstrația tehnică a instalatorului nu înlocuiește un program de instruire cu obiective, materiale și verificarea înțelegerii.

7.9.1 Conținut și competențe

Se tratează operarea normală, armarea, alarmele, confirmarea, escaladarea, exportul de dovezi, protecția datelor, defectele, modurile degradate, acțiunile interzise, apelarea mentenanței și schimbarea controlată. Pentru administratori se includ conturile, copiile, actualizările, jurnalele și restaurarea autorizată.

7.9.2 Evidență și reîmprospătare

Se păstrează agenda, materialele, lista participanților, rolurile, data, formatorul și rezultatul evaluării. Instruirea se repetă la schimbări majore, incidente relevante, rotația personalului sau degradarea indicatorilor operaționali. Documentele sunt disponibile în limba și forma adecvate utilizatorilor.

7.10 Dosarul final al sistemului

Dosarul final reprezintă configurația de referință predată beneficiarului și baza exploataării, mentenanței, auditului și modificărilor. Conținutul este controlat, indexat și corelat cu elementele fizice. Documentele sensibile au clasificare, destinatari, reguli de păstrare și canal de predare adecvat.

7.10.1 Conținut minim

Dosarul include proiectul și modificările aprobate, planurile conform execuției, schemele, inventarul și seriile, versiunile, licențele, calculele actualizate, configurațiile și copiile, matricea cauză–efect, registrele interfețelor, certificatele și declarațiile aplicabile, procesele-verbale, rezultatele testelor, neconformitățile, instrucțiunile, garanțiile și planul de mentenanță.

7.10.2 Integritate, acces și actualizare

Se verifică deschiderea fișierelor, completitudinea, semnăturile, reviziile și concordanța dintre formatul editabil și cel aprobat. Parolele și cheile nu se includ în exemplare cu circulație generală. Beneficiarul confirmă primirea și custodia. Dosarul devine baza controlată pentru managementul schimbării din Capitolul 8.

Închiderea Capitolului 7

Rezultatul Capitolului 7 este un sistem a cărui conformitate a fost demonstrată controlat, configurat și testat în stările relevante, acceptat printr-o decizie documentată și predat împreună cu dovezile și competențele necesare exploataării. Orice rezervă rămasă are responsabil, termen, măsură compensatorie și criteriu de închidere.

Referințe tehnice și normative pentru Capitolul 7

- [R1] IEC 62676-4:2025 — sisteme de supraveghere video pentru aplicații de securitate; ghid de aplicare privind planificarea, instalarea, testarea, punerea în funcțiune și mentenanța.
- [R2] IEC 60839-11-2:2014 — sisteme electronice de control al accesului; cerințe și ghiduri pentru planificare, instalare, punere în funcțiune, mentenanță și documentare.
- [R3] IEC TS 62642-7:2011 — sisteme de alarmare la efracție și atac; ghid de aplicare pentru proiectare, instalare, punere în funcțiune și mentenanță.
- [R4] IEC 62642-1:2010 — sisteme de alarmare la efracție și atac; cerințe de sistem.
- [R5] ISO/IEC/IEEE 15288:2023 — procese ale ciclului de viață al sistemelor; verificare, validare, tranziție și managementul configurației.

- [R6] ISO/IEC/IEEE 29148:2018 — ingineria cerințelor și caracteristicile cerințelor verificabile.
- [R7] ISO 10005:2018 — linii directoare pentru planurile calității.
- [R8] ISO 10012:2003 — procese de măsurare și managementul echipamentelor de măsurare.
- [R9] ISO 9001:2015 și Amd 1:2024 — controlul informațiilor documentate, al furnizării, al eliberării și al neconformităților.
- [R10] Legea nr. 333/2003, H.G. nr. 301/2012 și actele modificatoare, în forma aplicabilă — cerințe naționale privind sistemele de alarmare împotriva efracției, proiectarea, instalarea și documentele asociate.

Notă de control normativ: edițiile, amendamentele, adoptările naționale și caracterul obligatoriu se verifică la data proiectului. Criteriile contractuale de recepție și atribuțiile participanților se corelează cu legislația, contractul și procedurile beneficiarului; metodologia nu substituie competența unei autorități ori a unei comisii legal constituite.

CAPITOLUL 8

Exploatare, mentenanță și managementul schimbării

Capitolul stabilește cadrul prin care performanța, disponibilitatea, securitatea și conformitatea sistemului sunt menținute după recepție, pe întreaga durată de viață. Exploatarea nu este o stare pasivă, iar mentenanța nu se reduce la remedierea defectelor: ele formează un proces controlat de operare, supraveghere, întreținere, învățare din incidente și adaptare la schimbarea contextului, a riscurilor, a tehnologiei și a cerințelor aplicabile.

8.1 Predarea în exploatare

Predarea în exploatare transformă sistemul recepționat într-un serviciu administrat. Beneficiarul desemnează proprietarul sistemului, administratorii tehnici și funcționali, operatorii, responsabilii pentru protecția datelor și securitate cibernetică, precum și furnizorii autorizați. Responsabilitățile se stabilesc nominal ori pe rol, cu limite de competență, înlocuitori și canale de escaladare.

8.1.1 Acceptarea operațională și perioada de stabilizare

Acceptarea operațională confirmă că documentele, competențele, accesurile, copiile de siguranță, licențele, piesele critice, serviciile de comunicații și mecanismele de suport sunt disponibile. În perioada de stabilizare se urmăresc alarmele nedorite, defectele intermitente, capacitatea, timpii de răspuns, sincronizarea temporală și reacția utilizatorilor. Problemele de proiectare sau execuție nu sunt transferate tacit în sarcina mentenanței.

8.1.2 Modelul de guvernanză

Pentru fiecare activitate se precizează cine solicită, cine aprobă, cine execută, cine verifică și cine este informat. Separarea atribuțiilor este proporțională cu criticitatea: o persoană nu trebuie să poată iniția, autoriza și ascunde singură o modificare critică. Contractele de servicii definesc domeniul, nivelurile de serviciu, accesul la date, confidențialitatea, notificarea incidentelor, proprietatea configurațiilor și condițiile de ieșire.

8.2 Instrucțiunile de utilizare

Instrucțiunile traduc proiectul și scenariile de securitate în acțiuni clare pentru fiecare rol. Ele sunt controlate ca versiune, accesibile la punctul de utilizare și corelate cu configurația reală. Manualul producătorului este o sursă tehnică, dar nu înlocuiește procedura beneficiarului privind alarmele, incidentele, escaladarea și continuitatea activității.

8.2.1 Proceduri normale, anormale și de urgență

Se descriu pornirea și oprirea autorizată, armarea și dezarmarea, acordarea și retragerea accesului, monitorizarea video, confirmarea alarmelor, exportul probelor, tratarea defectelor, pierderea comunicațiilor, funcționarea degradată și revenirea. Instrucțiunile stabilesc acțiunile permise, acțiunile interzise, limitele de timp și persoana căreia i se escaladează situația.

8.2.2 Competență și controlul utilizării

Dreptul de operare se acordă după instruire proporțională cu rolul și se revizuieste periodic. Interfețele, mesajele și nomenclatoarele se mențin inteligibile. Erorile repetate ale utilizatorilor sunt tratate ca semnal privind procedura, ergonomia, instruirea sau configurația, nu exclusiv ca abatere individuală. Modificarea instrucțiunilor declanșează comunicarea și, după caz, reinstruirea.

8.3 Menținerea preventivă și corectivă

Programul de menținere se bazează pe criticitatea funcțiilor, condițiile de mediu, intensitatea utilizării, istoricul defectelor, recomandările producătorului, obligațiile aplicabile și efectul indisponibilității. Frecvențele nu se copiază mecanic: ele sunt justificate, revizuite prin rezultate și nu pot coborî sub minimele legale, normative ori contractuale aplicabile.

8.3.1 Strategia și planul de menținere

Planul identifică activele, operațiile, periodicitatea sau declanșatorul, competența, instrumentele, consumabilele, piesele, fereastra de lucru, măsurile compensatorii, criteriile de acceptare și înregistrările. Se combină menținerea calendaristică, cea bazată pe stare și cea corectivă. Funcțiile ascunse sau rare — sabotaj, autonomie, redundanță, restaurare — sunt testate explicit, deoarece simpla lipsă a alarmelor nu demonstrează sănătatea sistemului.

8.3.2 Intervenția corectivă și revenirea în serviciu

Sesizarea este înregistrată, clasificată după impact și corelată cu activul. Înaintea intervenției se evaluează riscul indisponibilității și se stabilesc măsuri compensatorii. După remediere se efectuează testul funcției, al dependențelor și, când este necesar, test de regresie. Sistemul revine în serviciu numai după confirmarea configurației, închiderea accesului temporar și actualizarea evidențelor.

8.4 Verificările periodice

Verificările periodice demonstrează că performanța proiectată se păstrează în condițiile reale. Domeniul lor include echipamentele, alimentările, comunicațiile, stocarea, sincronizarea timpului, interfețele, alarmele de defect, protecțiile fizice și cibernetice, documentația și capacitatea operatorilor. Rezultatul se compară atât cu criteriul tehnic, cât și cu valoarea de referință stabilită la punerea în funcțiune.

8.4.1 Program, eșantionare și criterii

Elementele critice se verifică integral sau printr-o strategie justificată de risc. Eșantionarea indică populația, metoda, dimensiunea și regula de extindere când apare o abatere. Condițiile de mediu relevante sunt consemnate. Rezultatul „funcționează” este insuficient dacă proiectul cere un timp, o calitate, o autonomie, o acoperire ori o capacitate măsurabilă.

8.4.2 Indicatori și revizuirea performanței

Organizația urmărește un set limitat de indicatori legați de obiective: disponibilitatea funcțiilor critice, numărul și cauza alarmelor nedorite, timpul mediu de restabilire (MTTR), defectele repetitive, procentul verificărilor executate la termen, restanța de mentenanță, succesul copiilor și restaurărilor, vulnerabilitățile restante și vechimea excepțiilor. Pragurile și tendințele declanșează acțiuni, nu doar raportare.

8.5 Gestionarea alarmelor și incidentelor

Alarma este un eveniment care solicită evaluare și răspuns; incidentul este o situație care afectează ori poate afecta securitatea, funcționarea, datele sau conformitatea. Procedura stabilește clasificarea, verificarea, escaladarea, intervenția, comunicarea, păstrarea dovezilor, restabilirea și analiza ulterioară. Jurnalele tehnice nu substituie consemnarea deciziilor operaționale.

8.5.1 Răspuns, dovezi și notificări

Operatorul confirmă identitatea evenimentului, sursa, timpul și starea sistemului, fără a întârzia măsurile de protecție. Exporturile, imaginile, jurnalele și configurațiile relevante sunt conservate cu integritate, control al accesului și lanț de custodie proporțional cu utilizarea. Notificările către conducere, autorități, persoane vizate, asigurător ori parteneri se fac numai potrivit obligațiilor și procedurilor aplicabile.

8.5.2 Analiza post-incident și lecțiile învățate

După stabilizare se reconstruiesc cronologia, condițiile, controalele care au funcționat sau au eșuat, cauzele și factorii contributivi. Acțiunile rezultate au proprietar, termen, prioritate și criteriu de verificare. Analiza poate modifica scenariile, procedurile, instruirea, mentenanța, configurația și evaluarea riscului; nu se limitează la înlocuirea componentei defecte.

8.6 Modificarea sistemului

Modificarea include orice schimbare fizică, logică, software, de rețea, licență, parametru, integrare, locație, utilizator privilegiat, furnizor sau serviciu care poate influența sistemul. Chiar și modificările aparent minore pot altera acoperirea, autonomia, retenția, interoperabilitatea, securitatea cibernetică, protecția datelor ori conformitatea.

8.6.1 Fluxul de management al schimbării

Solicitarea descrie motivul, domeniul, urgența și rezultatul urmărit. Evaluarea identifică cerințele și activele afectate, impactul, riscurile, compatibilitatea, resursele, oprirea, planul de test, planul de revenire și aprobările. Implementarea folosește o versiune controlată; verificarea și validarea confirmă atât execuția corectă, cât și satisfacerea nevoii. Închiderea actualizează toate documentele și retrace variantele depășite.

8.6.2 Schimbări urgente și modificări temporare

Pentru o urgență se folosesc aprobări accelerate, domeniu limitat, jurnal complet și plan de revenire. Evaluarea formală, testarea completă și actualizarea documentației se finalizează într-un termen stabilit după restabilire. O măsură temporară are proprietar, expirare și condiție de închidere; dacă persistă, este reevaluată ca modificare permanentă, nu prelungită tacit.

8.7 Reevaluarea riscului

Riscul este reevaluat periodic și ori de câte ori se modifică premisele pe care s-au bazat scenariile și cerințele. Proiectantul, administratorul și mentenanța furnizează date tehnice și observații, iar evaluatorul de risc ori rolul competent revizuieste riscul în limitele atribuțiilor sale. O funcționare fără incidente nu dovedește, singură, că riscul a rămas acceptabil.

8.7.1 Declanșatori

Reevaluarea este analizată la modificarea activelor, proceselor, programului, ocupării, amenințărilor, vecinătăților, infrastructurii, fluxurilor de acces, cerințelor legale, tehnologiilor, furnizorilor sau interconectărilor; după incidente, defecte sistemice, alarme nedorite persistente, vulnerabilități semnificative, pierderea suportului ori depășirea capacității; precum și la expirarea intervalului stabilit de organizație sau de cadrul aplicabil.

8.7.2 Decizia și riscul rezidual

Rezultatul poate confirma măsurile, poate impune controale suplimentare, modificarea procedurilor, limitarea temporară, reproiectarea ori retragerea unei funcții. Riscul rezidual este prezentat decidentului competent împreună cu ipotezele, incertitudinile, perioada de valabilitate și măsurile compensatorii. Lipsa bugetului nu constituie, în sine, justificare tehnică pentru acceptarea riscului.

8.8 Evidența configurației

Managementul configurației păstrează corespondența dintre sistemul fizic, configurația logică, documentație și dovezi. Unitatea de configurație poate fi echipament, software, firmware, regulă, hartă, utilizator privilegiat, certificat, licență, interfață, fișier ori document. Fiecare are identificator, proprietar, versiune sau stare, locație, relații și istoric.

8.8.1 Baseline, inventar și copii de siguranță

Configurația de referință aprobată include inventarul, seriile, adresele, versiunile, parametrii, dependențele, licențele, certificatele și exporturile necesare restaurării. Copiile sunt protejate, separate adecvat, testate prin restaurare și păstrate conform criticității. Existența unui fișier de backup neverificat nu demonstrează recuperabilitatea.

8.8.2 Vulnerabilități, actualizări și suport

Se urmăresc notificările furnizorilor și sursele relevante, se evaluează expunerea și se prioritizează remedierea după risc. Actualizările sunt autentice, verificate pentru compatibilitate, testate și însoțite de plan de revenire. Excepțiile de la actualizare au motiv, măsuri compensatorii, proprietar și termen de revizuire. Sfârșitul suportului este tratat anticipat ca risc de ciclu de viață și intrare în planul de înlocuire.

8.9 Scoaterea din funcțiune

Scoaterea din funcțiune este un proiect controlat, nu simpla deconectare a echipamentului. Ea poate fi totală, parțială, temporară ori determinată de înlocuire și trebuie să mențină protecția activelor în tranziție. Se stabilesc autoritatea, domeniul, dependențele, măsurile alternative, data încetării serviciului și criteriul de finalizare.

8.9.1 Conservarea, migrarea și eliminarea datelor

Înainte de oprire se identifică datele, jurnalele și configurațiile care trebuie păstrate din motive operaționale, probatorii, contractuale sau legale. Datele necesare sunt exportate și validate; restul este șters controlat din echipamente, suporturi, servicii și copii, conform regulilor aplicabile. Cheile, certificatele, tokenurile, conturile și conexiunile sunt revocate, iar suporturile sunt reutilizate, returnate ori distruse documentat.

8.9.2 Închiderea tehnică și administrativă

Se elimină alimentările și traseele în siguranță, se actualizează planurile, inventarul, contractele, licențele și registrele, se retrag accesurile furnizorilor și se confirmă funcționarea sistemelor rămase. Echipamentele transferate au starea și destinația consemnate. Raportul final documentează ceea ce a fost retras, datele tratate, riscurile rămase și acceptarea de către proprietarul sistemului.

Închiderea Capitolului 8

Rezultatul Capitolului 8 este un sistem administrat pe durata de viață prin roluri clare, proceduri controlate, mentenanță proporțională cu criticitatea, indicatori care declanșează acțiuni, incidente analizate, schimbări autorizate, configurație reproductibilă și o retragere planificată. Exploatarea furnizează permanent informații către context, risc și cerințe, închizând bucla de îmbunătățire a metodologiei S.I.G.M.A.

Referințe tehnice și normative pentru Capitolul 8

- [R1] IEC 62676-4:2025 — sisteme de supraveghere video pentru aplicații de securitate; ghid de aplicare care include menținerea sistemelor VSS.
- [R2] IEC 60839-11-2:2014 — sisteme electronice de control al accesului; cerințe și ghiduri privind operarea, mentenanța și documentarea.
- [R3] IEC TS 62642-7:2011 — sisteme de alarmare la efracție și atac; ghid de aplicare pentru proiectare, instalare, punere în funcțiune, exploatare și mentenanță.
- [R4] ISO 55001:2024 — managementul activelor; cerințe privind deciziile, planificarea, datele, cunoștințele și operațiile ciclului de viață.

- [R5] ISO/IEC/IEEE 15288:2023 — procese ale ciclului de viață al sistemelor, inclusiv operare, mentenanță, managementul configurației și eliminare.
- [R6] ISO 22301:2019 și Amd 1:2024 — managementul continuității activității și reziliența la perturbări.
- [R7] ISO/IEC 27001:2022 și Amd 1:2024, împreună cu ISO/IEC 27002:2022 — managementul securității informațiilor și controale de securitate.
- [R8] ISO/IEC 27035-1:2023 — principii și proces pentru managementul incidentelor de securitate a informațiilor.
- [R9] Regulamentul (UE) 2016/679 — protecția datelor cu caracter personal, inclusiv securitatea, păstrarea și ștergerea datelor.
- [R10] Directiva (UE) 2022/2555 (NIS 2), O.U.G. nr. 155/2024 și Legea nr. 124/2025, în domeniul lor de aplicare — managementul riscurilor de securitate cibernetică și raportarea incidentelor.
- [R11] Legea nr. 333/2003, H.G. nr. 301/2012 și actele modificatoare, în forma aplicabilă — obligații naționale privind exploatarea, reviziile, întreținerea și evidențele sistemelor de alarmare împotriva efracției.
- [R12] ISO 9001:2015 și Amd 1:2024 — controlul informațiilor documentate, al furnizorilor, al schimbărilor, neconformităților și îmbunătățirii.

Notă de control normativ: edițiile, amendamentele, adoptările naționale, domeniul de aplicare și caracterul obligatoriu al fiecărei referințe se verifică la data exploatării și înaintea fiecărei schimbări relevante. Periodicitățile, competențele și obligațiile de notificare se stabilesc din cadrul legal, documentația sistemului, contract și evaluarea riscului; metodologia nu substituie o cerință imperativă ori decizia autorității competente.

ANEXE

Fluxuri, matrici, registre și liste de verificare

Anexele transformă cerințele metodologiei S.I.G.M.A. în instrumente de lucru controlabile. Modelele sunt minime: organizația le poate extinde, dar nu trebuie să elimine identificarea, responsabilitatea, criteriul de acceptare, dovada, starea și legătura cu cerința ori riscul. Câmpurile neaplicabile se marchează „N/A” și se justifică; ele nu se lasă necompletate fără explicație.

Indexul anexelor

Anexa A1 — Fluxul integrat și porțile de control

Fluxul se adaptează dimensiunii proiectului fără a elimina funcțiile de control. Iterațiile sunt permise și așteptate; revenirea la o etapă anterioară se înregistrează când o ipoteză, o cerință, un risc ori o interfață se modifică.

A1.1 Fișa unei porți de control

Anexa A2 — Matricea de conformitate normativă

Matricea se completează la nivel de cerință, nu doar la nivel de titlu de act sau standard. Se consemnează ediția și data verificării, domeniul de aplicare, caracterul cerinței și modul concret în care proiectul demonstrează conformitatea.

A2.1 Clasificarea statutului

Anexa A3 — Registrul contextului, activelor și părților interesate

A3.1 Fișa contextului obiectivului

A3.2 Registrul activelor

A3.3 Registrul părților interesate

Anexa A4 — Registrul scenariilor, riscurilor și tratamentelor

Registrul păstrează delimitarea responsabilităților: proiectantul nu modifică unilateral evaluarea riscului. Când datele sunt insuficiente ori contradictorii, se înregistrează problema și se solicită clarificarea rolului competent.

A4.1 Planul de tratare și riscul rezidual

Anexa A5 — Matricea de trasabilitate a cerințelor

Cerințele se formulează singular, verificabil și independent de marcă, dacă nu există o justificare aprobată. Fiecare cerință primește sursă, prioritate, criteriu de acceptare și metodă de verificare. Legăturile dintre cerințe se mențin la modificare.

A5.1 Controlul calității unei cerințe

Anexa A6 — Registrul interfețelor și matricea cauză–efect

A6.1 Registrul interfețelor

A6.2 Matricea cauză–efect

A6.3 Fișa modului degradat

Anexa A7 — Matricea de verificare, validare și recepție

Verificarea răspunde întrebării dacă livrabilul este realizat corect față de cerințe; validarea confirmă dacă sistemul răspunde nevoii reale în contextul de utilizare. Recepția este actul de acceptare contractuală și nu șterge neconformități ori responsabilități neclarificate.

A7.1 Proces-verbal sintetic de test

A7.2 Registrul punctelor de recepție

Anexa A8 — Registrele de neconformități, decizii și ipoteze

A8.1 Registrul neconformităților

A8.2 Registrul deciziilor și derogărilor

A8.3 Registrul ipotezelor, dependențelor și acțiunilor

Anexa A9 — Registrele ciclului de viață

A9.1 Registrul activelor și configurației

A9.2 Planul și jurnalul de mentenanță

A9.3 Registrul alarmelor și incidentelor

A9.4 Registrul schimbărilor

A9.5 Registrul indicatorilor

Anexa A10 — Listele de verificare C1–C8

Bifarea confirmă existența unei dovezi identificabile. „N/A” este acceptabil numai cu justificare și cu confirmarea persoanei care deține autoritatea asupra cerinței. O poartă poate fi aprobată condiționat numai dacă riscurile și acțiunile rămase au proprietar, termen și criteriu de închidere.

A10.1 C1 — Inițiere și guvernanță

A10.2 C2 — Cadrul aplicabil

A10.3 C3 — Date și amplasament

A10.4 C4 — Context, risc și cerințe

A10.5 C5 — Proiectarea subsistemelor

A10.6 C6 — Integrare, reziliență și informații

A10.7 C7 — Verificare, punere în funcțiune și recepție

A10.8 C8 — Exploatare și schimbare

A10.9 Decizia consolidată

Controlul și adaptarea anexelor

Modelele A1–A10 constituie setul minim recomandat pentru aplicarea metodologiei. Ele pot fi separate în formulare, baze de date sau aplicații, cu condiția păstrării câmpurilor obligatorii, a identificatorilor și a relațiilor dintre înregistrări. Orice adaptare se controlează ca versiune și se testează pe un proiect înainte de utilizarea generală.

Structura editorială generală

Planul de dezvoltare al versiunii sintetice

Notă editorială: documentul-master va fi completat succesiv. La fiecare revizie vor fi actualizate istoricul, cuprinsul, referințele și corelările dintre capitole. Versiunea finală pentru aprobare va include numai texte validate profesional și referințe normative verificate la data emiterii.

Câmp

Conținut

Denumirea documentului

ARES S.I.G.M.A. — Metodologie integrată pentru proiectarea sistemelor de securitate fizică

Tipul documentului

Metodologie profesională — versiune sintetică

Emitent propus

Asociația pentru Reziliență, Evaluare și Securitate (ARES)

Cod document

ARES-SIGMA-MET-01

Ediție / revizie

Ediția 1 / Revizia 0

Statut

Proiect pentru consultare profesională; neaprobat la data redactării

Domeniu

Proiectarea integrată a sistemelor de detecție și alarmare la efracție, supraveghere video, control al accesului și a interfețelor asociate

Public-țintă

Proiectanți, instalatori, integratori, evaluatori de risc, beneficiari, verficatori și personal responsabil de exploatare

Regim de actualizare

Revizuire la modificarea cadrului legal, normativ, tehnologic sau a practicii profesionale relevante

0.6

11.08.2026

0.7

11.08.2026

0.8

11.08.2026

0.9

11.08.2026

REGULĂ DE UTILIZARE Nicio recomandare din metodologie nu poate fi invocată pentru diminuarea unei obligații legale, normative, contractuale ori profesionale aplicabile proiectului.

Ediție

Revizie

Data

Descriere

Statut

1

0

10.08.2026

Versiune de lucru v0.2: elemente preliminare, Capitolul 1 și Capitolul 2

Proiect

1

0

10.08.2026

Versiune de lucru v0.3: integrarea Capitolului 3 — Procesul integrat de proiectare

Proiect

1

0

10.08.2026

Versiune de lucru v0.4: integrarea Capitolului 4 — Context, cerințe și riscuri

Proiect

1

0

11.08.2026

Versiune de lucru v0.9: integrarea Capitolului 5 — Proiectarea subsistemelor

Proiect

MESAJ INSTITUȚIONAL Proiectarea unui sistem de securitate este un act de responsabilitate inginerească. Valoarea proiectului se măsoară prin claritatea cerințelor, justificarea soluțiilor, posibilitatea verificării și eficacitatea sistemului pe întreg ciclul său de viață.

Etapă

Întrebare centrală

Rezultat principal

Context

Ce trebuie protejat și în ce condiții?

Date validate despre obiectiv, active, utilizare și constrângeri

Risc

Ce se poate întâmpla și cu ce efect?

Scenarii și priorități de tratare

Cerințe

Ce trebuie să realizeze soluția?

Cerințe funcționale, de performanță și conformitate

Concept

Cum va fi organizată protecția?

Concept operațional și arhitectură de securitate

Proiectare

Prin ce mijloace se obține performanța?

Calcul, selecții, planuri, scheme și specificații

Verificare

Este soluția corectă și completă?

Dovezi de conformitate și închiderea neconformităților

Ciclu de viață

Rămâne soluția eficientă în timp?

Mentenanță, evidența configurației și reevaluare

CRITERIU S.I.G.M.A. O soluție tehnică este complet justificată numai dacă necesitatea, performanța, implementarea și verificarea sa pot fi urmărite fără rupturi în documentația proiectului.

Termen

Definiție operațională S.I.G.M.A.

Activ

- persoană, bun, informație, proces, capacitate sau reputație care are valoare pentru organizație și poate necesita protecție.

Amenințare

- cauză potențială a unui eveniment nedorit, intenționat sau neintenționat, capabil să producă prejudicii.

Vulnerabilitate

- slăbiciune sau condiție care poate fi exploatată de o amenințare ori poate amplifica efectele unui eveniment.

Risc

- efectul incertitudinii asupra obiectivelor, exprimat metodologic prin corelarea scenariului, probabilității și consecințelor.

Probabilitate

- aprecierea posibilității ca un eveniment sau scenariu să se producă într-un interval și context definite.

Consecință / impact

- efectul producerii evenimentului asupra persoanelor, bunurilor, informațiilor, operațiunilor, conformității ori reputației.

Măsură de securitate

- mijloc tehnic, fizic, uman, procedural sau organizațional care modifică riscul.

Tratarea riscului

- procesul de selectare și implementare a opțiunilor pentru modificarea riscului.

Risc rezidual

- riscul rămas după aplicarea măsurilor de tratare, inclusiv incertitudinile asociate eficacității acestora.

Cerință

- nevoie sau așteptare declarată, obligatorie ori implicită, care trebuie transformată într-o condiție verificabilă.

Performanță

- rezultat măsurabil referitor la capacitatea unui sistem, subsistem sau element de a îndeplini o funcție.

Nivel de securitate

- stare rezultată din ansamblul măsurilor și performanțelor raportate la riscurile și criteriile de acceptare stabilite.

PRINCIPIU DE COERENȚĂ Nu se proiectează o măsură izolată de scenariul pe care îl tratează și nu se declară un risc acceptabil fără identificarea nivelului rezidual și a autorității care îl acceptă.

Nivel

Conținut

Dovadă principală

Strategic

Context, active, criterii, risc și priorități

Temă, analiză, decizie de acceptare

Funcțional

Scenarii, funcții, cerințe și concept operațional

Registrul cerințelor și conceptul de securitate

Tehnic

Arhitectură, dimensionare, selecție și documentație

Memoriu, calcule, planșe, scheme, specificații

Asigurare

Revizuire, verificare, testare și recepție

Liste de verificare, protocoale și procese-verbale

Ciclu de viață

Exploatare, mentenanță, modificări și reevaluare

Dosarul sistemului și evidența configurației

Cod

Principiu

Regulă de aplicare

P1

Legalitate și conformitate

Soluția respectă cerințele obligatorii și documentează baza aplicabilă.

P2

Orientare către risc

Prioritățile și măsurile sunt justificate prin scenarii și consecințe relevante.

P3

Abordare integrată

Tehnologia, oamenii, procedurile și infrastructura sunt analizate ca ansamblu.

P4

Performanță verificabilă

Cerințele sunt formulate astfel încât îndeplinirea lor să poată fi demonstrată.

P5

Proportionalitate

Profunzimea și costul soluției sunt adecvate riscului și consecințelor.

P6

Apărare în profunzime

Măsurile complementare previn dependența de un singur control sau punct de defect.

P7

Trasabilitate

Fiecare decizie relevantă are sursă, justificare și dovadă de verificare.

P8

Reziliență

Sistemul gestionează defectele, întreruperile și schimbările în mod previzibil.

P9

Neutralitate tehnologică

Cerințele nu sunt limitate nejustificat la un producător sau produs.

P10

Îmbunătățire continuă

Experiența din exploatare și modificările contextului sunt reintegrate în proces.

Cod

Rezultat

Conținut esențial

R1

Fișa de inițiere

mandat, obiective, părți interesate, limite și responsabilități

R2

Tema de proiectare

cerințe inițiale, date de intrare, constrângeri și livrabile

R3

Registrul cerințelor

sursă, formulare, prioritate, responsabil, soluție și verificare

R4

Modelul riscurilor

active, amenințări, vulnerabilități, scenarii și risc rezidual

R5

Conceptul de securitate

funcții, zonare, fluxuri operaționale și principii de răspuns

R6

Arhitectura sistemului

subsisteme, interfețe, comunicații, alimentare și moduri degradate

R7

Documentația tehnică

memorii, calcule, planuri, scheme, liste și specificații

R8

Planul de verificare

metode, criterii, responsabilități și dovezi necesare

R9

Dosarul final

configurația instalată, testele, instruirea, exploatarea și mentenanța

R10

Registrul schimbărilor

modificări, impact, aprobări, versiuni și necesitatea reevaluării

LIVRABIL INTERMEDIAR Capitolul 1 stabilește baza comună de interpretare. Capitolele următoare vor transforma această bază în reguli de conformitate, etape de proiectare, criterii tehnice și instrumente de verificare.

REGULĂ S.I.G.M.A. Nicio soluție nu se declară conformă numai prin enumerarea unor acte normative sau standarde. Conformitatea trebuie demonstrată prin cerințe identificate, soluții trasabile și dovezi de verificare.

Nivel

Exemple

Regulă de aplicare

L1 — Dreptul Uniunii Europene și legea națională

regulamente UE; legi; ordonanțe și ordonanțe de urgență

Se aplică în domeniul și condițiile stabilite de act; prevalează asupra surselor inferioare.

L2 — Acte administrative normative

hotărâri ale Guvernului; ordine; instrucțiuni; reglementări tehnice

Detaliază aplicarea legii; nu pot restrânge, extinde ori contrazice nepermis actul superior.

L3 — Standarde și specificații tehnice

standarde SR, EN, IEC, ISO; ghiduri de aplicare; specificații de interoperabilitate

Sunt aplicate în condițiile în care sunt impuse, asumate contractual ori selectate ca referință tehnică.

L4 — Cerințe ale autorităților și avize

condiții oficiale, prescripții, acorduri și avize aplicabile obiectivului

Se verifică emitentul, temeiul, domeniul, valabilitatea și forma oficială.

L5 — Contract și tema de proiectare

caiet de sarcini, ofertă acceptată, cerințe ale beneficiarului, politici interne

Sunt obligatorii între părți dacă sunt legale, clare și incluse în domeniul convenit.

L6 — Documentații și reguli profesionale

- instrucțiuni ale producătorului, bune practici, metodologia S.I.G.M.A.

Completează soluția; nu diminuează cerințele de nivel superior și trebuie folosite în ediția relevantă.

CITAT LEGAL — O.G. NR. 39/1998 „Aplicarea unui standard național are caracter voluntar.” [N4]

Document

Rol în proiectare

Control necesar

Legea nr. 333/2003, modificată inclusiv prin O.U.G. nr. 37/2026

stabilește cadrul primar, activitățile licențiate, obligațiile unității și regimul proiectelor și al sistemelor

forma consolidată, data intrării în vigoare și eventualele acte de aprobare/modificare a ordonanței

H.G. nr. 301/2012 și anexele sale

detaliază cerințele minimale, organizarea activităților și normele tehnice aplicabile sistemelor

forma actualizată și compatibilitatea dispozițiilor cu legea modificată ulterior

Instrucțiunile M.A.I. nr. 9/2013

reglementează efectuarea analizelor de risc la securitatea fizică

aplicabilitatea la tipul unității și corelarea cu noile dispoziții legale privind analiza de risc și fișa de securitate

Acte sectoriale

pot introduce cerințe suplimentare pentru domenii precum financiar-bancar, jocuri de noroc, infrastructuri, patrimoniu sau obiective speciale

domeniu, autoritate competentă, condiții speciale și actualitate

CITAT LEGAL — LEGEA NR. 333/2003, ART. 27 ALIN. (6) „Instalarea ori modificarea sistemelor [...] se realizează conform proiectului” [N1].

REGULĂ TRANZITORIE În caz de necorelare între Legea nr. 333/2003, modificată prin O.U.G. nr. 37/2026, și H.G. nr. 301/2012, proiectantul documentează conflictul, aplică ierarhia juridică și solicită clarificare oficială când procedura concretă rămâne incertă.

Domeniu

Familii de referință

Utilizare principală

Cerințe generale și mediu

SR EN 50130, părțile aplicabile

compatibilitate electromagnetică, condiții și clase de mediu, metode comune de încercare

Efracție și jaf armat

SR EN 50131; ghidurile de aplicare aferente

grade de securitate, funcții, componente, surse de alimentare, interconectări și proiectarea aplicației

Transmiterea alarmelor

SR EN 50136 și standardele asociate centrelor de recepție

performanță, disponibilitate, căi de transmisie, echipamente și supravegherea legăturilor

Supraveghere video

SR EN/IEC 62676, părțile aplicabile

cerințe de sistem, proiectare, performanța imaginii, transmisie, testare și mentenanță

Control electronic al accesului

SR EN/IEC 60839-11, părțile aplicabile

funcții, grade, componente, planificare, instalare, punere în funcțiune și operare

Sisteme combinate și integrate

SR EN 50398-1 și documente de interoperabilitate aplicabile

integrare, interfețe, priorități, integritate și comportare la defect

Infrastructură electrică și comunicații

seria SR HD 60364, I 7/2011, standarde de cablare și protecție aplicabile

alimentare, protecții, separare, trasee, legare la pământ, continuitate și condiții de instalare

REGULĂ DE SELECȚIE Marcajul, certificarea sau conformitatea unei componente nu transferă automat conformitatea asupra arhitecturii, amplasării, programării ori exploatării întregului sistem.

Clasă

Exemple

Tratament S.I.G.M.A.

Conformitate

obligații legale, cerințe minimale, avize și condiții oficiale

se identifică temeiul și metoda de demonstrare; nu se negociază sub nivelul obligatoriu

Funcțională

detectare, verificare video, autorizare acces, transmitere alarmă

se exprimă prin rezultat observabil și scenariu de utilizare

Performanță

autonomie, acoperire, densitate de pixeli, capacitate, timp, disponibilitate

se cuantifică și se leagă de o metodă de calcul sau testare

Operațională

roluri, program, fluxuri, răspuns, mentenanță, continuitate

se validează cu utilizatorii și se integrează în conceptul de operare

Contractuală

buget, termene, formate, livrabile, garanție, instruire

se corelează cu domeniul, riscurile și criteriile de acceptanță

Restricție

arhitectură existentă, spațiu, estetică, patrimoniu, IT, confidențialitate

se evaluează impactul; restricțiile incompatibile se escaladează

Participant

Responsabilitate principală

Nu poate transfera tacit

Beneficiar / conducătorul unității

definește mandatul, furnizează datele, aprobă cerințele și riscul rezidual; asigură transmiterea documentelor impuse de lege

decizia de acceptare a riscului și obligațiile proprii de conformitate

Evaluator de risc

fundamentează scenariile, vulnerabilitățile, nivelurile de risc și măsurile necesare, în limitele cadrului aplicabil
proiectarea tehnică detaliată și selectarea nejustificată a produselor

Proiectant

transformă cerințele în arhitectură, calcule, planuri, specificații și criterii de verificare
răspunderea pentru coerența și conformitatea soluției în faza de proiect

Instalator

execută conform proiectului, manualelor și reglementărilor; documentează lucrările și neconformitățile
aprobarea unilaterală a modificărilor cu impact asupra funcțiilor proiectate

Verificator / revizor

controlează completitudinea, corectitudinea și trasabilitatea în domeniul mandatului și competenței
responsabilitatea autorului sau aprobarea riscului de către beneficiar

Integrator

coordonează interfețele, fluxurile, configurațiile și testarea între subsisteme
responsabilitățile specialiștilor pentru fiecare domeniu

Furnizor / producător

furnizează date corecte de produs, condiții de utilizare, compatibilități și dovezi de conformitate
adecvarea aplicației concrete, dacă nu are mandat și informații de proiectare

Utilizator / operator

validează fluxurile operaționale, participă la testare și exploatează sistemul conform instrucțiunilor
deficiențele de proiect sau execuție pe care nu le-a aprobat informat

Mentenanță

menține funcțiile, înregistrează defectele și modificările, raportează degradările
schimbarea necontrolată a configurației și cerințelor inițiale

CITAT NORMATIV — H.G. NR. 301/2012, ART. 70 ALIN. (3) „Proiectantul sistemului de securitate răspunde [...] în faza de proiect” [N3].

Conflict

Criteriu de soluționare

Dovadă

Lege modificată ulterior vs. normă metodologică necorelată

prevalează actul superior și ulterior; procedura incertă se clarifică oficial

notă legislativă, solicitare/răspuns, registrul versiunilor

Control acces vs. evacuare la incendiu

siguranța vieții și condițiile de evacuare nu pot fi diminuate de funcția de securitate

scenariu, matrice cauză–efect, aviz/validare de specialitate, test integrat

Acoperire video extinsă vs. minimizarea datelor

se limitează captarea la scopul legitim și necesar; se analizează măsuri mai puțin intruzive

analiza scopului, unghiuri, mascări, perioadă de stocare, evaluare de impact când este necesară

Buget vs. cerință de performanță

se optimizează soluția fără a masca reducerea performanței; riscul rezultat se escaladează

analiza alternativelor și decizia informată a beneficiarului

Standard nou vs. ediție contractuală

se verifică obligația contractuală, perioada de tranziție și impactul tehnic al noii ediții

notă de impact și decizie de aplicare

Instrucțiune de produs vs. condiții reale

produsul se utilizează numai în limitele declarate sau se selectează o soluție adecvată

fișă tehnică, calcul, probă și confirmarea producătorului

TESTUL ECHIVALENȚEI „Diferit” nu înseamnă automat „neconform”, iar „mai performant” nu înseamnă automat „compatibil”. Echivalența se demonstrează pentru toate funcțiile și condițiile relevante, nu printr-un singur indicator favorabil.

Câmp minim

Conținut

ID

cod unic al referinței

Tip

lege, hotărâre, ordin, standard, contract, aviz, manual, politică

Referință completă

număr, titlu, emitent și domeniu

Ediție / formă

an, amendament, consolidare, versiune software ori revizie

Statut

în vigoare, înlocuit, retras, proiect, perioadă de tranziție

Aplicabilitate

obligatoriu, contractual, recomandat, informativ; domeniul exact

Cerințe derivate

ID-urile cerințelor introduse în registrul proiectului

Responsabil

persoana care verifică și aplică documentul

Data verificării

data consultării sursei oficiale

Dovadă / observații

link, copie controlată, conflict, clarificare sau derogare

LIVRABIL INTERMEDIAR Baza de conformitate aprobată devine intrare obligatorie pentru Capitolul 3 — Procesul integrat de proiectare S.I.G.M.A. Orice schimbare ulterioară trebuie tratată prin managementul configurației și al cerințelor.

PRINCIPIUL INTEGRĂRII Nicio etapă nu este considerată închisă numai pentru că a fost produs un document. Etapa se închide atunci când intrările au fost verificate, deciziile critice sunt trasabile, rezultatele sunt aprobate de rolurile competente, iar neclaritățile cu impact au fost soluționate sau controlate explicit.

Etapă

Întrebarea de control

Rezultat dominant

Poartă

3.1 Inițiere

Există un mandat legitim, un domeniu preliminar și resurse adecvate?

Fișa de inițiere și planul procesului

G1

3.2 Tema de proiectare

Este definit ce trebuie obținut și în ce limite?

Tema aprobată și criteriile de acceptanță

G2

3.3 Colectarea informațiilor

Sunt datele necesare suficiente, actuale și controlate?

Dosarul datelor de intrare

G3

3.4 Investigarea amplasamentului

Au fost confirmate condițiile reale ale obiectivului?

Raportul de investigare și releveul validat

G4

3.5 Cerințele de securitate

Sunt riscurile transformate în cerințe clare și verificabile?

Registrul cerințelor și matricea de trasabilitate

G5

3.6 Conceptul de securitate

Este definit modul în care oamenii, procedurile și tehnologia vor trata scenariile?

Conceptul operațional și alternativa selectată

G6

3.7 Arhitectura sistemului

Sunt funcțiile alocate coerent subsistemelor și interfețelor?

Arhitectura funcțională și tehnică înghețată

G7

3.8 Dimensionare și echipamente

Poate soluția atinge performanța în condițiile reale?

Calcul, selecții și dovezi de adecvare

G8

3.9 Documentația tehnică

Este soluția descrisă complet, univoc și executabil?

Pachetul de proiect controlat

G9

3.10 Verificare și validare

Este proiectul corect și răspunde nevoii aprobate?

Raport de verificare, validare și autorizare a emiterii

G10

CITAT DE REFERINȚĂ — ISO/IEC/IEEE 15288:2023 Standardul „does not prescribe a specific system life cycle model” [P1]. În consecință, S.I.G.M.A. stabilește rezultate și controale necesare, dar permite adaptarea modelului de lucru la proiect.

Element

Definire

Scop

autorizarea controlată a proiectului și stabilirea cadrului de lucru

Intrări

solicitarea beneficiarului, contractul sau mandatul, date preliminare despre obiectiv, analiza de risc disponibilă, termenele și restricțiile cunoscute

Decizia critică

acceptarea, condiționarea sau refuzul inițierii în raport cu competența, legalitatea, informațiile și resursele

Livrabile

fișa de inițiere, domeniul preliminar, matricea rolurilor, planul etapelor, registrul inițial al riscurilor de proiect și lista datelor solicitate

POARTA G1 — AUTORIZAREA INIȚIERII Se poate trece la definirea temei numai dacă mandatul este clar, rolurile esențiale sunt desemnate, accesul la date este posibil, iar nicio restricție cunoscută nu face proiectul nelegal, neexecutabil sau incompatibil cu competența echipei.

Element

Definire

Scop

stabilirea bazei aprobate pentru dezvoltarea proiectului

Intrări

fișa de inițiere, cerințele beneficiarului, documentele de risc și conformitate, informațiile preliminare despre amplasament și exploatare

Decizia critică

confirmarea caracterului suficient, coerent, legal și verificabil al temei

Livrabile

tema de proiectare aprobată, lista criteriilor de acceptanță, limitele și excluderile, registrul ipotezelor și al clarificărilor

POARTA G2 — APROBAREA TEMEI Tema poate fi înghețată numai dacă domeniul, rezultatele urmărite, limitele, responsabilitățile și criteriile de acceptanță sunt suficient de clare pentru a ghida colectarea datelor și analiza ulterioară.

Element

Definire

Scop

constituirea unui set de date controlat, suficient și verificabil

Intrări

tema aprobată, lista informațiilor solicitate, registrele inițiale, accesul la persoane, documente și sisteme

Decizia critică

acceptarea datelor ca suficiente pentru investigarea și definirea cerințelor sau stabilirea măsurilor compensatorii

Livrabile

registruul datelor de intrare, lista lipsurilor și contradicțiilor, inventarul sistemelor existente, dosarul documentelor validate

POARTA G3 — ACCEPTAREA BAZEI DE DATE Colectarea se consideră suficientă când informațiile critice sunt confirmate, diferențele dintre surse sunt rezolvate ori controlate, iar lipsurile rămase au o strategie documentată care nu compromite investigația și proiectarea.

Element

Definire

Scop

validarea condițiilor reale, a constrângerilor și a posibilității de implementare

Intrări

tema, dosarul datelor, planul investigației, listele de verificare, instrumentele și aprobările de acces

Decizia critică

confirmarea fezabilității fizice și identificarea măsurilor necesare pentru diferențele față de datele documentare

Livrabile

raport de investigare, relevu și fotografii controlate, măsurători, marcaje de amplasament, lista discrepanțelor și a riscurilor de implementare

POARTA G4 — VALIDAREA AMPLASAMENTULUI Se poate continua când situația reală este suficient documentată, măsurătorile critice sunt disponibile, discrepanțele au fost evaluate și nu există obstacole necunoscute care să invalideze tema sau fezabilitatea soluției.

Element

Definire

Scop

constituirea unei baze unice, aprobate și verificabile a cerințelor

Intrări

tema, analiza de risc, cadrul aplicabil, dosarul datelor, raportul de investigare și cerințele părților interesate

Decizia critică

acceptarea cerințelor ca necesare, coerente, fezabile, prioritizate și verificabile

Livrabile

registrul cerințelor, matricea de trasabilitate, alocarea preliminară, conflictele și criteriile de verificare

Atribut minim

Rol în controlul cerinței

ID unic

permite referirea fără ambiguitate și menține istoricul

Sursă și justificare

leagă cerința de risc, lege, contract, utilizator sau decizie

Text verificabil

definește rezultatul și condițiile în care trebuie obținut

Prioritate / criticitate

susține alocarea resurselor și controlul modificărilor

Responsabil / aprobator

stabilește cine clarifică și cine acceptă cerința

Metodă și criteriu de verificare

arată cum se va demonstra îndeplinirea

Alocare

indică subsistemul, procedura, rolul uman sau interfața care o realizează

Stare și versiune

controlează propunerea, aprobarea, modificarea, înlocuirea și închiderea

POARTA G5 — ÎNGHEȚAREA BAZEI DE CERINȚE Registrul poate deveni bază de proiectare numai după ce cerințele critice sunt aprobate, conflictele sunt rezolvate ori escaladate, criteriile de verificare sunt definite, iar trasabilitatea către riscuri și surse este demonstrată.

Element

Definire

Scop

selectarea unei strategii coerente de tratare a riscurilor și operare a securității

Intrări

baza de cerințe, scenariile, fluxurile operaționale, constrângerile amplasamentului și alternativele fezabile

Decizia critică

alegerea conceptului care îndeplinește cerințele cu risc rezidual, complexitate și cost de ciclu de viață acceptabile

Livrabile

conceptul operațional, scenariile de utilizare și defect, zonarea, principiile de răspuns și raportul de selecție a alternativei

POARTA G6 — APROBAREA CONCEPTULUI Conceptul poate fi aprobat când tratează scenariile prioritare, alocă roluri între tehnologie și oameni, definește funcționarea normală și degradată, iar alternativa selectată are o justificare acceptată de beneficiar.

Element

Definire

Scop

alocarea coerentă a funcțiilor și cerințelor către elementele sistemului și interfețe

Intrări

conceptul aprobat, registrul cerințelor, datele amplasamentului, infrastructurile disponibile și constrângerile interdisciplinare

Decizia critică

înghețarea structurii de bază și confirmarea că dependențele, interfețele și modurile degradate sunt controlate

Livrabile

diagrame funcționale și tehnice, matrice de interfețe, matrice cauză–efect preliminară, bugete de capacitate și registrul dependențelor

POARTA G7 — ÎNGHEȚAREA ARHITECTURII Arhitectura poate fi înghețată când toate cerințele critice sunt alocate, interfețele au proprietari și comportamente definite, punctele unice de defect sunt tratate, iar bugetele preliminare demonstrează fezabilitatea.

Element

Definire

Scop

demonstrarea cantitativă a performanței și selectarea unor produse compatibile, conforme și sustenabile

Intrări

arhitectura înghețată, cerințele alocate, datele măsurate, standardele aplicabile și informațiile controlate ale producătorilor

Decizia critică

acceptarea calculelor, rezervelor, compatibilității și dovezilor de adecvare pentru fiecare selecție critică

Livrabile

memorii de calcul, fișe de selecție, liste de echipamente, verificări de compatibilitate, bugete de capacitate și excepții aprobate

POARTA G8 — ACCEPTAREA DIMENSIONĂRII Soluția poate fi trecută în documentația finală numai dacă performanța este demonstrată, produsele sunt adecvate mediului și utilizării, interfețele și versiunile sunt compatibile, iar rezervele sunt explicate și suficiente.

Element

Definire

Scop

emiterea unui pachet coerent, executabil, verificabil și controlat

Intrări

tema, cerințele, conceptul, arhitectura, calculele, selecțiile, coordonările și deciziile aprobate

Decizia critică

confirmarea completitudinii și coerenței interne pentru starea de emitere solicitată

Livrabile

memoriu, planuri, scheme, detalii, specificații, liste, calcule, matrice, plan de testare, borderou și registrul reviziilor

POARTA G9 — AUTORIZAREA PACHETULUI PENTRU VERIFICARE Pachetul este pregătit pentru verificare numai dacă piesele obligatorii sunt prezente, informațiile sunt coerente, starea și revizia sunt clare, iar proiectul poate fi evaluat fără explicații informale ale autorului.

Element

Definire

Scop

demonstrarea corectitudinii, completitudinii, conformității și adecvării proiectului

Intrări

pachetul de proiect, registrele, baza de conformitate, matricea de trasabilitate, criteriile și dovezile etapelor anterioare

Decizia critică

autorizarea emiterii, emiterea condiționată, returnarea pentru corecții sau respingerea proiectului

Livrabile

liste de verificare, raport de revizuire, registrul neconformităților, dovezi de validare, declarația de conformitate și aprobarea emiterii

POARTA G10 — EMITEREA PENTRU EXECUȚIE Proiectul se emite numai după închiderea neconformităților critice și majore, confirmarea trasabilității, aprobarea abaterilor și validarea soluției. Acțiunile minore rămase trebuie să aibă responsabil, termen și să nu afecteze executabilitatea, conformitatea sau funcțiile de securitate.

Rezultat obligatoriu

Dovada minimă

Mandat și guvernare

fișa de inițiere, roluri, domeniu și planul porților

Baza de proiectare

tema aprobată, cadrul aplicabil și dosarul datelor

Realitatea amplasamentului

raport, relevee, măsurători și discrepanțe controlate

Baza de cerințe

registru, priorități, criterii și trasabilitate

Concept și arhitectură

scenarii, alocări, interfețe, moduri și decizii

Demonstrația tehnică

calcul, selecții, compatibilități și rezerve

Pachet executabil

documente codificate, coerente, revizuite și distribuite controlat

Dovada calității

rapoarte de verificare și validare, neconformități închise și autorizarea emiterii

REGULA DE ÎNCHIDERE Un proiect este pregătit pentru execuție atunci când se poate demonstra, fără dependență de explicații verbale, ce problemă tratează, ce cerințe îndeplinește, prin ce soluție, pe baza căror calcule și cum va fi verificat.

CITAT NORMATIV — INSTRUCȚIUNILE M.A.I. NR. 9/2013 „Analiza de risc la securitatea fizică constituie fundamentul adoptării măsurilor de securitate” [R1]. Proiectarea trebuie să păstreze vizibilă această relație, fără să confunde atribuțiile evaluatorului cu cele ale proiectantului.

Nivel

Întrebare

Responsabilitate dominantă

Rezultat controlat

Context

În ce realitate funcționează obiectivul?

beneficiar, utilizatori, proiectant și specialități relevante

profilul contextual și baza de date validată

Evaluarea riscului

Ce evenimente pot afecta obiectivele și cu ce nivel?

evaluatorul de risc și conducătorul unității, în cadrul aplicabil

analiza de risc, măsurile și nivelurile aprobate

Analiza de proiectare

Sunt intrările suficiente și implementabile tehnic?

proiectantul, cu solicitarea clarificărilor necesare

registrul lacunelor, ipotezelor și constrângerilor

Cerințe

Ce trebuie să realizeze soluția și cum se demonstrează?

proiectantul împreună cu proprietarii cerințelor

baza de cerințe și matricea de trasabilitate

Domeniu

Aspecte de documentat

Organizațional

misiune, conducere, responsabilități, toleranță la întrerupere, politici și resurse

Fizic și teritorial

limite, vecinătăți, accesibilitate, relief, iluminat, căi de apropiere, construcții și zone comune

Operațional

program, fluxuri, activități, perioade de vârf, excepții, evenimente, lucru izolat și intervenție

Tehnic

sisteme existente, alimentări, rețele, spații tehnice, interfețe, redundanțe și limitări

Uman

categorii de utilizatori, vizitatori, contractori, competențe, comportamente previzibile și factori de eroare

Juridic și informațional

obligații, avize, contracte, confidențialitate, protecția datelor și clasificarea informațiilor

Temporal și extern

sezonalitate, lucrări, schimbări planificate, criminalitate relevantă, servicii publice și dependențe externe

CRITERIU DE IEȘIRE 4.1 Contextul este suficient numai dacă limitele, procesele, dependențele, persoanele cu rol decizional și condițiile reale de operare pot fi urmărite până la surse validate.

Atribut

Utilitate în proiectare

ID și denumire

identificare univocă în scenarii, cerințe, planuri și teste

Proprietar și custode

validarea valorii, regulilor de acces și acceptării riscului

Locație și mobilitate

stabilirea zonelor, traseelor, perioadelor de expunere și a limitelor

Valoare și criticitate

estimarea consecințelor pe dimensiuni comparabile

Cerințe de protecție

confidențialitate, integritate, disponibilitate, siguranță și trasabilitate

Dependențe

identificarea efectelor în cascadă și a punctelor unice de defect

Variație temporală

diferențierea programului normal, vârfurilor, transportului și stocării

REGULĂ PRIVIND ACTIVELE Dacă un element nu este înregistrat ca activ sau dependență, scenariile care îl afectează tind să dispară din analiză, iar cerințele necesare rămân fără sursă.

CRITERIU DE CALITATE O amenințare este descrisă util atunci când poate fi combinată cu un activ, o vulnerabilitate și o succesiune de acțiuni pentru a forma un scenariu verificabil.

Domeniu

Exemple de condiții vulnerabile

Fizic și constructiv

închideri slabe, accesibilitate necontrolată, căi mascate, goluri, geometrii și materiale neadecvate

Tehnic

zone neacoperite, alimentări comune, comunicații neprotejate, configurări implicite, capacități insuficiente

Operațional

proceduri inaplicabile, lipsa verificării alarmelor, timpi de răspuns nerealistici, gestionarea slabă a cheilor

Uman

instruire insuficientă, privilegii excesive, roluri conflictuale, oboseală, ocolirea controlului și eroare previzibilă

Informațional și cibernetic

conturi comune, lipsa segmentării, jurnalizare insuficientă, actualizări necontrolate, expunerea planurilor

Ciclu de viață

mentenanță inaccesibilă, lipsa pieselor, configurații neînregistrate, testare rară și modificări neverificate

REGULĂ DE FORMULARE Vulnerabilitatea se descrie ca o condiție observabilă și efectul ei asupra scenariului, nu ca justificare retrospectivă pentru echipamentul preferat.

Câmp

Conținut

ID și denumire

cod unic și formulare scurtă orientată către eveniment

Active și obiective afectate

persoane, bunuri, informații, procese și dependențe

Sursă / actor

capacitate, acces, intenție sau mecanism de producere

Condiții și vulnerabilități

loc, timp, stare, acces, defecte și factori favorizanți

Secvență

inițiere, apropiere, pătrundere, acțiune, ieșire și propagare

Măsuri existente

prevenire, descurajare, detectare, întârziere, răspuns și recuperare

Consecințe

efecte directe, indirecte, în cascadă și durata lor

Dovezi și incertitudine

surse, ipoteze, lipsuri și nivelul de încredere

TESTUL UTILITĂȚII SCENARIULUI Dacă scenariul nu permite derivarea unei funcții, a unui criteriu de performanță sau a unei acțiuni operaționale, el este prea general ori nerelevant pentru proiectare.

CRITERIU DE CREDIBILITATE Un scor fără scenariu, criterii, surse și incertitudine nu reprezintă o justificare suficientă pentru o decizie de proiectare.

REGULĂ DE GUVERNANȚĂ Riscul rezidual se acceptă explicit; nu apare implicit prin omiterea unei măsuri, epuizarea bugetului sau închiderea administrativă a proiectului.

Strategie / funcție

Scop în scenariu

Evitare

eliminarea activității, traseului sau condiției care generează expunerea

Prevenire și descurajare

reducerea oportunității și a atractivității inițierii

Detectare și verificare

identificarea evenimentului și obținerea informației necesare deciziei

Întârziere și limitare

câștigarea timpului și restrângerea propagării până la răspuns

Răspuns

acțiunea umană sau automată adecvată, autorizată și realizabilă

Recuperare și continuitate

restabilirea funcțiilor, păstrarea dovezilor și limitarea efectelor

Transfer / partajare

alocarea contractuală sau financiară a unor consecințe, fără eliminarea responsabilităților indelegabile

Acceptare

asumarea informată a riscului rezidual în limitele permise

PRINCIPIUL APĂRĂRII ÎN PROFUNZIME Straturile de protecție trebuie să fie complementare, temporizate și controlabile. Multiplicarea unor măsuri cu aceeași vulnerabilitate nu constituie reziliență.

REGULĂ DE CONTINUITATE Acceptarea riscului este valabilă numai cât timp ipotezele, măsurile și condițiile pe care se bazează rămân adevărate și controlate.

Cod sursă

Categorie

Exemple de conținut

LEG

legală / normativă

obligații, grade, documente, protecția persoanelor și condiții ale autorităților

RSK

derivată din risc

funcții și performanțe necesare tratării unui scenariu

STK

parte interesată

nevoi aprobate ale beneficiarului, utilizatorilor, intervenției și mentenanței

OPS

operațională

roluri, fluxuri, moduri, timpi, priorități și comportare la eveniment

INT

interfață

schimburi de date, semnale, stări, responsabilități și condiții de integrare

PRV/CYB

date și securitate cibernetică

minimizare, retenție, acces, jurnalizare, segmentare și actualizare

LCM

ciclu de viață

instalare, testare, instruire, mentenanță, modificare, suport și scoatere din funcțiune

ȘABLON DE CERINȚĂ [Sistemul / rolul] trebuie să [realizeze rezultatul] în [condițiile definite], cu [criteriul de performanță], iar îndeplinirea se verifică prin [metoda și criteriul de acceptanță].

Atribut

Conținut minim

ID și stare

cod stabil; propusă, analizată, aprobată, implementată, verificată, retrasă

Sursă și justificare

referință legală, scenariu, decizie, solicitant și motiv

Formulare și criteriu

rezultat, condiții, performanță, toleranță și excepții

Prioritate și criticitate

obligatorie, esențială, dorită; efectul neîndeplinirii

Alocare

subsistem, componentă, rol, procedură sau interfață responsabilă

Verificare

analiză, inspecție, calcul, demonstrație sau test; rezultat acceptat

Trasabilitate și versiune

legături amonte/aval, autor, aprobare, revizie și modificări

Lanț de trasabilitate

Exemplu generic

Context / activ

zonă cu bunuri critice, neocupată în afara programului

Scenariu

acces neautorizat printr-o cale periferică vulnerabilă

Obiectiv de tratare

detectarea timpurie, verificarea evenimentului și inițierea răspunsului

Cerință

funcția trebuie să producă și să transmită informația de alarmă în condițiile și performanța aprobate

Alocare

detecție, comunicație, verificare, operator, procedură și surse de alimentare

Dovadă

calcul, inspecție și test de scenariu cu criterii de acceptanță

POARTA DE CONTROL C4 Capitolul 4 este închis numai dacă scenariile prioritare au proprietari și tratamente, cerințele sunt aprobate și verificabile, iar matricea permite urmărirea fără rupturi de la context și risc până la dovada planificată.

Rezultat obligatoriu

Dovada minimă

Profil contextual

limite, procese, părți interesate, dependențe și surse validate

Baza activelor

registru, proprietari, criticitate, locații și relații

Baza scenariilor

amenințări, vulnerabilități, secvențe, consecințe și incertitudini

Decizia privind riscul

metodă, criterii, priorități, tratamente și risc rezidual

Baza de cerințe

ID-uri, formulări verificabile, proprietari, alocări și stări

Trasabilitate

legături între surse, riscuri, cerințe, soluții și verificări

Regulă S.I.G.M.A. — Niciun echipament nu se introduce în proiect numai pentru că este disponibil, uzual sau preferat. Fiecare funcție și fiecare element relevant trebuie să aibă o justificare trasabilă, o condiție de utilizare și o metodă de verificare.

Element de control

Întrebare obligatorie

Dovadă proiectată

Scop operațional

Ce rezultat de securitate trebuie obținut?

cerință identificată și scenariu asociat

Condiții

În ce mediu, regim și stare trebuie obținut?

date de amplasament, ipoteze și limite

Performanță

Cât de bine și în ce timp?

valoare, toleranță sau clasă

Defect

Ce se întâmplă la pierderea unei funcții?

mod degradat, semnalizare și măsură compensatorie

Verificare

Cum se demonstrează rezultatul?

inspecție, calcul, măsurare sau test

Strat

Obiect proiectat

Aspecte de verificat

Perimetral

limita terenului sau incintei

relief, vegetație, animale, interferențe, acces tehnic

Periferic

anvelopa clădirii

uși, ferestre, vitraje, acoperiș, goluri și căi ascunse

Volumetric

spațiul interior

geometrie, obstacole, curenți, surse termice și regim de ocupare

Punctual

activul ori containerul

atac, deplasare, deschidere și transmiterea vibrațiilor

Atac/panică

persoana și locul de operare

acces discret, prevenirea acționării accidentale și procedura de răspuns

Exemplu de calcul — Pentru o imagine utilă de 2688 pixeli și o cerință de 250 px/m, lățimea maximă teoretică la planul țintei este 10,75 m. Valoarea nu validează singură identificarea: se verifică unghiul feței, iluminarea, timpul de expunere, compresia, mișcarea și poziția reală a persoanei.

Parametru

Unitate

Documentare minimă

Rezoluție utilă

pixeli

flux principal și secundar, raport de aspect

Frecvență cadre

fps

valoare pe scenă și justificarea mișcării

Debit

Mbit/s

mediu, maxim proiectat și metodă de estimare

Retenție

zile/ore

regim de înregistrare și ipoteze

Latență

ms/s

limită pentru operare și integrare

Disponibilitate

% sau durată

redundanță, recuperare și alarmarea defectului

Calcul

Date de intrare

Rezultat controlat

Putere/curent

consum normal, alarmă, pornire, pierderi

sursă, protecții și rezervă

Cădere tensiune

curent, lungime, secțiune, material

tensiune minimă la consumator

Autonomie

curenți, durate, temperatură, îmbătrânire

capacitate baterie și durată demonstrată

PoE

clasă dispozitiv, porturi, cablu, temperatură

buget pe port și total switch

Continuitate

defecte, comutare, trasee comune

mod degradat și alarmare

Poarta de control C5 — Capitolul poate fi considerat închis numai dacă fiecare funcție critică are o soluție, fiecare soluție are o justificare și fiecare cerință are o metodă de verificare. Necunoscutele critice blochează emiterea sau sunt tratate prin condiții explicite și aprobate.

Regulă S.I.G.M.A. — O interfață nu este considerată proiectată prin simpla menționare a unui protocol ori a compatibilității comerciale. Pentru fiecare schimb de date sau comandă se definesc sursa, destinația, semnificația, condițiile, prioritatea, securitatea, comportarea la defect și proba de acceptare.

Principiu

Întrebare de control

Dovadă

Necesitate

Ce scenariu justifică interfața?

cerință și caz de utilizare

Autoritate

Cine poate comanda și cine confirmă?

roluri și drepturi definite

Determinism

Ce rezultat apare în fiecare stare?

logică și matrice cauză–efect

Izolare

Cum este limitată propagarea defectului?

zone, separare și mod degradat

Verificare

Cum se demonstrează traseul complet?

test integrat și jurnal

Câmp de interfață

Conținut minim

Criteriu de acceptare

Identitate

sursă, destinație, proprietar

punctele coincid cu schemele

Funcție

eveniment, comandă, stare, confirmare

semantica este neechivocă

Performanță

latență, frecvență, capacitate

valoarea este măsurabilă

Securitate

identitate, drepturi, criptare, jurnal

control adecvat riscului

Defect

timeout, repetare, fallback, alarmare

starea degradată este previzibilă

Test

stimul, rezultat, toleranță, dovadă

traseul complet este demonstrat

Cauză

Condiție

Efect principal

Confirmare / defect

Alarmă efracție zonă critică

sistem armat

afișare prioritară + camere asociate

imagine și primire operator; alarmă dacă fluxul lipsește

Ușă forțată

fără acces autorizat

eveniment control acces + înregistrare marcată

stare contact și clip disponibil

Pierdere comunicație

depășire timeout

alarmă tehnică + funcționare locală

restabilire jurnalizată și reconciliere

Comandă de urgență

condiție aprobată

acțiuni definite interdisciplinar

stare fizică verificată; nereușita escaladată

Perturbare

Funcție menținută

Măsură proiectată

Probă

Pierdere rețea publică

detecrie și control local

surse de rezervă + alarmare

test autonomie și revenire

Defect server integrare

funcții locale critice

autonomie locală / redundanță

oprire controlată și failover

Întrerupere comunicație

decizii locale și jurnal temporar

segmentare + stocare locală

rupere legătură și reconciliere

Compromitere configurație

restabilire controlată

backup protejat + versiune aprobată

restaurare și verificare funcțională

Domeniu

Cerință minimă de proiect

Dovadă la predare

Active

inventar și proprietar

registru hardware/software/versiuni

Acces

identități, roluri, MFA unde este cerut

matrice drepturi și test conturi

Rețea

zone și fluxuri permise

diagramă logică și reguli controlate

Configurare

bază sigură și servicii minime

export configurație și checklist

Vulnerabilități

proces de evaluare și actualizare

procedură, suport și versiuni

Incidente

jurnale, alarmare, izolare, restaurare

test și responsabilități

Notă de responsabilitate — Proiectantul introduce cerințele tehnice necesare protecției datelor, dar nu stabilește în locul operatorului scopul, temeiul juridic sau durata de păstrare. Necunoscutele juridice care influențează soluția sunt consemnate și trebuie clarificate înainte de configurarea finală.

Poarta de control C6 — Capitolul poate fi închis numai dacă interfețele critice sunt inventariate și aprobate, matricea cauză–efect este completă, modurile degradate sunt definite, măsurile cibernetice și de protecție a datelor sunt proiectate, iar fiecare funcție integrată are un test cap-la-cap și un responsabil.

Regulă S.I.G.M.A. — Nicio funcție critică nu este declarată conformă fără legătura completă dintre cerință, metodă de verificare, configurație testată, rezultat așteptat, rezultat obținut, dovadă și persoana care a consemnat ori aprobat rezultatul.

Obiect

Metodă

Dovadă minimă

Cerințe

trasabilitate și analiză

matrice actualizată

Calculule

recalculare / eşantionare justificată

foaie de verificare

Planuri şi scheme

confruntare interdisciplinară

marcaje şi observaţii închise

Produce şi versiuni

comparare cu specificaţia

fişe aprobate şi registru

Teste

revizuire criterii şi acoperire

plan de încercări aprobat

Tip de probă

Exemplu

Criteriu

Examinare

document, etichetă, versiune

identitate şi completitudine

Inspecţie

amplasare şi traseu

conform planului şi mediului

Măsurare

tensiune, autonomie, densitate pixeli

valoare în toleranţă

Încercare funcţională

stimul-răspuns local

efect corect în timp admis

Încercare integrată

scenariu cap-la-cap

toate efectele și jurnalele corecte

Grup de livrabile

Exemple

Control final

Conformitate

proiect, avize, declarații

revizii și aplicabilitate

Configurație

inventar, versiuni, exporturi

restaurare verificată

Dovezi

inspecții, măsurări, teste

trasabilitate și semnături

Exploatare

manuale, proceduri, mentenanță

roluri și acces

Securizat

conturi, chei, certificate

predare separată și confirmată

Poarta de control C7 — Capitolul poate fi închis numai dacă documentația și execuția au fost verificate, testele funcționale și integrate au rezultate trasabile, neconformitățile incompatibile cu acceptarea sunt închise, configurația finală este protejată, instruirea este consemnată, iar dosarul final a fost predat și confirmat.

Regulă S.I.G.M.A. — Orice intervenție care poate modifica o funcție, o interfață, un parametru, un drept de acces, o versiune, o dovadă ori un risc trebuie identificată, autorizată, executată controlat, verificată și introdusă în configurația de referință. Urgența poate comprima etapele, dar nu poate elimina trasabilitatea și analiza ulterioară.

Rol

Răspundere principală

Dovadă de control

Proprietar sistem

obiective, risc, buget și acceptarea schimbărilor majore

decizii și revizuri

Administrator funcțional

reguli de operare, utilizatori și drepturi

registru acces și rapoarte

Administrator tehnic

configurație, copii, actualizări și restaurare

jurnale și baseline

Mentenanță

inspecții, teste, remediere și raportare

fișe de intervenție

Operator

monitorizare, reacție și escaladare

jurnal de tură / incident

Categorie

Declanșator

Rezultat obligatoriu

Preventivă

interval, utilizare sau condiție

funcție verificată și uzură evaluată

Bazată pe stare

tendință, diagnostic sau prag

intervenție înaintea pierderii funcției

Corectivă

defect ori performanță sub criteriu

cauză remediată și revenire testată

Perfectivă

nevoie justificată de îmbunătățire

schimbare aprobată și validată

De urgență

risc imediat sau serviciu critic indisponibil

control provizoriu, restaurare și analiză ulterioară

Indicator

Interpretare

Semnal de acțiune

Disponibilitate

timp în care funcția poate îndeplini scopul

scădere sub ținta aprobată

MTTR

durata medie până la restabilire

tendință crescătoare / SLA depășit

Alarme nedorite

evenimente fără cauză relevantă de securitate

recurență pe zonă, tip sau interval

Restanță mentenanță

activități scadente neînchise

creștere ori acumulare pe funcții critice

Restaurări reușite

copii utilizabile, nu doar create

orice eșec nerecuperat

Etapă

Întrebare de control

Înregistrare

Solicitare

de ce este necesară și ce rezultat urmărește?

cerere identificată

Evaluare

ce cerințe, riscuri, date și interfețe afectează?

analiză de impact

Aprobare

cine acceptă riscul, costul și indisponibilitatea?

decizie autorizată

Implementare

care este versiunea, fereastra și revenirea?

jurnal de intervenție

Verificare / validare

a fost realizată corect și răspunde nevoii?

teste și acceptare

Închidere

baseline-ul și documentele sunt actualizate?

registru schimbare închis

Poarta de control C8 — Ciclul de exploatare este controlat numai dacă responsabilitățile sunt acceptate, instrucțiunile corespund configurației, mentenanța și verificările sunt la termen, incidentele și schimbările au trasabilitate, riscul este reevaluat la declanșatori, baseline-ul poate fi restaurat, vulnerabilitățile și sfârșitul suportului sunt gestionate, iar scoaterea din funcțiune protejează continuitatea, datele și dovezile.

Regulă de utilizare — Fiecare formular primește identificator unic, proiect, obiectiv, versiune, dată, autor, verficator și statut. Înregistrările se păstrează împreună cu documentele-sursă și cu dovezile la care fac trimitere. Modelele nu substituie formularele obligatorii stabilite prin lege, contract, autoritate sau schemă de certificare.

Cod

Instrument

Utilizare principală

Poartă / capitol

A1

Fluxul integrat și porțile de control

guvernanța procesului și autorizarea trecerilor

C1–C8 / cap. 3

A2

Matricea de conformitate normativă

determinarea și demonstrarea cerințelor aplicabile

C2 / cap. 2

A3

Registrul contextului, activelor și părților interesate

fundamentarea domeniului și a cerințelor

C1–C4 / cap. 4

A4

Registrul scenariilor, riscurilor și tratamentelor

legătura risc–măsură–risc rezidual

C4 / cap. 4

A5

Matricea de trasabilitate a cerințelor

urmărirea cerinței până la dovada de acceptare

C4–C7 / cap. 4–7

A6

Registrul interfețelor și matricea cauză–efect

controlul integrării și al modurilor degradate

C5–C6 / cap. 5–6

A7

Matricea de verificare, validare și recepție

planificarea testelor și acceptarea rezultatelor

C7 / cap. 7

A8

Registrele de neconformități, decizii și ipoteze

controlul abaterilor și justificarea deciziilor

transversal

A9

Registrele ciclului de viață

mentenanță, incidente, configurație și schimbări

C8 / cap. 8

A10

Listele de verificare C1–C8

evaluarea formală a porților de control

C1–C8

Cod

Responsabil de completare

Moment de utilizare

Înregistrare rezultată

A1

Managerul de proiect / proiectantul coordonator

la inițiere și la fiecare trecere de etapă

planul porților și procese-verbale de decizie

Etapă

Intrare minimă

Activitate dominantă

Livrabil

Poartă

Decizie

1. Inițiere

mandat, obiectiv, părți

definire scop, roluri, plan

fișa proiectului

C1

continuați / completați

2. Conformitate

context juridic și contractual

determinarea cerințelor aplicabile

registru normativ

C2

acceptați baza

3. Date și amplasament

documente, releveu, acces

culegere și validare date

raport de date și ipoteze

C3

date suficiente

4. Context și risc

active, amenințări, analiză risc

scenarii și cerințe

registre risc și cerințe

C4

cerințe aprobate

5. Subsisteme

cerințe aprobate

arhitectură și calcule

soluție tehnică

C5

soluție completă

6. Integrare

interfețe și dependențe

cauză–efect, reziliență, cyber

arhitectură integrată

C6

integrare controlată

7. Verificare și recepție

proiect, execuție, teste

V&V, PIF, remediere, predare

dosar final

C7

acceptare / reținere

8. Ciclul de viață

baseline și responsabilități

operare, mentenanță, schimbări

registre operaționale

C8

menținere / reevaluare

Câmp

Conținut de completat

Proiect / obiectiv / fază

Poartă și data evaluării

Livrabile supuse controlului și versiuni

Criterii satisfăcute / nesatisfăcute / N/A

Riscuri, ipoteze și neconformități deschise

Condiții, responsabili și termene

Decizie

- ☐ aprobat ☐ aprobat condiționat ☐ respins ☐ revenire

Decident / semnătură / dată

Cod

Responsabil de completare

Moment de utilizare

Înregistrare rezultată

A2

Proiectantul coordonator, cu aport juridic/tehnic după caz

la C2 și înaintea fiecărei emiteri relevante

registru cerințelor aplicabile și dovezilor

ID

Sursă / ediție / articol

Cerință aplicabilă

Statut

Aplicabilitate / motiv

Soluție / document

Dovadă / stare

Cod

Statut

Regulă de utilizare

L

obligație legală

cerință imperativă din act aplicabil; prevalează asupra regulii metodologice

T

cerință tehnică obligatorie

impusă prin lege, contract, aviz, caiet de sarcini sau certificare

C

cerință contractuală

acceptată de părți; se urmăresc ierarhia documentelor și modificările

R

recomandare / bună practică

aplicată sau justificat neaplicată, în raport cu riscul

M

- regulă S.I.G.M.A.

cerință internă de proces; nu este prezentată drept obligație legală

Control obligatoriu — Orice conflict aparent, derogare sau soluție echivalentă se înregistrează distinct în A8, cu autoritatea deciziei și dovada acceptării. Formularea „conform standardelor în vigoare” nu este suficientă fără identificarea documentelor și edițiilor relevante.

Cod

Responsabil de completare

Moment de utilizare

Înregistrare rezultată

A3

Proiectantul, cu date validate de beneficiar și evaluatorul de risc

la C1–C4 și la schimbări de context

baza contextuală aprobată

Domeniu

Informații și surse

Condiții / limitări / ipoteze

Validat de / data

misiune și activități

amplasament și vecinătăți

program, ocupare și fluxuri

processe și dependențe critice

mediu fizic și infrastructuri

incidente și experiență operațională

constrângeri juridice / contractuale

schimbări previzibile și orizont de proiectare

ID

Activ / grup

Proprietar

Valoare / criticitate

Consecințe relevante

Loc / interval

Sursă

ID

Parte / rol

Nevoie / obligație

Autoritate / influență

Interfață / responsabil

Validare

Cod

Responsabil de completare

Moment de utilizare

Înregistrare rezultată

A4

Evaluatorul de risc pentru evaluare; proiectantul pentru transpunerea aprobată

la C4 și la declanșatorii din cap. 8

scenarii aprobate și plan de tratare trasabil

ID

Activ / obiectiv

Amenințare / eveniment

Vulnerabilitate / condiție

Scenariu și consecință

Evaluare inițială

Sursă / autor

Risc

Opțiune

Măsură / cerință

Responsabil

Termen

Dovadă de eficacitate

Risc rezidual / decident

Criteriu de închidere — Un risc este închis în registru numai după identificarea măsurii, a proprietarului, a dovezii de eficacitate și a decidentului competent pentru riscul rezidual. Transferul, evitarea ori acceptarea sunt decizii documentate, nu rubrici bifate automat.

Cod

Responsabil de completare

Moment de utilizare

Înregistrare rezultată

A5

Proiectantul coordonator

de la C4 până la C7 și la fiecare schimbare

baseline-ul cerințelor și dovada satisfacerii

ID

Sursă / risc

Cerință verificabilă

Prioritate

Alocare / soluție

Criteriu de acceptare

Metodă / test

Stare

Întrebare

Da / Nu / N/A

Observație

Are un singur înțeles și exprimă o singură obligație?

Este necesară și are o sursă identificată?

Este fezabilă în condițiile și constrângerile proiectului?

Este măsurabilă sau observabilă printr-o metodă definită?

Nu impune prematur o marcă sau o soluție nejustificată?

Este compatibilă cu cerințele dependente și cu modurile degradate?

Are proprietar, prioritate, criteriu de acceptare și stare?

Cod

Responsabil de completare

Moment de utilizare

Înregistrare rezultată

A6

Proiectantul de integrare / proiectantul coordonator

la C5–C6, înainte de configurare și la modificări

specificația controlată a interfețelor

ID

Sursă → destinație

Semnal / date / protocol

Stări și temporizări

Comportare la defect

Cyber / acces

Test / proprietar

ID

Cauză / condiție

Precondiții

Efect automat

Acțiune operator

Prioritate / timp

Resetare / revenire

Dovadă

Câmp

Conținut

Defect / indisponibilitate inițatoare

Funcții păstrate și funcții pierdute

Detectare, alarmare și vizibilitate pentru operator

Măsuri compensatorii și limite temporale

Criteriu de escaladare / oprire sigură

Metodă de restaurare și test de revenire

Responsabil și dovadă

Cod

Responsabil de completare

Moment de utilizare

Înregistrare rezultată

A7

Responsabilul V&V / comisia desemnată, cu separare adecvată

planificare înaintea execuției; completare la C7

plan, rezultate, dovezi și acceptare

Test ID

Cerință / funcție

Nivel / configurație

Metodă și condiții

Rezultat așteptat

Rezultat / dovadă

Responsabil

Stare

Câmp

Conținut de completat

Proiect / sistem / locație

Test ID / versiune procedură / data și ora

Configurație, firmware, licențe și baseline

Echipamente de măsură / valabilitate metrologică

Condiții inițiale și date de test

Pași executați și deviații aprobate

Rezultat observat / atașamente / jurnal

Verdict

- ☐ admis ☐ admis condiționat ☐ respins ☐ netestat

Executant / martor / acceptant

ID

Cerință / livrabil

Constatare

Clasă

Responsabil

Termen

Dovadă închidere

Acceptare

Cod

Responsabil de completare

Moment de utilizare

Înregistrare rezultată

A8

Emitentul constatării; proprietarul desemnat pentru soluționare

pe întreg ciclul de viață

istoric controlat al abaterilor și deciziilor

NC ID

Sursă / dată

Cerință încălcată

Constatare și impact

Clasă

Corecție / cauză / acțiune

Responsabil / termen

Verificare / stare

ID

Subiect / opțiuni

Temei și criterii

Impact / risc

Decident / autoritate

Condiții / expirare

Dovadă / legături

ID

Tip

Enunț / dependență

Sursă / proprietar

Validare / termen

Efect dacă este falsă

Stare / decizie

Regulă de severitate — Clasificarea se bazează pe efectul asupra siguranței, securității, conformității, performanței și recepției. Închiderea administrativă fără dovada corecției și fără verificarea eficacității nu reprezintă închiderea neconformității.

Cod

Responsabil de completare

Moment de utilizare

Înregistrare rezultată

A9

Proprietarul sistemului și administratorii desemnați

după C7 și pe întreaga durată de exploatare

evidențe operaționale și baseline actualizat

ID activ

Tip / locație

Producător / model / serie

Versiune / adresă

Criticitate / proprietar

Baseline / backup

Suport / EOL

Stare

ID

Activ / funcție

Tip / operație

Periodicitate / declanșator

Criteriu acceptare

Data / executant

Rezultat / măsură

Acțiune / termen

ID / timp

Sursă / tip

Clasificare

Răspuns / escaladare

Impact / date

Dovezi / custodie

Cauză / lecție

Acțiune / stare

CR ID

Motiv / domeniu

Impact / risc

Aprobări

Versiune / implementare

Teste / revenire

Documente / baseline

Închidere

Indicator

Definiție / formulă

Sursă date

Țintă / prag

Frecvență

Rezultat / tendință

Decizie / acțiune

Cod

Responsabil de completare

Moment de utilizare

Înregistrare rezultată

A10

Responsabilul porții și decidentul desemnat

Înainte autorizării trecerii la etapa următoare

listă semnată și decizie de poartă

Cod

Criteriu de control

Rezultat

Dovadă / referință

Observație / acțiune

C1.01

Mandatul, obiectivul, domeniul și limitele proiectului sunt aprobate.

- ☐ Da ☐ Nu ☐ N/A

C1.02

Părțile interesate, rolurile, competențele și autoritățile sunt identificate.

- ☐ Da ☐ Nu ☐ N/A

C1.03

Livrabilele, etapele, porțile, resursele și calendarul sunt definite.

- ☐ Da ☐ Nu ☐ N/A

C1.04

Canalele de comunicare, aprobările și controlul documentelor sunt stabilite.

- ☐ Da ☐ Nu ☐ N/A

C1.05

Ipotezele inițiale, dependențele și riscurile de proiect sunt înregistrate.

- ☐ Da ☐ Nu ☐ N/A

Cod

Criteriu de control

Rezultat

Dovadă / referință

Observație / acțiune

C2.01

Actele, standardele, avizele și cerințele contractuale sunt identificate cu ediție.

- ☐ Da ☐ Nu ☐ N/A

C2.02

Domeniul și caracterul obligatoriu al fiecărei cerințe sunt determinate.

- ☐ Da ☐ Nu ☐ N/A

C2.03

Conflictele, derogările și punctele de reverificare sunt înregistrate.

- ☐ Da ☐ Nu ☐ N/A

C2.04

Responsabilitățile legale și profesionale sunt delimitate.

- ☐ Da ☐ Nu ☐ N/A

C2.05

Matricea de conformitate are proprietari și dovezi planificate.

- ☐ Da ☐ Nu ☐ N/A

Cod

Criteriu de control

Rezultat

Dovadă / referință

Observație / acțiune

C3.01

Documentele și releveele au fost verificate față de situația reală.

- ☐ Da ☐ Nu ☐ N/A

C3.02

Vizita, măsurătorile și condițiile de mediu sunt documentate.

- ☐ Da ☐ Nu ☐ N/A

C3.03

Fluxurile, programul, ocuparea, infrastructurile și dependențele sunt confirmate.

- ☐ Da ☐ Nu ☐ N/A

C3.04

Datele lipsă sau contradictorii au ipoteze și termene de clarificare.

- ☐ Da ☐ Nu ☐ N/A

C3.05

Informațiile sunt suficiente și controlate pentru etapa de analiză.

- ☐ Da ☐ Nu ☐ N/A

Cod

Criteriu de control

Rezultat

Dovadă / referință

Observație / acțiune

C4.01

Activele, părțile interesate și scenariile relevante sunt identificate.

- ☐ Da ☐ Nu ☐ N/A

C4.02

Analiza de risc este utilizată în limitele rolurilor și are statut cunoscut.

- ☐ Da ☐ Nu ☐ N/A

C4.03

Tratamentele și riscul rezidual au proprietar și autoritate de acceptare.

- ☐ Da ☐ Nu ☐ N/A

C4.04

Cerințele sunt univoce, verificabile, prioritizate și trasabile la sursă.

- ☐ Da ☐ Nu ☐ N/A

C4.05

Baseline-ul cerințelor este aprobat; modificările sunt controlate.

- ☐ Da ☐ Nu ☐ N/A

Cod

Criteriu de control

Rezultat

Dovadă / referință

Observație / acțiune

C5.01

Fiecare subsistem este alocat unor cerințe și scenarii aprobate.

- ☐ Da ☐ Nu ☐ N/A

C5.02

Arhitectura, amplasarea, gradele/clasele și performanțele sunt justificate.

- ☐ Da ☐ Nu ☐ N/A

C5.03

Calculule de acoperire, capacitate, stocare, bandă și autonomie sunt verificabile.

- ☐ Da ☐ Nu ☐ N/A

C5.04

Alimentarea, comunicațiile, cablarea, sabotajul și defectele sunt tratate.

- ☐ Da ☐ Nu ☐ N/A

C5.05

Planurile, schemele, listele și specificațiile sunt coordonate și neutre tehnologic ori justificate.

- ☐ Da ☐ Nu ☐ N/A

Cod

Criteriu de control

Rezultat

Dovadă / referință

Observație / acțiune

C6.01

Interfețele au proprietar, specificație, versiune și criteriu de test.

- ☐ Da ☐ Nu ☐ N/A

C6.02

Matricea cauză–efect tratează priorități, temporizări, resetare și excepții.

- ☐ Da ☐ Nu ☐ N/A

C6.03

Defectele, dependențele, modurile degradate și măsurile compensatorii sunt definite.

- ☐ Da ☐ Nu ☐ N/A

C6.04

Riscurile cibernetice, accesurile, actualizările, jurnalele și copiile sunt controlate.

- ☐ Da ☐ Nu ☐ N/A

C6.05

Protecția datelor, interoperabilitatea și portabilitatea sunt demonstrate.

- ☐ Da ☐ Nu ☐ N/A

Cod

Criteriu de control

Rezultat

Dovadă / referință

Observație / acțiune

C7.01

Fiecare cerință critică are metodă, criteriu, configurație și responsabil de test.

- ☐ Da ☐ Nu ☐ N/A

C7.02

Execuția și configurația „as-built” corespund proiectului sau abaterilor aprobate.

- ☐ Da ☐ Nu ☐ N/A

C7.03

Testele funcționale, integrate, de defect și de restaurare au dovezi complete.

- ☐ Da ☐ Nu ☐ N/A

C7.04

Neconformitățile sunt clasificate, tratate și închise ori acceptate autorizat.

- ☐ Da ☐ Nu ☐ N/A

C7.05

Instruirea, dosarul final, accesurile și responsabilitățile sunt predate controlat.

- ☐ Da ☐ Nu ☐ N/A

Cod

Criteriu de control

Rezultat

Dovadă / referință

Observație / acțiune

C8.01

Proprietarul, administratorii, operatorii și mentenanța au responsabilități acceptate.

- ☐ Da ☐ Nu ☐ N/A

C8.02

Instrucțiunile și planul de mentenanță corespund baseline-ului real.

- ☐ Da ☐ Nu ☐ N/A

C8.03

Indicatorii, incidentele, vulnerabilitățile și restaurările sunt urmărite.

- ☐ Da ☐ Nu ☐ N/A

C8.04

Schimbările permanente, temporare și urgente au aprobare, test și revenire.

- ☐ Da ☐ Nu ☐ N/A

C8.05

Reevaluarea riscului, sfârșitul suportului și scoaterea din funcțiune au declanșatori și planuri.

- ☐ Da ☐ Nu ☐ N/A

Poartă

Rezultat

Condiții deschise

Responsabil / termen

Decident / dată

C1

- ☐ aprobat ☐ condiționat ☐ respins

C2

- ☐ aprobat ☐ condiționat ☐ respins

C3

- ☐ aprobat ☐ condiționat ☐ respins

C4

- ☐ aprobat ☐ condiționat ☐ respins

C5

- ☐ aprobat ☐ condiționat ☐ respins

C6

- ☐ aprobat ☐ condiționat ☐ respins

C7

- ☐ aprobat ☐ condiționat ☐ respins

C8

- ☐ aprobat ☐ condiționat ☐ respins

Poarta anexelor — Setul de instrumente este apt pentru utilizare atunci când codificarea este unică, rolurile sunt definite, câmpurile obligatorii pot fi completate, legăturile dintre registre sunt verificabile, istoricul modificărilor este păstrat și rezultatele pot fi exportate într-o formă inteligibilă și durabilă.

Structura editorială — buget orientativ al versiunii sintetice

- **Elemente preliminare** — Statut, control, reguli de utilizare, cuprins și abrevieri — 5–7 pagini.
- **Introducere instituțională** — Cuvânt înainte, necesitate și domeniu profesional — 3–4 pagini.
- **Capitolul 1** — Fundamentele metodologiei S.I.G.M.A. — 9–11 pagini.
- **Capitolul 2** — Cadrul normativ, responsabilități și conformitate — 8–10 pagini.
- **Capitolul 3** — Procesul integrat de proiectare — 13–15 pagini.
- **Capitolul 4** — Context, cerințe și riscuri — 10–12 pagini.
- **Capitolul 5** — Proiectarea subsistemelor — 17–20 pagini.
- **Capitolul 6** — Integrare, reziliență și securitatea informațiilor — 7–9 pagini.
- **Capitolul 7** — Verificare, punere în funcțiune și recepție — 7–9 pagini.
- **Capitolul 8** — Exploatare, mentenanță și managementul schimbării — 5–7 pagini.
- **Anexe** — Fluxuri, matrici, registre și liste de verificare — 8–10 pagini.