Ciga Energy®
EPIC ENGINEERING PROCUREMENT INNOVATION CONSTRUCTION

Rompetrol Petromidia - Cerinte pentru Securitate Cibernetică

Octombrie 2026

Faza:

LICITATIE EPC CONTRACTOR

Denumire:

Achiziție servicii, furnizare bunuri si execuție

lucrări (proiectare, furnizare, executie, punere in functiune si testare pentru conformitate) în cadrul proiectului

CONSTRUIRE CENTRALA ELECTRICA FOTOVOLTAICĂ PENTRU AUTOCONSUM – ROMPETROL RAFINARE

Cod SMIS – 352708

CONTINUT

1 CONTEXT (BACKGROUND) 3
2 STRUCTURA REȚELEI 5
3 OT SECURITY HAZOP (CYBER HAZOP) 8
3.1 OBIECTIVE 8
3.2 ETAPELE PROIECTULUI ÎN CARE SE REALIZEAZĂ STUDIUL 8
3.3 METODOLOGIE 10
3.4 ECHIPA DE STUDIU 10
3.5 DATE DE INTRARE 11
3.6 LIVRABILE ȘI URMĂRIREA RECOMANDĂRILOR 11
4 CONSOLIDARE (HARDENING) 13
4.1 INTERFEȚE 13
4.2 SERVICII ȘI SOFTWARE 14
4.3 MONITORIZARE ȘI DETECTARE CYBERSECURITY 14
4.4 MANAGEMENTUL VULNERABILITĂȚILOR 15
5 ACCES LA DISTANȚĂ 16
6 FIREWALL 17
7 MANAGEMENTUL UTILIZATORILOR 18
8 PROTOCOL DE JURNALIZARE A SISTEMULUI 19
8.1 PROTECȚIA ANTI-MALWARE ȘI LISTA ALBĂ A APLICAȚIILOR (APPLICATION ALLOWLISTING) 19
9 BACKUP, RESTAURARE ȘI CONTINUITATE 21
10 RĂSPUNS LA INCIDENTE ȘI RAPORTARE 22
11 SECURITATEA LANȚULUI DE APROVIZIONARE 23
12 TESTAREA SECURITĂȚII (CYBER FAT / CYBER SAT) 24
13 MANAGEMENTUL MODIFICĂRILOR ȘI INSTRUIRE 25
14 CERINȚE MINIME PENTRU INFRASTRUCTURA HARDWARE CYBERSECURITY 26
14.1 Infrastructura centrală de administrare și securitate cibernetică 26
14.2 ECHIPAMENTE INDUSTRIALE EDGE 26
15 DOCUMENTAȚIE 28

1 CONTEXT (BACKGROUND)

Contractorii EPC care dezvoltă proiecte energetice la nivel global se confruntă cu provocări tot mai mari în domeniul securității cibernetice, pe măsură ce operațiunile industriale devin din ce în ce mai interconectate cu infrastructurile IT și cu Internetul Lucrurilor (IoT).

Abordarea trebuie să asigure politicile de securitate necesare pentru o exploatare sigură și cu un nivel redus de risc și să includă, fără a se limita la, următoarele secțiuni principale ale sistemului:

- **Oameni – procese – tehnologie** și interacțiunea dintre acestea (organizațiile implicate în proiectarea, livrarea, integrarea și mentenanța sistemelor OT ale proiectului vor funcționa pe baza unui CSMS/ISMS implementat);
- **Sistem de Management al Securității Cibernetice (CSMS/ISMS)** bazat pe **ISO/IEC 27001:2022** sau echivalent (cu controalele din **ISO/IEC 27002:2022** sau echivalent și ISO/IEC 27019 sau echivalent pentru sectorul energetic) sau pe cadrul de securitate cibernetică **NIST CSF 2.0** sau echivalent, corelat cu **IEC 62443-2-1** pentru mediul OT; CONTRACTORUL EPC și subcontractanții săi, în calitate de furnizori de servicii de integrare și mentenanță, vor demonstra capabilitățile cerute de **IEC 62443-2-4** sau echivalent.

Pentru sistemele OT/IACS, proiectarea și implementarea măsurilor de securitate cibernetică vor respecta principiile seriei IEC 62443 (în special IEC 62443-2-4, IEC 62443-3-2, IEC 62443-3-3, IEC 62443-4-1 și IEC 62443-4-2) și recomandările NIST SP 800-82 Rev. 3, fără a impune certificarea formală a soluției dacă aceasta nu este solicitată explicit de BENEFICIAR. Conformitatea va fi însă demonstrată prin documentație și prin testele Cyber FAT / Cyber SAT (capitolul 12).

Prezentul document stabilește cerințele minime de securitate cibernetică pentru sistemele OT/IACS și infrastructura IT asociate, furnizate de CONTRACTORUL EPC în cadrul proiectului (Cod SMIS 352708): centrala fotovoltaică (CEF), posturile de transformare și stația electrică (IED-uri, IEC 61850), sistemele de conducere (PPC, SCADA, HMI, historian), infrastructura de comunicații, conexiunea cu dispecerul și accesul la distanță al furnizorilor. Sistemele furnizate nu vor introduce riscuri cibernetice suplimentare pentru centrala nouă sau pentru rețelele IT/OT existente ale BENEFICIARULUI.

Un incident cibernetic poate conduce la comenzi neautorizate de putere activă/reactivă, la modificarea neautorizată a parametrilor invertoarelor, PPC-ului sau protecțiilor electrice, la compromiterea funcției de zero-export, la manevre neautorizate în instalațiile electrice, la pierderea controlului asupra CEF sau la propagarea incidentului către rețelele BENEFICIARULUI.

Cerințele au la bază seria IEC 62443, NIST SP 800-82 Rev. 3, Directiva (UE) 2022/2555 (NIS2) transpusă prin OUG nr. 155/2024, ISO/IEC 27001:2022 și ISO/IEC 27002:2022, precum și bunele practici SANS pentru sisteme industriale (SANS ICS Five Critical Controls: răspuns la incidente specific ICS, arhitectură defensabilă, vizibilitate și monitorizare a rețelei ICS, acces la distanță securizat și management al vulnerabilităților bazat pe risc). Măsurile de securitate OT vor fi integrate în sistemul de management al securității informației (ISMS) al BENEFICIARULUI, conform ISO/IEC 27001 (în corelare cu IEC 62443-2-1 și ISO/IEC 27019 pentru sectorul energetic), iar documentația predată va susține procesele acestuia de management al riscurilor, activelor, accesului, furnizorilor, incidentelor și modificărilor, inclusiv măsurile de gestionare a riscurilor prevăzute la art. 21 alin. (2) din Directiva NIS2 și obligațiile de raportare a incidentelor prevăzute la art. 23.

Principii de bază: siguranța și disponibilitatea instalației au prioritate față de confidențialitate, iar măsurile de securitate nu vor afecta funcțiile de protecție și control; securitatea este integrată din faza de proiectare (security by design), aplicată pe mai multe straturi (defence-in-depth) și dimensionată pe baza riscului (Cyber HAZOP – capitolul 3); cerințele sunt neutre tehnologic, iar soluțiile echivalente sunt acceptate cu aprobarea BENEFICIARULUI.

Precedență: în cazul unor neconcordanțe între prezentul document, standardele de referință, cerințele operatorului de rețea / dispecerului și politicile BENEFICIARULUI, se va aplica cerința mai restrictivă, cu condiția ca aceasta să nu afecteze siguranța și disponibilitatea instalației. Orice abatere de la prezentele cerințe va fi documentată, justificată prin analiza de risc, însoțită de măsuri compensatorii și aprobată în scris de BENEFICIAR.

.

2 STRUCTURA REȚELEI

CONTRACTORUL EPC va prezenta spre aprobarea BENEFICIARULUI arhitectura de securitate și matricea fluxurilor de comunicație, incluzând cel puțin sursa, destinația, protocolul/portul și scopul comunicației, fără limitarea soluției la o anumită tehnologie, arhitectură proprietară sau marcă.

În cazul accesului la distanță sau al interconectării cu rețeaua IT a BENEFICIARULUI ori cu alte rețele externe, accesul către sistemele OT va fi realizat exclusiv prin mecanisme securizate și controlate, amplasate în zona demilitarizată industrială (IDMZ), cu autentificare multifactor (MFA) și conturi nominale, fără acces direct către echipamentele de comandă și control (IEC 62443-3-3 SR 1.13, SR 5.2; capitolul 5).

Arhitectura rețelei va fi structurată pe niveluri ierarhice, conform modelului de referință Purdue, aplicat împreună cu conceptul de zone și conduite din IEC 62443 (IEC 62443-1-1, IEC 62443-3-2 și IEC 62443-3-3, în special SR 5.1 – Segmentarea rețelei și SR 5.2 – Protecția limitelor zonelor). Fiecare nivel va constitui cel puțin o zonă de securitate distinctă, iar comunicațiile între zone vor fi realizate exclusiv prin conduite definite, documentate și controlate. Structura minimă a nivelurilor este următoarea:

Nivel	Denumire	Echipamente / sisteme tipice	Cerințe principale de securitate
Level 0	Proces fizic (câmp)	Senzori, traductoare, actuatori, transformatoare de măsură, întrerupătoare și separatoare, stații meteo, module PV	Protecție fizică a echipamentelor și a cablurilor; acces numai prin echipamentele din Level 1; interfețele locale de configurare/mentenanță protejate și dezactivate când nu sunt utilizate.
Level 1	Control de bază și protecție	PLC, RTU, IED-uri de protecție și control (inclusiv IEC 61850), controlere invertoare, Power Plant Controller (PPC), sisteme de protecție	Zonă dedicată, fără acces direct din niveluri superioare lui Level 2; comunicații limitate la protocoalele industriale necesare (de ex. Modbus TCP, IEC 61850 MMS/GOOSE, DNP3); modificarea logicii și a configurației numai din stații de inginerie autorizate; funcțiile de protecție nu vor depinde de funcționarea componentelor de securitate cibernetică.
Level 2	Supraveghere și control	SCADA local, HMI, stații de inginerie, gateway-uri/convertoare de protocol, servere de comunicație (de ex. IEC 60870-5-104)	Conturi nominale și privilegii bazate pe rol; hardening și application allowlisting; comunicații către Level 1 numai de la sistemele autorizate; monitorizare pasivă a traficului.
Level 3	Operații și management site (OT)	Historian, server de alarme și evenimente, servicii de identitate OT (AD/LDAP/RADIUS), servere antivirus și patch management OT, backup,	Servicii de infrastructură OT separate de cele IT; identități/domeniu OT separate de domeniul IT, fără relație de încredere directă, cu excepția cazurilor justificate prin analiza de risc; jurnalizare

		colector Syslog/SIEM, sistem de monitorizare OT (IDS), server NTP	centralizată a evenimentelor de securitate.
Level 3.5	Zona demilitarizată industrială (IDMZ)	Jump server/bastion host, secure remote access gateway, replică historian, server relay pentru actualizări antivirus și patch-uri, server de transfer securizat de fișiere	Punct unic de trecere între IT și OT; toate sesiunile IT–OT se termină în IDMZ; delimitată de firewall-uri pe ambele laturi (sau firewall cu interfețe/zone separate, conform analizei de risc); MFA pentru accesul la distanță; nu va stoca date primare de proces.
Level 4	Rețeaua enterprise (IT) a BENEFICIARULUI	Rețeaua corporativă, aplicații de business, servicii IT centrale, utilizatori IT, conexiuni externe	Interconexiunea cu IDMZ va fi realizată conform politicilor BENEFICIARULUI; accesul către sistemele OT va fi permis numai prin Level 3.5.

Reguli pentru comunicațiile între niveluri:

- Comunicațiile vor fi permise, de regulă, numai între niveluri adiacente; fluxurile care traversează mai multe niveluri vor fi interzise, cu excepția celor justificate prin analiza de risc și aprobate de BENEFICIAR.
- Nu vor exista fluxuri directe între Level 4 și Level 3, 2, 1 sau 0; orice schimb de date între IT și OT va fi intermediat de sistemele din Level 3.5.
- Fluxurile de date dinspre OT către IT vor fi, de preferință, inițiate din zona OT (de exemplu, replicarea datelor din historian către IDMZ).
- Regulile de firewall vor aplica principiul „deny by default / allow by exception” și vor specifica sursa, destinația, protocolul/portul și scopul, conform matricei fluxurilor de comunicație.
- Trecerea de la un nivel la altul va necesita autentificare separată, cu conturi nominale; aceleași credențiale nu vor fi utilizate pe niveluri diferite.
- Separarea între niveluri poate fi fizică sau logică; separarea exclusiv prin VLAN, fără un mecanism de filtrare a traficului (firewall sau echivalent), nu va fi considerată suficientă ca limită între zone.

- Vor fi instalate obligatoriu firewall-uri (firewall industrial / NGFW sau echivalent), configurate conform principiului „deny by default / allow by exception”, cel puțin la următoarele limite între zone: Level 4 – Level 3.5, Level 3.5 – Level 3 și Level 3 – Level 2. Nu vor exista căi de comunicație care să ocolească aceste firewall-uri. Pentru limita Level 2 – Level 1, necesitatea unui firewall sau a unui mecanism echivalent de filtrare va fi stabilită prin evaluarea de risc conform IEC 62443-3-2 (cerințele detaliate sunt prezentate în capitolul 6).
    - Nivelul de securitate țintă (SL-T) pentru fiecare zonă și conduită va fi stabilit prin evaluarea de risc conform IEC 62443-3-2 și documentat în specificația de proiectare.
    - Conexiunea cu dispecerul energetic / operatorul de rețea, după caz, va fi tratată ca o conduită dedicată, conform cerințelor operatorului și ale BENEFICIARULUI.

- Pentru protocoalele de stație și telecontrol (IEC 61850 MMS/GOOSE/SV, IEC 60870-5-104, DNP3) se vor utiliza, acolo unde sunt suportate de echipamente și de operatorul de rețea, mecanismele de securitate din seria IEC 62351 (de exemplu TLS pentru IEC 60870-5-104/MMS, autentificarea GOOSE/SV) sau DNP3 Secure Authentication. Acolo unde acestea nu sunt disponibile (echipamente existente sau limitări de performanță), vor fi definite măsuri compensatorii la nivel de conduită (IEC 62443-3-3 SR 3.1, SR 4.3).
    - Rețelele wireless, dacă sunt prevăzute, vor fi tratate ca zone distincte și nu vor fi conectate direct la Level 0 sau Level 1.
- Nu vor exista echipamente conectate simultan la mai multe zone (dual-homed) care să ocolească limitele dintre zone, cu excepția componentelor de securitate proiectate în acest scop (firewall-uri, gateway-uri dedicate).
- Interfețele de management ale echipamentelor de rețea și de securitate vor fi accesibile numai dintr-o rețea/zonă de management dedicată; protocoalele de administrare nesecurizate (Telnet, HTTP, FTP, SNMP v1/v2c) vor fi dezactivate și înlocuite cu variante securizate (SSH, HTTPS, SFTP, SNMPv3), acolo unde echipamentele permit.
- Toate sistemele OT vor fi sincronizate de la o sursă de timp OT de încredere (server NTP/PTP intern, de preferință cu referință GPS și protecție împotriva manipulării), pentru corelarea evenimentelor și funcționarea corectă a protecțiilor (IEC 62443-3-3 SR 2.11; ISO/IEC 27002:2022 8.17).

Rețelele funcționale ale proiectului se vor încadra în această structură astfel: rețeaua controlerelor principale și a echipamentelor de comandă, control și protecție (CEF, stație electrică) – Level 1; rețeaua sistemelor de supraveghere și monitorizare (SCADA, HMI) – Level 2; serviciile interne de administrare, identitate, jurnalizare și backup – Level 3; accesul la distanță și schimbul de date cu rețelele IT/externe – Level 3.5 (IDMZ). Încadrarea finală va fi confirmată prin studiul Cyber HAZOP (capitolul 3).

3 OT SECURITY HAZOP (CYBER HAZOP)

CONTRACTORUL EPC va organiza și va realiza, împreună cu BENEFICIARUL, un studiu OT Security HAZOP (Cyber HAZOP / Cyber PHA) pentru sistemele OT/IACS incluse în scopul proiectului: CEF, stația electrică, SCADA/PPC și infrastructura de comunicații aferentă. Studiul va constitui evaluarea riscului de securitate cibernetică a proiectului, în sensul IEC 62443-3-2, și va sta la baza definirii zonelor și conduitelor, a stabilirii nivelurilor de securitate țintă (SL-T) și a selectării măsurilor de securitate descrise în prezentul document.

Cyber HAZOP extinde analizele de pericole de proces și de siguranță ale proiectului (HAZOP/PHA, studiile de protecții) cu scenarii în care cauza deviației este o acțiune cibernetică, intenționată sau neintenționată: transmiterea de comenzi sau valori de consemn neautorizate, modificarea logicii de control sau a configurației, compromiterea stațiilor de inginerie, pierderea vizibilității sau a controlului, indisponibilitatea comunicațiilor, dezactivarea ori modificarea funcțiilor de protecție. Consecințele vor fi evaluate din perspectiva sănătății, securității și mediului (HSE), dar și din perspectiva disponibilității instalației, a obligațiilor față de operatorul de rețea / dispecer și a impactului financiar.

3.1 OBIECTIVE

- identificarea sistemului analizat (System under Consideration – SuC) și a limitelor acestuia;
- identificarea scenariilor relevante de amenințare cibernetică și a consecințelor potențiale, inclusiv a celor asupra siguranței persoanelor și integrității echipamentelor;
- partiționarea sistemului în zone și conduite și validarea arhitecturii descrise în capitolul 2;
- stabilirea SL-T pentru fiecare zonă și conduită, sub forma unui vector SL pentru cele șapte cerințe fundamentale (FR 1 – FR 7) din IEC 62443-3-3;
- identificarea măsurilor de securitate existente și a măsurilor suplimentare necesare pentru reducerea riscului rezidual la un nivel tolerabil, conform criteriilor de risc ale BENEFICIARULUI;
- elaborarea Specificației cerințelor de securitate cibernetică (Cybersecurity Requirements Specification – CRS), utilizată inclusiv pentru cerințele adresate furnizorilor de echipamente și sisteme OT.

3.2 ETAPELE PROIECTULUI ÎN CARE SE REALIZEAZĂ STUDIUL

Cyber HAZOP nu reprezintă o activitate unică. Studiul va fi realizat etapizat, pe parcursul ciclului de viață al proiectului, astfel încât rezultatele să poată influența arhitectura înainte ca aceasta să fie înghețată și înainte de achiziționarea echipamentelor OT. Etapele minime sunt următoarele:

Etapa proiectului	Activitate Cyber HAZOP	Rezultate principale	Moment / termen
1. Ofertare (licitație EPC)	Prezentarea metodologiei Cyber HAZOP, a componenței	Metodologie și plan preliminar al studiului	Odată cu oferta tehnică

	echipei și a calificărilor facilitatorului		
2. Proiectare de bază (Basic Design / FEED)	Cyber HAZOP de nivel înalt: identificarea SuC, evaluarea inițială a riscului, partiționarea preliminară în zone și conduite, compararea riscului inițial cu riscul tolerabil (IEC 62443-3-2, ZCR 1 – ZCR 4)	Lista zonelor și conduitelor, diagrama preliminară, SL-T inițial, lista scenariilor de amenințare	Înainte de înghețarea arhitecturii și de emiterea comenzilor pentru echipamentele OT/IACS (SCADA, PPC, IED-uri, invertoare, echipamente de rețea)
3. Proiectare de detaliu	Cyber HAZOP detaliat pentru fiecare zonă și conduită (ZCR 5 – ZCR 7): amenințări, vulnerabilități, consecințe, probabilitate, risc inițial, măsuri existente, risc rezidual și măsuri suplimentare	Raport Cyber HAZOP, SL-T final (vector SL), CRS, registrul recomandărilor	Finalizat și aprobat de BENEFICIAR cu cel puțin 2 luni înainte de Cyber FAT; constituie dată de intrare pentru Specificația de proiectare funcțională a securității OT (capitolul 15)
4. Achiziție și integrare	Verificarea capabilităților de securitate ale echipamentelor propuse (SL-C) față de SL-T; definirea măsurilor compensatorii acolo unde SL-C < SL-T	Analiza de tip gap SL-C / SL-T, măsuri compensatorii aprobate	Înainte de comanda fermă a echipamentelor
5. Cyber FAT / Cyber SAT / punere în funcțiune	Verificarea implementării măsurilor rezultate din studiu și închiderea recomandărilor	Registrul recomandărilor actualizat, dovezi de implementare, nivelul de securitate atins (SL-A)	La Cyber FAT și la Cyber SAT
6. Predare	Actualizarea studiului conform configurației as-built; acceptarea formală a riscului rezidual de către BENEFICIAR	Raport Cyber HAZOP as-built, registrul riscurilor reziduale	La predarea sistemului
7. Exploatare	Revalidarea studiului, sub responsabilitatea BENEFICIARULUI, cu suportul CONTRACTORULUI EPC pe perioada de garanție	Raport Cyber HAZOP revizuit	La orice modificare semnificativă (MOC), după incidente relevante, la schimbări semnificative ale peisajului de amenințări și periodic, de regulă împreună cu revalidarea HAZOP-ului de proces

Cyber HAZOP va fi realizat după finalizarea HAZOP-ului de proces / electric al proiectului sau în paralel cu acesta, astfel încât scenariile cu consecințe HSE identificate să fie preluate ca date de intrare. Recomandările care afectează funcțiile de protecție sau de siguranță vor fi coordonate cu proiectantul

protecțiilor și cu echipa responsabilă de siguranța funcțională și nu vor fi implementate fără evaluarea impactului asupra acestor funcții.

3.3 METODOLOGIE

- Studiul va fi realizat în sesiuni de lucru facilitate (workshop-uri), pe baza metodologiei IEC 62443-3-2, combinată cu tehnica HAZOP (noduri și cuvinte-ghid) sau, cu acordul BENEFICIARULUI, cu tehnica SWIFT.
- Nodurile de analiză vor fi zonele și conduitele definite conform capitolului 2.
- Pentru fiecare nod vor fi analizate cel puțin următoarele deviații cibernetice: comenzi sau valori de consemn neautorizate; modificarea logicii sau a configurației; pierderea vizibilității sau a controlului; afișarea de date false către operator; indisponibilitatea comunicațiilor sau a serviciilor; acces neautorizat local sau de la distanță; introducerea de malware prin medii detașabile, prin accesul furnizorilor sau prin lanțul de aprovizionare.
- Pentru fiecare scenariu se vor documenta: cauza (amenințarea și vectorul de atac), vulnerabilitățile exploatate, consecințele, măsurile de protecție existente, probabilitatea, riscul inițial, riscul rezidual și recomandările.
- Riscul va fi evaluat utilizând matricea de risc a BENEFICIARULUI. În lipsa acesteia, CONTRACTORUL EPC va propune o matrice de risc spre aprobare.
- Funcțiile programabile (software/firmware) nu vor fi considerate bariere independente într-un scenariu cibernetic dacă pot fi compromise prin același vector de atac. Vor fi creditate cu prioritate barierele neprogramabile sau independente, de exemplu protecțiile electrice cu funcționare independentă, interblocările hardwired, dispozitivele mecanice.
- Scenariile vor fi corelate, după caz, cu tehnicile din MITRE ATT&CK for ICS.
    - Scenariile vor ține cont de informații actuale despre amenințările relevante pentru sectorul energetic (threat intelligence – ISO/IEC 27002:2022 5.7), de exemplu avertizările DNSC, ENISA și CISA ICS, și vor prioritiza consecințele cu impact asupra siguranței și asupra rețelei electrice (abordare orientată pe consecințe).
- SL-T va fi stabilit pentru fiecare zonă și conduită pe baza riscului maxim identificat. Acolo unde capabilitățile echipamentelor (SL-C) nu permit atingerea SL-T, vor fi definite măsuri compensatorii, care vor fi supuse aprobării BENEFICIARULUI.

3.4 ECHIPA DE STUDIU

Echipa de studiu va include, după caz:

- un facilitator (lider de studiu) independent de echipa de proiectare, cu experiență demonstrabilă în Cyber HAZOP / Cyber PHA și în aplicarea IEC 62443 (de exemplu, certificare ISA/IEC 62443 Cybersecurity Risk Assessment Specialist sau echivalent);
- reprezentanți ai BENEFICIARULUI: OT Security, IT Security, operare, mentenanță și HSE;

- reprezentanți ai CONTRACTORULUI EPC: proiectantul SCADA / automatizări, proiectantul rețelelor de comunicații și proiectantul electric și de protecții;
- reprezentanți ai furnizorilor principali (invertoare, PPC, IED-uri de protecție, SCADA), pentru sesiunile care privesc echipamentele acestora.

Înainte de începerea studiului, CONTRACTORUL EPC va transmite BENEFICIARULUI, spre aprobare, CV-ul facilitatorului și componența nominală a echipei.

3.5 DATE DE INTRARE

- rezultatele analizelor de pericole și ale studiilor HAZOP/PHA aplicabile CEF și interfețelor cu instalațiile existente ale rafinăriei, precum și studiile de protecții;
- arhitectura de rețea, preliminară sau de detaliu, și diagrama zonelor și conduitelor;
- matricea fluxurilor de comunicație (sursă, destinație, protocol/port, scop);
- inventarul activelor OT (denumire, funcție, versiune software/firmware, responsabil);
- documentația de securitate a furnizorilor: ghiduri de hardening, certificări IEC 62443-4-1 / 4-2, dacă există, și vulnerabilitățile cunoscute ale produselor;
- cerințele operatorului de rețea / dispecerului și ale BENEFICIARULUI privind conectarea la sisteme externe și accesul la distanță;
- politicile și procedurile BENEFICIARULUI și criteriile acestuia de toleranță la risc.

3.6 LIVRABILE ȘI URMĂRIREA RECOMANDĂRILOR

- Raportul Cyber HAZOP, incluzând metodologia, participanții, ipotezele și constrângerile, precum și foile de lucru complete;
- lista zonelor și conduitelor și diagrama aferentă;
- registrul scenariilor de amenințare și al riscurilor;
- SL-T pentru fiecare zonă și conduită (vector SL);
- Specificația cerințelor de securitate cibernetică (CRS);
- registrul recomandărilor, cu responsabil, termen și stare pentru fiecare recomandare;
- registrul riscurilor reziduale, acceptat formal de BENEFICIAR.

Toate recomandările vor fi urmărite până la închidere. Recomandările asociate riscurilor ridicate vor fi închise înainte de Cyber FAT sau, dacă acest lucru nu este posibil, vor fi tratate prin măsuri compensatorii temporare aprobate de BENEFICIAR. Orice modificare a arhitecturii sau a echipamentelor după aprobarea studiului va fi evaluată prin procedura de management al modificărilor (MOC), iar studiul va fi actualizat corespunzător.

Raportul Cyber HAZOP conține informații sensibile privind vulnerabilitățile instalației și va fi clasificat și distribuit restricționat, conform politicilor BENEFICIARULUI.

4 CONSOLIDARE (HARDENING)

CONTRACTORUL EPC va implementa măsuri de hardening pentru serverele, stațiile de lucru, echipamentele de rețea și celelalte sisteme OT/IACS, în conformitate cu funcționalitatea acestora, recomandările producătorilor și cerințele de securitate aplicabile.

Accesul la sisteme va fi realizat pe baza unor **conturi nominale și a unor niveluri de privilegii diferențiate în funcție de rol**, conform cerințelor din capitolul 7.

Configurațiile de securitate vor avea la bază ghidurile de hardening ale producătorilor și, pentru sistemele de operare și echipamentele de rețea de uz general, ghiduri recunoscute (de exemplu CIS Benchmarks), adaptate mediului OT. Pentru fiecare tip de activ se va defini și documenta o configurație de referință (security baseline), verificată la Cyber FAT / Cyber SAT (IEC 62443-3-3 SR 7.6, SR 7.7; ISO/IEC 27002:2022 8.9). Toate parolele și cheile implicite din fabrică vor fi schimbate înainte de punerea în funcțiune, iar conturile implicite nefolosite vor fi dezactivate sau eliminate (SR 1.5). Dulapurile, rack-urile și camerele tehnice care găzduiesc echipamente OT vor fi protejate fizic (încuiere, control și jurnalizare a accesului, sigilii/detecție de deschidere, după caz) (ISO/IEC 27002:2022 7.1–7.4).

4.1 INTERFEȚE

Pentru serverele, stațiile de lucru și echipamentele care permit configurarea BIOS/UEFI sau a unui mecanism echivalent, CONTRACTORUL EPC va asigura securizarea configurației de pornire, inclusiv:

- protejarea accesului la BIOS/UEFI prin parolă sau mecanism echivalent;
- configurarea și restricționarea dispozitivelor de boot;
- excluderea mediilor detașabile din secvența normală de pornire, cu excepția situațiilor autorizate de mentenanță;
- dezactivarea sau restricționarea porturilor și interfețelor destinate mediilor de stocare detașabile, prin BIOS/UEFI, sistemul de operare, politici de securitate sau alte mecanisme echivalente, cu excepția cazurilor necesare pentru operare sau mentenanță, justificate de CONTRACTORUL EPC și acceptate de BENEFICIAR.

Porturile și interfețele de comunicație neutilizate vor fi dezactivate logic și/sau fizic, în măsura în care acest lucru este suportat de echipamentul respectiv și nu afectează funcționarea, mentenanța sau garanția acestuia.

Mediile de stocare detașabile, inclusiv hard-diskurile externe și dispozitivele USB, nu vor fi disponibile automat utilizatorilor. Funcțiile **Automount/Autoplay** sau funcțiile echivalente vor fi dezactivate, acolo unde sistemul de operare permite acest lucru.

Utilizarea mediilor detașabile în sistemele OT va fi permisă numai în condițiile și conform procedurilor de securitate aprobate de BENEFICIAR.

4.2 SERVICII ȘI SOFTWARE

CONTRACTORUL EPC va asigura dezactivarea serviciilor, protocoalelor, conturilor implicite și funcționalităților software care nu sunt necesare funcționării, administrării sau mentenanței sistemului.

Instrumentele de dezvoltare, depanare sau diagnosticare care nu sunt necesare funcționării sistemului în exploatare vor fi dezactivate sau eliminate. Instrumentele necesare mentenanței vor fi protejate împotriva utilizării neautorizate.

Configurațiile de securitate aplicate nu vor afecta funcțiile de control, protecție, siguranță, disponibilitate sau performanță ale sistemelor OT.

Sistemele de operare, aplicațiile și firmware-ul echipamentelor OT vor fi menținute la nivelul de patch-uri de securitate aprobat de producător, conform unui proces de management al patch-urilor aliniat cu IEC 62443-2-3: monitorizarea patch-urilor disponibile, verificarea compatibilității (patch-uri calificate de producătorul sistemului de control), testarea într-un mediu de test sau pe un sistem reprezentativ, aplicarea prin procedura de management al modificărilor (MOC) într-o fereastră de mentenanță aprobată și existența unui plan de revenire (rollback). Pe perioada de garanție, CONTRACTORUL EPC va furniza și, după caz, va aplica patch-urile de securitate relevante; acolo unde un patch nu poate fi aplicat, vor fi propuse măsuri compensatorii.

4.3 MONITORIZARE ȘI DETECTARE CYBERSECURITY

Soluția va permite monitorizarea evenimentelor și comunicațiilor relevante din rețeaua OT în vederea identificării, după caz, a:

- comunicațiilor neautorizate sau suspecte;
- tentativelor de acces neautorizat;
- utilizării unor protocoale sau servicii nepermise;
- anomaliilor relevante de comunicație;
- modificărilor neautorizate ale configurațiilor;
- tentativelor de exploatare a vulnerabilităților cunoscute.

Monitorizarea rețelelor OT se va realiza **preponderent prin mecanisme pasive sau prin alte metode care nu afectează disponibilitatea și performanța instalației**.

Implementarea unor funcții automate de blocare sau prevenție asupra traficului OT va fi realizată numai dacă este justificată prin analiza de risc, compatibilă cu echipamentele și protocoalele utilizate și aprobată în prealabil de BENEFICIAR.

CONTRACTORUL EPC nu este limitat la utilizarea unui anumit tip de IDS/IPS, appliance, platformă software sau producător, cu condiția demonstrării funcționalităților solicitate.

Soluția de monitorizare OT va asigura cel puțin: vizibilitatea traficului pe toate conduitele critice și în zonele Level 1–3 (prin porturi SPAN sau TAP-uri pasive); inventarierea pasivă și continuă a activelor și detectarea echipamentelor noi; stabilirea unei linii de bază a comunicațiilor și alertarea la abateri; decodarea protocoalelor industriale utilizate (de exemplu IEC 61850, IEC 60870-5-104, Modbus TCP, DNP3), inclusiv detectarea comenzilor de scriere, a descărcărilor de logică/firmware și a modificărilor de configurație; transmiterea alertelor către SIEM/SOC-ul BENEFICIARULUI într-un format standard (de exemplu Syslog/CEF). Procedurile de tratare a alertelor vor fi agreate cu BENEFICIARUL (IEC 62443-3-3 SR 6.2; ISO/IEC 27002:2022 8.16; SANS ICS Critical Control 3 – vizibilitate și monitorizare a rețelei ICS).

4.4 MANAGEMENTUL VULNERABILITĂȚILOR

CONTRACTORUL EPC va prevedea un proces pentru identificarea, evaluarea și tratarea vulnerabilităților sistemelor OT, inclusiv verificarea versiunilor software/firmware, patch-urilor de securitate și configurațiilor relevante.

Monitorizarea pasivă, inventarierea echipamentelor, analiza vulnerabilităților cunoscute și verificările de configurație vor fi utilizate cu prioritate pentru echipamentele OT sensibile.

Scanările active asupra echipamentelor și rețelelor OT aflate în exploatare nu vor fi executate automat sau necontrolat. Acestea vor putea fi efectuate numai după evaluarea impactului, verificarea compatibilității cu recomandările producătorului, aprobarea BENEFICIARULUI și, după caz, într-o fereastră de mentenanță sau într-un mediu de test.

Pentru servere, stații de lucru și alte sisteme care permit scanarea fără afectarea procesului tehnologic, metodologia și periodicitatea verificărilor vor fi stabilite în Specificația de proiectare funcțională a securității OT (capitolul 15) și agreate cu BENEFICIARUL.

Rezultatele evaluărilor și vulnerabilitățile relevante identificate vor fi documentate și transmise BENEFICIARULUI împreună cu măsurile recomandate de remediere sau compensare.

Vulnerabilitățile vor fi prioritizate pe baza riscului, ținând cont de exploatabilitatea reală (de exemplu existența în catalogul CISA KEV), de expunerea activului (zona și conduitele aferente) și de consecințele asupra procesului, nu exclusiv pe baza scorului CVSS (SANS ICS Critical Control 5). Sursele monitorizate vor include cel puțin avertizările de securitate ale producătorilor (PSIRT), avertizările CISA ICS, baza de date europeană de vulnerabilități (ENISA EUVD) și alertele DNSC. Pe perioada de garanție, CONTRACTORUL EPC va notifica BENEFICIARUL cu privire la orice vulnerabilitate nou publicată care afectează sistemele furnizate, în cel mult 5 zile lucrătoare (24 de ore pentru vulnerabilitățile exploatate activ), împreună cu evaluarea impactului și măsurile recomandate (Directiva NIS2 art. 21 alin. (2) lit. (e); ISO/IEC 27002:2022 8.8).

5 ACCES LA DISTANȚĂ

1. CONTRACTORUL EPC va proiecta și implementa o **soluție dedicată** de acces la distanță **securizat** pentru sistemele OT, amplasată în IDMZ (Level 3.5), conformă cu IEC 62443-3-3 SR 1.13 (acces prin rețele nesigure) și SR 2.6 (terminarea sesiunilor la distanță) și cu SANS ICS Critical Control 4 (acces la distanță securizat). Soluția va respecta cerințele minime din prezentul capitol, va fi descrisă în Specificația de proiectare funcțională a securității OT, aprobată de BENEFICIAR și verificată la Cyber FAT / Cyber SAT.
2. Sistemul va permite aprobarea **pentru fiecare eveniment** a oricărei conexiuni la distanță de către managerul de operare al centralei sau de către personalul desemnat de BENEFICIAR.
3. Orice conexiune la distanță va fi documentată și jurnalizată, iar log-urile vor fi transmise către un server **syslog sau către o soluție centralizată echivalentă de colectare și păstrare a jurnalelor**.
4. Sesiunea de acces la distanță va fi privată și criptată, pe baza unei conexiuni **VPN**, iar autentificarea utilizatorilor va utiliza **conturi nominale și autentificare multifactor (MFA)**.
5. Orice conexiune va fi limitată în timp și va fi deconectată automat la expirarea perioadei autorizate.
6. **Conexiunile** la distanță către sistemele OT vor fi realizate printr-un mecanism intermediar securizat de tip **jump server/bastion host/secure access gateway** sau soluție echivalentă, care să permită accesul controlat exclusiv către sistemele autorizate. Soluția va include măsuri de application control/allowlisting sau mecanisme echivalente, după caz.
7. Sesiunile de acces la distanță vor fi terminate în IDMZ (Level 3.5); nu vor fi permise conexiuni inițiate din exterior direct către Level 1–3 și nici instrumente de acces la distanță instalate pe sistemele OT care inițiază conexiuni către servicii cloud ale terților (de exemplu TeamViewer, AnyDesk sau echivalente) sau modemuri/routere celulare necontrolate.
8. Conturile furnizorilor vor fi nominale, dezactivate implicit și activate numai pe durata intervenției aprobate; privilegiile vor fi limitate la sistemele și funcțiile strict necesare (de exemplu doar citire, acolo unde scrierea nu este necesară). Sesiunile cu privilegii administrative sau care pot modifica logica/configurația vor fi monitorizate în timp real și înregistrate (session recording), iar înregistrările vor fi păstrate conform politicii BENEFICIARULUI.
9. Transferul de fișiere către sistemele OT se va realiza numai prin serverul de transfer securizat din IDMZ, cu scanare anti-malware (de preferință cu mai multe motoare de scanare) și verificarea integrității/semnăturii fișierelor. Personalul BENEFICIARULUI va dispune de un mecanism local de întrerupere imediată a tuturor sesiunilor de acces la distanță, care nu afectează funcționarea procesului..

6 FIREWALL

Segmentarea rețelei și regulile de firewall vor fi stabilite pe baza rezultatelor **studiului de securitate (Cyber HAZOP)** realizat împreună cu BENEFICIARUL (capitolul 3) și vor fi conforme cu arhitectura pe niveluri din capitolul 2 (IEC 62443-3-3 SR 5.1, SR 5.2; ISO/IEC 27002:2022 8.20, 8.22).

În general:

- Vor fi instalate firewall-uri cel puțin la limitele dintre zone prevăzute în capitolul 2 (Level 4 – Level 3.5, Level 3.5 – Level 3 și Level 3 – Level 2), precum și la conexiunile către medii externe (dispecer / operator de rețea, furnizori). Firewall-urile de segmentare internă vor permite monitorizarea traficului dintre zonele rețelei centralei fotovoltaice și stației electrice.
- Firewall-ul de la limita IT–OT / mediul extern va suporta controlul accesului la distanță, inclusiv **VPN**, **autentificare multifactor (MFA)** și integrarea cu soluția de acces securizat din IDMZ (capitolul 5).
- Firewall-urile vor include cel puțin funcțiile de **Antivirus, Sistem de Prevenire a Intruziunilor (IPS) și Sistem de Detectare a Intruziunilor (IDS)**. Pe limitele către IT și mediul extern (Level 4 / Level 3.5), funcțiile de prevenție vor fi active. Pe limitele interne OT (Level 3 și inferioare), funcțiile IPS vor funcționa implicit în mod de detecție; blocarea automată a traficului OT va fi activată numai în condițiile prevăzute în subcapitolul 4.3 (justificare prin analiza de risc, testare și aprobarea BENEFICIARULUI), pentru a evita întreruperea comunicațiilor de control și protecție.
- Firewall-urile dintre zonele OT vor suporta inspecția protocoalelor industriale utilizate (Deep Packet Inspection pentru IEC 60870-5-104, IEC 61850 MMS, Modbus TCP, DNP3), cu posibilitatea de a restricționa funcțiile de scriere / comandă la sursele autorizate.
- Firewall-urile amplasate pe căi critice pentru control vor fi configurate în înaltă disponibilitate (HA) sau vor avea un comportament definit la defectare, stabilit prin analiza de risc. Administrarea se va face numai din rețeaua de management, cu conturi nominale și MFA; jurnalele vor fi transmise către colectorul central (capitolul 8); configurațiile vor fi salvate după fiecare modificare, iar setul de reguli va fi revizuit cel puțin anual și la fiecare modificare a matricei fluxurilor de comunicație.

Configurația și funcționalitățile indicate mai sus au caracter de referință și nu impun o arhitectură fixă. CONTRACTORUL EPC poate propune soluții tehnice alternative sau echivalente, inclusiv în ceea ce privește numărul, tipul și modul de implementare al firewall-urilor și al funcțiilor de securitate, cu condiția asigurării unui nivel cel puțin echivalent de securitate, funcționalitate și disponibilitate și cu aprobarea BENEFICIARULUI.

7 MANAGEMENTUL UTILIZATORILOR

Autentificarea și autorizarea utilizatorilor vor fi gestionate centralizat, acolo unde este suportat și adecvat arhitecturii OT, prin servicii de identitate și autentificare centralizată (de exemplu Domain Controller/Active Directory, LDAP, RADIUS sau soluții echivalente), conform politicilor BENEFICIARULUI.

  - Identitățile și domeniul OT vor fi separate de domeniul IT al BENEFICIARULUI, fără relații de încredere directe, cu excepția cazurilor justificate prin analiza de risc (IEC 62443-3-3 SR 1.1, SR 1.3).
  - Se vor utiliza conturi nominale (individuale) pentru toți utilizatorii; conturile partajate vor fi permise numai acolo unde funcționarea în siguranță o impune (de exemplu stații HMI de operare continuă), cu măsuri compensatorii documentate (acces fizic controlat, jurnalizare, registru de tură).

- Drepturile vor fi acordate pe bază de rol (RBAC) și conform principiului privilegiului minim, documentat în User & Role Matrix; conturile administrative vor fi separate de cele de utilizare curentă. CONTRACTORUL EPC / furnizorul de servicii va întocmi lista drepturilor de acces și a privilegiilor necesare pentru prestarea serviciilor convenite. Aceste drepturi și privilegii vor fi definite formal în User & Role Matrix (matricea RBAC) și vor fi menționate în contract, care va constitui autorizarea oficială și temeiul acordării accesului (SR 2.1; ISO/IEC 27002:2022 5.15, 5.18, 8.2).
- CONTRACTORUL EPC / furnizorul nu va prelucra, stoca, transmite și nu va accesa în alt mod date cu caracter personal, date financiare sau alte informații sensibile, cu excepția cazului în care o astfel de prelucrare este aprobată în mod explicit de BENEFICIAR și se supune cerințelor aplicabile privind protecția datelor, securitatea și conformitatea. Orice astfel de activitate de prelucrare a datelor va fi evaluată și documentată separat înainte de implementare.
  - Autentificarea multifactor (MFA) va fi obligatorie pentru accesul la distanță și pentru accesul privilegiat la sistemele din Level 3 și IDMZ, acolo unde este suportată (Directiva NIS2 art. 21 alin. (2) lit. (j)).
  - Politica de parole va respecta cerințele BENEFICIARULUI și capabilitățile echipamentelor (lungime, complexitate, blocare după încercări eșuate – SR 1.7, SR 1.11). Blocarea conturilor și a sesiunilor (SR 2.5) nu va fi aplicată pe stațiile de operare acolo unde ar putea împiedica intervenția operatorului.
  - Conturile de serviciu vor fi inventariate, fără drept de autentificare interactivă și cu parole complexe gestionate controlat. Conturile de urgență (break-glass) vor fi păstrate securizat (seif fizic sau soluție de tip PAM), iar orice utilizare a acestora va fi jurnalizată și analizată.
  - La predare, toate conturile temporare de punere în funcțiune ale CONTRACTORULUI EPC și ale furnizorilor vor fi dezactivate sau eliminate, iar credențialele vor fi transferate BENEFICIARULUI și schimbate. CONTRACTORUL EPC va furniza procedura de gestionare a ciclului de viață al conturilor (creare, modificare, revocare) și de revizuire periodică a drepturilor.

8 PROTOCOL DE JURNALIZARE A SISTEMULUI

Va exista un server Syslog / colector de jurnale pentru centrală, capabil să colecteze mesajele legate de securitate de la toate echipamentele IT, OT și de comunicații de pe amplasament, inclusiv:

- Sisteme și componente de securitate ale rețelei operaționale (firewall-uri, IDS, antivirus, application allowlisting, soluția de acces la distanță);
- Componente de comunicație (switch-uri, routere, gateway-uri, convertoare de protocol);
- Servere și stații de lucru (SCADA, HMI, historian, stații de inginerie);
- Controlere și echipamente de câmp care suportă jurnalizarea (PLC, RTU, IED-uri, PPC, controlere de invertor) – evenimente de autentificare, schimbări de mod, descărcări de logică/firmware și modificări de configurație;
- Acces utilizatori (autentificări reușite și eșuate, utilizarea privilegiilor, gestionarea conturilor).

Soluția va asigura colectarea centralizată și păstrarea jurnalelor relevante de securitate, utilizând Syslog sau alte protocoale/mecanisme suportate de echipamente. Colectarea poate fi realizată printr-un server local, collector, SIEM sau soluție echivalentă.

- Evenimentele auditabile vor include cel puțin: control acces, erori de solicitare, evenimente ale sistemului de operare, evenimente de control, evenimente de backup/restaurare, modificări de configurație și evenimente de audit (IEC 62443-3-3 SR 2.8; ISO/IEC 27002:2022 8.15).
- Toate înregistrările vor avea marcaj de timp sincronizat (SR 2.11); capacitatea de stocare va fi dimensionată pentru păstrarea locală a jurnalelor cel puțin 12 luni sau conform politicii BENEFICIARULUI, cu alertare la umplerea spațiului sau la întreruperea colectării (SR 2.9, SR 2.10).
- Jurnalele vor fi protejate împotriva modificării și ștergerii neautorizate (acces restricționat, transfer criptat acolo unde este suportat, copie în afara sistemului sursă).
- Jurnalele și alertele relevante vor fi transmise, printr-o conduită controlată via IDMZ, către SIEM-ul / SOC-ul BENEFICIARULUI, pentru a permite detectarea și raportarea incidentelor în termenele NIS2 (SR 6.1, SR 6.2).
- Jurnalizarea nu va afecta performanța sau determinismul funcțiilor de control și protecție.

8.1 PROTECȚIA ANTI-MALWARE ȘI LISTA ALBĂ A APLICAȚIILOR (APPLICATION ALLOWLISTING)

- Fiecare server și stație de lucru (Windows/Linux) din zonele OT și IDMZ va fi echipat cu o soluție de application allowlisting, compatibilă și calificată de producătorul sistemului de control; pentru echipamentele care nu suportă allowlisting vor fi definite măsuri compensatorii.

- Soluția va permite rularea exclusiv a executabilelor, serviciilor, bibliotecilor (DLL), scripturilor și driverelor aprobate și va proteja cheile de registry și fișierele critice împotriva modificărilor neautorizate (IEC 62443-3-3 SR 3.2, SR 3.4).
- Elementele aprobate vor fi identificate prin semnătură digitală și/sau hash criptografic.
- Soluția va fi pusă în funcțiune inițial în mod de audit, pe o perioadă agreată, apoi trecută în mod de blocare după validarea cu operarea; evenimentele de blocare vor fi transmise colectorului central de jurnale.
- Soluția va permite management și actualizare centralizată din Level 3, fără dependență de conexiuni directe la Internet. Aceasta completează, nu înlocuiește, protecția anti-malware (ISO/IEC 27002:2022 8.7).

- Serverele și stațiile de lucru vor fi echipate cu o soluție anti-malware calificată de producătorul sistemului de control, cu administrare centralizată din Level 3 și actualizarea semnăturilor prin serverul relay din IDMZ, după validare. Excepțiile de scanare vor fi limitate la cele recomandate de producător și documentate; scanările programate nu vor afecta performanța aplicațiilor de control (ISO/IEC 27002:2022 8.7; IEC 62443-3-3 SR 3.2).

Arhitectura și soluția tehnică prezentate în acest capitol au caracter de referință. CONTRACTORUL EPC poate propune soluții alternative sau echivalente, cu condiția demonstrării unui nivel cel puțin echivalent de securitate, funcționalitate și disponibilitate și cu aprobarea BENEFICIARULUI.

9 BACKUP, RESTAURARE ȘI CONTINUITATE

CONTRACTORUL EPC va proiecta, implementa și testa o soluție de backup și restaurare pentru toate sistemele OT furnizate, care să permită refacerea funcționării în valorile RTO/RPO stabilite de BENEFICIAR (IEC 62443-3-3 SR 7.3, SR 7.4; ISO/IEC 27002:2022 8.13, 5.30; Directiva NIS2 art. 21 alin. (2) lit. (c)). Cerințe minime:

- backup pentru imaginile complete ale serverelor și stațiilor de lucru, bazele de date, aplicațiile, precum și pentru programele, logica, fișierele de configurare și setările PLC-urilor, RTU-urilor, IED-urilor, PPC-ului, controlerelor de invertor și echipamentelor de rețea și securitate;
- aplicarea regulii 3-2-1, cu cel puțin o copie offline sau imuabilă, protejată împotriva ransomware-ului și păstrată separat fizic de sistemele sursă;
- criptarea copiilor de backup stocate în afara zonelor OT și verificarea integrității acestora (hash/semnătură);
- păstrarea unor imagini de referință (golden images) validate, a mediilor de instalare și a cheilor de licență necesare reinstalării complete;
- testarea restaurării complete a cel puțin unui sistem reprezentativ din fiecare categorie la Cyber SAT și recomandarea unei periodicități de testare pentru exploatare;
- definirea modurilor de funcționare degradată / manuală a instalației în cazul indisponibilității sistemelor de supraveghere și a strategiei pentru piese de schimb critice.

10 RĂSPUNS LA INCIDENTE ȘI RAPORTARE

CONTRACTORUL EPC va elabora, împreună cu BENEFICIARUL, un Plan de răspuns la incidente de securitate cibernetică specific OT, integrat în procesul de gestionare a incidentelor al BENEFICIARULUI (ISO/IEC 27002:2022 5.24–5.28; IEC 62443-2-1; NIST SP 800-82 Rev. 3; SANS ICS Critical Control 1 – plan de răspuns la incidente specific ICS). Planul va include cel puțin:

- roluri, responsabilități și date de contact (BENEFICIAR, CONTRACTOR EPC, furnizori principali), disponibile 24/7 pe perioada de garanție;
- scenarii (playbook-uri) derivate din Cyber HAZOP, de exemplu: ransomware pe stații SCADA/HMI, comenzi neautorizate de putere activă/reactivă, compromiterea accesului la distanță al unui furnizor, modificarea neautorizată a parametrilor invertoarelor, PPC-ului, funcției de zero-export sau protecțiilor electrice;
- criterii de izolare, inclusiv posibilitatea de deconectare controlată a zonelor OT de rețelele IT/externe la nivelul IDMZ, fără afectarea funcțiilor de control și protecție locale, precum și criteriile de trecere în regim de funcționare manuală sau de oprire în siguranță;
- reguli pentru păstrarea dovezilor (jurnale, imagini de memorie/disc, capturi de trafic) fără a compromite siguranța instalației;
- pași de recuperare corelați cu Planul de recuperare în caz de dezastru și cu soluția de backup (capitolul 9).

Pentru a permite BENEFICIARULUI respectarea obligațiilor de raportare prevăzute la art. 23 din Directiva NIS2 și în OUG nr. 155/2024 (avertizare timpurie în 24 de ore, notificare a incidentului în 72 de ore și raport final în cel mult o lună, către DNSC / autoritatea competentă), CONTRACTORUL EPC și subcontractanții săi vor notifica BENEFICIARUL fără întârzieri nejustificate, dar nu mai târziu de 4 ore de la detectare, cu privire la orice incident sau suspiciune de incident care afectează sistemele furnizate sau mijloacele de acces la acestea (inclusiv compromiterea propriei infrastructuri, a conturilor sau a lanțului de aprovizionare). Planul va fi exersat printr-un exercițiu de tip tabletop, cu participarea operării, înainte de predare.

11 SECURITATEA LANȚULUI DE APROVIZIONARE

CONTRACTORUL EPC va aplica cerințele de securitate cibernetică întregului lanț de aprovizionare pentru echipamentele, software-ul și serviciile OT furnizate (Directiva NIS2 art. 21 alin. (2) lit. (d) și (e); ISO/IEC 27002:2022 5.19–5.22; IEC 62443-2-4; IEC 62443-4-1 / 4-2):

- vor fi preferate componentele dezvoltate conform unui proces de dezvoltare securizată certificat IEC 62443-4-1 și componentele cu capabilități de securitate demonstrate conform IEC 62443-4-2 (de exemplu certificare ISASecure sau certificare emisă de un organism acreditat); pentru fiecare componentă critică se va declara SL-C atins;
- furnizorii vor pune la dispoziție ghidul de hardening, lista porturilor/serviciilor utilizate, lista conturilor implicite și declarația privind absența conturilor ascunse sau a mecanismelor de acces nedocumentate;
- pentru software-ul și firmware-ul furnizat se va preda lista componentelor software (SBOM), într-un format standard (de exemplu SPDX sau CycloneDX), actualizată la fiecare versiune livrată;
- firmware-ul și software-ul vor fi obținute numai din surse oficiale, cu verificarea semnăturii digitale / hash-ului înainte de instalare; toate mediile livrate vor fi scanate anti-malware înainte de conectarea la sistemele OT;
- furnizorii vor avea un proces public de gestionare și divulgare a vulnerabilităților (PSIRT) și vor declara durata minimă de suport pentru actualizări de securitate; nu vor fi acceptate produse aflate la sfârșitul ciclului de viață (EoL/EoS) sau anunțate pentru retragere în perioada de garanție; după caz, produsele vor respecta Regulamentul (UE) 2024/2847 (Cyber Resilience Act);
- contractele cu subcontractanții vor include clauze privind confidențialitatea, notificarea incidentelor, dreptul de audit al BENEFICIARULUI, respectarea politicilor de acces și obligația de a transfera aceste cerințe mai departe în lanțul de aprovizionare;
- personalul CONTRACTORULUI EPC responsabil de securitatea OT va deține calificări relevante (de exemplu ISA/IEC 62443 Cybersecurity Expert / Specialist, GIAC GICSP sau GRID ori echivalent), iar personalul cu acces la sistemele BENEFICIARULUI va fi verificat conform politicilor acestuia. Nu se solicită demonstrarea îndeplinirii acestor cerințe la depunerea ofertei. Îndeplinirea lor va fi demonstrată de Contractorul EPC doar pe durata executării contractului, la soli-citarea Beneficiarului.

12 TESTAREA SECURITĂȚII (CYBER FAT / CYBER SAT)

Implementarea cerințelor de securitate cibernetică va fi verificată prin teste dedicate, pe baza unor proceduri Cyber FAT și Cyber SAT transmise spre aprobare BENEFICIARULUI cu cel puțin o lună înainte de fiecare test (IEC 62443-3-3 SR 3.3; ISO/IEC 27002:2022 8.29). Testele vor acoperi cel puțin:

- verificarea configurației de referință (hardening), a conturilor și a eliminării parolelor implicite;
- verificarea regulilor de firewall față de matricea fluxurilor de comunicație și a absenței căilor de ocolire;
- testarea accesului la distanță (MFA, aprobare per sesiune, limitare în timp, înregistrare, deconectare de urgență);
- testarea jurnalizării, a sincronizării timpului și a transmiterii alertelor către SIEM/SOC, precum și a detecției IDS pentru scenarii agreate;
- testarea protecției anti-malware și a application allowlisting-ului;
- testarea backup-ului și a restaurării;
- scanarea de vulnerabilități și, după caz, testul de penetrare, efectuate la Cyber FAT în mediul de test, de o echipă independentă de echipa de proiectare; la Cyber SAT, pe sistemele în exploatare, se vor utiliza cu prioritate metode pasive, iar testele active numai în condițiile din subcapitolul 4.4;
- verificarea nivelului de securitate atins (SL-A) față de SL-T și închiderea recomandărilor din Cyber HAZOP.

Neconformitățile vor fi înregistrate, clasificate după risc și remediate; neconformitățile cu risc ridicat vor fi închise înainte de Cyber SAT, respectiv înainte de predare. Rapoartele de test vor fi predate BENEFICIARULUI.

13 MANAGEMENTUL MODIFICĂRILOR ȘI INSTRUIRE

Pentru menținerea nivelului de securitate pe durata proiectului și la trecerea în exploatare se vor aplica următoarele cerințe:

- După înghețarea configurației pentru Cyber FAT, orice modificare de arhitectură, configurație, software, firmware, logică de control sau reguli de firewall va fi realizată numai prin procedura de management al modificărilor (MOC) agreată cu BENEFICIARUL, cu evaluarea impactului asupra securității și siguranței, actualizarea documentației as-built și, după caz, a studiului Cyber HAZOP (ISO/IEC 27002:2022 8.32).
- Configurațiile și logica de control vor fi gestionate cu control al versiunilor; CONTRACTORUL EPC va furniza mijloacele de comparare a configurației curente cu cea aprobată (detectarea modificărilor neautorizate).
- CONTRACTORUL EPC va asigura instruirea personalului de operare, mentenanță și IT/OT Security al BENEFICIARULUI privind utilizarea și administrarea soluțiilor de securitate furnizate, procedurile de acces la distanță, backup/restaurare, răspuns la incidente și utilizarea mediilor detașabile, înainte de predare; instruirea va fi documentată (Directiva NIS2 art. 20 alin. (2) și art. 21 alin. (2) lit. (g); ISO/IEC 27002:2022 6.3).
- Personalul CONTRACTORULUI EPC și al subcontractanților care lucrează pe amplasament sau cu acces la sistemele OT va fi instruit cu privire la politicile de securitate ale BENEFICIARULUI înainte de începerea activității.

14 CERINȚE MINIME PENTRU INFRASTRUCTURA HARDWARE CYBERSECURITY

Arhitectura va fi proiectată de CONTRACTORUL EPC conform principiilor de segmentare, *defence-in-depth* și cerințelor IEC 62443 aplicabile.

Configurațiile de mai jos reprezintă **soluția tehnică de referință a BENEFICIARULUI**. Sunt acceptate soluții alternative, cu condiția asigurării unui nivel cel puțin echivalent de performanță, securitate și disponibilitate.

14.1 INFRASTRUCTURA CENTRALĂ DE ADMINISTRARE ȘI SECURITATE CIBERNETICĂ

CONTRACTORUL EPC va asigura infrastructura centrală necesară funcțiilor de virtualizare, administrare și securitate cibernetică ale CEF. Resursele existente ale BENEFICIARULUI pot fi utilizate pe baza informațiilor puse la dispoziție de acesta și cu aprobarea sa prealabilă scrisă. Oferta va preciza resursele reutilizate și va include toate echipamentele, licențele și serviciile suplimentare necesare.

Configurație de referință:

- Procesor: minimum 16 nuclee / 32 fire de execuție, echivalent sau superior Intel Xeon Performance 6517P;
- RAM: minimum 128 GB ECC;
- Stocare: minimum 3 × 960 GB SSD Enterprise, în configurație redundantă;
- Alimentare și răcire redundante;
- Interfețe de rețea și funcții de management securizat, conform arhitecturii propuse.

Dimensionarea finală va fi realizată de CONTRACTORUL EPC în funcție de soluția tehnică implementată.

14.2 ECHIPAMENTE INDUSTRIALE EDGE

Se recomandă echipamente Edge dedicate pentru principalele zone funcționale: **CEF și Stația Electrică**.

Configurație de referință minimă:

- Procesor industrial minimum 4 nuclee, echivalent sau superior Intel Pentium J6426;
- RAM: minimum 16 GB;
- Stocare: minimum 512 GB SSD;
- Interfețe Ethernet suficiente pentru segmentarea rețelelor;
- Funcții de securitate hardware și management securizat;
- Echipament adecvat funcționării continue în mediu industrial;
- Garanție minimum 5 ani.

Numărul, amplasarea și configurația finală a echipamentelor vor fi stabilite de CONTRACTORUL EPC în funcție de arhitectura de cybersecurity propusă.

Comunicațiile între zonele de securitate vor fi controlate prin firewall-uri industriale / NGFW sau soluții echivalente, conform principiului **„deny by default / allow by exception”**.

Arhitectura finală și eventualele abateri față de soluția de referință vor fi prezentate BENEFICIARULUI spre aprobare.

Echipamentele hardware și sistemele de operare propuse vor avea suport de securitate din partea producătorului pe întreaga perioadă de garanție și vor fi compatibile cu soluțiile de securitate solicitate (allowlisting, anti-malware, jurnalizare, backup). Funcțiile de securitate hardware (Secure Boot / UEFI, TPM, acolo unde sunt disponibile) vor fi activate.

CONTRACTORUL EPC este responsabil de furnizarea tuturor materialelor și serviciilor necesare realizării traseului de comunicație prin fibră optică dintre echipamentele instalate și infrastructura hardware existentă a BENEFICIARULUI. Traseele de comunicație vor fi protejate fizic, iar conexiunea cu infrastructura BENEFICIARULUI va fi realizată numai prin conduitele și firewall-urile definite în capitolele 2 și 6.

15 DOCUMENTAȚIE

Terminologia utilizată în documentație va fi conformă cu ISO/IEC 27000:2018 și IEC 62443-1-1, iar conținutul documentației va acoperi cerințele aplicabile din standardele de referință indicate în capitolul 1.

CONTRACTORUL EPC va preda documentația as-built relevantă pentru securitatea cibernetică, incluzând, fără a se limita la, cel puțin următoarele:

- schema rețelei și a segmentării (zone și conduite);
- matricea fluxurilor de comunicație;
- inventarul activelor IT/OT;
- configurațiile și parametrii relevanți de securitate ai soluției implementate (security baseline);
- procedurile de administrare;
- matricea utilizatorilor și rolurilor (User & Role Matrix);
- procedura de acces la distanță;
- licențele și abonamentele (subscriptions) necesare, cu perioada de valabilitate.

CONTRACTORUL EPC va asigura configurarea, integrarea, testarea și punerea în funcțiune a soluțiilor de securitate cibernetică incluse în scopul proiectului.

Implementarea cerințelor de securitate cibernetică va fi verificată prin testele Cyber FAT / Cyber SAT descrise în capitolul 12 și la punerea în funcțiune. CONTRACTORUL EPC va fi disponibil pentru clarificări, întâlniri cu părțile relevante și teste de sistem pe toată durata proiectului.

Documentația finală va fi actualizată conform configurației as-built și predată BENEFICIARULUI la finalizarea lucrărilor. Documentația care conține informații sensibile (arhitectură, adresare IP, reguli de firewall, credențiale, vulnerabilități) va fi clasificată, transmisă pe canale securizate și distribuită restricționat, conform politicilor BENEFICIARULUI. Documentele și termenele de predare sunt prezentate în tabelul următor:

Titlu	Descriere	Termen de predare
Specificația de proiectare funcțională a securității OT	Acoperă toate considerentele de proiectare arhitecturală privind securitatea OT care nu ar trebui să se modifice după finalizare și până la predarea sistemului. Aceasta va include următoarele informații: - Descriere generală a arhitecturii, fără desene - Proiectarea măsurilor de hardening (protecție fizică și logică) - Proiectarea jurnalizării evenimentelor de securitate - Planul de adresare IP - Studiul de disponibilitate și proiectarea rețelei wireless, dacă este cazul - Proiectarea accesului la distanță - Proiectarea accesului logic - Proiectarea protecției împotriva programelor malware	Cu 1 lună înainte de Cyber FAT

	- Proiectarea managementului patch-urilor - Proiectarea soluției de backup - Proiectarea monitorizării OT (IDS) și a integrării cu SIEM/SOC - Matricea de corespondență cu standardele, completată cu modul de îndeplinire a cerințelor	
Desene de arhitectură	- Proiectare de detaliu / Vedere logică a serviciilor (LLD-LSV) - Proiectare de detaliu / Vedere logică a rețelei (LLD-LNV) - Proiectare de detaliu / Vedere fizică a rețelei (LLD-PNV) - Proiectare de detaliu / Vedere fizică de amplasament (LLD-PUV)	LLD-LSV: cu 1 lună înainte de Cyber FAT LLD-LNV, LLD-PNV și LLD-PUV: cu 2 luni înainte de Cyber SAT
Inventarul activelor	- Lista SISTEMELOR furnizate - Lista ACTIVELOR pentru fiecare SISTEM - Lista REȚELELOR pentru fiecare ACTIV - Lista serviciilor de rețea utilizate și justificarea aferentă, pentru fiecare activ - Lista software-ului instalat pentru fiecare activ - Lista serviciilor care rulează pe fiecare activ - Lista regulilor de firewall pentru fiecare activ - Lista comunicațiilor pentru fiecare activ - Lista excepțiilor antivirus pentru fiecare activ - Lista setărilor de securitate ale sistemului de operare - Permisiunile sistemului de fișiere, pe activ și folder - Lista mediilor de instalare, a dongle-urilor și a cheilor de licență	Cu 1 lună înainte de Cyber FAT
Politica antivirus și procedura de operare	- Strategia și politica de actualizare a soluției antivirus - Modul de actualizare a semnăturilor antivirus și a agenților de scanare - Modul de administrare a excepțiilor de scanare - Modul de operare a firewall-ului software local, dacă este cazul	Cu 3 luni înainte de predare
Politica de management al patch-urilor și procedura de operare	Va descrie politica de aplicare a patch-urilor de securitate și modul de operare a distribuirii acestora	Cu 2 luni înainte de Cyber SAT
Politica de backup și restaurare și procedura de operare	- Instrucțiuni pentru efectuarea unui backup complet al fiecărui sistem, utilizând cel puțin una dintre următoarele metode: medii detașabile / offline dedicate sau arhitectură distribuită, în care fiecare sistem de backup salvează un subset; - Tipurile de date incluse în backup: imaginea sistemului, sistemul de operare, programele aplicației, datele de arhivă și istorice, logica și configurațiile controlerelor (PLC, RTU, IED, PPC), configurațiile și setările componentelor de rețea și de securitate; - Instrucțiuni privind restaurarea sistemului sau a componentelor acestuia la starea normală de funcționare și verificarea integrității copiilor (capitolul 9).	Cu 2 luni înainte de Cyber SAT
Procedura de instalare	Va descrie modul de instalare de la zero a sistemului, utilizând mediile software sau orice altă metodologie necesară. Aceasta va fi necesară dacă backupul nu este disponibil, indiferent de motiv, sau nu este coerent.	Cu 1 lună înainte de predare
Pornire / Oprire	Pentru unele sisteme este foarte importantă respectarea unei anumite secvențe de pornire a diferitelor componente, pentru a obține un sistem coerent și complet operațional. Același principiu se aplică secvenței de oprire.	Cu 1 lună înainte ca sistemul să

		fie expediat la amplasament
Plan de recuperare în caz de dezastru	Va descrie strategia de menținere a valorilor RTO și RPO definite pentru fiecare componentă a SISTEMULUI	Cu 1 lună înainte ca sistemul să fie expediat la amplasament
Raportul Cyber HAZOP și Specificația cerințelor de securitate cibernetică (CRS)	Conform subcapitolului 3.6, inclusiv SL-T pentru fiecare zonă și conduită, registrul recomandărilor și registrul riscurilor reziduale	Conform tabelului din subcapitolul 3.2; versiunea as-built la predare
Proceduri și rapoarte Cyber FAT / Cyber SAT	Procedurile de test conform capitolului 12, rapoartele de test, rapoartele de scanare a vulnerabilităților / testare de penetrare și registrul neconformităților	Procedurile: cu 1 lună înainte de fiecare test; rapoartele: în 2 săptămâni după fiecare test
Planul de răspuns la incidente OT	Conform capitolului 10, inclusiv playbook-urile, matricea de contacte și raportul exercițiului tabletop	Cu 2 luni înainte de predare
Documentația de securitate a furnizorilor	Conform capitolului 11: certificări / declarații IEC 62443-4-1 / 4-2 și SL-C, ghiduri de hardening, SBOM, declarații privind conturile implicite, durata de suport de securitate și contactele PSIRT	Înainte de comanda fermă a echipamentelor; SBOM actualizat la predare