Îmbunătățirea securității cibernetice pentru sistemele inteligente din cadrul industriei 4.0

CONDUCĂTOR DE DOCTORAT,
C.S.I dr. ing. habil. Cristinel Ioan ILIE

DOCTORAND,
Ing. Adelin Marian BERINDEI

TÂRGOVIŞTE
2026

CUPRINS

1. INTRODUCERE

1.1. Context și motivație

Lucrarea abordează securitatea cibernetică în contextul digitalizării accelerate și al interconectării sistemelor mecatronice în cadrul Industriei 4.0. Evoluția de la mecanică la mecatronică și ulterior la sisteme cyber-fizice (CPS – Cyber-Physical Systems) reflectă integrarea profundă dintre mediul fizic și cel digital, generând arhitecturi capabile de comunicare autonomă și procesare distribuită.

Această transformare tehnologică amplifică dependența infrastructurilor industriale de rețele informatice și extinde suprafața de atac cibernetic. Concepte precum Internet of Things (IoT), Industrial Internet of Things (IIoT) și sistemele inteligente aduc beneficii majore în eficiență și optimizare operațională, dar introduc vulnerabilități cu impact potențial asupra continuității proceselor industriale și a siguranței operaționale.

În acest context, securitatea cibernetică devine o componentă strategică a proiectării și exploatării sistemelor mecatronice. Necesitatea unei evaluări sistematice a riscurilor asociate infrastructurilor industriale moderne a fundamentat alegerea temei, cu accent pe identificarea și analizarea vulnerabilităților specifice mediilor integrate IT/OT.
Cercetarea are un caracter aplicativ, fiind realizată pe o arhitectură industrială reală utilizată în producție, ceea ce conferă relevanță practică rezultatelor obținute. Demersul interdisciplinar integrează mecatronica, sistemele SCADA, tehnologiile pentru sisteme inteligente și securitatea cibernetică, evidențiind complexitatea protejării infrastructurilor critice în era digitală.

Un element de noutate îl constituie adaptarea metodelor avansate de testare ofensivă la constrângerile mediului industrial și identificarea unei vulnerabilități critice nedocumentate public, recunoscută oficial de producător prin emiterea certificatului nr. EEBDM-235865430-1059 din 21.08.2025 (Anexa 1), consolidând relevanța științifică și aplicativă a cercetării.

1.2. Scop și obiective

Transformarea digitală a mediului industrial și convergența IT–OT generează atât oportunități de optimizare, cât și riscuri cibernetice sporite. Interconectivitatea extinsă permite propagarea rapidă a unui incident, o singură vulnerabilitate putând afecta procese industriale critice.

Scopul tezei este investigarea aprofundată a securității cibernetice în infrastructuri industriale moderne, prin identificarea, testarea și validarea vulnerabilităților într-un cadru experimental care reproduce condiții reale de exploatare. Cercetarea demonstrează implementarea controlată a unui lanț complet de atac — de la vectorul inițial de acces până la interacțiunea cu echipamentele de control — pentru fundamentarea unor măsuri de securitate adaptate mediului analizat.

Obiectivele principale includ:

- dezvoltarea unei metodologii avansate de testare ofensivă pentru infrastructuri industriale;
- adaptarea tehnicilor de penetrare la constrângerile mediilor critice;
- documentarea riguroasă a vulnerabilităților identificate;
- formularea unui cadru de securitate personalizat, integrând bune practici internaționale și particularitățile infrastructurii analizate;
- propunerea de măsuri tehnice și organizatorice pentru creșterea rezilienței cibernetice.

Lucrarea are, de asemenea, o dimensiune strategică, oferind repere aplicabile operatorilor industriali și specialiștilor în securitate, contribuind la fundamentarea deciziilor privind protecția infrastructurilor din ecosistemul Industriei 4.0.

1.3. Structura lucrării

Lucrarea este organizată în opt capitole, urmărind o progresie de la fundamentarea teoretică la validarea experimentală și formularea soluțiilor aplicabile.

Structura adoptată asigură coerența demersului științific și integrarea dimensiunii inginerești cu cerințele moderne de securitate cibernetică.

1.4 Concluzii de capitol

Capitolul introductiv a fundamentat necesitatea abordării securității cibernetice în contextul transformării digitale generate de Industria 4.0, evidențiind impactul acesteia asupra infrastructurilor mecatronice și cyber-fizice.

Au fost prezentate motivația cercetării, scopul și obiectivele urmărite, precum și structura lucrării, conturând cadrul conceptual și aplicativ al demersului științific. Protejarea infrastructurilor industriale moderne este evidențiată ca o condiție esențială pentru funcționarea sigură și fiabilă a sistemelor inteligente integrate în mediul operațional.

2. STADIUL ACTUAL AL SISTEMELOR INTELIGENTE DIN DOMENIUL MECATRONICII

„Un sistem inteligent este capabil să demonstreze în mod autonom și adaptiv cât mai multe capacități cognitive de nivel înalt precum percepția, acțiunea, învățarea, planificarea, memoria, decizia, recunoașterea limbajului, emoția etc.“ [1]

Sistemele inteligente rezultă din integrarea mecatronicii cu electronica și tehnologiile informatice, dezvoltând capacități decizionale prin antrenarea pe seturi relevante de date. Acestea percep mediul, procesează informații și acționează autonom în vederea optimizării proceselor industriale.

Integrarea tehnologiilor IoT, a analizei datelor și a tehnicilor de inteligență artificială permite transformarea infrastructurilor clasice în „fabrici inteligente”, caracterizate prin flexibilitate, eficiență și adaptabilitate ridicată .

Internet of Things (IoT) reprezintă un domeniu tehnologic cu impact major tehnic, economic și social, bazat pe interconectarea globală a dispozitivelor inteligente prin infrastructuri digitale. Rețelele moderne de comunicații permit schimbul continuu de date între senzori, echipamente industriale și sisteme informatice, configurând un ecosistem digital interdependent [3].

2.1 Mecatronica

„Mecatronica este combinația sinergică și sistematică a mecanicii, electronicii și a informaticii în timp real.” [4]

Mecatronica reprezintă o disciplină interdisciplinară care integrează mecanica, electronica și tehnologia informației încă din fazele incipiente ale proiectării, urmărind obținerea unei sinergii funcționale optime. De la apariția termenului în 1969, pentru a descrie sisteme controlate de CPU ce combină mecanica și electronica, domeniul a evoluat într-o veritabilă filozofie inginerească .

Inițial centrată pe tehnologiile servo și pe automatizări industriale, dezvoltarea microprocesoarelor a accelerat integrarea controlului digital în sisteme mecanice. Ulterior, progresul electronicii digitale și miniaturizarea au permis apariția senzorilor și actuatorilor inteligenți, a sistemelor cu procesare distribuită hardware–software și a aplicațiilor complexe din industria auto, semiconductorilor și automatizărilor industriale.

În prezent, mecatronica include tehnologii avansate de comunicație, sisteme mobile și interconectate, precum și integrarea nano-tehnologiilor, contribuind la dezvoltarea echipamentelor inteligente, sigure și eficiente. Domeniul a devenit unul dintre pilonii proiectării moderne, având un rol esențial în dezvoltarea sistemelor capabile să coopereze inteligent cu utilizatorul și mediul operațional.

2.2 Cyber-mecatronica

Cyber-mecatronica reprezintă evoluția mecatronicii clasice către sisteme inteligente interconectate, integrate în arhitecturi digitale distribuite. Aceasta combină mecanica, electronica, tehnologia informației și principiile ciberneticii într-un cadru unitar, orientat către autonomie operațională, interoperabilitate și procesare în timp real.

Dezvoltarea cyber-mecatronicii a fost accelerată de progresul tehnologiilor informației și comunicațiilor după anul 2000, prin integrarea rețelelor industriale, a Internet of Things (IoT) și a tehnologiilor precum inteligența artificială, machine learning și analiza volumelor mari de date. Astfel, sistemele mecatronice tradiționale au evoluat către sisteme cyber-fizice capabile de auto-adaptare și comunicare permanentă în ecosisteme industriale extinse [9-10].

Prin integrarea controlului distribuit, a comunicațiilor industriale și a platformelor digitale de monitorizare, cyber-mecatronica permite gestionarea și optimizarea proceselor la distanță, sporind eficiența și scalabilitatea infrastructurilor industriale. În același timp, interconectivitatea extinsă introduce noi vectori de risc, transformând securitatea cibernetică într-o componentă esențială a proiectării și exploatării sistemelor inteligente .

2.3 Evoluția tehnnologică (mecanică → mecatronică → sisteme cyber fizice)

Evoluția tehnologică industrială a progresat de la mecanică la mecatronică și ulterior la sisteme cyber-fizice (Cyber-Physical Systems – CPS), marcând integrarea progresivă a mediului fizic cu cel digital [13].

Mecanica a constituit fundamentul dezvoltării mașinilor și sistemelor fizice, fiind centrată pe principii inginerești clasice. Apariția mecatronicii a permis integrarea mecanicii cu electronica și informatica, facilitând automatizarea și dezvoltarea echipamentelor inteligente.

Etapa actuală este caracterizată de sistemele cyber-fizice, care unifică componente fizice și software într-o arhitectură interconectată prin rețele de comunicații. CPS permit monitorizare, control și procesare în timp real, fiind capabile să interacționeze adaptiv cu

mediul prin senzori și mecanisme de control distribuit [14]. Prin integrarea inteligenței artificiale și a analizei avansate a datelor, aceste sisteme pot învăța și lua decizii autonome [13–14].

Două concepte fundamentale susțin această evoluție: SCADA și Industria 4.0.
SCADA (Supervisory Control and Data Acquisition) reprezintă infrastructura de monitorizare și control a proceselor industriale în timp real, bazată pe integrarea PLC-urilor, RTU-urilor, serverelor și interfețelor HMI. Arhitectura SCADA presupune convergența zonelor IT (gestionarea datelor, servere, aplicații, rețele) și OT (echipamente de teren, senzori, actuatori, controlere), formând baza operațională a infrastructurilor industriale moderne.

Industria 4.0 reprezintă etapa de digitalizare avansată a producției, caracterizată prin integrarea CPS, IoT, comunicațiilor industriale și analizei datelor, în vederea realizării fabricilor inteligente complet interconectate [54]. Această paradigmă amplifică eficiența și flexibilitatea proceselor, dar extinde simultan suprafața de atac cibernetic.

2.4 IoT – Internet of Things

Internet of Things (IoT) constituie un pilon esențial al Industriei 4.0, facilitând interconectarea echipamentelor industriale și colectarea continuă de date pentru optimizarea proceselor. Prin monitorizare în timp real și analiză predictivă, IoT susține mentenanța preventivă și crește eficiența operațională [21].

Dezvoltarea fragmentată a ecosistemului IoT a generat însă probleme de interoperabilitate și standardizare, complicând integrarea și securizarea dispozitivelor. Dispozitivele IoT gestionează frecvent date sensibile, iar lipsa unor mecanisme uniforme de protecție poate conduce la compromiterea confidențialității și a siguranței operaționale [21].

Provocarea securității IoT

Extinderea conectivității amplifică vulnerabilitățile sistemice. Dispozitivele IoT pot deveni puncte de intrare pentru atacuri cibernetice, mai ales în absența actualizărilor regulate și a mecanismelor robuste de autentificare și segmentare a rețelei.

În mediile industriale, compromiterea unui senzor sau a unui echipament conectat poate genera erori decizionale automate, opriri neplanificate sau afectarea mecanismelor de siguranță. Securitatea IoT trebuie astfel tratată ca element critic al continuității operaționale, nu doar ca problemă tehnică.

Dispozitivele IoT prezintă particularități distincte: distribuție largă, cicluri de viață extinse, capacitate limitată de actualizare și uniformitate hardware, ceea ce face ca exploatarea unei vulnerabilități să poată afecta simultan un număr mare de echipamente. Prin urmare, protecția trebuie fundamentată pe evaluarea riscurilor, segmentarea rețelei, controlul accesului și actualizarea continuă a componentelor [21].

Cercetarea experimentală prezentată în lucrare confirmă aceste riscuri prin identificarea și exploatarea controlată a vulnerabilităților în echipamente IoT integrate în infrastructuri industriale reale, evidențiind necesitatea unor măsuri de securitate adaptate mediului operațional.

2.5 Concluzii de capitol

Capitolul a prezentat tranziția de la mecanică la mecatronică și ulterior la sisteme cyber-fizice, evidențiind integrarea progresivă a tehnologiilor digitale în infrastructurile industriale moderne.

Au fost analizate rolul SCADA și al Industriei 4.0 în digitalizarea proceselor, precum și impactul IoT asupra interconectivității și automatizării. În același timp, s-a subliniat faptul că extinderea conectivității implică vulnerabilități suplimentare, iar securitatea cibernetică devine o condiție esențială pentru reziliența și continuitatea operațională a sistemelor inteligente industriale.

3. Industria 4.0

Tehnologia produce transformări profunde în mediul industrial, prin integrarea automatizării, conectivității și procesării avansate a datelor. Conceptul de Industrie 4.0, apărut inițial în Germania ca inițiativă strategică susținută la nivel guvernamental, desemnează a patra revoluție industrială și este asociat cu noțiuni precum „industrie inteligentă” sau „industrie interconectată” [23].

Industria 4.0 reprezintă tranziția de la sisteme industriale tradiționale la un model bazat pe digitalizare, interconectare și automatizare avansată. Aceasta acoperă întreg ciclul de viață al produsului – de la proiectare și producție până la monitorizare și reciclare – prin integrarea sistemelor cyber-fizice (CPS), a comunicațiilor industriale și a analizei datelor [23].

Evoluția industrială poate fi sintetizată astfel:

- Industria 1.0 – mecanizare prin utilizarea energiei aburului și apei;
- Industria 2.0 – producție de masă și electrificare;
- Industria 3.0 – automatizare și introducerea computerelor;
- Industria 4.0 – integrare digitală completă și interconectare inteligentă.

Industria 4.0 nu este rezultatul unei singure inovații, ci al convergenței mai multor tehnologii avansate, printre care:

- Internet of Things (IoT);
- Big Data și analiza avansată a datelor;
- integrarea cyber-mecatronică;
- robotică avansată și sisteme autonome;
- securitate cibernetică [23].

Această paradigmă influențează nu doar procesele de fabricație, ci și lanțurile de aprovizionare, piața muncii și modelele organizaționale. Lanțurile logistice devin transparente și adaptabile prin monitorizare în timp real, iar producția permite personalizare de masă prin tehnologii flexibile. În același timp, crește necesarul de competențe în domenii precum analiza datelor, inginerie software și securitate cibernetică.

Un element definitoriu îl reprezintă integrarea orizontală și verticală a proceselor, care asigură conectivitatea de-a lungul lanțului valoric și între nivelurile operaționale și manageriale. Prin colectarea și analizarea continuă a datelor, procesele devin optimizabile în timp real, iar resursele pot fi utilizate mai eficient.

Principiile fundamentale ale Industriei 4.0 includ:

- interoperabilitatea între sisteme cyber-fizice, echipamente și platforme informatice;
- descentralizarea decizională prin echipamente autonome;
- analiza datelor în timp real;
- virtualizarea și simularea proceselor industriale;
- orientarea către servicii;
- modularitatea și scalabilitatea infrastructurilor.

Aplicarea acestor principii conduce la creșterea productivității, optimizarea resurselor, reducerea defectelor prin testare virtuală și scurtarea timpului de lansare pe piață. Totodată, implementarea implică investiții semnificative, instruirea personalului și adoptarea unor măsuri stricte de securitate cibernetică.

Extinderea conectivității și integrarea infrastructurilor industriale cu rețele externe amplifică riscul de atacuri cibernetice. În acest context, protejarea datelor, a sistemelor de control și a proprietății intelectuale devine o prioritate strategică, iar securitatea cibernetică reprezintă un element esențial al ecosistemului Industriei 4.0.

Industria 4.0 marchează astfel tranziția de la mecatronică la cyber-mecatronică, transformând echipamentele tradiționale în dispozitive inteligente integrate în ecosisteme digitale colaborative. Această transformare creează oportunități majore de inovare și creștere, dar impune abordări tehnologice și organizaționale adaptate complexității noilor infrastructuri industriale.

3.1. IIoT – Industrial Internet of Things

Industrial Internet of Things (IIoT) reprezintă extinderea conceptelor IoT în mediul industrial, prin interconectarea echipamentelor, senzorilor și sistemelor de control în vederea colectării și analizării datelor pentru creșterea eficienței, productivității și siguranței proceselor. IIoT integrează senzori inteligenți, platforme software avansate, soluții de automatizare și infrastructuri de comunicații, generând rețele industriale distribuite și interdependente.

Spre deosebire de IoT-ul orientat către aplicații comerciale sau casnice, IIoT trebuie adaptat cerințelor specifice mediului industrial. În acest context, concepte precum IACS (Industrial Automation and Control Systems), SCADA și CPS converg către implementarea principiilor Industriei 4.0, prin integrarea zonelor IT și OT într-un cadru operațional unitar.

Adoptarea IIoT aduce beneficii semnificative, precum mentenanța predictivă, optimizarea consumului de energie și creșterea flexibilității liniilor de producție. Prin analiza datelor în timp real, pot fi identificate abateri operaționale și prevenite opririle neplanificate. Cu toate acestea, implementarea implică provocări legate de interoperabilitate, integrarea sistemelor legacy și gestionarea volumelor mari de date .

IIoT depășește funcționalitățile tradiționale ale IACS și SCADA prin integrarea infrastructurilor cloud și edge computing, transformând echipamentele industriale în noduri inteligente ale unor sisteme cyber-fizice. Aplicațiile sunt extinse în domenii precum industria auto, sectorul energetic și transporturile inteligente, unde analiza datelor în timp real permite optimizarea proceselor și reducerea costurilor operaționale [75–76].

Extinderea conectivității industriale amplifică însă suprafața de atac cibernetic. Breșele de securitate pot afecta continuitatea producției și infrastructurile critice. În acest context, securizarea IIoT presupune segmentarea rețelelor, autentificare robustă, criptarea comunicațiilor, monitorizare continuă și adoptarea standardelor internaționale precum ISA/IEC 62443.

Astfel, IIoT devine un pilon strategic al Industriei 4.0, conectând și optimizând ecosistemele industriale prin integrarea dispozitivelor inteligente și a infrastructurilor digitale distribuite.

3.2 Concluzii de capitol

Capitolul a evidențiat transformarea profundă a mediului industrial generată de conceptul de Industrie 4.0, reliefând modul în care integrarea tehnologiilor digitale, a comunicațiilor avansate și a infrastructurilor conectate influențează procesele de producție și modelul operațional al întreprinderilor moderne.

S-a subliniat importanța Industrial Internet of Things (IIoT), a rețelelor inteligente de senzori și a platformelor de interconectare în dezvoltarea și funcționarea sistemelor mecatronice și cyber-fizice, evidențiindu-se faptul că aceste progrese nu substituie principiile ingineriei mecanice, ci le completează prin funcționalități avansate care contribuie la creșterea eficienței, flexibilității și rezilienței infrastructurilor industriale.

4. SECURITATE CIBERNETICĂ

Securitatea cibernetică reprezintă ansamblul de măsuri tehnice, organizaționale și manageriale destinate protejării sistemelor informatice, rețelelor și datelor împotriva accesului neautorizat și a amenințărilor digitale. Conform NIST, aceasta vizează prevenirea, protecția și restaurarea sistemelor informaționale, asigurând confidențialitatea, integritatea și disponibilitatea (triada CIA). Standardul ITU-T X.1205 definește securitatea cibernetică drept un set integrat de politici, practici și tehnologii utilizate pentru protejarea mediului cibernetic și a activelor organizaționale.

Triada CIA constituie fundamentul oricărui sistem de securitate: confidențialitatea limitează accesul la entități autorizate, integritatea garantează corectitudinea datelor, iar disponibilitatea asigură accesul continuu la resurse. Implementarea acestor principii se realizează prin controale tehnice, operaționale și manageriale, cu rol preventiv, detectiv și corectiv.

La nivel strategic, gestionarea riscurilor este susținută de cadre metodologice precum NIST Cybersecurity Framework, structurat pe funcțiile identificare, protecție, detecție, răspuns și recuperare. Acest model oferă o abordare sistematică aplicabilă inclusiv infrastructurilor industriale complexe, unde convergența IT–OT amplifică expunerea la riscuri.

În contextul Industriei 4.0, securitatea cibernetică devine un element esențial al guvernanței organizaționale și al rezilienței infrastructurilor cyber-mecatronice, fundamentând măsurile proactive prezentate în capitolele experimentale ale lucrării.

4.1 Cadrul de securitate al infrastructurii IT

Cadrul de securitate al infrastructurii IT se bazează pe identificarea amenințărilor, vulnerabilităților și a măsurilor de protecție necesare pentru menținerea confidențialității, integrității și disponibilității (triada CIA) [31]. Literatura de specialitate distinge două perspective complementare: defensivă și ofensivă. Abordarea defensivă vizează prevenirea și detectarea incidentelor prin controale tehnice și procedurale (firewall, IDS/IPS, monitorizare, planuri de răspuns), în timp ce abordarea ofensivă urmărește identificarea proactivă a vulnerabilităților prin tehnici de recunoaștere și evaluare a suprafeței de atac [31].

Ingineria socială rămâne un vector relevant, exploatând factorul uman prin tehnici precum phishing sau pretexting [37–39]. De asemenea, aplicațiile web sunt frecvent vizate,

riscurile majore fiind sintetizate în OWASP Top 10 (2021), incluzând deficiențe de control al accesului, erori criptografice și configurări incorecte [40]. În cadrul cercetării, o parte dintre aceste metode au fost replicate controlat pentru a demonstra progresia de la acces inițial la extinderea controlului în infrastructură.

Reverse proxy-ul funcționează ca intermediar între client și serverele interne, oferind mascarea infrastructurii și control al traficului. În context ofensiv, poate facilita intermedierea comunicațiilor C2; contramăsurile includ monitorizarea traficului de ieșire, segmentarea și validarea certificatelor .

CVE (Common Vulnerabilities and Exposures) furnizează identificatori standardizați ai vulnerabilităților, fiind utilizat pentru managementul patch-urilor sau pentru selectarea exploit-urilor adecvate. Reducerea riscului presupune actualizări rapide și monitorizarea continuă a bazelor de date specializate [79].

Pivoting-ul desemnează utilizarea unui sistem compromis pentru accesarea altor resurse interne, fiind specific scenariilor de lateral movement. Limitarea acestuia implică segmentare strictă, aplicarea principiului „least privilege” și autentificare multi-factor.

4.2 Paradigma securității cibernetice pentru sisteme cyber-mecatronice

Industria 4.0 amplifică riscurile prin creșterea conectivității, integrarea dispozitivelor inteligente și necesitatea comunicației continue între componentele ecosistemului. Un cadru relevant propune gruparea securității în trei domenii: securitatea IoT, securitatea mediului de transport și securitatea în cloud. În infrastructurile industriale, sistemele SCADA rămân critice pentru colectarea datelor și control, iar atacurile pot viza hardware-ul, software-ul sau comunicațiile, având ca efect alterarea datelor de control și/sau indisponibilitatea proceselor.

În practică, IoT/IIoT introduce dificultăți suplimentare: vizibilitate redusă, diversitate de platforme, cicluri de viață lungi și integrare incompletă în controalele IT, ceea ce transformă aceste dispozitive în suprafețe de atac majore. În plus, convergența IT–OT expune mecanisme industriale critice la amenințări similare celor din IT, însă cu impact operațional mult mai sever. Protocoalele industriale utilizate frecvent (de ex. Modbus, DNP3) pot avea limitări de autentificare/criptare, sporind riscul exploatării (inclusiv scenarii zero-day). Aceste aspecte au fost validate în cercetarea experimentală prin demonstrarea compromiterii unei infrastructuri industriale pornind de la vulnerabilități critice, cu impact asupra întregului lanț operațional.

4.3 Viziunea/perspectiva securității cibernetice pentru sistemele cyber-mecatronice

În mediile specifice Industriei 4.0, diferențierea dintre IT și OT devine esențială: deși obiectivul general este funcționarea sigură și eficientă, prioritățile diferă. În IT, triada CIA este centrată pe confidențialitate, integritate și disponibilitate; în OT, prioritatea este disponibilitatea și siguranța operațională, iar aplicarea directă a măsurilor IT în OT poate genera riscuri operaționale. Convergența IT–OT și apariția IIoT impun politici și controale adaptate specificului industrial, în care ferestrele de mentenanță, actualizările rare și cerințele de continuitate impun o guvernanță diferită față de mediile IT clasice [57].

Pentru reducerea riscurilor sunt recomandate segmentarea și segregarea activelor în zone, controlul strict al comunicațiilor între zone și utilizarea unei DMZ între zona de întreprindere și zona de control, conform bunelor practici și standardelor (ex. IEC 62443, ISO 27001/27002, NIST SP 800-82, NIST CSF). Zonele de control includ tipic niveluri supervizor (HMI/SCADA), control de bază (PLC), zone de siguranță (SIS) și zone de proces (senzori/actuatori), iar controlul fluxurilor între acestea este determinant pentru limitarea propagării atacurilor [43,45]. În acest context, rolul SCADA și al componentelor de tip Historian în logare și corelare devine relevant inclusiv pentru investigații post-incident [57]. Standardizarea comunicațiilor și adoptarea criptării end-to-end, acolo unde este fezabil, contribuie la creșterea rezilienței, în special pentru dispozitivele IIoT.

4.4 Concluzii de capitol

Capitolul a evidențiat că securitatea cibernetică în Industria 4.0 trebuie tratată ca parte integrantă a funcționării infrastructurilor industriale, nu doar ca problemă IT. Diferențele de priorități și constrângeri între IT și OT impun politici, arhitecturi și controale adaptate mediilor industriale, cu accent pe segmentare, monitorizare și guvernanță specifică proceselor critice. Conceptele operaționale precum reverse proxy, consultarea CVE și pivoting sunt relevante atât pentru analiza defensivă, cât și pentru simularea realistă a scenariilor de atac, constituind punți directe către etapa experimentală a lucrării.

5. METODOLOGIA DE CERCETARE EXPERIMENTALĂ - ARHITECTURA INDUSTRIALĂ ANALIZATĂ

5.1 Metodologia de cercetare

Prezenta cercetare are ca obiectiv îmbunătățirea securității cibernetice a sistemelor inteligente din cadrul Industriei 4.0, prin analizarea vulnerabilităților rezultate din integrarea componentelor fizice (hardware) cu cele digitale (software) și prin validarea unor măsuri concrete de protecție aplicabile infrastructurilor industriale reale.

Demersul experimental s-a desfășurat în două etape distincte, utilizând o infrastructură industrială din sectorul energetic, implementată efectiv în mediul de producție, dar adaptată la scară de laborator pentru a permite testarea controlată a vulnerabilităților. Sistemul utilizează surse regenerabile de energie pentru consum propriu și pentru injectarea energiei electrice în rețeaua națională, fiind compus din echipamente de conversie, dispozitive de protecție și control, precum și un punct central de comandă și monitorizare.

În prima etapă a fost realizată documentarea și analiza arhitecturii sistemului, investigând topologia de interconectare, componentele hardware și aplicațiile software utilizate. Configurația logică și echipamentele de comunicație au fost identice cu cele din mediul operațional real, diferența constând în simularea echipamentelor de teren (turbine eoliene, panouri fotovoltaice) prin senzori specializați. Această corespondență 1:1 a permis identificarea și analizarea vulnerabilităților într-un cadru realist, fără a afecta infrastructura critică din exploatare.

Arhitectura generală a sistemului utilizat în cercetare este ilustrată în Fig. 5.1.1, care evidențiază interconectarea componentelor IT și OT și mecanismele de segmentare implementate.

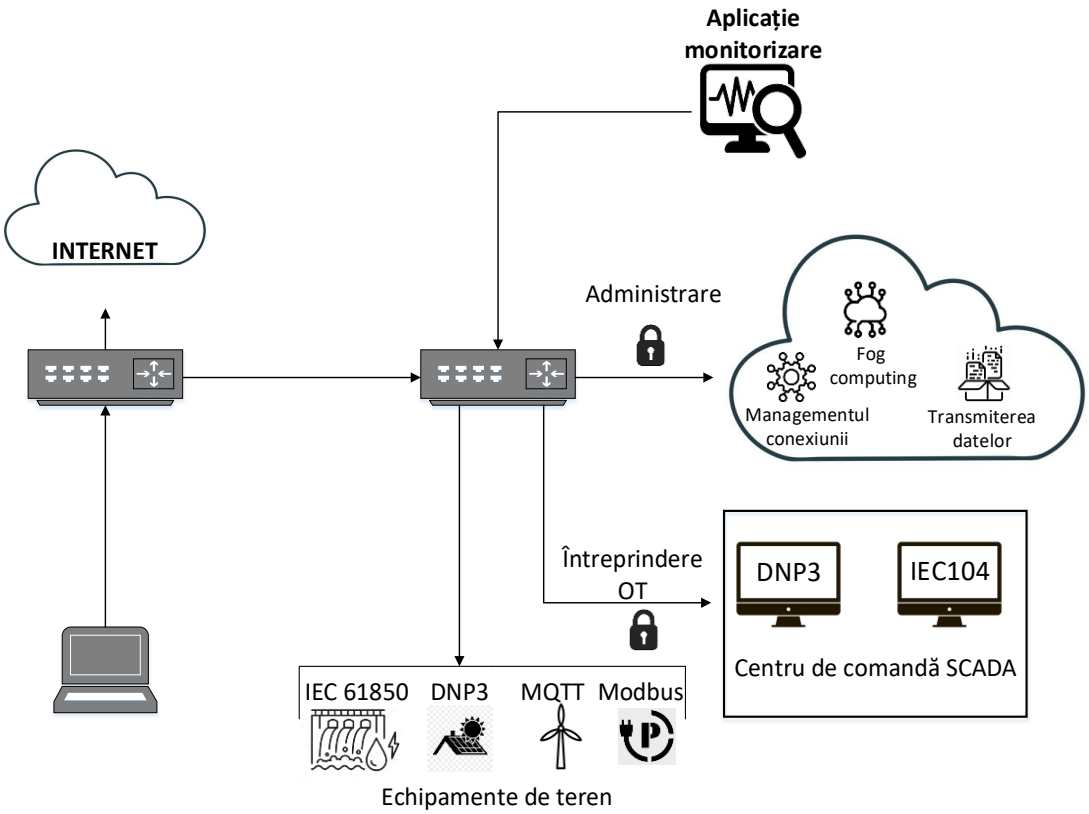

Fig. 5.1.1 Arhitectura generală a sistemului inteligent

A doua etapă a cercetării a vizat identificarea, exploatarea controlată și evaluarea vulnerabilităților, urmată de elaborarea unui plan de măsuri proactive pentru consolidarea securității cibernetice. Vulnerabilitățile descoperite au fost analizate și prioritizate în funcție de impactul asupra disponibilității și integrității sistemului, iar eficiența măsurilor propuse a fost validată prin retestare.

În mediul analizat, infrastructura OT este complet izolată de internet, adoptând un model clasic de protecție bazat pe separare fizică și control strict al accesului.

Această configurație permite analizarea rezilienței unei infrastructuri industriale reale care, deși izolată conform principiilor tradiționale de securitate, rămâne expusă riscurilor generate de interacțiunea controlată dintre zonele IT și OT.

5.2 Detaliere componentelor arhitecturale

Arhitectura analizată integrează componente IT și OT interconectate prin mecanisme controlate de filtrare și segmentare.

Zona IT include infrastructura de comunicație pentru acces la internet și stația administratorului, care poate accesa exclusiv platforma de monitorizare printr-un echipament

configurat cu liste de control al accesului (ACL), permițând doar traficul autorizat și reducând suprafața de expunere.

Zona operațională (OT) constituie nucleul infrastructurii și include:

- PLC Siemens SIPROTEC 7SJ82, utilizat pentru protecția și controlul rețelei electrice, compatibil cu protocoale industriale standard și dotat cu mecanisme moderne de securitate;
- RTU ES2000, implementat pe platforma Cisco IOx, responsabil pentru colectarea și procesarea datelor operaționale și integrarea comunicațiilor SCADA;
- HMI, care permite monitorizarea și controlul sistemului în regim manual și automat;
- platforma Nagios XI, utilizată pentru supravegherea disponibilității echipamentelor.
- RTU-ul reprezintă elementul central al ecosistemului, asigurând interfațarea dintre dispozitivele de teren, PLC și sistemele de monitorizare, precum și vizualizarea parametrilor operaționali în timp real.

Deși implementată la scară de laborator, infrastructura reproduce arhitectura și mecanismele de segmentare din mediul real, ceea ce susține validitatea rezultatelor și posibilitatea extrapolării concluziilor către infrastructuri industriale critice.
Originalitatea cercetării constă în testarea securității cibernetice într-un sistem industrial real, complet funcțional, dar controlat experimental, oferind un cadru relevant pentru evaluarea rezilienței și formularea de măsuri aplicabile operațional.

5.3 Concluzii de capitol

Capitolul a prezentat metodologia experimentală și arhitectura industrială utilizată în cercetare, evidențiind caracterul aplicativ al demersului și corespondența directă cu mediul real de producție din sectorul energetic.

Analiza a demonstrat importanța unei abordări integrate asupra securității cibernetice, care să ia în considerare interdependența dintre componentele fizice și cele digitale. Configurația 1:1 între mediul de test și cel operațional constituie fundamentul etapelor experimentale următoare și susține dezvoltarea unor soluții concrete pentru creșterea rezilienței sistemelor mecatronice și cyber-fizice utilizate în infrastructuri critice.

6. IDENTIFICAREA ȘI EXPLOATAREA VULNERABILITĂȚILOR PENTRU INFRASTRUCTURA INDUSTRIALĂ – CERCETARE EXPERIMENTALĂ

6.1. Contextul actual al cercetării

Spre deosebire de infrastructurile IT clasice, caracterizate prin interconectare permanentă la internet, sistemele industriale de tip OT (Operational Technology) au fost proiectate tradițional pentru funcționare izolată, cu accent pe continuitatea operațională și securitatea fizică. Această paradigmă a condus la o cultură de securitate diferită, în care riscurile cibernetice au fost adesea considerate secundare.

Tranziția către Industria 4.0 modifică însă acest echilibru. Integrarea sistemelor fizice cu platforme digitale, utilizarea comunicațiilor la distanță și interconectarea cu infrastructuri IT extind semnificativ suprafața de atac. În mediul OT, impactul unui incident nu se limitează la pierderi informaționale, ci poate afecta direct procese fizice critice, cu consecințe asupra producției, echipamentelor și siguranței personalului.

În acest context, cercetarea a urmărit analizarea vulnerabilităților unei infrastructuri SCADA reale, printr-o metodologie experimentală controlată. Un element central al demersului îl constituie abordarea vectorului non-tehnic reprezentat de ingineria socială, integrat într-un scenariu realist de compromitere. Deși literatura menționează frecvent utilizarea phishing-ului în atacuri asupra infrastructurilor ICS/SCADA [60–61], documentarea detaliată a unor scenarii experimentale aplicate direct în astfel de medii este limitată.

Un exemplu notoriu îl reprezintă atacul asupra rețelei electrice din Ucraina (2015), unde vectorul inițial a fost un e-mail de tip spear-phishing care a condus ulterior la compromiterea sistemelor SCADA [62–63]. Spre deosebire de acel caz, în cadrul prezentei lucrări infrastructura analizată a fost izolată fizic de internet, iar scenariul experimental a utilizat un mecanism controlat, conceput special pentru demonstrarea vulnerabilității, fără utilizarea unui malware complex preexistent.

Rezultatele au evidențiat faptul că, chiar și în condițiile unei segmentări stricte și ale izolării fizice, factorul uman rămâne un element critic al lanțului de securitate. Astfel, cercetarea a trecut din zona teoretică în cea aplicată prin definirea și implementarea unei metodologii dedicate identificării vulnerabilităților într-un ecosistem industrial real.

6.2. Planul și etapele cercetării experimentale

Planul de testare a fost conceput pentru a simula, într-un cadru controlat, pașii tipici ai unui posibil atacator, fără a afecta infrastructura operațională reală. Metodologia a combinat tehnici consacrate de securitate ofensivă cu adaptări specifice mediului industrial analizat, pentru evaluarea completă a suprafeței de atac.

Analiza preliminară a indicat absența serviciilor expuse direct către internet și existența unei segmentări stricte. În aceste condiții, vectorul inițial de acces a fost identificat la nivelul factorului uman, prin scenarii de inginerie socială, fundamentând dezvoltarea unei metodologii experimentale orientate pe evaluarea rezilienței sistemului SCADA.

Etapele cercetării au acoperit întreg lanțul unui posibil atac:

1. Simularea unei infrastructuri de tip Command and Control (CnC) într-un mediu virtual dedicat testării.
2. Livrarea controlată a unui vector de acces inițial prin e-mail, pentru evaluarea vulnerabilităților asociate factorului uman.
3. Stabilirea unei conexiuni de tip reverse shell, adaptată constrângerilor arhitecturale (comunicație permisă doar LAN → WAN).
4. Analiza privilegiilor și a posibilităților de escaladare și propagare laterală.
5. Evaluarea securității aplicației de monitorizare, inclusiv prin corelarea cu vulnerabilități publice (CVE).
6. Utilizarea componentelor compromise ca punct de pivotare către zona operațională.
7. Compromiterea controlată a RTU-ului ES2000, demonstrând escaladarea din zona IT către mediul OT.

Utilizarea tehnicii reverse shell a permis respectarea politicilor de segmentare existente, conexiunea fiind inițiată din interiorul infrastructurii. Această abordare a evidențiat modul în care mecanismele clasice de protecție pot fi ocolite prin exploatarea comportamentului legitim al sistemelor.

Prin succesiunea acestor etape, cercetarea a demonstrat un lanț complet de compromitere specific mediilor industriale, în care un punct periferic poate deveni pivot către active operaționale critice, delimitând clar suprafața reală de atac și mecanismele potențiale de progresie.

6.3. Configurarea unei mașini virtuale Kali Linux cu rol de server CnC

Pentru implementarea scenariului experimental a fost configurată o infrastructură de tip Command and Control (CnC), utilizată exclusiv în mediu controlat pentru evaluarea rezilienței infrastructurii industriale analizate. Aceasta a avut rolul de a primi conexiuni inițiate din interiorul rețelei, în conformitate cu politica existentă care interzicea conexiunile dinspre mediul public către LAN.

Rolul serverului CnC a fost atribuit unei mașini virtuale ce rulează Kali Linux, distribuție specializată pentru testare de penetrare. Sistemul a fost implementat într-un mediu de virtualizare compatibil laboratorului, cu adresare IP statică pentru asigurarea stabilității și repetabilității experimentale (Fig. 6.3.2).

Serverul a fost configurat în mod pasiv (listener), fără inițierea de conexiuni către infrastructura țintă, în acord cu arhitectura segmentată a sistemului, unde comunicarea este permisă exclusiv LAN → WAN.

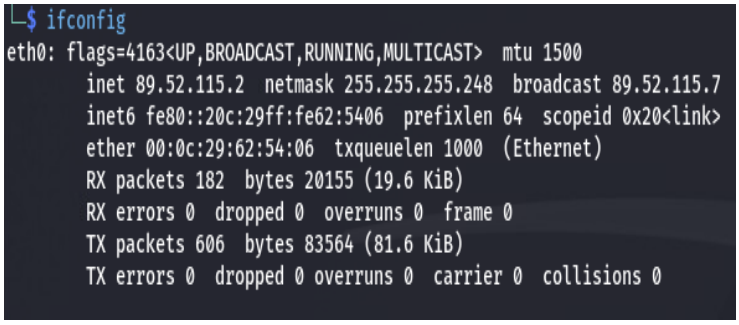

Fig. 6.3.2 Configurația server-ului de CnC

Pentru simularea unui scenariu realist, serverul a fost setat să accepte conexiuni TCP pe un port asociat traficului securizat, frecvent permis de firewall-urile industriale. Inițializarea modului de ascultare a fost realizată printr-un utilitar dedicat (Fig. 6.3.3), permițând monitorizarea conexiunilor și a fluxului bidirecțional de date.

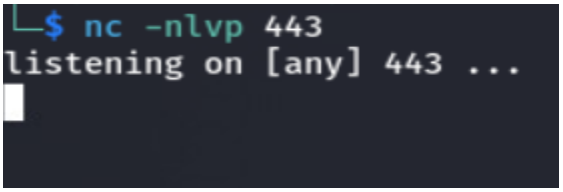

Fig. 6.3.3 Deschidere port 443 pe server-ul de CnC

Această etapă a furnizat infrastructura necesară validării compromiterii inițiale și a demonstrat că, în condițiile unei segmentări unidirecționale, inițierea controlată din interior reprezintă un vector fezabil de comunicare.

6.4 Atac de tip phishing și conexiune reverse shell

În urma analizei infrastructurii industriale nu au fost identificate servicii expuse direct către Internet, iar politica de securitate implementată interzicea inițierea conexiunilor dinspre mediul public către rețeaua internă. În aceste condiții, vectorul realist de acces inițial a fost identificat ca fiind factorul uman.

Pentru validarea acestei ipoteze a fost conceput un atac de tip spear-phishing direcționat către administratorul infrastructurii SCADA. Mesajul transmis a avut un context profesional credibil, iar documentul atașat, în format Microsoft Word, a inclus un mecanism automatizat capabil să inițieze o conexiune de tip reverse shell la deschidere.

Reverse shell-ul reprezintă o tehnică prin care sistemul compromis inițiază o conexiune către un server extern, permițând acces la distanță printr-un canal bidirecțional. Alegerea acestei metode a fost determinată de arhitectura segmentată a infrastructurii, unde comunicarea era permisă exclusiv din LAN către WAN.

La deschiderea documentului și activarea conținutului, mecanismul integrat a declanșat executarea unui proces care a inițiat conexiunea către serverul Command and Control configurat anterior. În momentul stabilirii conexiunii, pe serverul CnC a fost înregistrată sesiunea activă, confirmând compromiterea stației administratorului (Fig. 6.4.6).

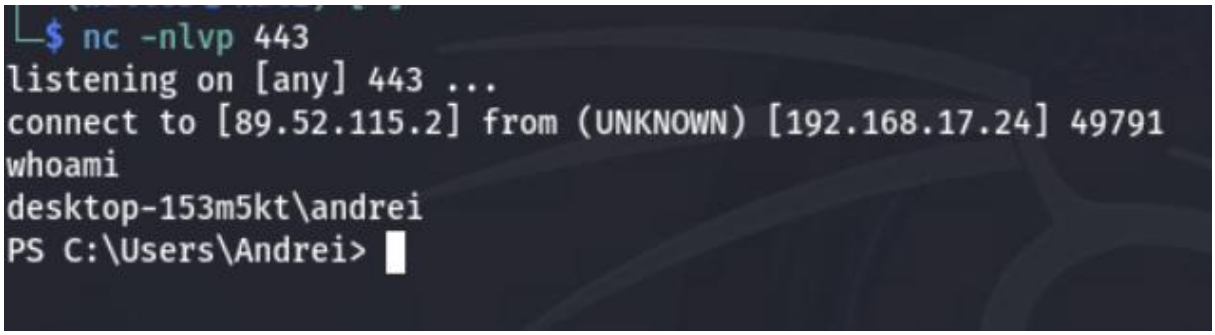

Fig. 6.4.6 Realizarea conexiunii de tip reverse shell

Această etapă a reprezentat punctul critic al scenariului experimental, demonstrând că izolarea fizică a infrastructurii nu elimină riscul compromiterii atunci când interacțiunea umană cu mediul extern este posibilă. Stabilirea conexiunii a permis acces la nivel de sistem și a creat premisa desfășurării etapelor ulterioare de analiză a configurației rețelei și a relațiilor existente între segmentele IT și OT.

6.5 Investigarea privilegiilor și a conexiunilor spre sistemele mecatronice

Accesul obținut la linia de comandă a stației administratorului a confirmat compromiterea inițială, însă s-a dovedit insuficient pentru o analiză completă a infrastructurii, din cauza lipsei interfeței grafice și a limitărilor privind utilizarea uneltelor avansate disponibile în mediul Linux.

Pentru extinderea vizibilității asupra rețelei interne, a fost implementat un mecanism de proxy tunneling utilizând utilitarul open-source Chisel. Scopul a fost redirecționarea traficului prin stația compromisă, astfel încât scanările și interogările să apară ca fiind inițiate din interiorul infrastructurii.

Chisel a fost configurat în arhitectură server–client: serverul pe infrastructura Command and Control, iar clientul pe stația compromisă, printr-un tunel inversat (reverse tunneling), care a expus un proxy SOCKS5 pe serverul C2. Activarea clientului este ilustrată în Fig. 6.5.4.

```
PS C:\Users\Public\Downloads> start-job {chisel.exe client 89.52.115.2:50050 R:1080:socks}

Id     Name            PSJobTypeName   State         HasMoreData     Location             Command
--     ----            -------------   -----         -----------     --------             -------
1      Job1            BackgroundJob   Running       True            localhost            chisel.exe client 89.5...
```

Fig. 6.5.4 Activare client proxy pe stația de lucru

Prin stabilirea tunelului SOCKS5, traficul generat din mediul Linux a fost redirecționat prin stația administratorului, permițând ocolirea restricțiilor firewall și ACL fără modificarea politicilor existente.

Scanările efectuate prin proxy au condus la identificarea unui serviciu web activ în segmentul intern (192.168.1.10). Accesarea acestuia, prin redirecționarea traficului browserului, a permis interacțiunea cu interfața web a platformei Nagios XI (Fig. 6.5.8).

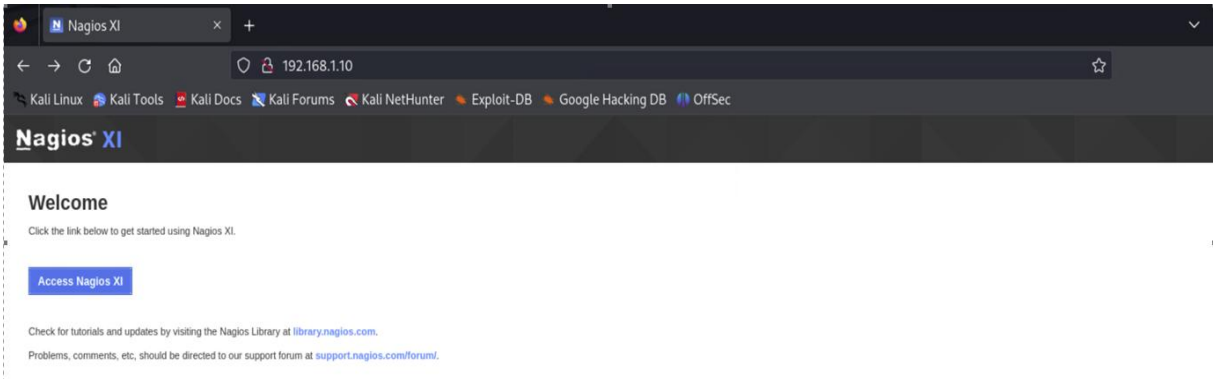

Fig. 6.5.8 Accesare platforma de monitorizare

Această etapă a demonstrat că, prin combinarea tehnicilor de tunneling și redirecționare a traficului, pot fi accesate resurse interne critice într-o infrastructură segmentată logic. Identificarea Nagios XI ca punct de interconectare între zona IT și SCADA evidențiază rolul sistemelor de monitorizare ca potențiale noduri de pivotare.

Din perspectivă metodologică, rezultatele confirmă că segmentarea și izolarea fizică nu elimină complet riscul de propagare laterală atunci când există sisteme intermediare la intersecția IT–OT.

6.6. Testarea compromiterii credențialelor aplicației ce monitorizează sistemele mecatronice

După identificarea aplicației Nagios XI ca punct de interconectare între infrastructura IT și zona SCADA, următoarea etapă a vizat evaluarea mecanismului de autentificare. Testarea inițială a exclus existența credențialelor implicite, fiind necesară aplicarea unei metode active de evaluare a robusteții parolelor.

Pentru simularea unui scenariu realist, a fost utilizat un instrument specializat de testare a autentificării, capabil să automatizeze verificarea combinațiilor utilizator–parolă prin trimiterea repetată de cereri HTTP POST și analiza răspunsurilor serverului. Metodologia a inclus identificarea endpoint-ului de autentificare, definirea unui set controlat de utilizatori și utilizarea unui dicționar restrâns de parole probabile.

Testarea controlată a condus la identificarea unei combinații valide cu privilegii administrative, permițând acces complet la interfața Nagios XI. Rezultatul evidențiază vulnerabilitatea sistemelor care nu implementează politici stricte de complexitate și limitare a tentativelor de autentificare.

Compromiterea Nagios XI a reprezentat un punct critic al cercetării, întrucât platforma funcționează ca nod de interconectare între zona IT și infrastructura SCADA. Figura 6.6.1 ilustrează progresul compromiterii: stația administratorului, tunelul proxy și aplicația de monitorizare.

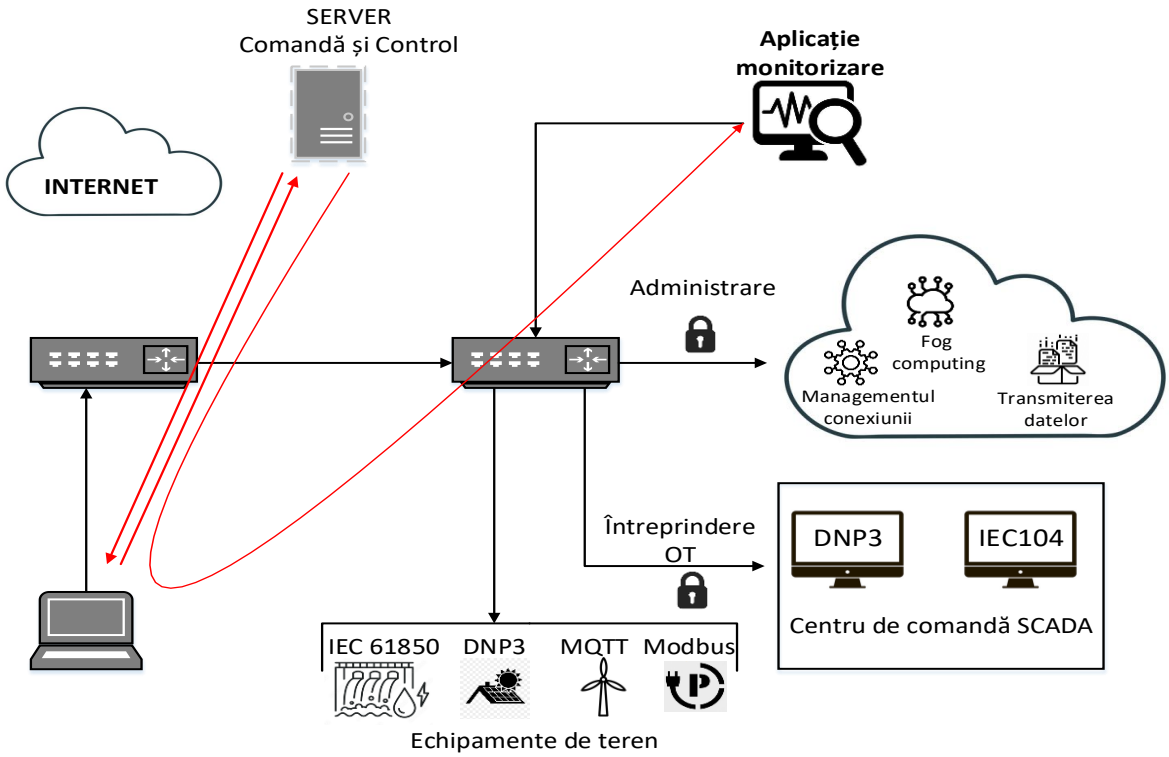

Fig. 6.6.1 Prima versiune a arhitecturii generale a sistemului inteligent actualizată cu punctele compromise

Accesul obținut a permis:

1. Control administrativ asupra platformei de monitorizare;
2. Vizibilitate asupra echipamentelor și serviciilor monitorizate;
3. Premise pentru propagare laterală către zona operațională.

Din perspectivă științifică, această etapă confirmă că sistemele de monitorizare pot deveni puncte critice de pivotare în arhitecturi IT–OT interconectate, în absența unor mecanisme robuste de autentificare.

6.7. Identificarea și exploatarea vulnerabilităților aplicației ce monitorizează sistemele mecatronice

După obținerea accesului administrativ în Nagios XI, analiza a continuat prin identificarea versiunii instalate (5.7.4) și verificarea existenței vulnerabilităților public documentate. Testele inițiale nu au evidențiat exploatări directe, astfel că versiunea a fost corelată cu baze de date publice de vulnerabilități.

Interogarea Exploit Database a indicat un exploit aplicabil versiunilor 5.7.x, care permite execuție de cod la distanță (RCE) în condițiile unei autentificări valide, prin exploatarea mecanismului de upload al pluginurilor.

Într-un mediu IT standard, aplicarea exploit-ului este directă. În infrastructura analizată însă, aplicația era izolată de Internet, ceea ce a impus proiectarea unei rute indirecte de comunicație pentru stabilirea unei conexiuni inverse către serverul Command and Control, fără modificarea politicilor de segmentare.

Pentru acest scop, a fost implementat un mecanism de redirecționare a traficului prin stația administratorului, care a funcționat ca intermediar între Nagios XI și serverul C2. În configurația finală:

1. Nagios XI inițiа conexiunea către stația administratorului;
2. stația redirecționa traficul către C2;
3. serverul C2 stabilea sesiunea de comandă.

Conexiunea inversă a fost stabilită cu succes prin mecanismul configurat, confirmând compromiterea aplicației și posibilitatea execuției de cod în contextul acesteia.

Figura 6.7.11 prezintă arhitectura actualizată, evidențiind punctele compromise și fluxul de date rezultat.

.

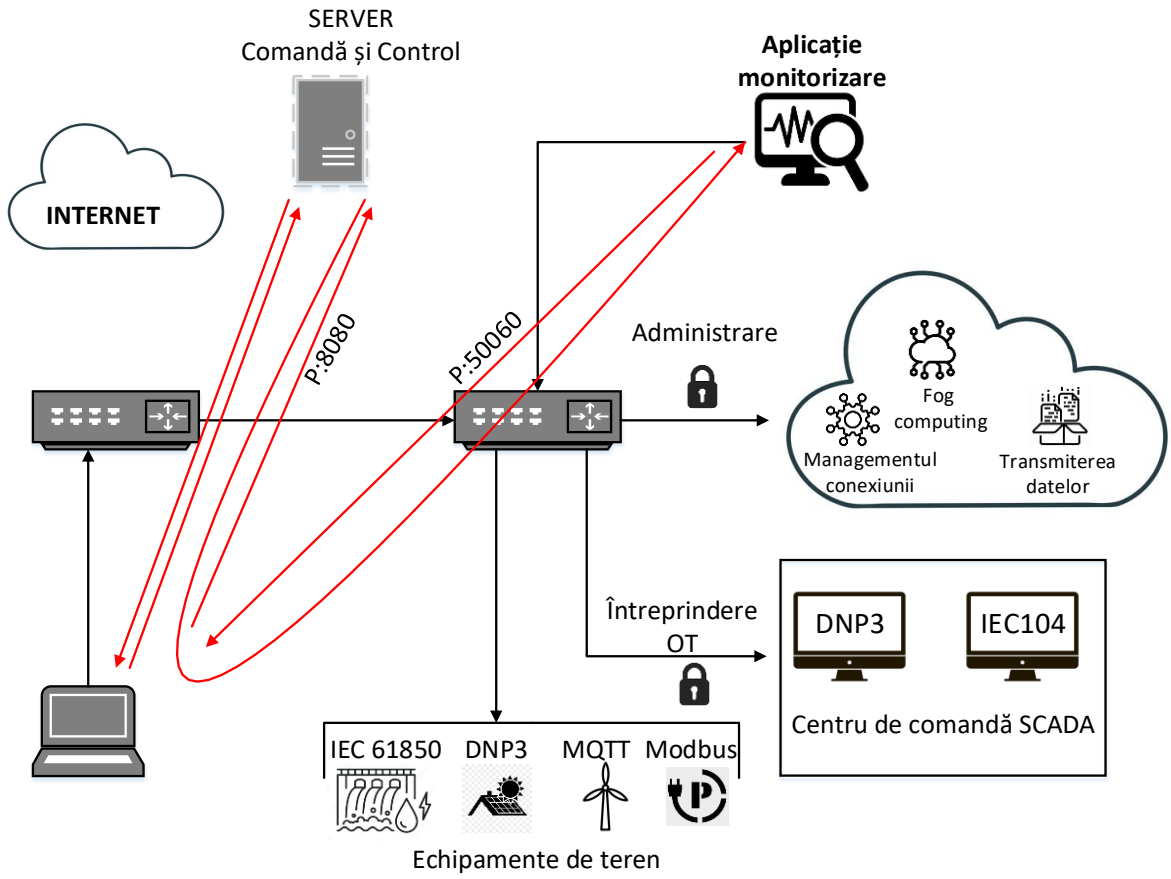

Fig. 6.7.11 A doua versiune a arhitecturii generale a sistemului inteligent actualizată cu punctele compromise

Această etapă demonstrează că:

1. Un serviciu legitim de monitorizare poate deveni punct de pivotare între IT și SCADA.
2. Segmentarea fizică și logică nu elimină riscul accesului indirect prin noduri administrative.
3. Exploit-urile publice pot fi adaptate la medii industriale restrictive prin arhitecturi controlate de tunelare.

Din perspectivă metodologică, contribuția constă în integrarea unui exploit public într-un scenariu industrial real, prin proiectarea unei rute de comunicație compatibile cu constrângerile arhitecturale existente. Rezultatele confirmă că platformele de monitorizare reprezintă elemente critice în securitatea OT și necesită măsuri suplimentare de segmentare și audit.

6.8. Compromiterea RTU-ului

Analiza arhitecturii generale a infrastructurii a evidențiat faptul că sistemele din zona SCADA acceptă trafic exclusiv din partea aplicației de monitorizare, orice alt tip de comunicare fiind filtrat la nivel de segmentare. Această configurație, specifică mediilor industriale cu separare strictă IT–OT, limitează suprafața de atac directă, dar concentrează riscul în punctele de interconectare administrativă.

Pentru evaluarea rezilienței componentelor SCADA fără modificarea politicilor existente, a fost implementat un mecanism de pivotare prin utilizarea aplicației Nagios XI ca intermediar legitim. Configurarea unui tunel proxy între serverul Command and Control (C2) și platforma de monitorizare a permis redirecționarea traficului astfel încât, din perspectiva infrastructurii SCADA, sursa să fie aplicația de monitorizare. Această abordare a permis desfășurarea testelor ca și cum ar fi fost inițiate din interiorul domeniului OT.

După stabilirea canalului indirect, au fost inițiate operațiuni de identificare a serviciilor active în segmentul SCADA. A fost detectată interfața web a RTU-ului, expusă pe portul 8443 și utilizând protocolul WebSocket pentru schimbul de mesaje bidirecțional, devenind astfel punctul central al analizei.

Pentru investigarea mecanismului de autentificare și a fluxului de date, Burp Suite a fost configurat pentru interceptarea traficului HTTP/HTTPS și WebSocket. Testele inițiale au constat în introducerea deliberată de credențiale incorecte pentru analizarea structurii

pachetelor și a răspunsurilor serverului. Deși autentificarea era respinsă corect, analiza a permis identificarea structurii mesajelor JSON utilizate în comunicare.

Etapa decisivă a constat în transmiterea manuală, prin modulul Repeater, a unor mesaje JSON specifice aplicației, în afara unui flux de autentificare valid. Au fost testate cereri asociate funcționalităților interne, precum subscriberea la fluxuri de date sau solicitarea de resurse interne. Manipularea mesajelor este ilustrată în Fig. 6.8.10.

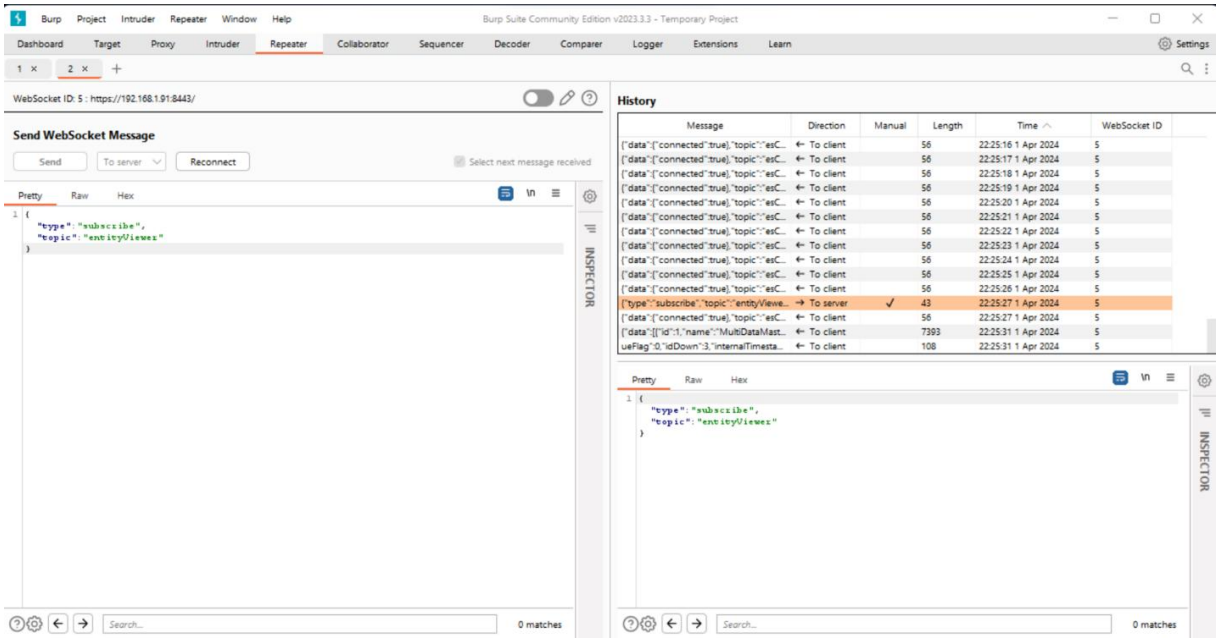

Fig. 6.8.10 Manipularea mesajului JSON *entityViewer*

Analiza răspunsurilor a evidențiat că anumite cereri erau procesate fără verificarea existenței unei sesiuni autentificate. Serverul furniza conținut și permitea acces la funcționalități interne, tratând conexiunea ca legitimă. Această situație confirmă existența unei vulnerabilități critice la nivelul validării mesajelor WebSocket, care permite ocolirea mecanismului de autentificare.

Exploatarea a depășit nivelul accesului informațional. Prin modificarea parametrilor din structura mesajelor JSON, au fost transmise comenzi către infrastructura controlată de RTU. În mod normal, aceste comenzi sunt generate prin interfața legitimă și validate prin mecanisme interne de autentificare și autorizare. În scenariul testat, manipularea mesajelor a permis transmiterea directă a unei comenzi de modificare a stării unui circuit electric.

Fluxul operațional standard presupune transmiterea comenzilor de la utilizator către RTU, apoi către HMI și ulterior către PLC-urile responsabile de execuția în teren. Prin manipularea mesajelor WebSocket, acest flux a fost influențat fără parcurgerea procesului legitim de autentificare, rezultând modificarea stării circuitului monitorizat.

Figura 6.8.16 evidențiază efectul direct al comenzii falsificate, respectiv închiderea circuitului electric.

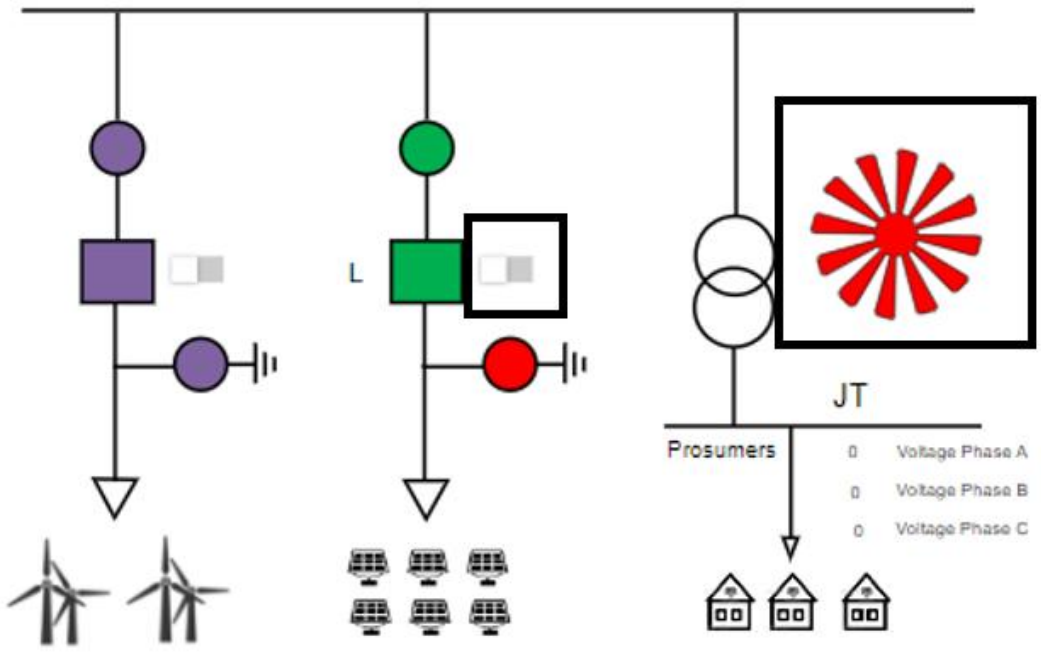

Fig. 6.8.16 – Inchderea circuitelor după falsificarea pachetelor

Această etapă confirmă că vulnerabilitatea identificată permite nu doar acces la date sau configurări, ci și intervenție asupra procesului fizic controlat de infrastructura SCADA. Impactul este semnificativ, demonstrând posibilitatea modificării stării echipamentelor industriale prin exploatarea unui punct de interconectare IT–OT și a unei deficiențe de validare la nivel de aplicație.

Din perspectivă metodologică, rezultatul validează ipoteza cercetării conform căreia sistemele de monitorizare și interfețele web asociate pot deveni puncte strategice de pivotare în arhitecturi segmentate. Deși segmentarea fizică și logică a fost respectată, existența unui nod administrativ cu rol dual (monitorizare IT și acces către SCADA) a permis extinderea controlată a accesului către zona operațională.

Rezultatele acestei etape constituie elementul central al contribuției experimentale, demonstrând, în condiții controlate, posibilitatea ocolirii autentificării și obținerea unui impact direct asupra infrastructurii fizice, fără modificarea politicilor de securitate și fără acces direct din Internet către zona SCADA.

6.9 Evaluarea impactului și a rezilienței pentru infrastructura industrială

Rezultatele cercetării experimentale confirmă faptul că infrastructurile industriale inteligente, chiar și atunci când sunt proiectate în regim de izolare fizică și segmentare logică strictă, nu sunt implicit protejate împotriva atacurilor cibernetice avansate. Prin aplicarea etapizată a metodelor de testare activă a fost demonstrată posibilitatea construirii unui lanț complet de compromitere, pornind de la infrastructura IT și extinzându-se până la nivelul echipamentelor operaționale controlate prin RTU și PLC.

Impactul cel mai relevant al cercetării constă în obținerea controlului funcțional asupra infrastructurii de producție prin exploatarea succesivă a unor vulnerabilități aparent izolate: compromiterea stației de administrare, pivotarea prin aplicația de monitorizare, exploatarea mecanismului WebSocket al RTU și injectarea de comenzi în fluxul operațional. Integrarea acestor etape într-un scenariu coerent a demonstrat că vulnerabilități minore, combinate strategic, pot conduce la un impact major asupra proceselor industriale.

Compromiterea interfeței web a RTU reprezintă punctul critic al cercetării, validat inclusiv prin certificatul emis de producător (EEBDM-235865430-1059 / 21.08.2025). Scenariul implementat a demonstrat posibilitatea ocolirii mecanismelor de autentificare și transmiterea de comenzi directe către infrastructura fizică, fără acces frontal din internet și fără modificarea politicilor de segmentare existente. Această realizare evidențiază vulnerabilitatea punctelor de interconectare IT–OT și necesitatea tratării aplicațiilor de monitorizare ca elemente critice de securitate.

Evaluarea impactului relevă consecințe potențiale majore:

- modificarea stării circuitelor electrice;
- accesarea și exfiltrarea bazelor de date operaționale;
- compromiterea credențialelor și a parametrilor de configurare;
- afectarea continuității proceselor industriale.

În acest context, reziliența infrastructurii devine un element central al securității cibernetice industriale. Reziliența nu trebuie limitată la capacitatea de recuperare post-incident, ci trebuie integrată ca mecanism activ, care include detectarea anomaliilor, izolarea rapidă a componentelor compromise, menținerea funcțiilor critice și restaurarea controlată a sistemului. Segmentarea adaptivă, monitorizarea continuă a traficului și auditarea periodică a fluxurilor dintre IT și OT reprezintă măsuri esențiale pentru reducerea impactului unor atacuri similare.

Cercetarea demonstrează că simpla izolare fizică sau logică nu este suficientă în arhitecturile moderne din Industria 4.0. Securitatea trebuie proiectată în corelație cu reziliența, iar infrastructurile industriale trebuie concepute pentru a anticipa compromiterea parțială și a funcționa în condiții controlate chiar și în prezența unor breșe.

6.10 Concluzii de capitol

Capitolul a reprezentat componenta aplicativă centrală a cercetării, demonstrând, într-o infrastructură industrială reală, posibilitatea compromiterii progresive a unui sistem SCADA prin corelarea mai multor vectori de atac. Au fost validate etapele fundamentale ale unui atac avansat: acces inițial, pivotare, escaladare, exploatare și impact operațional.

Rezultatele obținute confirmă că interconectarea IT–OT introduce puncte critice care pot fi exploatate chiar și în condiții de segmentare strictă. Aplicațiile de monitorizare și interfețele administrative reprezintă zone cu risc strategic, capabile să devină canale de extindere a accesului către zona operațională.

Cercetarea evidențiază necesitatea unei abordări integrate a securității industriale, în care prevenția, detecția și reziliența funcționează complementar. Măsurile tradiționale de protecție trebuie completate cu mecanisme proactive de testare, audit și simulare a incidentelor, precum și cu politici clare de răspuns și recuperare.

Prin validarea experimentală a unui scenariu complet de compromitere, lucrarea oferă un model aplicativ pentru evaluarea securității infrastructurilor industriale inteligente și fundamentează dezvoltarea unor strategii moderne de apărare adaptate mediilor critice.

7. ÎMBUNĂTĂȚIREA SECURITĂȚII CIBERNETICE A UNUI SISTEM MECATRONIC INTELIGENT DIN INDUSTRIA 4.0

7.1. Identificarea și caracterizarea vulnerabilității critice în RTU ES2000

Etapa experimentală a condus la identificarea unei vulnerabilități critice în RTU ES2000, componentă esențială a infrastructurii SCADA. Analiza comunicațiilor WebSocket dintre interfața web și backend a evidențiat absența unui mecanism de autentificare pentru anumite mesaje JSON transmise prin portul 8443.

Testarea a fost realizată printr-un script Python dezvoltat în cadrul cercetării, care a inițiat conexiuni WebSocket directe și a transmis mesaje precum:

- {"type":"downloadDatabase"}
- {"type":"subscribe","topic":"entityViewer"}
- {"type":"logs"}

Serverul a procesat aceste mesaje fără validarea identității utilizatorului, furnizând date sensibile și permițând acces la funcționalități interne. Vulnerabilitatea permitea inclusiv transmiterea de comenzi către infrastructura controlată prin RTU și PLC.

Breșa identificată nu este documentată public și nu are asociat un CVE, iar validarea oficială a fost confirmată prin certificatul EEBDM-235865430-1059 (21.08.2025, Anexa 1). Contribuția lucrării constă în identificarea, exploatarea controlată și raportarea responsabilă a acestei vulnerabilități într-un mediu industrial real.

7.2. Consecințele operaționale și implicațiile asupra infrastructurii

Vulnerabilitatea identificată are implicații directe asupra funcționării infrastructurii industriale. Lipsa autentificării în procesarea mesajelor WebSocket permite intervenții neautorizate asupra datelor și proceselor operaționale.

Impactul potențial include:

- descărcarea bazei de date a sistemului;
- accesarea logurilor și informațiilor interne;
- modificarea stării circuitelor electrice;
- perturbarea continuității proceselor industriale.

Testarea a demonstrat practic posibilitatea transmiterii de comenzi către infrastructura fizică, evidențiind legătura directă dintre o vulnerabilitate aplicațională și efecte asupra echipamentelor controlate prin PLC și RTU.

Rezultatele confirmă că segmentarea rețelei și izolarea logică nu sunt suficiente în absența unor mecanisme robuste de autentificare și validare la nivel aplicațional, în special în arhitecturile IT–OT specifice Industriei 4.0.

7.3. Măsuri proactive de îmbunătățire a securității infrastructurilor mecatronice și industriale

Pentru consolidarea securității, au fost definite măsuri proactive orientate spre reducerea suprafeței de atac și creșterea rezilienței operaționale, integrând acțiuni tehnice și organizaționale.

1. Responsible disclosure și remediere tehnică

Vulnerabilitatea a fost raportată producătorului în cadrul unui proces de responsible disclosure. Măsura corectivă implementată constă în utilizarea unui token de sesiune generat la autentificare și validat printr-un handshake WebSocket inițial, respingând conexiunile fără token valid. Același mecanism este aplicat și interfețelor HTTPS.

Certificatul EEBDM-235865430-1059 confirmă impactul practic al cercetării și contribuția directă la întărirea securității aplicației.

2. Consolidarea factorului uman

Scenariul experimental a demonstrat că vectorul inițial poate fi non-tehnic (interacțiune prin e-mail). Se impune instruirea continuă a personalului privind phishing-ul, utilizarea documentelor cu macrocomenzi și riscurile asociate aplicațiilor de monitorizare. Evaluările periodice și exercițiile controlate trebuie să transforme componenta umană într-un mecanism activ de detecție și reacție timpurie [51].

3. Integrarea unei soluții specializate OT – Cisco Cyber Vision

A fost integrată soluția Cisco Cyber Vision pentru inventariere automată, vizualizarea topologiei și corelarea cu baze CVE. Platforma a fost implementată ca mașină virtuală, cu integrare non-intruzivă (out-of-band), pe bază de trafic duplicat, fără afectarea continuității operaționale.

În urma analizei a fost identificată o vulnerabilitate suplimentară – CVE-2023-20076 (scor 7.2 CVSS v3.1), asociată mediului Cisco IOx, cu potențial de execuție de comenzi în anumite condiții de acces.

Fig 7.3.3 Identificare CVE pentru echipamentul de tip router

Conform recomandărilor producătorului, remedierea se realizează prin aplicarea patch-urilor oficiale [53].

Identificarea acestui CVE confirmă că riscurile pot apărea pe multiple componente ale lanțului operațional, ceea ce impune măsuri defensive distribuite și corelate.

Prin combinarea raportării responsabile, a instruirii personalului și a integrării unei soluții specializate de detecție OT, sunt conturate măsuri aplicabile direct infrastructurii analizate, cu impact asupra securității și reziliență ecosistemului SCADA.

7.4 Concluzii de capitol

Capitolul evidențiază faptul că securitatea cibernetică a infrastructurilor mecatronice și industriale trebuie abordată integrat, prin corelarea măsurilor tehnice, organizaționale și educaționale. Identificarea vulnerabilităților critice și tratarea lor sistematică reprezintă punctul de plecare pentru reducerea suprafeței de atac și creșterea rezilienței operaționale.

Cercetarea a contribuit prin: colaborarea directă cu producătorul pentru remedierea vulnerabilității identificate, consolidarea componentei umane prin instruire adaptată mediului industrial și integrarea unei soluții specializate de monitorizare OT (Cisco Cyber Vision) pentru detecția și corelarea automată a riscurilor.

În ansamblu, capitolul confirmă că protecția infrastructurilor inteligente necesită o strategie proactivă, orientată spre prevenție, monitorizare continuă și reziliență operațională.

8. CONCLUZII GENERALE, CONTRIBUȚII ORIGINALE ȘI PERSPECTIVE DE DEZVOLTARE

8.1 Concluzii generale

Prezenta lucrare a analizat securitatea cibernetică în contextul Industriei 4.0, cu accent pe infrastructurile SCADA, IIoT și convergența IT–OT. Partea teoretică a evidențiat tranziția de la arhitecturi industriale izolate la ecosisteme digitale integrate și riscurile asociate interconectării, raportate la standarde precum NIST Cybersecurity Framework și ISO/IEC 27001.

Cercetarea a demonstrat că integrarea IT–OT, deși generează beneficii operaționale, extinde suprafața de atac și impune o abordare unitară, orientată pe întreg lanțul digital–operațional. În aceste medii, securitatea trebuie tratată ca un proces continuu ce combină măsuri tehnice, politici organizaționale și adaptare la amenințări dinamice.

Pentru validarea acestor premise, conceptele teoretice au fost transpuse într-un cadru experimental pe o infrastructură industrială reală, caracterizată prin segmentare strictă IT–OT și politici de tip air-gap. Metodologia a reprodus etapele unui lanț realist de atac, de la acces inițial până la evaluarea impactului asupra componentelor operaționale, demonstrând posibilitatea compromiterii controlate a unor mecanisme considerate robuste.

Rezultatele confirmă că o vulnerabilitate exploatată în zona IT poate deveni pivot către resurse OT critice, ceea ce susține necesitatea unei strategii integrate, completată de capabilități de detecție, răspuns și recuperare rapidă. În concluzie, lucrarea validează ipoteza că securitatea sistemelor industriale inteligente trebuie abordată holistic, prin corelarea segmentării arhitecturale, a mecanismelor proactive de monitorizare și a instruirii continue a personalului.

8.2 Contribuții originale

Punctul de pornire al scenariului l-a constituit integrarea factorului uman într-o arhitectură industrială reală, prin transmiterea unui e-mail direcționat către administratorul SCADA, conținând un document Word cu macrocomenzi malițioase. Macrocomanda, dezvoltată în VBA, a fost concepută pentru a inița o conexiune de tip reverse shell către un server Command and Control (CnC), adaptată constrângerilor arhitecturale ale mediului SCADA prin configurarea Netcat în regim listener pe portul 443. Utilizarea acestui port,

asociat traficului HTTPS legitim, a permis integrarea fluxului în comunicațiile permise LAN→WAN, reducând probabilitatea de detecție.

Deși macro-uri Office și reverse shell-uri sunt documentate în literatura de specialitate, acestea sunt tratate în contexte generice de pen-testing. Contribuția lucrării constă în adaptarea deliberată a acestui mecanism la o infrastructură SCADA segmentată, demonstrând aplicabilitatea practică a unui vector teoretic într-un mediu industrial real.

Pe baza conexiunii inițiale, a fost construit un mecanism de tunelare avansată utilizând Chisel pentru implementarea unui proxy SOCKS5 prin stația administratorului. Această arhitectură a permis mascarea originii traficului și simularea unui flux legitim din interiorul infrastructurii, traversând controlat segmentarea IT–OT și principiile de tip air-gap.

În acest context, Nmap a fost integrat prin tunelul SOCKS5 realizat cu Chisel, permițând activități de recunoaștere într-un mediu SCADA real fără modificarea regulilor de firewall sau ACL. Noutatea nu constă în utilizarea uneltei în sine, ci în integrarea acesteia într-un lanț de proxy chaining adaptat unei infrastructuri industriale restrictive.

Analiza a condus la identificarea platformei Nagios XI ca unic punct de interconectare între IT și SCADA. Compromiterea controlată a acesteia a validat ipoteza conform căreia sistemele de monitorizare pot deveni noduri strategice de pivotare în arhitecturi segmentate.

Un alt element de originalitate îl reprezintă adaptarea unui exploit public pentru Nagios XI într-un context industrial real, prin construirea unei arhitecturi de redirecționare a traficului bazate pe Socat, Netcat și Chisel. Configurarea unui mecanism de reverse proxy sincronizat cu infrastructura existentă a permis aplicarea exploit-ului în condiții restrictive, fără încălcarea explicită a politicilor de segmentare.

Etapa critică a cercetării a fost compromiterea controlată a RTU-ului ES2000. Utilizând Burp Suite, a fost interceptat și manipulat traficul WebSocket, fiind reproduse și modificate structuri JSON legitime pentru a ocoli mecanismul de autentificare și a transmite comenzi direct către infrastructura controlată de RTU și PLC. Transpunerea acestei tehnici într-un mediu SCADA real și segmentat reprezintă o contribuție metodologică semnificativă.

Identificarea unei vulnerabilități nepublicate în mecanismul de autentificare WebSocket al RTU-ului ES2000, fără CVE asociat, constituie contribuția centrală a lucrării. Rezultatul a fost validat oficial de producător prin certificatul EEBDM-235865430-1059 (21.08.2025, Anexa 1), conferind cercetării caracter distinctiv și relevanță practică.

Demersul experimental a fost completat prin responsible disclosure și integrarea platformei CyberVision pentru validarea măsurilor defensive și evaluarea impactului în timp real,

transformând procesul de exploatare controlată într-un model aplicativ de consolidare a securității infrastructurilor industriale.

8.3 Perspective de dezvoltare

Rezultatele obținute creează premisele dezvoltării unui cadru standardizat de audit proactiv pentru infrastructuri SCADA, bazat pe scenarii realiste de penetrare și evaluare a rezilienței. Metodologia elaborată, construită pe recunoaștere, tunelare, pivotare și exploatare controlată, poate fi transformată într-un proces iterativ, aplicat periodic pentru identificarea și remedierea timpurie a vulnerabilităților emergente.

Pe termen mediu și lung, extinderea metodologiei către alte arhitecturi SCADA, cu particularități tehnologice și operaționale diferite, poate conduce la un portofoliu comparativ de studii de caz, util pentru identificarea tiparelor recurente de vulnerabilitate și pentru formularea unor ghiduri de bune practici aplicabile transversal.

Un rezultat cu relevanță practică îl reprezintă reacția producătorului RTU-ului analizat, care a implementat modificări asupra mecanismelor de autentificare și validare a comunicațiilor ca urmare a raportării vulnerabilității. Această experiență susține necesitatea unui cadru de colaborare continuă între operatori industriali, producători și experți în securitate, orientat către identificarea timpurie și remedierea vulnerabilităților critice.

Valorificarea rezultatelor obținute în cadrul cercetării, prin integrarea lor în politici operaționale și programe de audit proactiv, poate transforma scenariile experimentale validate aici într-un instrument recurent de prevenție și optimizare a securității. În acest fel, metodologia elaborată nu rămâne doar un exercițiu științific, ci se consolidează ca o resursă practică, capabilă să sprijine în mod direct consolidarea rezilienței infrastructurilor critice și să contribuie la crearea unui ecosistem industrial mai sigur, bazat pe schimb real de informații și pe replicarea soluțiilor eficiente între sectoare.

8.4 Sinteza contribuțiilor originale

1. Am analizat infrastructura industrială și am identificat stația de lucru a administratorului ca unic punct de acces la Internet și, implicit, vector principal de compromitere, fapt ce a permis integrarea ingineriei sociale ca risc non-tehnic într-un scenariu experimental realist, demonstrând vulnerabilitatea factorului uman chiar și în medii izolate fizic.

2. Am adaptat tehnica reverse shell la infrastructura industrială analizată, configurând serverul CnC pe portul 443 și integrând un mecanism pasiv de ascultare, demonstrând că o metodă consacrată poate fi calibrată pentru a respecta constrângerile LAN→WAN și a ocoli politicile stricte de securitate implementate.

3. Am conceput și aplicat un scenariu de phishing direcționat asupra administratorului SCADA, prin realizarea de la zero a unui document Word cu macrocomenzi malițioase, adaptat infrastructurii industriale analizate și utilizat pentru inițierea unei conexiuni reverse shell către serverul de comandă și control.

4. Am implementat un tunel proxy SOCKS5 prin utilitarul Chisel, configurat între serverul C2 și stația de lucru a administratorului, pentru a masca originea traficului și a simula un flux legitim din infrastructura industrială analizată, această contribuție demonstrând caracterul original al cercetării și adaptabilitatea la constrângerile rețelelor critice.

5. Am utilizat Nmap în combinație cu tunelul SOCKS5 realizat cu Chisel, adaptând instrumentul la infrastructura industrială analizată; această abordare a permis mascare originii traficului prin stația administratorului și ocolirea restricțiilor firewall și ACL, demonstrând fezabilitatea testării securității în condiții restrictive și cu relevanță practică.

6. Am identificat platforma Nagios XI ca unic punct de interconectare între domeniul IT și zona SCADA din infrastructura industrială analizată și am compromis-o prin atac de tip brute force, demonstrând importanța segmentelor de tranziție și a gestionării credențialelor ca puncte critice de securitate.

7. Am identificat un exploit public pentru platforma Nagios XI și l-am exploatat în infrastructura industrială analizată, prin construirea unui flux de comunicații bazat pe socat, netcat și chisel, integrând mecanisme de reverse tunneling și proxying, ceea ce a permis compromiterea aplicației în condiții reale și restrictive.

8. Am identificat RTU-ul ES2000 ca element al infrastructurii OT prin utilizarea unor tehnici de pivoting prin aplicația Nagios XI pentru a extinde vizibilitatea și accesul în infrastructura critică fără a compromite politicile existente de segmentare a traficului.

9. După identificarea RTU-ului ES2000 ca element critic al infrastructurii OT, am adaptat instrumentul Burp Suite pentru a analiza traficul specific generat de acest echipament, cu scopul de a intercepta și manipula protocoalele de autentificare. Această adaptare a demonstrat că unelte consacrate mediului IT pot fi calibrate pentru a funcționa eficient în infrastructuri industriale reale, oferind vizibilitate asupra fluxurilor de date și evidențiind riscurile asociate comunicațiilor dintre echipamentele SCADA.

10. Prin tehnicile și metodele aplicate, am identificat o vulnerabilitate în mecanismul de autentificare al interfeței web a RTU-ului ES2000. Această vulnerabilitate nu este documentată public și nu are un CVE asociat, iar demersul meu a fost validat de producător prin certificatul EEBDM-235865430-1059, fapt ce confirmă caracterul original și valoarea științifică a cercetării.

11. Am integrat un instrument consacrat într-o infrastructură industrială reală, printr-o metodologie completă de instalare, configurare și validare, demonstrând aplicabilitatea practică a acestuia cu ajutorul platformei CyberVision.

DISEMINAREA REZULTATELOR

O parte semnificativă a rezultatelor obținute în cadrul acestei lucrări a fost valorificată prin publicarea unor articole științifice în reviste de specialitate. Aceste publicații confirmă calitatea și originalitatea contribuțiilor aduse, abordând atât aspecte teoretice, cât și soluții aplicative în domeniul securității cibernetice și al Industriei 4.0. Prin intermediul lor, rezultatele cercetării au devenit accesibile comunității științifice și pot constitui bază pentru dezvoltări și aprofundări ulterioare.

Publicarea acestor articole a contribuit, de asemenea, la consolidarea vizibilității tematicii abordate într-un context internațional, oferind oportunitatea de comparare a rezultatelor obținute cu alte cercetări din domeniu. Prin integrarea lor în reviste de specialitate, lucrările au facilitat schimbul de idei și bune practici între cercetători, stimulând apariția unor noi direcții de investigație și crearea de punți de colaborare în domeniul Industriei 4.0 și al securității cibernetice.

Articolele publicate sunt:

1. Berindei, Adelin-Marian; Ilie, Cristinel; Badea, Florentina, *The Cyber Security Paradigm in Industry 4.0*, International Journal of Mechatronics and Applied Mechanics, Issue 13, 2023, pp. 226–229, e-ISSN: 2559-6497, DOI: 10.17683/ijomam/issue13.27; -

2. Berindei Adelin-Marian, *Cyber Security for Smart System in Industry 4.0*, International Journal of Mechatronics and Applied Mechanics, Issue 9, 2021, pp. 182–185, e-ISSN: 2559-6497, DOI: 10.17683/IJOMAM/ISSUE9.26;

3. Albei, Victor-Eduard; Ilie, Cristinel; Popa, Marius; Tănase, Nicolae; Ovezea, Dragoș; Constantin, Alexandru; Nedelcu, Adrian; Berindei, Adelin-Marian, *The Implementation of a Highly Configurable Control Standard in the Development of a Robotics Platform for the Inspection of Confined Spaces, International Journal of Mechatronics and Applied Mechanics*, Issue 13, 2023, pp. 7–15, e-ISSN: 2559-6497, DOI: 10.17683/ijomam/issue13.1;

BIBLIOGRAFIE

1. *** Universitatea Politehnica din București, *Sisteme inteligente de conducere*, disponibil la: http://acs.pub.ro/doc/master/ro/short_description/SIC-short-ro.pdf, accesat la 12.01.2020.

3. *** Cisco Networking Academy, *Introduction to IoT* – curs online, disponibil la: www.netacad.com, accesat în martie 2022.

4. *** Wikipedia, *Mecatronică*, disponibil la: https://ro.wikipedia.org/wiki/Mecatronică, accesat în iunie 2021.

9. Rawat, Danda B.; Rodrigues, Joel J.P.C., *Cyber-Physical Systems: From Theory to Practice*, CRC Press, 2015, ISBN 978-1-4822-6303-1.

10. Bolton, W., *Mechatronics: Electronic Control Systems in Mechanical and Electrical Engineering*, 6th Edition, Pearson, 2015, ISBN 978-1-292-07407-9.

13. David H. Wolpert; Bruce Tidor, *Introduction to Cyber-Physical Systems*

14. Gaddadevara Matt Siddesh; G. N. Kodanda Ramaiah; K. Srujan Raju, *Cyber-Physical Systems: A Computational Perspective*, CRC Press, 2021. ISBN 978-0367643264.

21. B.K. Tripathy; J. Anuradha, *Internet of Things (IoT): Technologies, Applications, Challenges and Solutions*, CRC Press, 2017. ISBN 978-1-138-30905-3.

23. Henning Kagermann; Wolf-Dieter Lukas; Wolfgang Wahlster, *Industrie 4.0: Smart Manufacturing for the Future*, Acatech STUDY, 2013. ISBN necunoscut.

31. P.W. Singer; Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, Oxford University Press, 2014. ISBN 978-0199918096.

37. Peter Kim, *The Hacker Playbook 3: Practical Guide to Penetration Testing*, Secure Planet, 2018. ISBN 978-1980901754.

38. Thomas A. Johnson, *Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare*, CRC Press, 2015. ISBN 978-1498703267.

39. Christopher Hadnagy, *Social Engineering: The Science of Human Hacking*, Wiley, 2018. ISBN 978-1119433385.

40. *** *OWASP Top Ten Project*, disponibil la: https://owasp.org/www-project-top-ten/, accesat în perioada septembrie 2023 – ianuarie 2024.

43. *** *NIST SP 800-82r2*, disponibil la: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf, descărcat în octombrie 2023.

45. Pascal Ackerman, *Industrial Cybersecurity: Efficiently secure critical infrastructure systems*, Packt Publishing, 2017. ISBN 978-1788394512.

51. Berindei, Adelin-Marian; Ilie, Cristinel; Badea, Florentina, *The Cyber Security Paradigm in Industry 4.0, International Journal of Mechatronics and Applied Mechanics*, Issue 13, 2023, pp. 226–229.

53. *** *Cisco Security Advisory – IOx*, disponibil la: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-8whGn5dL, accesat la 20.02.2024.

54. Berindei, Adelin-Marian, *Cyber Security for Smart System in Industry 4.0, International Journal of Mechatronics and Applied Mechanics*, Issue 9, 2021, pp. 182–185.

57. K. Stouffer; V. Pillitteri; S. Lightman; M. Abrams; A. Hahn, *Guide to Industrial Control Systems (ICS) Security*, NIST Special Publication 800-82 Revision 3, 2022.

60. *** *ScienceDirect – Article on SCADA Security*, disponibil la: https://www.sciencedirect.com/science/article/abs/pii/S0167404816300268?via%3Dihub, accesat la 20.08.2025.

61. *** *SCADA/ICS Social Engineering Attacks – InfoSec Institute*, disponibil la: https://www.infosecinstitute.com/resources/scada-ics-security/ics-scada-social-engineering-attacks/, accesat la 20.08.2025.

62. Dawn Silverman; Yen-Hung (Frank) Hu; Mary Ann Hoppa, *A Study on Vulnerabilities and Threats to SCADA Devices*, Journal of The Colloquium for Information Systems Security Education, Vol. 7, No. 1, Summer 2020. ISSN 1550-7998.

63. *** *CISA ICS Alert (IR-ALERT-H-16-056-01)*, disponibil la: https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01, accesat la 16.05.2023.

68. *** *MITRE ATT&CK for ICS – T0866: Exploitation of Remote Services*, accesat în 2025.

75. J. Lee; B. Bagheri; H.A. Kao, *A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems*, Manufacturing Letters, vol. 3, pp. 18–23, 2015. ISSN 2213-8463.

76. F. Wortmann; K. Flüchter, *Internet of Things*, Business & Information Systems Engineering, vol. 57, nr. 3, pp. 221–224, 2015. ISSN 1867-0202.

79. MITRE Corporation, *Common Vulnerabilities and Exposures (CVE)*, raport, 2023.

LISTĂ DE FIGURI

ANEXE

Anexa 1 – Certificatul EEBDM-235865430-1059 din 21.08.2025

Această anexă face referire la certificatul oficial EEBDM-235865430-1059 din data de 21.08.2025, emis în urma procesului de *responsible disclosure*, care confirmă validarea vulnerabilității critice identificate în echipamentul RTU ES2000.

EXIMPROD ENGINEERING S.A.

Parte a Grupului Eximprod

Registration number:EEBDM-235865430-1059

21.08.2025

Certificat de confirmare a raportării unei vulnerabilități de securitate cibernetică pentru sisteme industriale (Responsible Disclosure)

Prin prezentul certificat, compania Eximprod Engineering, în calitate de dezvoltator și deținător al platformei industriale *ES2000 RTU Virtual Platform*, certifică faptul că domnul Adelin - Marian Berindei a identificat și raportat în mod responsabil o vulnerabilitate critică de securitate în cadrul aplicației noastre.

Detalii privind vulnerabilitatea:

- **Produs afectat:** Server web RTU ES2000
- **Tip vulnerabilitate:** La nivelul aplicației web, comunicația WebSocket nu impune autentificare. Astfel, pentru entitățile care inițiază cereri prin WebSocket, identitatea nu este verificată.
- **Dată raportare:** 04.03.2024
- **Metoda de raportare:** Responsible Disclosure, prin comunicare directă cu echipa noastră de dezvoltare
- **Mod de remediere:** Lansarea unei versiuni actualizate a software-ului
- **Descrierea remedierii:** Comunicarea prin WebSocket a fost securizată prin introducerea unui mecanism de autentificare bazat pe generarea și validarea unui token, accesul prin conexiuni WebSocket este permis exclusiv sesiunilor autentificate. Remedierea a fost implementata cu success in baza recomandarilor din raportul prezentat.

Această recunoaștere este emisă în scop documentar și poate fi utilizată în context academic, profesional sau științific, ca dovadă a contribuției autorului în domeniul securității cibernetice industriale.

Posea Sabin Nicolae

Director Dezvoltare

MINISTERUL EDUCAŢIEI ŞI CERCETĂRII
UNIVERSITATEA „VALAHIA” din TÂRGOVIŞTE
IOSUD – ŞCOALA DOCTORALĂ DE ŞTIINŢE INGINEREŞTI
DOMENIUL INGINERIE MECANICĂ

Enhancing Cybersecurity for Intelligent Systems in Industry 4.0

PhD Supervisor,

PhD, Habil. Cristinel Ioan ILIE

PhD Candidate

Adelin Marian BERINDEI

TÂRGOVIŞTE

2026

Table of Contens

1. INTRODUCTION

1.1. Context and Motivation

This paper addresses cybersecurity in the context of accelerated digitalization and the interconnection of mechatronic systems within Industry 4.0. The evolution from mechanics to mechatronics and subsequently to cyber-physical systems (CPS) reflects the deep integration between the physical and digital environments, generating architectures capable of autonomous communication and distributed processing.

This technological transformation increases the dependence of industrial infrastructures on IT networks and expands the cyberattack surface. Concepts such as the Internet of Things (IoT), the Industrial Internet of Things (IIoT), and intelligent systems provide significant benefits in operational efficiency and optimization, yet they also introduce vulnerabilities that may impact process continuity and operational safety.

In this context, cybersecurity becomes a strategic component in the design and operation of mechatronic systems. The need for a systematic assessment of risks associated with modern industrial infrastructures underlies the selection of this research topic, with emphasis on identifying and analyzing vulnerabilities specific to integrated IT/OT environments.

The research has a strong applied character, being conducted on a real industrial architecture used in production environments, thus ensuring the practical relevance of the results. The interdisciplinary approach integrates mechatronics, SCADA systems, intelligent system technologies, and cybersecurity, highlighting the complexity of protecting critical infrastructures in the digital era.

A novel contribution consists in adapting advanced offensive testing methods to the constraints of industrial environments and identifying a previously undocumented critical vulnerability, officially acknowledged by the manufacturer through the issuance of certificate no. EEBDM-235865430-1059 dated 21.08.2025 (Annex 1), thereby reinforcing the scientific and practical relevance of the research.

1.2. Aim and Objectives

The digital transformation of industrial environments and IT–OT convergence generate both optimization opportunities and increased cybersecurity risks. Extended

interconnectivity enables the rapid propagation of incidents, where a single exploited vulnerability may affect critical industrial processes.

The aim of this thesis is to conduct an in-depth investigation of cybersecurity challenges in modern industrial infrastructures by identifying, testing, and validating vulnerabilities within an experimental framework that faithfully reproduces real exploitation scenarios. The research demonstrates the controlled implementation of a complete attack chain — from the initial access vector to interaction with control equipment — in order to substantiate tailored security measures for the analyzed environment.

The main research objectives include:

- developing an advanced offensive testing methodology for industrial infrastructures;
- adapting penetration testing techniques to the constraints of critical environments;
- rigorously documenting identified vulnerabilities;
- formulating a customized security framework integrating international best practices with the specific characteristics of the analyzed infrastructure;
- proposing technical and organizational measures to enhance cyber resilience.

The thesis also has a strategic dimension, providing practical guidance for industrial operators and cybersecurity professionals, contributing to informed decision-making processes regarding infrastructure protection within the Industry 4.0 ecosystem.

1.3. Structure of the Thesis

The thesis is organized into eight chapters, following a progression from theoretical foundations to experimental validation and the formulation of applicable solutions.

The adopted structure ensures coherence of the scientific approach and integrates engineering principles with modern cybersecurity requirements.

1.4 Chapter Conclusions

The introductory chapter established the necessity of addressing cybersecurity within the context of digital transformation driven by Industry 4.0, highlighting its impact on mechatronic and cyber-physical infrastructures.

It presented the research motivation, aim, and objectives, as well as the structure of the thesis, outlining the conceptual and applied framework of the scientific approach. Protecting modern industrial infrastructures is emphasized as an essential condition for the safe and reliable operation of intelligent systems integrated into operational environments.

2. CURRENT STATE OF INTELLIGENT SYSTEMS IN MECHATRONICS

"An intelligent system is capable of autonomously and adaptively demonstrating as many high-level cognitive capabilities as possible, such as perception, action, learning, planning, memory, decision-making, language recognition, emotion, etc." [1]
Intelligent systems result from the integration of mechatronics with electronics and information technologies, developing decision-making capabilities through training on relevant datasets. These systems perceive the environment, process information, and act autonomously in order to optimize industrial processes.

The integration of IoT technologies, data analytics, and artificial intelligence techniques enables the transformation of traditional infrastructures into "smart factories," characterized by high flexibility, efficiency, and adaptability.

The Internet of Things (IoT) represents a technological domain with major technical, economic, and social impact, based on the global interconnection of intelligent devices through digital infrastructures. Modern communication networks enable the continuous exchange of data between sensors, industrial equipment, and information systems, forming an interdependent digital ecosystem [3].

2.1 Mechatronics

"Mechatronics is the synergistic and systematic combination of mechanics, electronics, and real-time informatics." [4]
Mechatronics is an interdisciplinary field that integrates mechanics, electronics, and information technology from the early stages of design, aiming to achieve optimal functional synergy. Since the term was first introduced in 1969 to describe CPU-controlled systems combining mechanics and electronics, the field has evolved into a comprehensive engineering philosophy .

Initially focused on servo technologies and industrial automation, the development of microprocessors accelerated the integration of digital control into mechanical systems. Advances in digital electronics and miniaturization later enabled the emergence of intelligent sensors and actuators, distributed hardware–software processing systems, and complex applications in the automotive, semiconductor, and industrial automation sectors.

Today, mechatronics encompasses advanced communication technologies, mobile and interconnected systems, and the integration of nanotechnologies, contributing to the development of intelligent, safe, and efficient equipment. It has become a pillar of modern design, playing a central role in the development of systems capable of intelligent interaction with users and operational environments.

2.2 Cyber-Mechatronics

Cyber-mechatronics represents the evolution of classical mechatronics toward interconnected intelligent systems integrated into distributed digital architectures. It combines mechanics, electronics, information technology, and cybernetic principles within a unified framework oriented toward operational autonomy, interoperability, and real-time processing [70,71].

The development of cyber-mechatronics was accelerated after 2000 by advances in information and communication technologies, including industrial networks, the Internet of Things (IoT), artificial intelligence, machine learning, and big data analytics. Traditional mechatronic systems thus evolved into cyber-physical systems capable of self-adaptation and continuous communication within extended industrial ecosystems [9–10].

By integrating distributed control, industrial communications, and digital monitoring platforms, cyber-mechatronics enables remote management and optimization of processes, increasing the efficiency and scalability of industrial infrastructures. At the same time, extended interconnectivity introduces new risk vectors, making cybersecurity an essential component of the design and operation of intelligent systems [11–12].

2.3 Technological Evolution (Mechanics → Mechatronics → Cyber-Physical Systems)

Industrial technological evolution has progressed from mechanics to mechatronics and subsequently to cyber-physical systems (CPS), marking the progressive integration of the physical and digital environments [13].

Mechanics provided the foundation for the development of machines and physical systems, being centered on classical engineering principles. The emergence of mechatronics enabled the integration of mechanics with electronics and informatics, facilitating automation and the development of intelligent equipment.

The current stage is characterized by cyber-physical systems, which unify physical and software components within interconnected communication architectures. CPS enable real-time monitoring, control, and processing, interacting adaptively with the environment through sensors and distributed control mechanisms [14]. Through the integration of artificial intelligence and advanced data analytics, these systems can learn and make autonomous decisions [13–14].

Two fundamental concepts support this evolution: SCADA and Industry 4.0.

SCADA (Supervisory Control and Data Acquisition) represents the real-time monitoring and control infrastructure for industrial processes, based on the integration of PLCs, RTUs, servers, and HMI interfaces [15–19]. SCADA architecture involves the convergence of IT zones (data management, servers, applications, networks) and OT zones (field equipment, sensors, actuators, controllers), forming the operational foundation of modern industrial infrastructures.

Industry 4.0 represents the advanced digitalization stage of production, characterized by the integration of CPS, IoT, industrial communications, and data analytics to create fully interconnected smart factories [54]. This paradigm increases efficiency and flexibility while simultaneously expanding the cyberattack surface.

2.4 IoT – Internet of Things

The Internet of Things (IoT) is a fundamental pillar of Industry 4.0, enabling the interconnection of industrial equipment and continuous data collection for process optimization. Through real-time monitoring and predictive analytics, IoT supports preventive maintenance and enhances operational efficiency [21].

However, the fragmented development of the IoT ecosystem has generated interoperability and standardization challenges, complicating device integration and security. IoT devices frequently manage sensitive data, and the lack of uniform protection mechanisms may compromise confidentiality and operational safety [21].

IoT Security Challenges

Expanded connectivity amplifies systemic vulnerabilities. IoT devices may become entry points for cyberattacks, particularly in the absence of regular updates and robust authentication and network segmentation mechanisms.

In industrial environments, the compromise of a sensor or connected device may lead to incorrect automated decisions, unplanned shutdowns, or the failure of safety mechanisms. IoT security must therefore be treated as a critical element of operational continuity rather than merely a technical issue.

IoT devices exhibit specific characteristics: large-scale distribution, extended life cycles, limited update capabilities, and hardware uniformity, meaning that exploiting a single vulnerability may affect numerous devices simultaneously. Consequently, protection strategies must be based on risk assessment, network segmentation, access control, and continuous component updates [21].

The experimental research presented in this thesis confirms these risks through the controlled identification and exploitation of vulnerabilities in IoT equipment integrated into real industrial infrastructures, highlighting the need for security measures adapted to operational environments.

2.5 Chapter Conclusions

This chapter presented the transition from mechanics to mechatronics and subsequently to cyber-physical systems, highlighting the progressive integration of digital technologies into modern industrial infrastructures.

The roles of SCADA and Industry 4.0 in process digitalization were analyzed, along with the impact of IoT on interconnectivity and automation. At the same time, it was emphasized that increased connectivity introduces additional vulnerabilities, and cybersecurity becomes an essential condition for the resilience and operational continuity of intelligent industrial systems.

3. INDUSTRY 4.0

Technology generates profound transformations in the industrial environment through the integration of automation, connectivity, and advanced data processing. The concept of Industry 4.0, initially developed in Germany as a strategic government-supported initiative, designates the fourth industrial revolution and is associated with notions such as "smart industry" or "interconnected industry" [23].

Industry 4.0 represents the transition from traditional industrial systems to a model based on digitalization, interconnection, and advanced automation. It encompasses the entire product lifecycle — from design and production to monitoring and recycling — through the integration of cyber-physical systems (CPS), industrial communications, and data analytics [23].

Industrial evolution can be summarized as follows:

- Industry 1.0 – mechanization through steam and water power;
- Industry 2.0 – mass production and electrification;
- Industry 3.0 – automation and the introduction of computers;
- Industry 4.0 – full digital integration and intelligent interconnectivity.

Industry 4.0 is not the result of a single innovation, but of the convergence of multiple advanced technologies, including:

- Internet of Things (IoT);
- Big Data and advanced analytics;
- cyber-mechatronic integration;
- advanced robotics and autonomous systems;
- cybersecurity [23].

This paradigm influences not only manufacturing processes but also supply chains, labor markets, and organizational models. Supply chains become transparent and adaptive through real-time monitoring, while production enables mass customization through flexible technologies. At the same time, there is an increasing demand for skills in data analytics, software engineering, and cybersecurity.

A defining element is the horizontal and vertical integration of processes, ensuring connectivity across the value chain and between operational and managerial levels. Continuous data collection and analysis enable real-time process optimization and more efficient resource utilization.

The fundamental principles of Industry 4.0 include:

- interoperability between cyber-physical systems, equipment, and IT platforms;
- decentralized decision-making through autonomous equipment;
- real-time data analytics;
- virtualization and simulation of industrial processes;
- service orientation;
- modularity and scalability of infrastructures.

The application of these principles leads to increased productivity, resource optimization, defect reduction through virtual testing, and shorter time-to-market. However, implementation requires significant investments, workforce training, and the adoption of strict cybersecurity measures .

Expanded connectivity and the integration of industrial infrastructures with external networks increase the risk of cyberattacks. In this context, protecting data, control systems, and intellectual property becomes a strategic priority, and cybersecurity represents a core component of the Industry 4.0 ecosystem.

Industry 4.0 thus marks the transition from classical mechatronics to cyber-mechatronics, transforming traditional equipment into intelligent devices integrated within collaborative digital ecosystems. This transformation creates major opportunities for innovation and growth but requires technological and organizational approaches adapted to the complexity of modern industrial infrastructures.

3.1. IIoT – Industrial Internet of Things

The Industrial Internet of Things (IIoT) represents the extension of IoT concepts into the industrial environment by interconnecting equipment, sensors, and control systems to collect and analyze data for improving efficiency, productivity, and process safety. IIoT integrates intelligent sensors, advanced software platforms, automation solutions, and communication infrastructures, creating distributed and interdependent industrial networks.

Unlike IoT applications oriented toward consumer or commercial domains, IIoT must be adapted to the specific requirements of industrial environments. In this context, concepts such as IACS (Industrial Automation and Control Systems), SCADA, and CPS converge toward the implementation of Industry 4.0 principles through the integration of IT and OT domains within a unified operational framework [73–74].

The adoption of IIoT brings significant benefits, including predictive maintenance, energy optimization, and increased flexibility of production lines. Through real-time data analytics, operational deviations can be identified and unplanned downtime prevented. However, implementation also involves challenges related to interoperability, integration of legacy systems, and management of large data volumes.

IIoT extends beyond traditional IACS and SCADA functionalities by integrating cloud and edge computing infrastructures, transforming industrial equipment into intelligent nodes within cyber-physical systems. Applications are widespread in sectors such as automotive manufacturing, energy, and intelligent transportation, where real-time data analysis enables process optimization and cost reduction [75–76].

However, increased industrial connectivity expands the cyberattack surface. Security breaches may disrupt production continuity and compromise critical infrastructures. In this context, IIoT security requires network segmentation, robust authentication, encrypted communications, continuous monitoring, and the adoption of international standards such as ISA/IEC 62443.

Thus, IIoT becomes a strategic pillar of Industry 4.0, connecting and optimizing industrial ecosystems through the integration of intelligent devices and distributed digital infrastructures.

3.2 Chapter Conclusions

This chapter highlighted the profound transformation of the industrial environment generated by Industry 4.0, emphasizing how the integration of digital technologies, advanced communications, and interconnected infrastructures reshapes production processes and operational models.

The importance of the Industrial Internet of Things (IIoT), intelligent sensor networks, and interconnection platforms in the development and operation of mechatronic and cyber-physical systems was emphasized. These technological advances do not replace classical mechanical engineering principles but complement them with advanced functionalities that enhance the efficiency, flexibility, and resilience of modern industrial infrastructures.

4. CYBERSECURITY

Cybersecurity represents the set of technical, organizational, and managerial measures aimed at protecting information systems, networks, and data against unauthorized access and digital threats. According to NIST, it involves the prevention, protection, and restoration of information systems, ensuring confidentiality, integrity, and availability (the CIA triad). The ITU-T X.1205 standard defines cybersecurity as an integrated set of policies, practices, and technologies used to protect the cyber environment and organizational assets.

The CIA triad constitutes the foundation of any security system: confidentiality limits access to authorized entities, integrity ensures data correctness, and availability guarantees continuous access to resources. The implementation of these principles is achieved through technical, operational, and managerial controls with preventive, detective, and corrective roles.

At a strategic level, risk management is supported by methodological frameworks such as the NIST Cybersecurity Framework, structured around the functions of Identify, Protect, Detect, Respond, and Recover. This model provides a systematic approach applicable also to complex industrial infrastructures, where IT–OT convergence increases exposure to risks.

In the context of Industry 4.0, cybersecurity becomes an essential element of organizational governance and the resilience of cyber-mechatronic infrastructures, forming the foundation for the proactive measures presented in the experimental chapters of this work.

4.1 The Security Framework of IT Infrastructure

The IT infrastructure security framework is based on identifying threats, vulnerabilities, and protective measures required to maintain confidentiality, integrity, and availability (the CIA triad) [31]. The literature distinguishes two complementary perspectives: defensive and offensive. The defensive approach focuses on preventing and detecting incidents through technical and procedural controls (firewalls, IDS/IPS, monitoring, response plans), while the offensive approach aims to proactively identify vulnerabilities through reconnaissance techniques and attack surface assessment [31].

Social engineering remains a significant attack vector, exploiting the human factor through techniques such as phishing and pretexting [37–39]. Web applications are also frequent targets, with major risks summarized in the OWASP Top 10 (2021), including

broken access control, cryptographic failures, and security misconfigurations [40]. In this research, some of these methods were replicated in a controlled manner to demonstrate the progression from initial access to the expansion of control within the infrastructure.

A reverse proxy acts as an intermediary between clients and internal servers, providing infrastructure masking and traffic control. In an offensive context, it can facilitate the intermediation of C2 communications; countermeasures include outbound traffic monitoring, network segmentation, and certificate validation.

CVE (Common Vulnerabilities and Exposures) provides standardized identifiers for vulnerabilities and is used for patch management or for selecting appropriate exploits. Risk reduction requires timely updates and continuous monitoring of specialized vulnerability databases [79].

Pivoting refers to the use of a compromised system to access other internal resources and is typical in lateral movement scenarios. Mitigation involves strict segmentation, enforcement of the principle of least privilege, and multi-factor authentication.

4.2 The Cybersecurity Paradigm for Cyber-Mechatronic Systems

Industry 4.0 amplifies risks through increased connectivity, integration of intelligent devices, and the need for continuous communication between ecosystem components. A relevant framework proposes dividing cybersecurity into three major domains: IoT security, transport-layer security, and cloud security [54]. Within industrial infrastructures, SCADA systems remain critical for data collection and control, and attacks may target hardware, software, or communications, leading to control data alteration and/or process unavailability.

In practice, IoT/IIoT introduces additional challenges: limited visibility, platform diversity, long life cycles, and incomplete integration into IT controls, transforming these devices into major attack surfaces. Furthermore, IT–OT convergence exposes critical industrial mechanisms to threats similar to those in IT environments, but with significantly greater operational impact. Frequently used industrial protocols (e.g., Modbus, DNP3) may lack authentication or encryption capabilities, increasing exploitation risks, including zero-day scenarios. These aspects were validated experimentally through the demonstration of industrial infrastructure compromise originating from critical vulnerabilities, affecting the entire operational chain.

4.3 Vision/Perspective of Cybersecurity for Cyber-Mechatronic Systems

In Industry 4.0 environments, distinguishing between IT and OT becomes essential: although the general objective is safe and efficient operation, priorities differ. In IT, the CIA triad is centered on confidentiality, integrity, and availability; in OT, priority is given to availability and operational safety, and the direct application of IT measures in OT environments may generate operational risks [51]. IT–OT convergence and the emergence of IIoT require policies and controls adapted to industrial specificity, where maintenance windows, infrequent updates, and continuity requirements impose governance models different from classical IT environments [57].

To reduce risks, asset segmentation and segregation into zones are recommended, along with strict control of communications between zones and the use of a DMZ between enterprise and control zones, in accordance with best practices and standards (e.g., IEC 62443, ISO 27001/27002, NIST SP 800-82, NIST CSF). Control zones typically include supervisory levels (HMI/SCADA), basic control (PLC), safety zones (SIS), and process zones (sensors/actuators), and controlling information flows between them is critical for limiting attack propagation [43,45]. In this context, the role of SCADA and Historian components in logging and correlation becomes relevant for post-incident investigations [57]. Standardization of communications and adoption of end-to-end encryption, where feasible, contribute to increased resilience, particularly for IIoT devices [68].

4.4 Chapter Conclusions

This chapter highlighted that cybersecurity in Industry 4.0 must be treated as an integral part of industrial infrastructure operation, not merely as an IT issue. Differences in priorities and constraints between IT and OT require policies, architectures, and controls specifically adapted to industrial environments, with emphasis on segmentation, monitoring, and governance of critical processes.

Operational concepts such as reverse proxy, CVE consultation, and pivoting are relevant both for defensive analysis and for realistic simulation of attack scenarios, constituting direct links to the experimental stage of this research.

5. EXPERIMENTAL RESEARCH METHODOLOGY – ANALYZED INDUSTRIAL ARCHITECTURE

5.1 Research Methodology

This research aims to improve the cybersecurity of intelligent systems within Industry 4.0 by analyzing vulnerabilities arising from the integration of physical (hardware) and digital (software) components and by validating concrete protection measures applicable to real industrial infrastructures.

The experimental approach was conducted in two distinct stages, using an industrial infrastructure from the energy sector, effectively deployed in a production environment but adapted to laboratory scale to enable controlled vulnerability testing. The system uses renewable energy sources for self-consumption and for injecting electricity into the national grid, comprising conversion equipment, protection and control devices, and a central command and monitoring point.

In the first stage, the system architecture was documented and analyzed, focusing on network topology, hardware components, and software applications. The logical configuration and communication equipment were identical to those used in the real operational environment, the only difference being the simulation of field equipment (wind turbines and photovoltaic panels) through specialized sensors. This 1:1 correspondence enabled the identification and analysis of vulnerabilities within a realistic framework, without affecting critical infrastructure in operation.

The overall system architecture used in the research is illustrated in Fig. 5.1.1, highlighting the interconnection between IT and OT components and the implemented segmentation mechanisms.

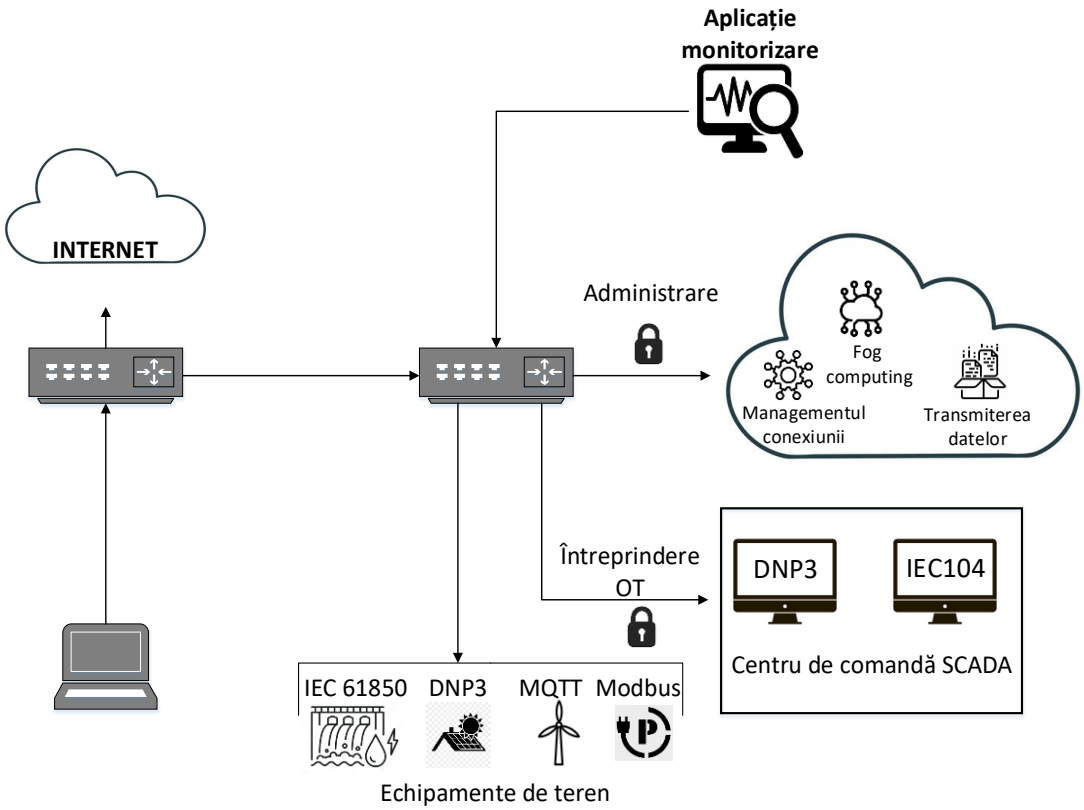

Fig. 5.1.1 General architecture of the intelligent system

The second stage of the research focused on the controlled identification and exploitation of vulnerabilities, followed by the development of a proactive set of measures aimed at strengthening cybersecurity. The identified vulnerabilities were analyzed and prioritized based on their impact on system availability and integrity, and the effectiveness of the proposed measures was validated through retesting.

In the analyzed environment, the OT infrastructure is completely isolated from the internet, adopting a classical protection model based on physical separation and strict access control. This configuration enables the assessment of the resilience of a real industrial infrastructure which, although isolated according to traditional security principles, remains exposed to risks generated by the controlled interaction between IT and OT zones.

5.2 Architectural Components Description

The analyzed architecture integrates IT and OT components interconnected through controlled filtering and segmentation mechanisms.

The IT zone includes the communication infrastructure for internet access and the administrator's workstation, which can access only the monitoring platform through an

interconnection device configured with Access Control Lists (ACLs), allowing only authorized traffic and reducing the exposure surface.

The operational zone (OT) represents the core of the infrastructure and includes:

- Siemens SIPROTEC 7SJ82 PLC, used for electrical network protection and control, compatible with standard industrial protocols and equipped with modern security mechanisms;
- RTU ES2000, deployed on the Cisco IOx platform, responsible for collecting and processing operational data and integrating SCADA communications;
- HMI, enabling system monitoring and control in both manual and automated modes;
- the Nagios XI platform, used to supervise equipment availability.
- The RTU is the central element of the ecosystem, ensuring interfacing between field devices, the PLC, and monitoring systems, as well as real-time visualization of operational parameters.

Although implemented at laboratory scale, the infrastructure replicates the architecture and segmentation mechanisms of the real production environment, supporting the external validity of the results and the extrapolation of conclusions to critical industrial infrastructures.

The originality of the research lies in testing cybersecurity within a real, fully functional industrial system under controlled experimental conditions, providing a relevant framework for resilience assessment and the formulation of operational security measures.

5.3 Chapter Conclusions

This chapter presented the experimental methodology and the industrial architecture used in the research, highlighting the applied nature of the approach and its direct correspondence with the real production environment in the energy sector.

The analysis demonstrated the importance of an integrated cybersecurity approach that considers the interdependence between physical and digital components. The 1:1 configuration between the test and operational environments forms the foundation of the subsequent experimental stages and supports the development of practical solutions for enhancing the resilience of mechatronic and cyber-physical systems used in critical infrastructures.

6. IDENTIFICATION AND EXPLOITATION OF VULNERABILITIES IN INDUSTRIAL INFRASTRUCTURE – EXPERIMENTAL RESEARCH

6.1. Current Research Context

Unlike traditional IT infrastructures, characterized by permanent Internet connectivity, industrial OT (Operational Technology) systems were historically designed to operate in isolation, with emphasis on operational continuity and physical security. This paradigm led to a distinct security culture in which cyber risks were often considered secondary.

The transition toward Industry 4.0 significantly alters this balance. The integration of physical systems with digital platforms, the use of remote communications, and interconnection with IT infrastructures considerably expand the attack surface. In OT environments, the impact of an incident is not limited to information loss but may directly affect critical physical processes, with consequences for production, equipment integrity, and personnel safety.

In this context, the research aimed to analyze the vulnerabilities of a real SCADA infrastructure through a controlled experimental methodology. A central element of the study is the non-technical attack vector represented by social engineering, integrated into a realistic compromise scenario. Although the literature frequently mentions phishing in attacks targeting ICS/SCADA infrastructures [60–61], detailed documentation of experimentally applied scenarios in such environments remains limited.

A well-known example is the 2015 attack on the Ukrainian power grid, where the initial vector was a spear-phishing email that ultimately led to SCADA system compromise [62–63]. Unlike that case, the infrastructure analyzed in this study was physically isolated from the Internet, and the experimental scenario relied on a controlled mechanism specifically designed to demonstrate vulnerability, without employing pre-existing complex malware.

The results highlighted that, even under strict segmentation and physical isolation conditions, the human factor remains a critical element in the security chain. Consequently, the research moved from theoretical analysis to applied experimentation by defining and implementing a dedicated methodology for vulnerability identification within a real industrial ecosystem.

6.2. Experimental Research Plan and Phases

The testing plan was designed to simulate, in a controlled environment, the typical steps of a potential attacker, without affecting the real operational infrastructure. The methodology combined established offensive security techniques with adaptations specific to the analyzed industrial environment, in order to achieve a comprehensive assessment of the attack surface.

The preliminary analysis indicated the absence of services directly exposed to the internet and the presence of strict network segmentation. Under these conditions, the initial access vector was identified at the human factor level, through social engineering scenarios, forming the basis for an experimental methodology focused on evaluating the resilience of the analyzed SCADA system.

The research stages covered the full chain of a potential attack:

1. Simulation of a Command and Control (CnC) infrastructure within a virtual testing environment.
2. Controlled delivery of an initial access vector via email to assess vulnerabilities related to the human factor.
3. Establishment of a reverse shell connection, adapted to architectural constraints (communication allowed only LAN → WAN).
4. Analysis of privileges and possibilities for escalation and lateral movement.
5. Security assessment of the monitoring application, including correlation with publicly documented vulnerabilities (CVE).
6. Use of compromised components as pivot points toward the operational zone.
7. Controlled compromise of the ES2000 RTU, demonstrating escalation from the IT zone to the OT environment.

The use of the reverse shell technique allowed compliance with existing segmentation policies, as the connection was initiated from within the infrastructure. This approach highlighted how traditional protection mechanisms can be bypassed by exploiting legitimate system behavior.

Through the succession of these stages, the research demonstrated a complete compromise chain specific to industrial environments, in which a peripheral entry point can become a pivot toward critical operational assets, clearly defining the real attack surface and the potential progression mechanisms.

6.3. Configuration of a Kali Linux Virtual Machine as a CnC Server

For the implementation of the experimental scenario, a Command and Control (CnC) infrastructure was configured and used exclusively in a controlled environment to evaluate the resilience of the analyzed industrial infrastructure. Its role was to receive connections initiated from within the internal network, in accordance with the existing security policy that explicitly prohibited connections from the public environment to the LAN.

The CnC server role was assigned to a virtual machine running Kali Linux, a distribution specialized in penetration testing. The system was deployed within a laboratory-compatible virtualization environment, using static IP addressing to ensure experimental stability and repeatability (Fig. 6.3.2).

The server was configured in passive mode (listener), without initiating connections toward the target infrastructure, in line with the segmented architecture of the system, where communication is allowed exclusively LAN → WAN.

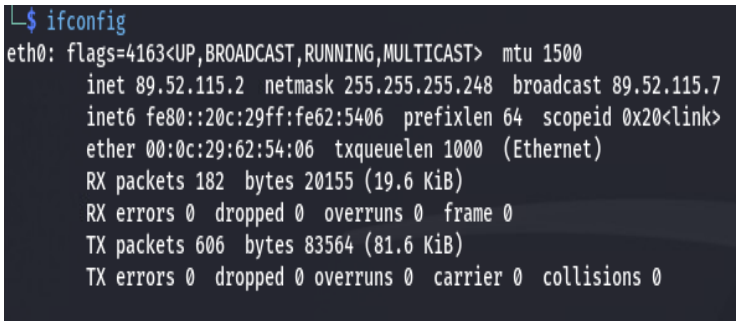

Fig. 6.3.2 CnC server configuration

To simulate a realistic scenario, the server was set to accept TCP connections on a port commonly associated with secure traffic and frequently allowed by industrial firewalls. The listening mode was initialized using a dedicated network utility (Fig. 6.3.3), enabling monitoring of connections and bidirectional data flow.

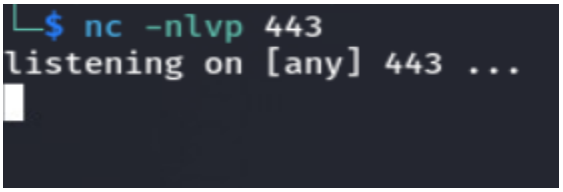

Fig. 6.3.3 Opening port 443 on the CnC server

This stage provided the necessary infrastructure to validate the initial compromise and demonstrated that, under unidirectional segmentation conditions, a controlled connection initiated from within represents a feasible communication vector.

6.4 Phishing Attack and Reverse Shell Connection

Following the analysis of the industrial infrastructure, no services directly exposed to the Internet were identified, and the implemented security policy prohibited connection initiation from the public environment toward the internal network. Under these conditions, the realistic initial access vector was identified as the human factor.

To validate this hypothesis, a spear-phishing attack was designed and directed at the SCADA infrastructure administrator. The transmitted message had a credible professional context, and the attached Microsoft Word document contained an automated mechanism capable of initiating a reverse shell connection upon opening.

A reverse shell is a technique whereby the compromised system initiates a connection to an external server, enabling remote access through a bidirectional channel. The choice of this method was determined by the segmented architecture of the infrastructure, where communication was permitted exclusively from LAN to WAN.

Upon opening the document and enabling its content, the embedded mechanism triggered the execution of a process that initiated a connection to the previously configured Command and Control server. At the moment the connection was established, an active session was registered on the CnC server, confirming the compromise of the administrator's workstation (Fig. 6.4.6).

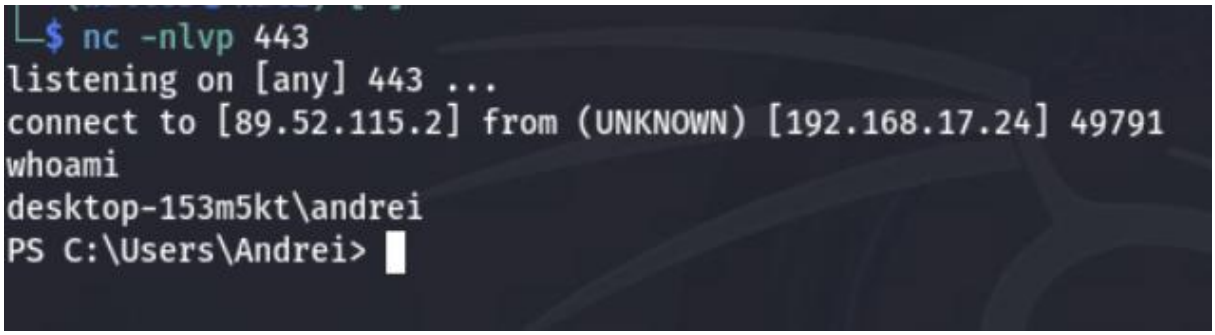

Fig. 6.4.6 Establishment of the reverse shell connection

This stage represented the critical point of the experimental scenario, demonstrating that physical isolation of the infrastructure does not eliminate compromise risk when human interaction with the external environment is possible. The established connection provided system-level access and created the premise for subsequent analysis of network configuration and relationships between IT and OT segments.

6.5 Investigation of Privileges and Connections to Mechatronic Systems

The access obtained to the administrator workstation's command line confirmed the initial compromise; however, it proved insufficient for a comprehensive infrastructure analysis due to the absence of a graphical interface and limitations in using advanced Linux-based tools.

To extend visibility into the internal network, a proxy tunneling mechanism was implemented using the open-source utility Chisel. The objective was to redirect traffic through the compromised workstation so that scans and queries would appear to originate from within the infrastructure.

Chisel was configured in a server–client architecture: the server ran on the Command and Control infrastructure, while the client was deployed on the compromised workstation using reverse tunneling, exposing a SOCKS5 proxy on the C2 server. The client activation is illustrated in Fig. 6.5.4.

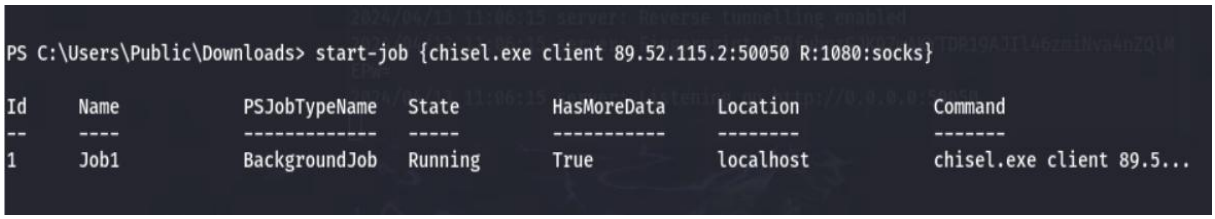

Fig. 6.5.4 Proxy client activation on the workstation

By establishing the SOCKS5 tunnel, traffic generated from the Linux environment was redirected through the administrator's workstation, enabling bypass of firewall and ACL restrictions without modifying existing policies.

Scans performed through the proxy led to the identification of an active web service within the internal segment (192.168.1.10). Accessing this service by redirecting browser traffic enabled interaction with the web interface of the Nagios XI monitoring platform (Fig. 6.5.8).

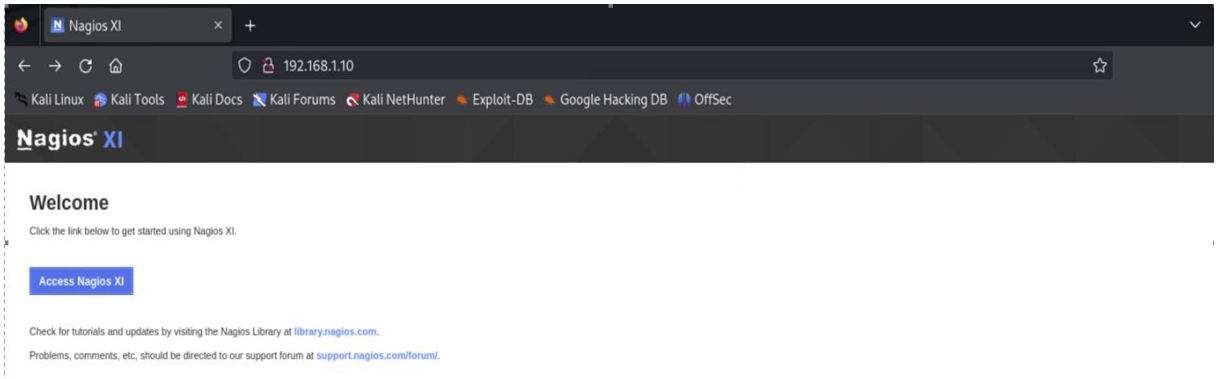

Fig. 6.5.8 Accessing the monitoring platform

This stage demonstrated that, by combining tunneling and traffic redirection techniques, critical internal resources can be accessed within a logically segmented infrastructure. Identifying Nagios XI as a point of interconnection between the IT and SCADA zones highlights the potential role of monitoring systems as pivot nodes between otherwise separated domains.

From a methodological perspective, the results confirm that strict segmentation and physical isolation do not completely eliminate the risk of lateral propagation when intermediary systems operate at the intersection of IT and OT domains.

6.6. Testing the Compromise of Credentials of the Application Monitoring Mechatronic Systems

After identifying the Nagios XI application as the interconnection point between the IT infrastructure and the SCADA zone, the next stage focused on evaluating the authentication mechanism. Initial testing excluded the presence of default credentials, requiring the application of an active method to assess password robustness.

To simulate a realistic compromise scenario, a specialized authentication testing tool was used to automate the verification of username–password combinations by repeatedly sending HTTP POST requests and analyzing the server responses. The methodology included identifying the authentication endpoint, defining a controlled set of potential users, and employing a restricted dictionary of likely passwords.

Controlled testing resulted in the identification of a valid combination with administrative privileges, enabling full access to the Nagios XI interface. This outcome highlights the vulnerability of systems that do not enforce strict password complexity policies and login attempt limitations.

The compromise of Nagios XI represented a critical moment in the research, as the platform functions as a node of interconnection between the IT zone and the SCADA infrastructure. Figure 6.6.1 illustrates the progression of the compromise: the administrator workstation, the proxy tunnel, and the monitoring application.

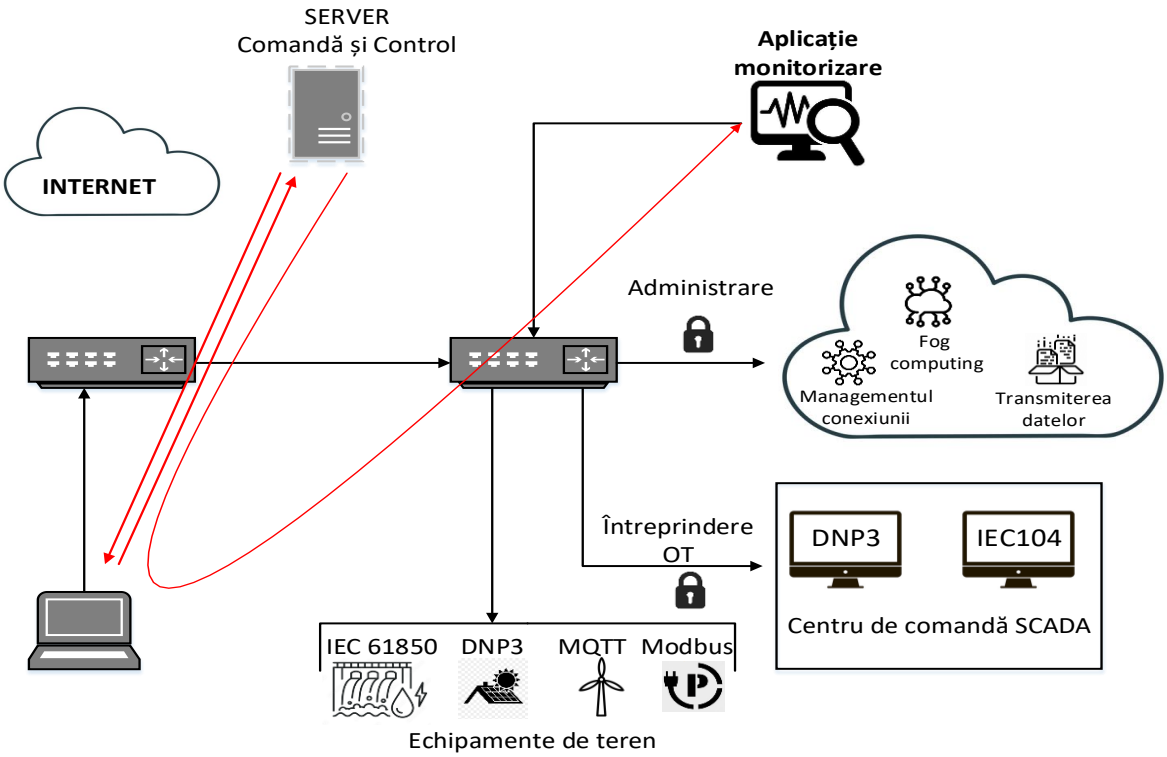

Fig. 6.6.1 First version of the general architecture of the intelligent system updated with the compromised points

The obtained access enabled:

1. Administrative control over the monitoring platform;
2. Visibility into monitored equipment and services;
3. The basis for lateral propagation toward the operational zone.

From a scientific perspective, this stage confirms that monitoring systems can become critical pivot points in interconnected IT–OT architectures when robust authentication mechanisms are not implemented.

6.7. Identification and Exploitation of Vulnerabilities in the Application Monitoring Mechatronic Systems

After obtaining administrative access to Nagios XI, the analysis continued with the identification of the installed version (5.7.4) and the verification of publicly documented vulnerabilities. Initial tests did not reveal any direct exploitation paths, therefore the version was correlated with public vulnerability databases.

A query in the Exploit Database identified an exploit applicable to versions 5.7.x, enabling remote code execution (RCE) under valid authentication conditions, by exploiting the plugin upload mechanism.

In a standard IT environment, applying the exploit is straightforward. However, in the analyzed infrastructure, the application was isolated from the Internet, which required the design of an indirect communication route to establish a reverse connection to the Command and Control server, without modifying the existing segmentation policies.

For this purpose, a traffic redirection mechanism was implemented through the administrator workstation, which functioned as an intermediary between Nagios XI and the C2 server. In the final configuration:

1. Nagios XI initiated the connection to the administrator workstation;
2. the workstation redirected the traffic to the C2 server;
3. the C2 server established the command session.

The reverse connection was successfully established through the configured mechanism, confirming the compromise of the application and the possibility of executing code within its context.

Figure 6.7.11 presents the updated system architecture, highlighting the sequentially compromised points and the resulting data flow.

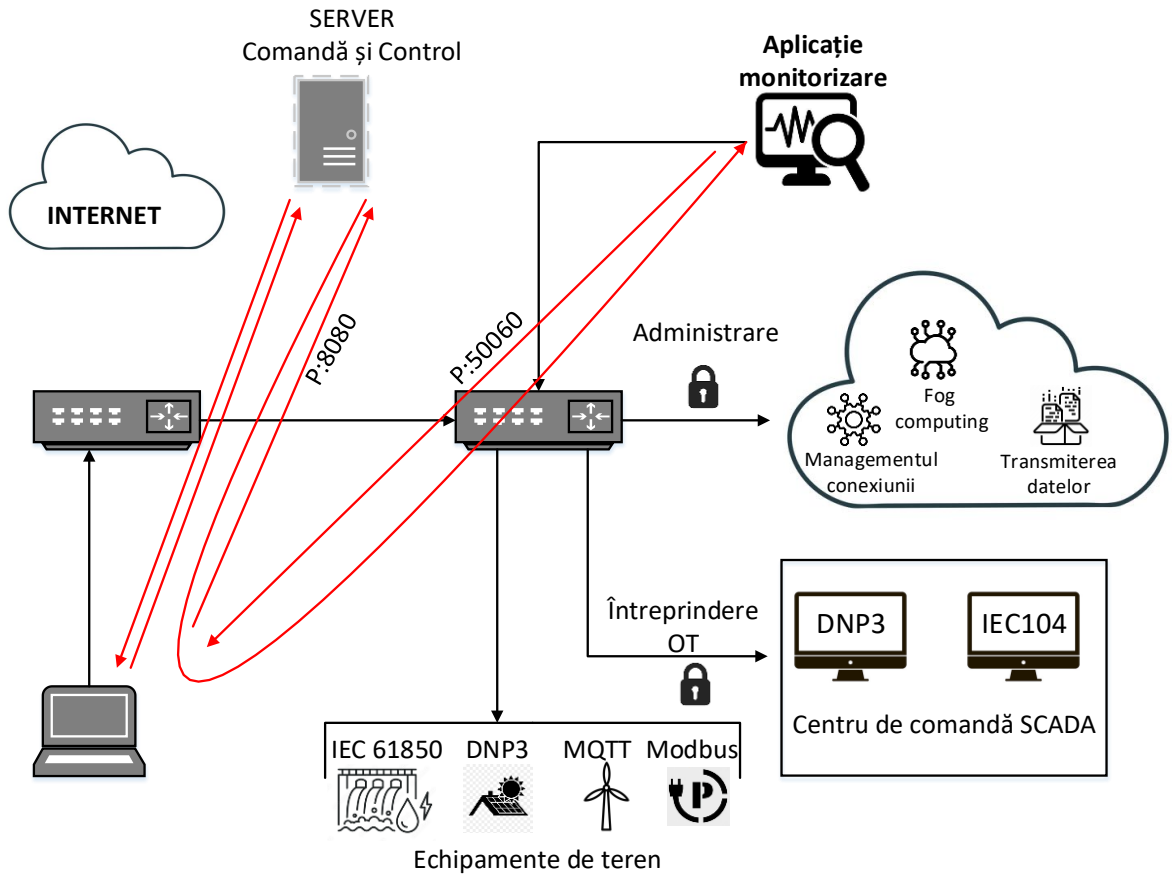

Fig. 6.7.11 Second version of the general architecture of the intelligent system updated with the compromised points

This stage demonstrates that:

1. A legitimate monitoring service can become a pivot point between IT and SCADA domains.
2. Physical and logical segmentation do not fully eliminate the risk of indirect access through administrative nodes.
3. Public exploits can be adapted to restrictive industrial environments through controlled tunneling architectures.

From a methodological perspective, the main contribution lies in integrating a public exploit into a real industrial scenario by designing a communication route compatible with the existing architectural constraints. The results confirm that monitoring platforms represent critical elements in OT security and require additional segmentation and auditing measures.

6.8. Compromise of the RTU

The analysis of the overall infrastructure architecture revealed that systems within the SCADA zone accept traffic exclusively from the monitoring application, while any other type of communication is filtered at the network segmentation level. This configuration, typical of industrial environments with strict IT–OT separation, significantly limits the direct attack surface but concentrates risk at administrative interconnection points.

To evaluate the resilience of SCADA components without modifying existing policies, a pivoting mechanism was implemented by using the Nagios XI application as a legitimate intermediary. By configuring a proxy tunnel between the Command and Control (C2) server and the monitoring platform, external traffic was redirected so that, from the SCADA infrastructure's perspective, the source appeared to be the monitoring application itself. This approach enabled testing activities to be conducted as if they were initiated from within the OT domain.

After establishing the indirect communication channel, operations were initiated to identify active services within the SCADA segment. The RTU web interface was detected, exposed on port 8443 and using the WebSocket protocol for bidirectional message exchange, becoming the focal point of the analysis.

To investigate the authentication mechanism and data flow, Burp Suite was configured to intercept HTTP/HTTPS and WebSocket traffic. Initial tests involved deliberately entering incorrect credentials in order to analyze packet structure and server responses. Although

authentication was correctly rejected, the analysis enabled the identification of the JSON message structure used in bidirectional communication.

The decisive stage consisted of manually transmitting, through the Repeater module, specific JSON messages outside a valid authentication flow. Requests associated with internal application functionalities—such as subscribing to data streams or requesting internal resources—were tested. The manipulation of messages is illustrated in Fig. 6.8.10.

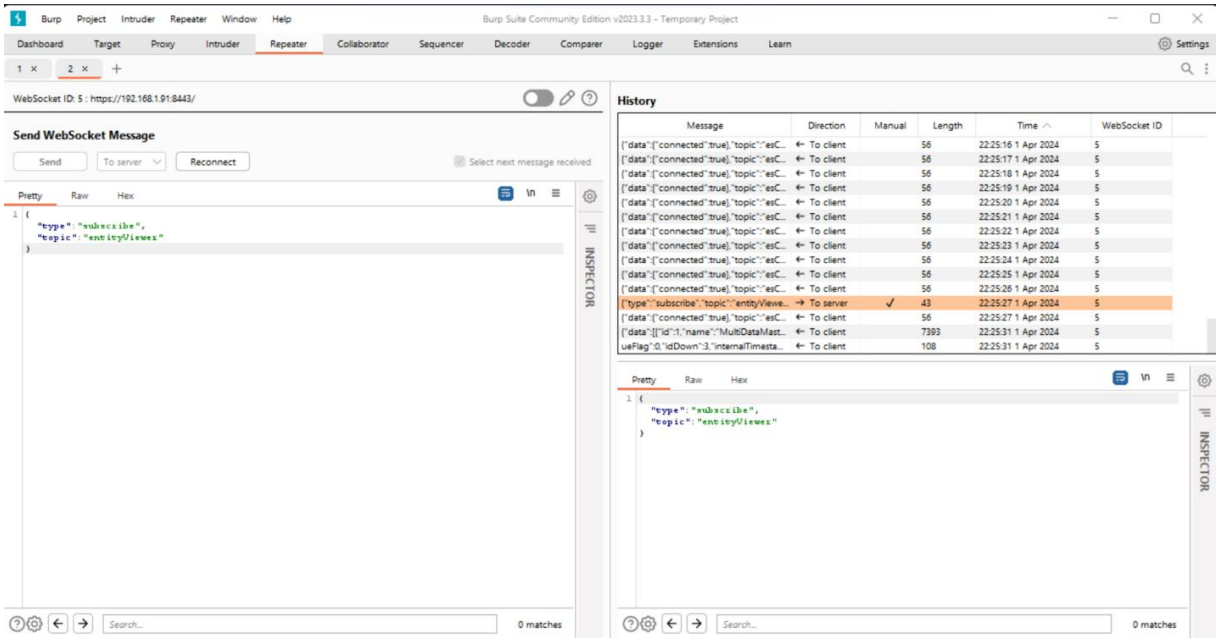

Fig. 6.8.10 Manipulation of the JSON *entityViewer* message

Analysis of server responses revealed that certain requests were processed without verifying the existence of an authenticated session. The server returned application content and allowed access to internal functionalities, treating the connection as legitimate. This confirms the existence of a critical vulnerability in WebSocket message validation, enabling authentication bypass.

The exploitation went beyond informational access. By modifying parameters within the JSON message structure, commands were transmitted to the infrastructure controlled by the RTU. Under normal conditions, such commands are generated exclusively through the legitimate user interface and validated through internal authentication and authorization mechanisms. In the tested scenario, message manipulation allowed the direct transmission of a command to change the state of an electrical circuit.

The standard operational flow involves transmitting commands from the user to the RTU, then to the HMI, and subsequently to the PLCs responsible for field execution. Through

manipulation of WebSocket messages, this flow was influenced without following the legitimate authentication process, resulting in a change in the state of the monitored circuit.

Figure 6.8.16 highlights the direct effect of the forged command, namely the closing of the electrical circuit.

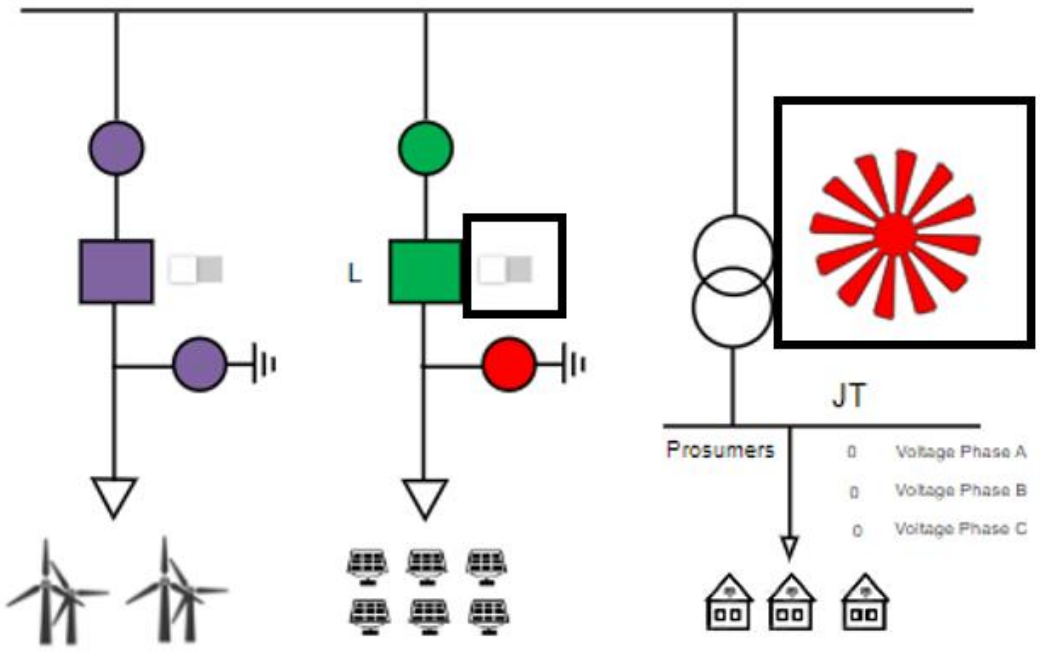

Fig. 6.8.16 – Closing of circuits after packet falsification

This stage confirms that the identified vulnerability enables not only access to data or configurations, but also intervention in the physical process controlled by the SCADA infrastructure. The impact is significant, demonstrating the possibility of modifying the state of industrial equipment by exploiting an IT–OT interconnection point and a validation flaw at the application level.

From a methodological perspective, the result validates the research hypothesis that monitoring systems and associated web interfaces can become strategic pivot points within segmented architectures. Although physical and logical segmentation were respected, the presence of an administrative node with a dual role (IT monitoring and SCADA access) enabled controlled extension of access into the operational zone.

The results of this stage constitute the central element of the experimental contribution, demonstrating, under controlled conditions, the possibility of bypassing authentication and achieving direct impact on physical infrastructure without altering security policies and without direct Internet access to the SCADA zone.

6.9 Impact and Resilience Assessment of the Industrial Infrastructure

The results of the experimental research confirm that intelligent industrial infrastructures, even when designed with physical isolation and strict logical segmentation, are not inherently protected against advanced cyberattacks. Through the phased application of active testing methods, it was demonstrated that a complete compromise chain can be constructed, starting from the IT infrastructure and extending to operational equipment controlled by RTUs and PLCs.

The most significant impact of the research lies in obtaining functional control over the production infrastructure through the successive exploitation of seemingly isolated vulnerabilities: compromise of the administrator workstation, pivoting through the monitoring application, exploitation of the RTU WebSocket mechanism, and injection of commands into the operational flow. The integration of these stages into a coherent scenario demonstrated that minor vulnerabilities, when strategically combined, can produce major effects on industrial processes.

The compromise of the RTU web interface represents the critical point of the research, validated by the certificate issued by the manufacturer (EEBDM-235865430-1059 / 21.08.2025). The implemented scenario demonstrated the possibility of bypassing authentication mechanisms and transmitting direct commands to the physical infrastructure, without direct Internet access and without altering existing segmentation policies. This outcome highlights the vulnerability of IT–OT interconnection points and the need to treat monitoring applications as critical security elements.

The impact assessment reveals potentially significant consequences:

- modification of electrical circuit states;
- access to and exfiltration of operational databases;
- compromise of credentials and configuration parameters;
- disruption of industrial process continuity.

In this context, infrastructure resilience becomes a central element of industrial cybersecurity. Resilience should not be limited to post-incident recovery, but integrated as an active mechanism encompassing anomaly detection, rapid isolation of compromised components, preservation of critical functions, and controlled system restoration. Adaptive segmentation, continuous traffic monitoring, and periodic auditing of IT–OT data flows represent essential measures for mitigating similar attacks.

The research demonstrates that simple physical or logical isolation is insufficient in modern Industry 4.0 architectures. Security must be designed in correlation with resilience, and industrial infrastructures must be engineered to anticipate partial compromise and maintain controlled operation even in the presence of breaches.

6.10 Chapter Conclusions

This chapter represents the central applied component of the research, demonstrating, within a real industrial infrastructure, the possibility of progressively compromising a SCADA system through the correlation of multiple attack vectors. The fundamental stages of an advanced attack were validated: initial access, pivoting, escalation, exploitation, and operational impact.

The results confirm that IT–OT interconnection introduces critical points that can be exploited even under strict segmentation conditions. Monitoring applications and administrative interfaces represent strategically sensitive areas capable of serving as channels for extending access into the operational domain.

The research highlights the need for an integrated approach to industrial security, in which prevention, detection, and resilience operate in a complementary manner. Traditional protection measures must be complemented by proactive testing, auditing, and incident simulation mechanisms, as well as by clearly defined response and recovery policies.

By experimentally validating a complete compromise scenario, the dissertation provides an applied model for assessing the security of intelligent industrial infrastructures and lays the foundation for developing modern defense strategies tailored to critical environments.

7. ENHANCING THE CYBERSECURITY OF AN INTELLIGENT MECHATRONIC SYSTEM IN INDUSTRY 4.0

7.1. Identification and Characterization of the Critical Vulnerability in RTU ES2000

The experimental phase led to the identification of a critical vulnerability in the RTU ES2000, a core component of the SCADA infrastructure. Analysis of the WebSocket communications between the web interface and the backend revealed the absence of an authentication mechanism for certain JSON messages transmitted through port 8443.

Testing was performed using a Python script developed within the research, which initiated direct WebSocket connections and transmitted messages such as:

- {"type":"downloadDatabase"}
- {"type":"subscribe","topic":"entityViewer"}
- {"type":"logs"}

The server processed these messages without validating the user's identity, providing sensitive data and granting access to internal functionalities. The vulnerability also allowed unauthorized command transmission to infrastructure controlled by the RTU and PLCs.

The identified breach is not publicly documented and has no associated CVE. Official validation was confirmed through certificate EEBDM-235865430-1059 (21.08.2025, Annex 1). The contribution of this work lies in the identification, controlled exploitation, and responsible disclosure of this vulnerability within a real industrial environment.

7.2. Operational Consequences and Infrastructure Implications

The identified vulnerability has direct implications for the operation of the industrial infrastructure. The lack of authentication in WebSocket message processing enables unauthorized intervention in operational data and processes.

Potential impact includes:

- downloading the system database;
- accessing logs and internal information;
- modifying the state of electrical circuits;
- disrupting the continuity of industrial processes.

Testing practically demonstrated the possibility of transmitting commands to the physical infrastructure, highlighting the direct link between an application-layer vulnerability and its effects on equipment controlled by PLCs and RTUs.

The results confirm that network segmentation and logical isolation are insufficient in the absence of robust authentication and application-level validation mechanisms, particularly within IT–OT architectures specific to Industry 4.0.

7.3. Proactive Measures for Improving the Security of Mechatronic and Industrial Infrastructures

To strengthen security, proactive measures were defined, aimed at reducing the attack surface and increasing operational resilience through integrated technical and organizational actions.

1. Responsible Disclosure and Technical Remediation

The vulnerability was reported to the manufacturer through a responsible disclosure process. The implemented corrective measure consists of a session token generated at authentication and validated through an initial WebSocket handshake, rejecting connections without a valid token. The same mechanism is applied to HTTPS interfaces.

Certificate EEBDM-235865430-1059 confirms the practical impact of the research and its direct contribution to strengthening the security of the application.

2. Strengthening the Human Factor

The experimental scenario demonstrated that the initial vector can be non-technical (email interaction). Continuous staff training is therefore required regarding phishing awareness, handling of macro-enabled documents, and risks associated with monitoring applications. Periodic evaluations and controlled exercises should transform the human component into an active detection and early response mechanism [51].

3. Integration of a Specialized OT Solution – Cisco Cyber Vision

Cisco Cyber Vision was integrated for automatic asset inventory, industrial topology visualization, and correlation with CVE databases. The platform was deployed as a virtual machine, with non-intrusive (out-of-band) integration based on mirrored traffic, ensuring operational continuity.

The analysis identified an additional vulnerability—CVE-2023-20076 (CVSS v3.1 score 7.2), associated with the Cisco IOx environment, with potential command execution under certain access conditions.

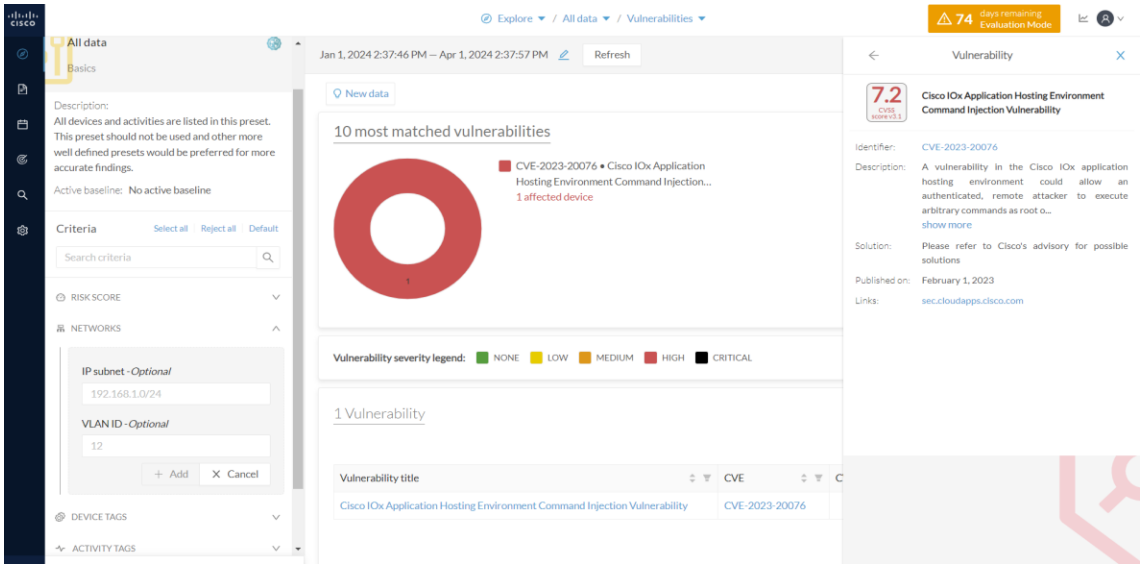

Fig. 7.3.3 Identification of CVE for the router-type equipment

According to the manufacturer's recommendations, remediation is achieved by applying official patches [53].

The identification of this CVE confirms that risks may arise across multiple components of the operational chain, requiring distributed and correlated defensive measures.

By combining responsible disclosure, targeted staff training, and the integration of a specialized OT detection solution, this section outlines practical measures directly applicable to the analyzed infrastructure, contributing to the security and resilience of the SCADA ecosystem.

7.4 Chapter Conclusions

This chapter highlights that cybersecurity in mechatronic and industrial infrastructures must be addressed through an integrated approach, correlating technical, organizational, and educational measures. The identification and systematic treatment of critical vulnerabilities represent the starting point for reducing the attack surface and enhancing operational resilience.

The research contributed through: direct collaboration with the manufacturer to remediate the identified vulnerability, strengthening the human component through industry-specific training, and integrating a specialized OT monitoring solution (Cisco Cyber Vision) for automated detection and risk correlation.

Overall, the chapter confirms that protecting intelligent infrastructures requires a proactive strategy focused on prevention, continuous monitoring, and operational resilience.

8. GENERAL CONCLUSIONS, ORIGINAL CONTRIBUTIONS AND FUTURE RESEARCH DIRECTIONS

8.1 General Conclusions

This dissertation analyzed cybersecurity in the context of Industry 4.0, with emphasis on SCADA infrastructures, IIoT, and IT–OT convergence. The theoretical framework highlighted the transition from isolated industrial architectures to integrated digital ecosystems and the risks associated with interconnection, in alignment with established standards such as the NIST Cybersecurity Framework and ISO/IEC 27001.

The research demonstrated that IT–OT integration, while generating significant operational benefits, expands the attack surface and requires a unified security approach addressing the entire digital–operational chain. In such environments, cybersecurity must be treated as a continuous process combining technical controls, organizational policies, and adaptive responses to evolving threats.

To validate these premises, the theoretical concepts were implemented within an experimental framework conducted on a real industrial infrastructure characterized by strict IT–OT segmentation and air-gap policies. The methodology reproduced the stages of a realistic attack chain, from initial access to impact assessment on operational components, demonstrating the feasibility of controlled compromise of mechanisms considered robust.

The results confirm that a vulnerability exploited in the IT domain may serve as a pivot toward critical OT resources, reinforcing the need for integrated security strategies complemented by detection, response, and rapid recovery capabilities. In conclusion, the dissertation validates the hypothesis that intelligent industrial systems must be secured through a holistic approach integrating architectural segmentation, proactive monitoring mechanisms, and continuous staff training.

8.2 Original Contributions

The starting point of the scenario consisted of integrating the human factor within a real industrial architecture by delivering a spear-phishing email to the SCADA administrator containing a malicious Word document with VBA macros. The macro was designed to initiate a reverse shell connection to a Command and Control (CnC) server, adapted to SCADA architectural constraints by configuring Netcat in listener mode on port 443. Using this port—

commonly associated with legitimate HTTPS traffic—allowed the generated communication to blend into permitted LAN→WAN flows, reducing detection probability.

Although Office macros and reverse shells are widely documented in cybersecurity literature, they are typically presented in generic penetration-testing contexts. The contribution of this research lies in deliberately adapting this mechanism to a segmented SCADA infrastructure, demonstrating the practical operationalization of a theoretical attack vector in a real industrial environment.

Building on the initial access channel, an advanced tunneling mechanism was implemented using Chisel to deploy a SOCKS5 proxy through the administrator's workstation. This architecture enabled traffic origin obfuscation and simulation of legitimate internal flows, allowing controlled traversal of IT–OT segmentation and air-gap policies.
Within this framework, Nmap was integrated through the SOCKS5 tunnel created with Chisel, enabling reconnaissance activities in a real SCADA environment without altering firewall or ACL rules. The novelty does not lie in the use of the tool itself, but in its integration into a proxy-chaining architecture tailored to a restrictive industrial network.

The infrastructure analysis led to the identification of Nagios XI as the unique interconnection node between the IT domain and SCADA. Its controlled compromise validated the hypothesis that monitoring platforms may act as strategic pivot points within segmented architectures.

Another original contribution consists in adapting and deploying a public exploit for Nagios XI in a real industrial context through a traffic redirection architecture based on Socat, Netcat, and Chisel. The implementation of a synchronized reverse proxy mechanism enabled exploit execution under restrictive segmentation constraints, without explicitly violating network policies.

The critical stage of the research involved the controlled compromise of the RTU ES2000. Using Burp Suite, WebSocket traffic was intercepted and manipulated, with legitimate JSON structures reproduced and altered to bypass authentication mechanisms and transmit commands directly to the infrastructure controlled by the RTU and PLCs. Transposing this technique into a real segmented SCADA environment represents a significant methodological contribution.

The identification of a previously undocumented vulnerability in the WebSocket authentication mechanism of the RTU ES2000, without an associated CVE identifier, constitutes the central contribution of the dissertation. The finding was officially validated by

the manufacturer through certificate EEBDM-235865430-1059 (21.08.2025, Annex 1), providing distinct scientific and practical relevance.

The experimental process was completed through responsible disclosure and the integration of the CyberVision platform for validation of defensive measures and real-time impact assessment, transforming controlled exploitation into an applied model for strengthening industrial cybersecurity.

8.3 Future Research Directions

The obtained results create the foundation for developing a standardized proactive audit framework for SCADA infrastructures based on realistic penetration scenarios and resilience assessment. The proposed methodology—structured around reconnaissance, tunneling, pivoting, and controlled exploitation—can evolve into an iterative process applied periodically to identify and remediate emerging vulnerabilities.

In the medium and long term, extending this methodology to other SCADA architectures with different technological and operational characteristics could generate a comparative portfolio of case studies, supporting the identification of recurring vulnerability patterns and the development of cross-sector best practice guidelines.

A practical outcome of the research is reflected in the response of the RTU manufacturer, who implemented authentication and communication validation improvements following vulnerability disclosure. This experience highlights the importance of continuous collaboration between industrial operators, equipment manufacturers, and cybersecurity experts to enable early identification and remediation of critical vulnerabilities.

Leveraging the research results through integration into operational policies and proactive audit programs can transform the validated experimental scenarios into recurring prevention and optimization tools. Thus, the developed methodology moves beyond a purely academic exercise and becomes a practical resource supporting the resilience of critical infrastructures and contributing to a more secure industrial ecosystem based on real information sharing and replication of effective solutions across sectors.

8.4 Synthesis of Original Contributions

1. I analyzed the industrial infrastructure and identified the administrator’s workstation as the sole Internet access point and primary compromise vector, integrating social

engineering as a non-technical risk factor in a realistic experimental scenario and demonstrating human-factor vulnerability even in physically isolated environments.

2. I adapted the reverse shell technique to the analyzed industrial infrastructure by configuring the CnC server on port 443 with a passive listener mechanism, demonstrating that a well-known method can be calibrated to comply with LAN→WAN constraints and bypass strict security policies.
3. I designed and executed a targeted phishing scenario against the SCADA administrator by developing a malicious macro-enabled Word document tailored to the analyzed industrial infrastructure, used to initiate a reverse shell connection to the C2 server.
4. I implemented a SOCKS5 proxy tunnel using Chisel between the C2 server and the administrator's workstation, masking traffic origin and simulating legitimate internal flows, demonstrating adaptability to critical network constraints.
5. I used Nmap in combination with the SOCKS5 tunnel created with Chisel, adapting reconnaissance techniques to the industrial infrastructure and bypassing firewall and ACL restrictions in a controlled manner.
6. I identified Nagios XI as the unique interconnection node between IT and SCADA and compromised it through a brute-force attack, highlighting the critical importance of transition segments and credential management.
7. I identified and exploited a public vulnerability in Nagios XI within the industrial infrastructure by constructing a communication chain based on Socat, Netcat, and Chisel, integrating reverse tunneling and proxying mechanisms.
8. I identified the RTU ES2000 as a critical OT component through pivoting techniques via Nagios XI, extending visibility and access without breaching existing segmentation policies.
9. I adapted Burp Suite to analyze and manipulate WebSocket traffic generated by the RTU, intercepting authentication-related communications and demonstrating that IT security tools can be calibrated for industrial environments.
10. I identified a previously undocumented vulnerability in the WebSocket authentication mechanism of the RTU ES2000, validated by the manufacturer through certificate EEBDM-235865430-1059, confirming the originality and scientific value of the research.

11. I integrated a recognized cybersecurity solution into a real industrial infrastructure through a complete methodology of installation, configuration, and validation, demonstrating its practical applicability with the support of the CyberVision platform.

DISSEMINATION OF RESULTS

A significant part of the results obtained within this dissertation has been disseminated through the publication of scientific articles in peer-reviewed journals. These publications confirm the quality and originality of the contributions made, addressing both theoretical aspects and applied solutions in the fields of cybersecurity and Industry 4.0. Through these works, the research findings have become accessible to the scientific community and may serve as a foundation for further development and in-depth studies.

The publication of these articles has also contributed to increasing the international visibility of the addressed topic, providing the opportunity to compare the obtained results with other research in the field. By integrating these works into specialized journals, the research has facilitated the exchange of ideas and best practices among scholars, fostering new research directions and establishing collaborative links in the areas of Industry 4.0 and cybersecurity.

The published articles are:

2. Berindei, Adelin-Marian; Ilie, Cristinel; Badea, Florentina, *The Cyber Security Paradigm in Industry 4.0*, International Journal of Mechatronics and Applied Mechanics, Issue 13, 2023, pp. 226–229, e-ISSN: 2559-6497, DOI: 10.17683/ijomam/issue13.27; -

2. Berindei Adelin-Marian, *Cyber Security for Smart System in Industry 4.0*, International Journal of Mechatronics and Applied Mechanics, Issue 9, 2021, pp. 182–185, e-ISSN: 2559-6497, DOI: 10.17683/IJOMAM/ISSUE9.26;

3. Albei, Victor-Eduard; Ilie, Cristinel; Popa, Marius; Tănase, Nicolae; Ovezea, Dragoș; Constantin, Alexandru; Nedelcu, Adrian; Berindei, Adelin-Marian, *The Implementation of a Highly Configurable Control Standard in the Development of a Robotics Platform for the Inspection of Confined Spaces*, *International Journal of Mechatronics and Applied Mechanics*, Issue 13, 2023, pp. 7–15, e-ISSN: 2559-6497, DOI: 10.17683/ijomam/issue13.1;

REFERENCES

1. *** Politehnica University of Bucharest, Intelligent Control Systems, available at: http://acs.pub.ro/doc/master/ro/short_description/SIC-short-ro.pdf, accessed on 12.01.2020.

3. *** Cisco Networking Academy, Introduction to IoT – online course, available at: www.netacad.com, accessed in March 2022.

4. *** Wikipedia, Mechatronics, available at: https://ro.wikipedia.org/wiki/Mecatronică, accessed in June 2021.

9. Rawat, Danda B.; Rodrigues, Joel J.P.C., *Cyber-Physical Systems: From Theory to Practice*, CRC Press, 2015, ISBN 978-1-4822-6303-1.

10. Bolton, W., *Mechatronics: Electronic Control Systems in Mechanical and Electrical Engineering*, 6th Edition, Pearson, 2015, ISBN 978-1-292-07407-9.

13. David H. Wolpert; Bruce Tidor, *Introduction to Cyber-Physical Systems*

14. Gaddadevara Matt Siddesh; G. N. Kodanda Ramaiah; K. Srujan Raju, *Cyber-Physical Systems: A Computational Perspective*, CRC Press, 2021. ISBN 978-0367643264.

21. B.K. Tripathy; J. Anuradha, *Internet of Things (IoT): Technologies, Applications, Challenges and Solutions*, CRC Press, 2017. ISBN 978-1-138-30905-3.

23. Kagermann, Henning; Lukas, Wolf-Dieter; Wahlster, Wolfgang, Industrie 4.0: Smart Manufacturing for the Future, Acatech STUDY, 2013.

31. P.W. Singer; Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, Oxford University Press, 2014. ISBN 978-0199918096.

37. Peter Kim, *The Hacker Playbook 3: Practical Guide to Penetration Testing*, Secure Planet, 2018. ISBN 978-1980901754.

38. Thomas A. Johnson, *Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare*, CRC Press, 2015. ISBN 978-1498703267.

39. Christopher Hadnagy, *Social Engineering: The Science of Human Hacking*, Wiley, 2018. ISBN 978-1119433385.

40. *** *OWASP Top Ten Project, available at: https://owasp.org/www-project-top-ten/*, accessed between *September 2023 – January 2024*.

43. ***NIST SP 800-82r2, available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf, downloaded in October 2023.

45. Pascal Ackerman, *Industrial Cybersecurity: Efficiently secure critical infrastructure systems*, Packt Publishing, 2017. ISBN 978-1788394512.

51. Berindei, Adelin-Marian; Ilie, Cristinel; Badea, Florentina, *The Cyber Security Paradigm in Industry 4.0, International Journal of Mechatronics and Applied Mechanics*, Issue 13, 2023, pp. 226–229.

53. *** *Cisco Security Advisory – IOx, available at: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-8whGn5dL, accessed on 20.02.2024*.

54. Berindei, Adelin-Marian, *Cyber Security for Smart System in Industry 4.0, International Journal of Mechatronics and Applied Mechanics*, Issue 9, 2021, pp. 182–185.

57. K. Stouffer; V. Pillitteri; S. Lightman; M. Abrams; A. Hahn, *Guide to Industrial Control Systems (ICS) Security*, NIST Special Publication 800-82 Revision 3, 2022.

60. *** *ScienceDirect – Article on SCADA Security, available at: https://www.sciencedirect.com/science/article/abs/pii/S0167404816300268?via%3Dihub, accessed on 20.08.2025*.

61. *** *SCADA/ICS Social Engineering Attacks – InfoSec Institute, available at: https://www.infosecinstitute.com/resources/scada-ics-security/ics-scada-social-engineering-attacks/, accessed on 20.08.2025*.

62. Dawn Silverman; Yen-Hung (Frank) Hu; Mary Ann Hoppa, *A Study on Vulnerabilities and Threats to SCADA Devices*, Journal of The Colloquium for Information Systems Security Education, Vol. 7, No. 1, Summer 2020. ISSN 1550-7998.

63. *** *CISA ICS Alert (IR-ALERT-H-16-056-01)*, disponibil la: https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01, *accessed on* 16.05.2023.

68. *** *MITRE ATT&CK for ICS – T0866: Exploitation of Remote Services*, accesat în 2025.

75. J. Lee; B. Bagheri; H.A. Kao, *A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems*, Manufacturing Letters, vol. 3, pp. 18–23, 2015. ISSN 2213-8463.

76. F. Wortmann; K. Flüchter, *Internet of Things*, Business & Information Systems Engineering, vol. 57, nr. 3, pp. 221–224, 2015. ISSN 1867-0202.

79. MITRE Corporation, *Common Vulnerabilities and Exposures (CVE)*, report, 2023.

LIST OF FIGURES

APPENDICES

Appendix 1 – Certificate EEBDM-235865430-1059 dated 21.08.2025

This appendix refers to the official certificate EEBDM-235865430-1059 dated 21.08.2025, issued following the responsible disclosure process, which confirms the validation of the critical vulnerability identified in the RTU ES2000 equipment.

EXIMPROD ENGINEERING S.A.

Parte a Grupului Eximprod

Registration number:EEBDM-235865430-1059

21.08.2025

Certificat de confirmare a raportării unei vulnerabilități de securitate cibernetică pentru sisteme industriale (Responsible Disclosure)

Prin prezentul certificat, compania Eximprod Engineering, în calitate de dezvoltator și deținător al platformei industriale *ES2000 RTU Virtual Platform*, certifică faptul că domnul Adelin - Marian Berindei a identificat și raportat în mod responsabil o vulnerabilitate critică de securitate în cadrul aplicației noastre.

Detalii privind vulnerabilitatea:

- **Produs afectat:** Server web RTU ES2000
- **Tip vulnerabilitate:** La nivelul aplicației web, comunicația WebSocket nu impune autentificare. Astfel, pentru entitățile care inițiază cereri prin WebSocket, identitatea nu este verificată.
- **Dată raportare:** 04.03.2024
- **Metoda de raportare:** Responsible Disclosure, prin comunicare directă cu echipa noastră de dezvoltare
- **Mod de remediere:** Lansarea unei versiuni actualizate a software-ului
- **Descrierea remedierii:** Comunicarea prin WebSocket a fost securizată prin introducerea unui mecanism de autentificare bazat pe generarea și validarea unui token, accesul prin conexiuni WebSocket este permis exclusiv sesiunilor autentificate. Remedierea a fost implementata cu success in baza recomandarilor din raportul prezentat.

Această recunoaștere este emisă în scop documentar și poate fi utilizată în context academic, profesional sau științific, ca dovadă a contribuției autorului în domeniul securității cibernetice industriale.

Posea Sabin Nicolae

Director Dezvoltare