HOLISUN

Contract nr.4 din 01/03/2024, etapa 1 - TROCI

RAPORT ȘTIINȚIFIC ȘI TEHNIC 2024

Referință 7077/02.12.2024

Manager de proiect: ***Daniela Delinschi***

Istoricul versiunilor

Versiune	Autor	Modificări
0.1	Daniela Delinschi	Versiunea inițială
0.5	Daniela Delinschi	Versiunea intermediară
1.0	Daniela Delinschi	Versiunea finală

Cuprins

Parteneri

Figura 1: Logo-ul proiectului TROCI

(a) University of Sheffield (UoS, UK) Coordonator

(b) University of Vienna (UNIVIE, Austria)

(c) Holisun SRL(Holisun, Romania)

(d) University College Dublin (UCD, Irlanda)

Figura 2: Partenerii proiectului *TROCI*

1 Introducere

TROCI își propune să dezvolte o platformă integrată de ultimă generație, capabilă să eficientizeze operarea și întreținerea infrastructurilor critice, precum și să optimizeze lanțurile de aprovizionare asociate. Soluția va permite monitorizarea continuă a funcționării și a stării de sănătate a acestor sisteme, oferind o gestionare eficientă a resurselor și reducerea riscurilor operaționale. Proiectul aspiră să creeze o platformă revoluționară, care va schimba paradigma utilizării tehnologiei bazate pe inteligența artificială, transformând-o într-un instrument accesibil, ușor de utilizat și aplicabil în diverse domenii critice pentru funcționarea societății moderne.

Prezentul raport oferă o imagine de ansamblu asupra cadrului operațional și a designului aplicației TROCI, responsabilă de interacțiunea dintre platformă și utilizatorii finali. Aplicația va extinde și completa funcționalitățile platformei digitale TROCI, oferind o soluție integrată pentru gestionarea și protejarea infrastructurilor critice.

2 Despre proiectul TROCI

Infrastructurile critice sunt necesare pentru funcționarea unei țări și stau la baza vieții de zi cu zi. În contextul evenimentelor geopolitice recente, protejarea acestor infrastructuri de diverse amenințări este esențială pentru asigurarea securității naționale și a bunăstării cetățenilor. Sistemele de instrumentație și control (I&C) sunt utilizate pe scară largă pentru a colecta date prin intermediul senzorilor din diferite noduri, a lua decizii și a asigura funcționarea fără probleme prin control de la distanță și/sau autonom al acestor infrastructuri. Adoptarea recentă a sistemelor digitale de I&C face ca aceste infrastructuri să fie vulnerabile la atacuri cibernetico-fizice prin creșterea numărului de suprafețe de atac. Încălcările securității cibernetice care vizează sistemele I&C reprezintă o preocupare tot mai mare la nivel global. Dacă nu sunt contracarate, atacurile pot avea consecințe grave.

Sistemele tradiționale I&C au fost proiectate într-o perioadă în care procesarea datelor era centralizată pentru analize și scopuri de control. Această abordare nu mai este adecvată din cauza complexității sistemului și a apariției unor noi actori și vectori de amenințare. Pentru a acoperi acest gol, ne propunem să dezvoltăm soluții hibride complexe, hardware-software, pentru securitate și confidențialitate, menite să îmbunătățească reziliența infrastructurii critice. Realizarea acestei viziuni va necesita o gândire la nivel de sistem, expertiză multidisciplinară și implicarea eficientă a utilizatorilor industriali.

Prin adoptarea unei abordări fundamental noi în proiectarea sistemelor I&C, soluția propusă va fi co-proiectată, punând accent pe optimizarea interacțiunii hardware-software, minimizarea fluxului de informații, reducerea riscului de defectare hardware prin redundanță și „smartificare”, diminuarea numărului de suprafețe expuse atacurilor prin amplasarea minimă a senzorilor, protejarea datelor de contaminare prin procesare locală și îmbunătățirea eficienței energetice prin proiectarea inovatoare a platformei software. Rezultatele vor fi dezvoltate împreună cu utilizatorii noștri industriali și vor fi implementate în cazuri de utilizare avansate care implică sisteme de distribuție a apei și centrale nucleare. Descoperirile științifice și tehnice promise în acest proiect vor deschide noi oportunități de cercetare în îmbunătățirea rezilienței infrastructurilor critice, vor promova crearea unor criterii de referință obiective, vor forma personal calificat și vor accelera adoptarea în industrie.

Pentru a atinge obiectivul general de creștere a rezilienței infrastructurilor critice (CI) prin dezvoltarea și implementarea de instrumente pentru securitatea și confidențialitatea sistemelor cibernetico-fizice (CPS), au fost stabilite următoarele obiective:

- **Obiectivul 1**. Vom dezvolta și implementa o infrastructură hardware I&C sigură, care va face sistemele reziliente fără a compromite performanța acestora.
- **Obiectivul 2**. Vom dezvolta și implementa o platformă software sigură și privată (împreună cu algoritmii asociați) pentru sistemele industriale I&C, având în vedere abordarea de co-design hardware-software.
- **Obiectivul 3**. Vom crește reziliența CPS a infrastructurilor critice de apă și energie prin implementarea soluției hibride hardware-software dezvoltate pentru securitate și confidențialitate.

Figura 3 prezintă principalele componente tehnice ale proiectului TROCI, împreună cu detalii tehnice ale pachetelor de lucru, care sunt prezentate mai jos în diagrama Gantt. Configurația experimentală va include un sistem hardware-in-the-loop în timp real pentru cazurile de aplicare, cu posibilitatea integrării senzorilor și a intrărilor/ieșirilor, capacități de preprocesare a datelor (de exemplu, senzori IoT și servere de margine), o infrastructură de comunicații eterogenă între senzorii distribuiți și dispozitivele IoT, precum și un cluster de calcul bazat pe cloud pentru analizele de date de bază și managementul central al întregului sistem.

Performanța întregului sistem va fi măsurată prin metrici precum „acuratețea inferenței” și „vârsta informației” pentru software, în timp ce pentru platforma fizică și sistemul de senzori vor fi utilizate metrici de fiabilitate hardware. Datele colectate vor fi puse la dispoziția comunității științifice la un nivel ridicat de granularitate și scară largă pentru a facilita reproducibilitatea și a promova cercetările viitoare.

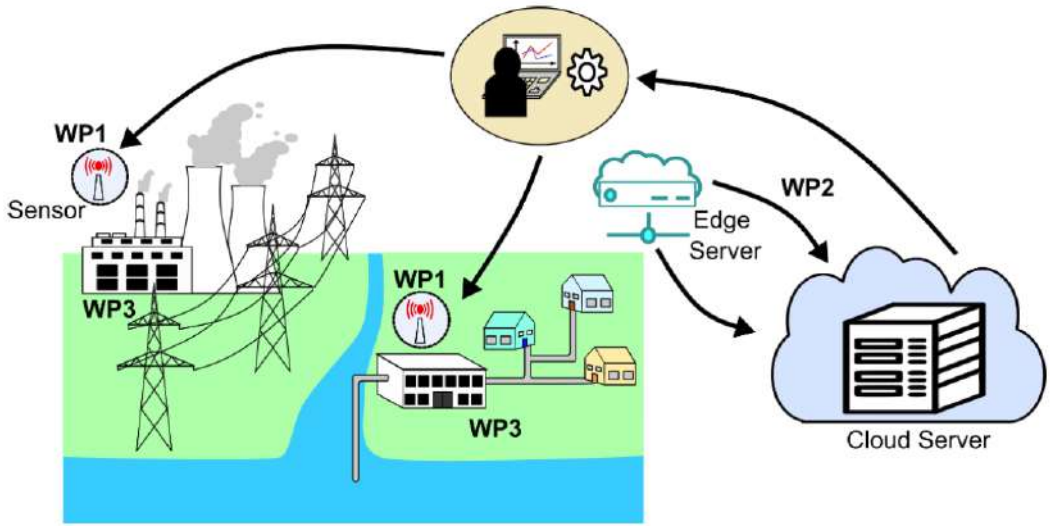

Figura 3: Principalele componente tehnice ale proiectului TROCI.

Proiectul este împărțit în 5 pachete de lucru (WP), fiecare cu sarcini clare care vor permite îndeplinirea obiectivelor proiectului printr-o structură coerentă care va facilita și managementul proiectului. Toate aceste WP-uri si sarcini detaliate sunt exemplificate în Diagrama GANTT de mai jos (Figura 4).

#	WP	Year 1												Year 2												Year 3											
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
WP1	**Secure I&C Infrastructure Design and Deployment**																																				
T1.1.	Analysis of the hardware security and privacy risks in existing systems																																				
T1.2.	Sensor placement																																				
T1.3.	Designing a secure I&C system																																				
T1.4.	Maintaining system performance																																				
WP2	**Secure Software Platform Design and Development**																																				
T2.1.	Literature review and Platform Architecture																																				
T2.2.	Design and Implementation of Algorithms																																				
T2.3.	Hardware - Software Co-Design																																				
T2.4.	Platform Testing and Validation																																				
T2.5.	Platform Implementation																																				
WP3	**Application Cases - Water and Energy System**																																				
T3.1.	CPS security problem identification for the use cases																																				
T3.2.	Sensor monitoring and smartification of networks																																				
T3.3.	Application of resilient sensors and associated systems to the instrumentation system of use cases																																				
T3.4.	Application of software cyber-security solution to the C&I systems of use cases																																				
T3.5.	Comprehensive integration of CPS security solutions for the resilient operation of use cases and demonstration																																				
WP4	**Project Coordination and Data and Project Management**																																				
T4.1.	General and financial management																																				
T4.2.	Technological and scientific management																																				
T4.3.	Quality assurance and risk management																																				
WP5	**Dissemination, Exploitation and Communication**																																				
T5.1.	Stakeholder Engagement meeting																																				
T5.2.	Establish and maintain website and social media presences																																				
T5.3.	Peer reviewed publications and national/international conferences/congresses																																				

Figura 4: Diagrama Gantt care arată calendarul pachetelor de lucru și activităților proiectului

3 Activități planificate

În perioada 01.03.2024 - 05.12.2024 au fost planificate următoarele activități:

- Cercetarea literaturii de specialitate;
- Cercetare pentru stabilirea nevoilor și cerințelor platformei *TROCI* ;
- Întâlniri lunare de progres.

4 Activități efectuate

În perioada 01.03.2024 - 05.12.2024 au fost efectuate următoarele activități:

- Cercetare pentru stabilirea nevoilor și cerințelor platformei *TROCI* ;
- 1 întalnire de kick-off a proiectului în data de 05.03.2024
- 7 întâlniri lunare de progres, în datele: 07.05.2024, 04.06.2024, 02.07.2024, 06.08.2024, 01.10.2024, 05.11.2024, 03.12.2024.
- 1 întâlnire fizică cu toți partenerii proiectului 10-11 Septembrie 2024 Derby, UK.

4.1 Devieri de la planificare

În perioada raportata nu au fost devieri de la planificare, sub nici un aspect.

5 Starea curentă a domeniului

5.1 Securitate hardware

Sistemele de instrumentație și control (I&C) pentru infrastructurile critice, cum ar fi WDS (Water Distribution Systems) și NPP (Nuclear Power Plants), joacă un rol crucial în asigurarea siguranței și fiabilității acestora. Cu toate acestea, aceste sisteme sunt vulnerabile la o gamă largă de riscuri de securitate, care pot avea consecințe grave, inclusiv încălcări ale datelor, defecțiuni ale sistemului și chiar daune fizice asupra infrastructurii în sine [19, 1].

Componentele hardware ale unui sistem I&C, care formează suprafața de atac, includ în mod obișnuit:

(i) senzori, utilizați pentru a măsura parametrii fizici, cum ar fi temperatura, presiunea, debitul și nivelul, în procesul sau sistemul monitorizat;

(ii) actuatoare, utilizate pentru a controla procesul sau sistemul prin manipularea parametrilor fizici, cum ar fi valvele, pompele și motoarele;

(iii) sisteme de control, utilizate pentru a procesa datele de la senzori și pentru a furniza semnale de control actuatoarelor;

(iv) rețele de comunicație, utilizate pentru a transmite date între senzori, actuatoare, sisteme de control și alte componente;

(v) interfețe om-mașină, care oferă o interfață între sistem și operatorii umani, permițându-le acestora să monitorizeze și să controleze procesul sau sistemul;

(vi) surse de alimentare, utilizate pentru a furniza energie electrică componentelor, asigurând o funcționare fiabilă;

(vii) incinte, utilizate pentru a proteja componentele împotriva condițiilor de mediu și a daunelor fizice.

5.1.1 Principalele riscuri de securitate

Unele dintre principalele riscuri de securitate care afectează sistemele I&C pentru infrastructurile critice includ:

- Manipularea sau daunele fizice: Manipularea fizică a senzorilor IoT, a echipamentelor de rețea sau a nodurilor de procesare poate permite accesul neautorizat sau manipularea datelor.
- Atacuri laterale: Atacatorii pot exploata caracteristicile fizice ale dispozitivelor IoT pentru a obține informații despre dispozitiv sau pentru a fura date.
- Dispozitive rău intenționate: Dispozitive rău intenționate pot fi adăugate la o rețea (de exemplu, prin lanțul de aprovizionare), permițând atacatorilor să obțină acces la rețea sau să perturbe comunicațiile.
- Conexiuni de rețea nesecurizate: Nodurile de procesare sau serverele pot avea conexiuni de rețea nesecurizate, permițând accesul neautorizat sau interceptarea datelor.

5.1.2 Soluții tehnologice pentru securitate

Tehnologia blockchain reprezintă o soluție unică pentru a depăși problemele de siguranță din sistemele SCADA și poate fi adoptată pentru a valida identitatea entităților autonome din rețea [8, 17]. Cu o astfel de platformă de validare, credențialele și datele importante legate de senzori și actuatoare din aceste medii SCADA bazate pe automatizare pot fi circulate prin intermediul tehnologiilor de registre distribuite (DLT), în timp ce validarea și siguranța pot fi stabilite prin contracte inteligente.

Funcțiile fizice neclonabile (PUF) reprezintă o zonă promițătoare pentru autentificarea Dispozitiv-la-Dispozitiv (D2D) și pot fi adoptate în mediile CPS (Cyber-Physical Systems). Acestea pot fi utilizate pentru a îmbunătăți siguranța și a preveni dispozitivele rău intenționate și încercările de deghizare. Conceptual, identitatea auto-suverană (SSI) și identitatea descentralizată (DID) sunt similare autentificării D2D bazate pe PUF, dar pot fi integrate într-o configurație blockchain [13].

Măsurile de securitate fizică, care pot elimina sau transfera credențialele relevante printr-un canal securizat în cazul detectării unei amenințări de manipulare, așa cum se menționează în [12], reprezintă o măsură viabilă de securitate hardware în această propunere.

5.2 Securitate software

Securitatea și siguranța software-ului încep încă din faza de dezvoltare a ciclului său de viață. Procesul de proiectare a sistemelor software critice necesită metode riguroase pentru a asigura robustețea și reziliența acestora, în special în contextul infrastructurilor critice și al sistemelor cibernetico-fizice. Islam și Storer [9] au prezentat o abordare agilă pentru dezvoltarea sistemelor critice de siguranță (Safety-Critical Systems - SFS). Această abordare nu limitează ciclurile de viață doar la modelele tradiționale, cum ar fi Spiral sau Waterfall, ci permite și utilizarea metodologiei agile, mai frecvent utilizată pentru dezvoltarea rapidă a aplicațiilor. Astfel, integrarea metodologiilor moderne de dezvoltare software în proiectele critice devine esențială.

Mai recent, au fost proiectate metodologii dedicate de verificare și validare pentru sistemele critice de siguranță. Aceste metodologii asigură conformitatea și robustețea aplicațiilor software prin procese sistematice [7, 16]. Verificarea și validarea sunt procese esențiale, având în vedere impactul potențial al defectelor software asupra infrastructurilor critice, cum ar fi cele din domeniul energiei, transporturilor și apei.

Pe lângă siguranță și securitate, reziliența software-ului în fața atacurilor și a defectelor interne devine din ce în ce mai importantă [2]. Acest lucru este cauzat, în mare parte, de utilizarea tot mai frecventă a sistemelor cibernetico-fizice (Cyber-Physical Systems - CPS), care sunt esențiale pentru infrastructurile critice [18]. Reziliența presupune capacitatea unui sistem de a detecta, răspunde și recupera în urma incidentelor sau defectelor, minimizând astfel impactul asupra funcționării infrastructurii critice.

În paralel, creșterea utilizării calculului la margine (IoT Edge Computing) [11] contribuie la eficientizarea infrastructurilor critice prin reducerea dependenței de centrele de date centrale și prin prelucrarea datelor aproape de sursa lor. Calculul la margine se bucură de o popularitate tot mai mare datorită disponibilității dispozitivelor de calcul mai puțin costisitoare, a consumului redus de energie [10] și a apariției unor soluții precum calculul în ceață (Fog Computing) [3], care elimină necesitatea unor infrastructuri cloud costisitoare și vulnerabile la întreruperi.

Mai mult, optimizările software au permis dezvoltarea de alternative performante la metodele clasice de învățare automată. Una dintre aceste metode este învățarea federată (Federated Learning), care sporește securitatea prin evitarea centralizării datelor, reducerea transferului acestora și eliminarea riscului de punct unic de eșec [15]. Aceste abordări moderne sunt critice pentru protejarea datelor sensibile și pentru asigurarea confidențialității utilizatorilor în cadrul infrastructurilor critice.

În concluzie, progresul tehnologic în securitatea software-ului, metodologiile de verificare și validare, calculul la margine și învățarea automată reprezintă direcții esențiale pentru îmbunătățirea rezilienței infrastructurilor critice. Aceste dezvoltări nu doar că susțin protecția împotriva amenințărilor cibernetice, dar și facilitează un cadru robust pentru proiectarea, implementarea și gestionarea sistemelor moderne.

6 Cerințele platformei

În dezvoltarea unei platforme hibride hardware-software pentru securitate și confidențialitate în sistemele de instrumentație și control (I&C) utilizate în infrastructurile critice (CI), este esențială o abordare multidisciplinară și sistemică. Această platformă trebuie să fie optimizată pentru a răspunde provocărilor actuale legate de securitate, reziliență și confidențialitate, fără a compromite performanța sistemului. Pe baza analizei de mai sus, cerințele platformei pot fi împărțite în două categorii: **cerințe funcționale** și **cerințe nonfuncționale** (Figura 5).

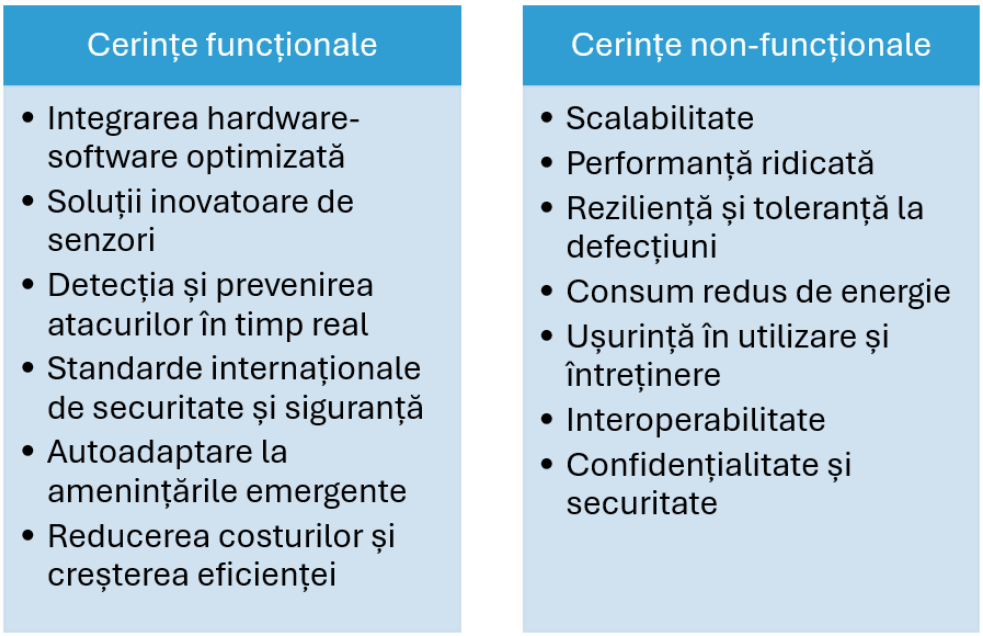

Figura 5: Cerințele funcționale și non-funcționale

6.1 Cerințe funcționale

1. **Integrarea hardware-software optimizată**
   - Co-design hardware-software care să asigure compatibilitatea și performanța optimă a întregii platforme.
   - Implementarea de algoritmi avansați pentru detectarea atacurilor și anomaliilor, având în vedere limitările de resurse computaționale și de rețea specifice sistemelor I&C.

2. **Soluții inovatoare de senzori**
   - Utilizarea tehnologiilor de senzori avansate, precum sistemele microelectromecanice (MEMS), pentru a detecta anomalii hardware.
   - Optimizarea plasării senzorilor pentru a îmbunătăți reziliența sistemului și a reduce cererea de senzori.
3. **Detecția și prevenirea atacurilor în timp real**
   - Dezvoltarea de metode bazate pe inteligența artificială (AI) pentru detectarea și reacția în timp real la atacuri și defecțiuni.
   - Implementarea funcțiilor de reconfigurare automată a rețelei pentru a crește reziliența în fața atacurilor cibernetice.
4. **Standarde internaționale de securitate și siguranță**
   - Respectarea standardelor internaționale privind securitatea hardware, software și funcțională pentru a asigura interoperabilitatea și conformitatea platformei.
5. **Autoadaptare la amenințările emergente**
   - Utilizarea AI pentru a adapta algoritmii la noi vectori de amenințare și atacuri în evoluție.
6. **Reducerea costurilor și creșterea eficienței**
   - Optimizarea utilizării resurselor prin reducerea numărului de senzori și a cerințelor de procesare a datelor.

6.2 Cerințe nonfuncționale

1. **Scalabilitate**
   - Platforma trebuie să fie capabilă să susțină extinderea la infrastructuri critice de dimensiuni mari, fără o scădere a performanței.
2. **Performanță ridicată**
   - Menținerea performanței sistemului în condițiile implementării soluțiilor de securitate avansate.
3. **Reziliență și toleranță la defecțiuni**
   - Asigurarea unei funcționări robuste în fața defecțiunilor hardware și software, inclusiv toleranța la atacuri cibernetice și fizice.
4. **Consum redus de energie**
   - Optimizarea consumului energetic al platformei prin utilizarea eficientă a hardware-ului și software-ului.
5. **Ușurință în utilizare și întreținere**
   - Interfață intuitivă pentru operatorii umani și instrumente avansate de monitorizare și diagnosticare pentru întreținerea platformei.
6. **Interoperabilitate**
   - Asigurarea integrării fără probleme cu alte sisteme și tehnologii utilizate în infrastructurile critice.
7. **Confidențialitate și securitate**
   - Implementarea de măsuri stricte de protecție a datelor pentru a asigura confidențialitatea informațiilor sensibile.

6.3 Impactul așteptat al platformei

Propunerea acestei platforme hibride hardware-software, cu accent pe integrarea AI, IoT și soluții de senzori inovatori, își propune să transforme paradigmele actuale ale sistemelor I&C utilizate în infrastructurile critice. Platforma va contribui la securitatea, reziliența și confidențialitatea infrastructurilor critice, reducând costurile operaționale și consumul energetic, fiind scalabilă și ușor de întreținut.

7 Rolul HOLISUN în cadrul proiectului

Rolul HOLISUN este dublu, atât în proiectarea și implementarea sistemului informatic ce va coordona preluarea, prelucrarea și salvarea datelor, cât și participarea în cercetarea fundamentală și aplicată referitoare la algoritmii inteligenți utilizați în cadrul platformei. Rolul acestor algoritmi este de a prelucra datele rezultate din funcționarea sistemelor de instrumentație și control (I&C), precum și de a oferi diferite predicții și sugestii utile în procesele aferente ce se desfășoară în cadrul infrastructurilor critice, cum ar fi sistemele de distribuție a apei și centralele nucleare.

Informațiile și cunoștințele rezultate vor fi catalogate și înregistrate în baza de date inteligentă din cadrul sistemului, modul implementat printr-o tehnologie hibridă bazată pe un sistem de baze de date de tip NewSQL[6, 4], precum și o bază de cunoștințe ontologică, bazată pe fișiere OWL[5, 14], versionate săptămânal pentru a asigura stabilitatea și omogenitatea cunoștințelor.

În cadrul proiectului, HOLISUN va finaliza dezvoltarea unui sistem complet, integrat și automat de catalogare și înregistrare a parametrilor de funcționare pentru sistemele I&C, un sistem extensibil, flexibil și rapid, cu posibilitatea de a fi adaptat în multe alte proiecte, atât interne cât și externe ale HOLISUN. De asemenea, HOLISUN va implementa pentru comercializare platforma software rezultată, gata de utilizare în diferite proiecte din domeniul securității și reziliței infrastructurilor critice.

8 Extras din planul de riscuri

În Tabelul 1 este reprezentat planul de riscuri ce ține de partea de implementare a proiectului.

Tabela 1: Tabel de analiză a riscurilor și metode de mitigare.

Risc	**Probabilitate**	**Impact**	**Valoare**	**Mitigare**
Încetează să funcționeze un senzor	1	4	4	Înlocuirea senzorului cu unul funcțional
Se întrerupe internetul	4	4	16	Backup local la date, sincronizare automată cu cloud-ul
Încetează să funcționeze un microcontroller	1	5	5	Înlocuire microcontroller, restaurarea softului și a datelor
Trimitere coruptă a datelor	1	5	5	Arhivare, mecanism CRC, menținere backup până la confirmare de la cloud
Date corupte de la senzor	2	4	8	Detectare anticipată, eliminarea valorilor defecte din baza de date, invalidarea înregistrărilor, anunțarea tehnicienilor locali
Generare model ML corupt sau defectuos	2	5	10	Generare multiplă, prin mai mulți algoritmi (minim 3) și folosirea unui sistem automat de votare pentru cel mai bun răspuns

9 Rezultatele proiectului

9.1 Livrabile

In perioada raportata am furnizat livrabile din tabela 2 și am început lucrul intens asupra celorlalte livrabile.

Tabela 2: Tabel cu livrabile și statusul acestora.

Nr. livrabil	Termen	Livrabil	Status livrabil
D5.2	M1	Site-ul web al proiectului și crearea unei platforme de social media, și anume, Twitter și LinkedIn	Livrat M1
D2.1	M14	Arhitectură software platformă, flux de date și co-proiectare hardware versiunea 1	În lucru

9.2 Articole științifice

În perioada de raportare s-a lucrat intens la mai multe articole științifice, unele dintre acestea au fost prezentate la conferințe, sau publicate în jurnale, iar unele urmează să fie prezentate/publicate.

În Tabelul sunt listate toate articolele din cadrul proiectului:

Tabela 3: Lista de articole

Articolul	Detalii Conferinta / Jurnal	Link pentru Acces
Daniela Delinschi, Rudolf Erdei, Emil Pașca, Iulia Bărăian, Oliviu Matei, "**Guide in Designing an Asynchronous Performance-Centric Framework for Heterogeneous Microservices in Time-Critical Cybersecurity Applications**"	Expert Systems Wiley Journal	În curs de publicare
Rudolf Erdei, Emil Pașca, Daniela Delinschi, Anca Avram, Ionela Chereja, Oliviu Matei, "**Privacy Assessment Methodology for Machine Learning Models and Data Source**"	19th International Conference on Soft Computing Models in Industrial and Environmental Applications (SOCO 2024)	Link articol
Emil Pașca, Rudolf Erdei, Daniela Delinschi, Oliviu Matei, "**Enhancing API Security Testing against BOLA and Authentication Vulnerabilities through an LLM-Enhanced Framework**"	19th International Conference on Soft Computing Models in Industrial and Environmental Applications (SOCO 2024)	Link articol
Emil Pașca, Daniela Delinschi, Rudolf Erdei, Oliviu Matei, "**LLM-Driven, Self-Improving Framework for Security Test Automation: Leveraging Karate DSL for Augmented API Resilience**"	IEEE ACCESS	În curs de review
Rudolf Erdei, Daniela Delinschi, Emil Pașca, Laura Andreica, Oliviu Matei "**Selective Survey of Distributed Learning Methodologies for Agricultural Applications: Challenges and Strategies for Ensuring Privacy and Resilience**"	SCIENTIFIC BULLETIN, Seria C: Inginerie Electrică şi Ştiinţa Calculatoarelor	În curs de publicare

10 Diseminare și exploatare

10.1 Activități de diseminare

Proiectul a fost diseminat în următoarele moduri:

- pe pagina web: https://research.holisun.com/ro/proiecte/critical-infrastructure/troci-ro, având un număr de 180 de vizitatori lunari
- pe pagina web a proiectului: https://troci.holisun.com/, având un număr de 14 de vizitatori lunari
- pe contul de LinkedIn: https://www.linkedin.com/company/holisun, cu 400 de adepți
- pe contul de LinkedIn al proiectului https://www.linkedin.com/company/troci2023/, cu 14 urmăritori
- pe pagina de Facebook: https://www.facebook.com/Holisun.IT/, având 1881 de urmăritori

Au fost desfășurate o serie de activități de diseminare în cadrul unor evenimente de afaceri, expoziții și evenimente de brokeraj sau networking, listate în Tabelul 4.

Tabela 4: Lista de activități de diseminare

Nume	**Data**	**Link**	**Participanți**	**Rezultate**
Cluj Innovation Days 2024	21.03.2024-22.03.2024	https://clujinnovationdays.com/	Oliviu Matei	Prezentare *TROCI*
BOOSTing European collaboration among Industry 4.0 stakeholders	16.04.2024-26.04.2024	https://boosting-european-collaboration-among-industry.b2match.io/	Rudolf Erdei	Prezentare *TROCI*
Derby TROCI Workshop	16.04.2024-26.04.2024	-	Rudolf Erdei Oliviu Matei	Prezentare *TROCI*
Clean Energy Transition Partnership	12.09.2024	https://www.b2match.com/e/clean-energy-transition-partnership-2024	Rudolf Erdei Daniela Delinschi	Prezentare *TROCI*

10.1.1 Alte activități de diseminare

Proiectul a mai fost diseminat prin următoarele canale:

Tabela 5: Lista canale de diseminare

Canal	**Adresa**	**Indicatori**
Pagina web	https://troci.holisun.com/	Vizitatori: 41
LinkedIn	https://www.linkedin.com/company/troci2023/	Urmăritori: 14

11 Concluzii

În acest prim an al proiectului, HOLISUN și-a concentrat eforturile pe studiul și cercetarea modalităților de proiectare și implementare a unei platforme destinate infrastructurilor critice. Activitățile au inclus analiza stadiului actual al domeniului, cu accent pe identificarea nevoilor și cerințelor beneficiarilor, precum și a limitărilor existente, cum ar fi constrângerile de buget, restricțiile de spațiu și resursele disponibile (ex. alimentarea cu energie, rețele de comunicații și condițiile de mediu). Scopul acestor analize a fost obținerea unei înțelegeri detaliate a contextului tehnologic și a cerințelor operaționale pentru dezvoltarea ulterioară a sistemului.

În anul următor, HOLISUN va finaliza arhitectura platformei și va începe integrarea datelor rezultate din WP-urile cu specific de cercetare în securitatea și reziliența infrastructurilor critice. Aceste date vor fi utilizate pentru generarea de modele de machine learning (ML) care vor permite sistemului să detecteze și să prevină amenințările, să optimizeze performanța și să ofere estimări predictive. Prin dezvoltarea și implementarea componentelor software, se va realiza verificarea și validarea soluțiilor tehnice propuse. Această activitate va avea loc la sediul partenerului tehnologic din cadrul consorțiului, asigurând astfel o testare riguroasă a soluțiilor propuse.

Sistemul rezultat, compus din mai multe module hardware și software integrate, va fi utilizat în activitățile de monitorizare, protecție și optimizare a infrastructurilor critice, generând date și informații valoroase pentru securitate și întreținere predictivă. Planul de extindere al proiectului include integrarea unor tehnologii inovatoare, cum ar fi noi tipuri de senzori și algoritmi de procesare a datelor distribuite, care vor contribui la creșterea rezilienței și eficienței acestor sisteme.

De asemenea, primul an al proiectului a marcat începutul activităților de diseminare și exploatare a rezultatelor. În acest sens, HOLISUN a dezvoltat și întreținut website-ul oficial al proiectului, care oferă informații detaliate despre obiectivele și progresul acestuia. În plus, au fost create și administrate profilele de social media asociate proiectului pe platforme precum LinkedIn pentru a crește vizibilitatea și a facilita colaborarea cu alți experți din domeniu. Aceste activități asigură o diseminare eficientă a rezultatelor, promovând impactul pozitiv al proiectului în domeniul protecției și rezilienței infrastructurilor critice.

Iar ce ține de partea științifică au fost prezentate 2 articole la o conferință iar alte 2 articole au fost trimise la jurnale de prestigiu.

Referințe

[1] Augello, A., et al.: A coexistence analysis of blockchain, scada systems, and openadr for energy services provision. IEEE Access **10**, 99088–99101 (2022)

[2] Babiceanu, R., Seker, R.: Cyber resilience protection for industrial internet of things: A software-defined networking approach. Computers in Industry **104**, 47–58 (2019)

[3] Bakhshi, Z., et al.: Dependable fog computing: A systematic literature review. In: 45th Euromicro Conference on Software Engineering and Advanced Applications. pp. 395–403. IEEE (2019)

[4] Chereja, I., Hahn, S.M.L., Matei, O., Avram, A.: Operationalizing analytics with newsql. In: Software Engineering and Algorithms: Proceedings of 10th Computer Science On-line Conference 2021, Vol. 1. pp. 249–263. Springer (2021)

[5] Delinschi, D., Erdei, R., Matei, O.: Ontology driven high performance messaging system for distributed software platforms. In: 2022 IEEE International Conference on Automation, Quality and Testing, Robotics (AQTR). pp. 1–6. IEEE (2022)

[6] Hahn, S.M.L., Chereja, I., Matei, O.: Analysis of transformation tools applicable on newsql databases. In: Software Engineering and Algorithms: Proceedings of 10th Computer Science On-line Conference 2021, Vol. 1. pp. 180–195. Springer (2021)

[7] Hardin, D.: Verified hardware/software co-assurance: Enhancing safety and security for critical systems. In: IEEE International Systems Conference (SysCon). pp. 1–6. IEEE (2020)

[8] Hossain, M.T., et al.: Porch: A novel consensus mechanism for blockchain-enabled future scada systems in smart grids and industry 4.0. In: IEEE International IoT, Electronics and Mechatronics Conference (IEMTRONICS). pp. 1–7 (2020)

[9] Islam, G., Storer, T.: A case study of agile software development for safety-critical systems projects. Reliability Engineering & System Safety **200**, 106954 (2020)

[10] Kumar, H., Tomar, V.: Design of low power with expanded noise margin subthreshold 12t sram cell for ultra-low power devices. Journal of Circuits, Systems and Computers **30**(6), 2150106 (2021)

[11] Liu, C., et al.: A cooperative indoor localization enhancement framework on edge computing platforms for safety-critical applications. In: 15th International Conference on Mobile Ad-Hoc and Sensor Networks (MSN). pp. 372–377. IEEE (2019)

[12] Lu, M.C., et al.: Psps: A step toward tamper resistance against physical computer intrusion. Sensors **22**(5), 1882 (2022)

[13] Maldonado-Ruiz, D., et al.: An innovative and decentralised identity framework based on blockchain technology. In: 11th IFIP International Conference on New Technologies, Mobility and Security (NTMS). pp. 1–8 (2021)

[14] Matei, O., Contraş, D., Pop, P.: Applying evolutionary computation for evolving ontologies. In: 2014 IEEE Congress on Evolutionary Computation (CEC). pp. 1520–1527. IEEE (2014)

[15] Nguyen, D., et al.: Federated learning for internet of things: A comprehensive survey. IEEE Communications Surveys & Tutorials **23**(3), 1622–1658 (2021)

[16] Rajabli, N., et al.: Software verification and validation of safe autonomous cars: A systematic literature review. IEEE Access **9**, 4797–4819 (2020)

[17] Stokkink, Q., Pouwelse, J.: Deployment of a blockchain-based self-sovereign identity. In: IEEE International Conference on Internet of Things (iThings), GreenCom, CPSCom, SmartData. pp. 1336–1342 (2018)

[18] Yaacoub, J., et al.: Cyber-physical systems security: Limitations, issues and future trends. Microprocessors and Microsystems **77**, 103201 (2020)

[19] Yastrebenetsky, M., Kharchenko, V.: Cyber security and safety of nuclear power plant instrumentation and control systems. IGI Global (2020)

info@holisun.com
http://www.holisun.com
+4-0262-226.778
Versiune document: 1.0 din 02.12.2024