HOLISUN

Contract nr.4 din 01/03/2024, etapa 2 - TROCI

RAPORT ȘTIINȚIFIC ȘI TEHNIC 2025

Referință 7765/ 24.11.2025

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

1 Introducere **4**

2 Despre proiectul TROCI **4**

3 Activități planificate **6**

4 Activități efectuate **6**

4.1 Devieri de la planificare 6

5 Platforma TROCI **7**

5.1 Modulele de bază ale platformei online 8

5.2 Dashboard Personalizabil și Modular 10

5.3 Detectarea și Înrolarea Automată a Senzorilor 11

5.4 Model de Securitate Stratificat 11

5.5 Motor de Evaluare Paralelă a Regulilor 12

5.6 Arhitectură distribuită, bazată pe API-uri 12

6 Rolul HOLISUN în cadrul proiectului **13**

7 Extras din planul de riscuri **14**

8 Rezultatele proiectului **15**

8.1 Livrabile 15

8.2 Articole științifice 15

9 Diseminare și exploatare **16**

9.1 Activități de diseminare 16

9.1.1 Alte activități de diseminare 16

10 Concluzii **17**

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.

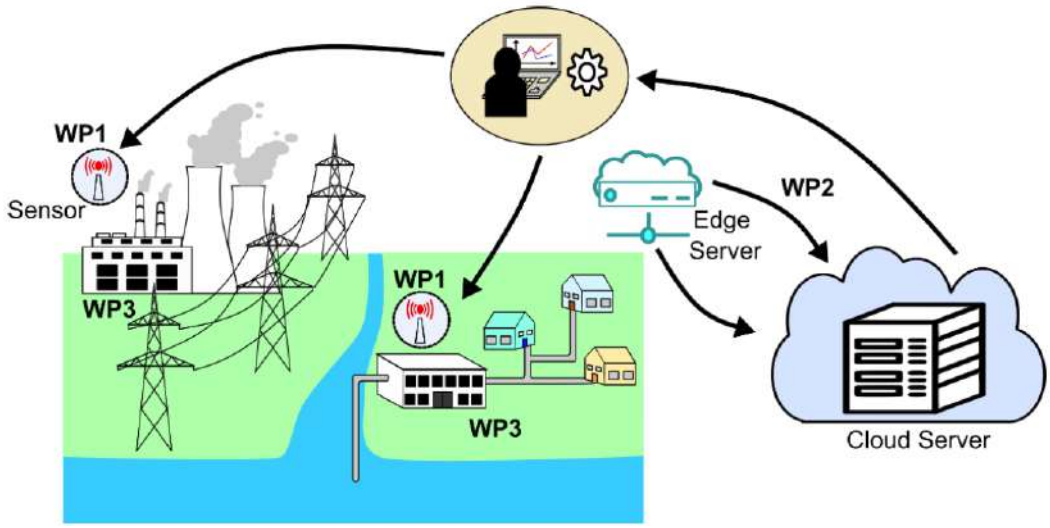

Figura 3: Principalele componente tehnice ale proiectului TROCI.

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).

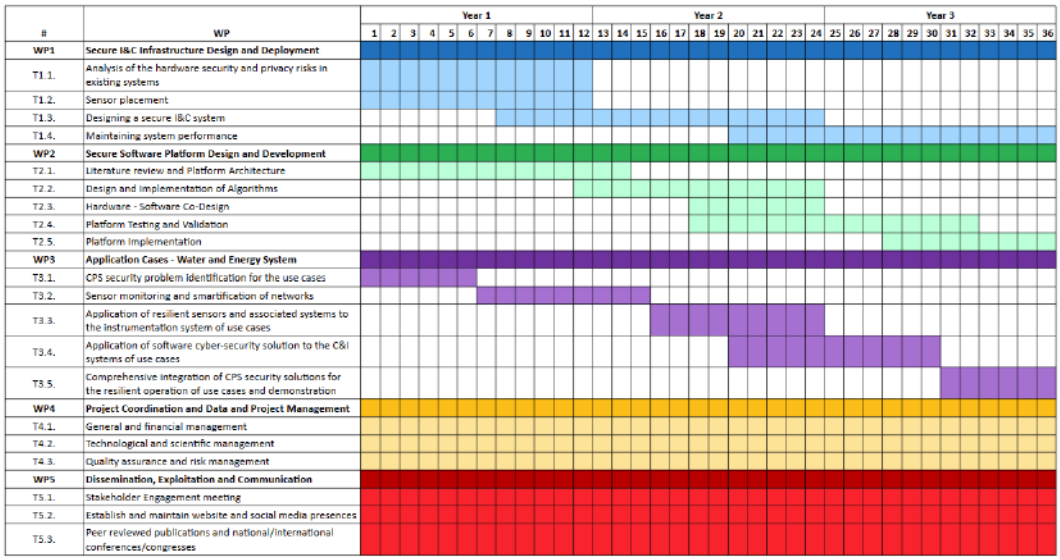

Figura 4: Diagrama Gantt care arată calendarul pachetelor de lucru și activităților proiectului

3 Activități planificate

În perioada Ianuarie - Decembrie 2025 au fost planificate următoarele activități:

- Cercetarea și dezvoltarea arhitecturii proiectului *TROCI* ;
- Dezvoltarea și implementarea panoului de control al aplicației *TROCI* ;
- Întâlniri lunare de progres.

4 Activități efectuate

În perioada Ianuarie - Decembrie 2025 au fost efectuate următoarele activități:

- Cercetarea și dezvoltarea arhitecturii proiectului *TROCI* ;
- Dezvoltarea și implementarea panoului de control al aplicației *TROCI* ;
- Întâlniri lunare de progres, cu toți partenerii proiectului.
- 1 întâlnire fizică cu toți partenerii proiectului 21 Octombrie 2025 Cluj-Napoca, Romania.

Figura 5: Întâlnire pe proiectul TROCI în Cluj-Napoca, Romania

4.1 Devieri de la planificare

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

5 Platforma TROCI

Platforma TROCI este considerată a fi centrul de comandă al instanței sistemului, locul din care operatorii pot avea o vedere de ansamblu asupra sistemului ca întreg. Platforma agregă informațiile venite de la senzorii sistemului, fie locali sau instalați la distanță. Acești senzori sunt sisteme calcul complete (senzori inteligenți IoT), având capacități avansate de pre-procesare, compresie, criptare și transmisie a datelor.

Arhitectura generală a sistemului este dezvoltată pe baza modelului arhitectural și al topologiei "Stea de Stele" (Figura 6). În această figură se pot observa cele două tipuri de comunicații propuse în cadrul cazului de utilizare referitor la managementul alimentării cu apă al orașelor. Linia punctată evidențiază comunicarea fără fir, de putere mică și distanță mare (LoRaWAN, etc), iar liniile continue sunt comunicarea de viteză mare, prin internet. Ambele tipuri de comunicare au riscurile proprii de securitate, fiind necesare componente hardware optimizate (parte acoperită de partenerii de la Universitatea din Viena și University College Dublin).

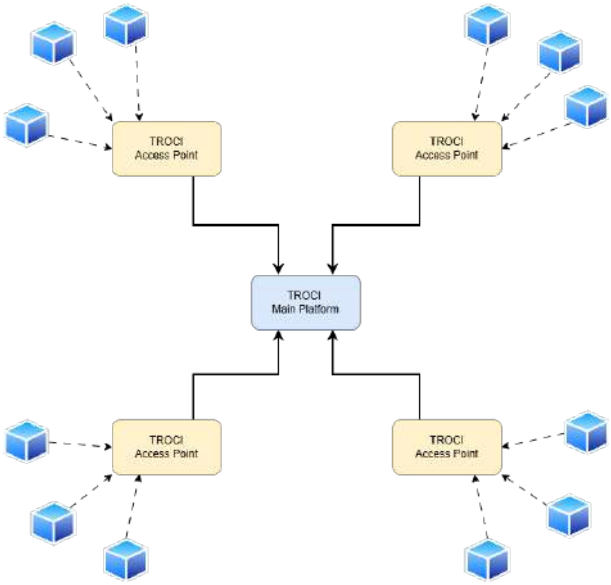

Figura 6: Arhitectura de comunicații a proiectului TROCI

Pe baza acestui hardware cu componente avansate de siguranță, platforma TROCI asigură centralizarea, agregarea și prelucrarea informațiilor. Agregarea are ca scop asigurarea unei centralizări holistice, în care datele de la alți senzori dau informații de context unui senzor anume, context a cărui influență scade invers proporțional cu distanța dintre cei doi senzori. Astfel, influența poate fi definită ca `Afinitate`[1] și calculată folosind Ecuația 1:

$$A_{i,j} = \frac{r_{i,j}}{d_{i,j}} \tag{1}$$

unde:

- Ai, j - *afinitatea* senzorului j asupra senzorului i,
- $r_{i,j}$ - corelația istorică Pearson a valorilor senzorilor i și j,
- $d_{i,j}$ - distanța fizică dintre senzorii i și j.

Implementarea acestui mecanism, pe baza corelației dintre senzori, deschide posibilitatea îmbunătățirii bazei de date centralizate, deoarece aceste valori corelate pot fi utilizate la calculul unei eventuale valori lipsă cu o acuratețe foarte mare.

Calculul acestei valori lipsă pentru un anumit senzor se poate realiza printr-o medie ponderată a valorilor celorlalți senzori din sistem, ponderile fiind reprezentate chiar de `afinitatea` pe care fiecare senzor o are asupra celui pentru

[1] Sau `relevanță contextuală`. Aceasta definește ponderea de proximitate spațio-corelațională dintre doi senzori diferiți

care se dorește estimarea. Astfel, valoarea estimată a senzorului i la momentul de timp t, notată $\hat{V}_i(t)$, poate fi calculată cu ajutorul Ecuației 2:

$$\hat{V}_i(t) = \sum_{j \in S, j \neq i} \tilde{A}_{i,j} \cdot V_j(t) \tag{2}$$

și:

$$\tilde{A}_{i,j} = \frac{A_{i,j}}{\sum_{j \in S, j \neq i} A_{i,j}} \tag{3}$$

unde:

- $\hat{V}_i(t)$ - valoarea estimată (lipsă) a senzorului i la momentul de timp t,
- $V_j(t)$ - valoarea măsurată de senzorul j la momentul de timp t,
- $\tilde{A}_{i,j}$ - *afinitatea* senzorului j asupra senzorului i, calculată conform Ecuației 1 și normalizată conform Ecuației 3,
- S - mulțimea tuturor senzorilor activi din sistem la momentul t.

Abordarea prezentată se asigură că senzorii cu o `afinitate` mai mare (adică cei mai apropiați fizic și cu o corelație istorică mai puternică) vor contribui mai mult la valoarea finală estimată. Mecanismul sporește robustețea și rezilienta sistemului, prin creșterea rezoluției estimărilor, permițând funcționarea continuă chiar și în cazul pierderii temporare a datelor de la unul sau mai mulți senzori. Aceasta rezultă într-o bază de date de calitate superioară, precum și la modele de învățare automată mai calitative.

5.1 Modulele de bază ale platformei online

Platforma online conține modulele necesare bunei funcționări. Pentru simplitate în modelare, nodurile au fost modelate ca utilizatori (Figura 7), folosindu-se astfel metodologia existentă de management și validare a identității actorilor din sistem. Această decizie de proiectare aduce o serie de avantaje strategice semnificative în ceea ce privește securitatea, mentenanța și scalabilitatea platformei.

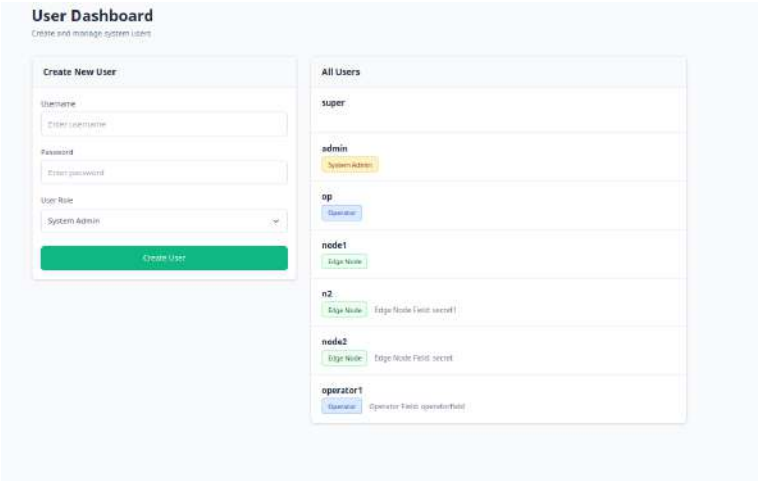

Figura 7: Management utilizatori si noduri

Principalul beneficiu constă în unificarea sistemului de Management al Identității și Accesului (IAM). Prin tratarea nodurilor ca utilizatori, se poate folosi o singură infrastructură atât pentru operatorii umani, cât și pentru entitățile automate. Acest lucru elimină necesitatea de a dezvolta și întreține sisteme paralele de autentificare și autorizare, reducând complexitatea generală a platformei prin folosirea de abstractizări. Fiecare nod poate avea propriile sale credențiale unice, cum ar fi chei API sau token-uri, gestionate prin aceleași mecanisme securizate folosite pentru conturile operatorilor umani.

Această abordare extinde capabilitățile de securitate granulară și auditabilitate asupra dispozitivelor fizice. Fiecărui nod i se pot atribui roluri și permisiuni specifice, la fel ca unui utilizator. De exemplu, un senzor poate avea permisiunea de a scrie date exclusiv într-o locație anume, fără a avea acces de citire sau scriere în alte părți ale sistemului. Toate acțiunile efectuate de un nod sunt înregistrate în jurnale de audit asociate "utilizatorului" corespunzător, asigurând o trasabilitate completă. În cazul compromiterii unui nod, "contul" său poate fi rapid dezactivat, izolând amenințarea fără a afecta restul rețelei.

Din punct de vedere al arhitecturii software, beneficiile sunt la fel de importante. Interfețele de programare (API-urile) nu mai trebuie să facă distincția între o cerere venită de la un operator și una de la un nod, deoarece logica de validare se aplică identității solicitantului, indiferent de natura sa. Acest lucru permite o reutilizare masivă a codului, precum middleware-ul de autentificare și autorizare, conducând la o arhitectură mai curată, mai robustă și mai ușor de întreținut.

În final, scalabilitatea și administrarea sistemului sunt considerabil simplificate. Procesul de adăugare de noi senzori în rețea (onboarding) devine echivalent cu procesul de creare a unui nou utilizator, operațiune ce poate fi ușor automatizată. Vizualizarea stării, activității sau a datelor istorice pentru un anumit senzor se poate face prin interfețe de administrare similare celor folosite pentru a gestiona utilizatorii umani, simplificând operațiunile de zi cu zi. Astfel, această abstractizare transformă problema complexă a managementului dispozitivelor IoT într-o problemă binecunoscută, cea a managementului utilizatorilor, permițând echipei de dezvoltare să se concentreze pe logica specifică proiectului.

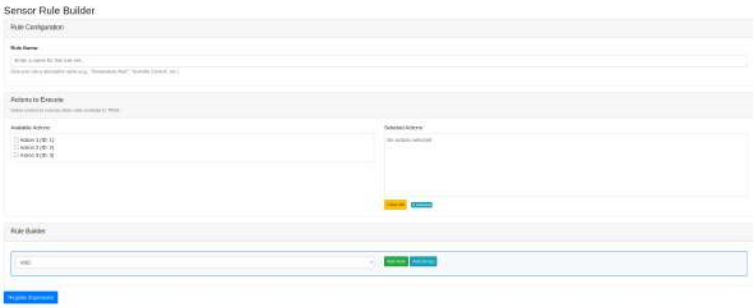

Figura 8: Crearea de conditii pentru executarea diferitelor actiuni

O componentă esențială a platformei TROCI este capacitatea de a automatiza operațiuni în funcție de condițiile de mediul monitorizat (Figura 8). Această funcționalitate este implementată printr-un Compozitor de Reguli (Rule Builder), care permite definirea, evaluarea și executarea unor acțiuni specifice în mod dinamic. Scopul acestui modul este de a transforma platforma dintr-un sistem pasiv de monitorizare într-unul activ, capabil să reacționeze autonom la evenimentele detectate în timp real de rețeaua de senzori.

Figura 9: Configurarea unei reguli analizând valorile venite de la senzori

Nucleul acestui sistem este "regula", o structură logică ce urmează un model de tip *IF <condiție> THEN <acțiune>*. Partea de condiție a regulii este o expresie logică ce evaluează starea unuia sau mai multor senzori. Aceasta poate include verificări simple, precum depășirea unui prag minim sau maxim (de ex., temperatura depășește 40℃), atingerea unei valori specifice sau menținerea unei stări pentru o anumită perioadă de timp. Acțiunea, pe de altă parte, definește operația ce trebuie executată dacă și numai dacă condiția (sau condițiile) este îndeplinită. Acțiunile pot varia de la trimiterea unei alerte către un operator, la comanda directă a unui actuator din sistem (de ex., închiderea unei valve, pornirea unei pompe) și la înregistrarea unui eveniment de interes în jurnalul de sistem.

Complexitatea sistemului este sporită prin capacitatea de a compune reguli. O condiție poate fi formată din multiple

sub-condiții care implică diferiți senzori, interconectate prin operatori logici precum conjuncția (AND) sau disjuncția (OR). Această flexibilitate permite modelarea unor scenarii complexe și interdependente, reflectând cu fidelitate logica operațională a sistemului monitorizat.

Figura 10: Regula salvata, status, si actiuni ce se pot lua asupra regulii

Platforma oferă două modalități complementare pentru definirea acestor reguli. Prima este cea manuală, printr-o interfață grafică numită "compozitor de reguli", unde operatorii umani pot construi și valida reguli pas cu pas. A doua, o abordare avansată, implică utilizarea inteligenței artificiale. Un mecanism bazat pe LLM (Large Language Model) poate acționa ca un interpretor, traducând cerințe formulate în limbaj natural de către un operator ("avertizează-mă când presiunea scade brusc") în reguli formale, executabile de către motor. Mai mult, sistemele de tip Agentic AI pot analiza datele istorice pentru a identifica corelații și a propune în mod proactiv reguli noi, optimizând automat performanța și siguranța sistemului fără intervenție umană directă.

5.2 Dashboard Personalizabil și Modular

Interfața principală de vizualizare a platformei TROCI este un dashboard personalizabil, conceput pentru a oferi fiecărui utilizator o sinteză vizuală a datelor, adaptată nevoilor și responsabilităților sale specifice. În loc să prezinte o interfață statică și identică pentru toți operatorii, platforma permite crearea unui spațiu de lucru dinamic, personalizat, unde informațiile cele mai relevante pentru rolul utilizatorului sunt prioritizate. Acest lucru este esențial într-un sistem complex, unde un manager ar putea fi interesat de indicatori de performanță la nivel înalt (KPIs), în timp ce un inginer de teren necesită acces rapid la datele brute și istoricul unui set specific de senzori.

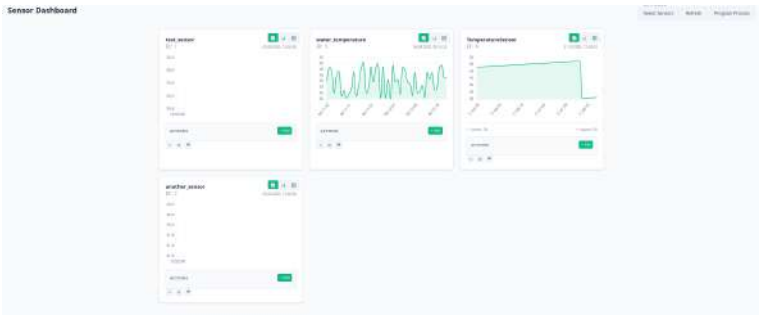

Figura 11: Dashboard-ul specific al unui singur operator/manager, modificabil

Arhitectura acestei interfețe se bazează pe un concept modular de tip **widget**. Fiecare widget este o componentă vizuală autonomă, responsabilă cu afișarea unui singur tip de informație. Platforma oferă o bibliotecă extinsă de widget-uri predefinite, cum ar fi:

- **Grafice de tip Time-Series:** Pentru vizualizarea evoluției în timp a valorilor unuia sau mai multor senzori.
- **Indicatoare de tip Gauge:** Pentru afișarea valorii curente a unui senzor în raport cu praguri predefinite (minim, maxim, optim).
- **Hărți GIS:** Pentru vizualizarea locației geografice a senzorilor și a stării acestora prin coduri de culoare.
- **Tabele de Alerte:** Pentru listarea în timp real a evenimentelor și anomaliilor detectate de sistem.

- **Indicatori de Stare (Status Indicators):** Pentru a arăta starea de funcționare (online/offline) a nodurilor din rețea.

Utilizatorii pot personaliza complet spațiul de lucru printr-un sistem intuitiv de tip **drag-and-drop** pe o grilă flexibilă. Aceștia pot adăuga widget-uri noi din biblioteca de componente, le pot redimensiona și repoziționa pentru a crea aranjamentul optim. Mai mult, fiecare widget în parte este configurabil. De exemplu, un utilizator poate configura un grafic pentru a afișa datele de presiune de la senzorii A și B pe intervalul ultimelor 24 de ore, în timp ce alt utilizator poate configura același tip de grafic pentru a monitoriza umiditatea de la senzorul C în ultima săptămână.

Figura 12: Dashboard-ul simplificat al unui operator

Configurația fiecărui dashboard este unică și persistentă, fiind salvată în profilul utilizatorului. La autentificare, platforma încarcă automat aranjamentul și configurațiile salvate, asigurând o experiență de lucru consistentă și eficientă. Suplimentar, sistemul permite definirea unor layout-uri implicite (default) bazate pe rolul utilizatorului. Astfel, la prima autentificare, un nou operator va primi un dashboard pre-configurat cu cele mai relevante widget-uri pentru funcția sa, pe care ulterior îl poate ajusta conform preferințelor personale. Această abordare modulară și centrată pe utilizator nu doar că sporește eficiența operațională, dar asigură și o scalabilitate facilă a interfeței, noi tipuri de widget-uri putând fi adăugate în viitor fără a afecta funcționalitatea existentă.

5.3 Detectarea și Înrolarea Automată a Senzorilor

Gestionarea eficientă a unei rețele extinse de dispozitive IoT necesită un mecanism robust pentru adăugarea de noi noduri, cu un minim de intervenție manuală. Platforma TROCI implementează un proces de înrolare automată (*automated onboarding*), care permite detectarea, validarea și integrarea noilor senzori în sistem imediat ce aceștia sunt conectați la rețea. Acest proces elimină erorile de configurare umană și reduce semnificativ timpul necesar pentru extinderea rețelei de monitorizare.

Fiecare senzor, fabricat pentru a fi compatibil cu sistemul TROCI, este prevăzut din fabrică cu un identificator unic și imutabil (Unique Universal Identifier - UUID) și un certificat digital. La prima pornire și conectare la rețea, senzorul inițiază un protocol de tip "handshake" cu serverul central. În cadrul acestui proces, senzorul își prezintă certificatul. Platforma verifică validitatea și autenticitatea acestui certificat folosind o autoritate de certificare prestabilită, asigurându-se că dispozitivul este unul legitim și nu o clonă sau un dispozitiv neautorizat.

Odată ce identitatea senzorului este confirmată, platforma inițiază procesul de *provizionare*. Pe baza informațiilor din certificatul digital (de ex., tipul și modelul senzorului), sistemul îi alocă automat un profil inițial. Acest profil include tipul de date pe care le va transmite (presiune, temperatură etc.), unitățile de măsură, frecvența de raportare implicită și un set de reguli de securitate de bază. Operatorul este apoi notificat în interfața de administrare despre prezența unui nou senzor, permițându-i să adauge, dacă este necesar, metadate contextuale, precum locația geografică exactă sau o denumire descriptivă (de ex., "Senzor presiune - conducta principală nord").

5.4 Model de Securitate Stratificat

Securitatea platformei TROCI este concepută pe baza unui model stratificat, cunoscut sub denumirea de "apărare în adâncime" (defense-in-depth), care combină măsuri preventive la nivel de rețea, aplicație și date. Abordarea nu se bazează pe un singur punct de control, ci pe o multitudine de bariere de securitate care protejează sistemul împotriva unei game largi de amenințări. La nivel de perimetru, toate căile de acces externe sunt securizate prin protocoale

de criptare a transportului (TLS 1.3), iar interfețele API sunt protejate împotriva atacurilor comune (ex. SQL Injection, Cross-Site Scripting) prin validări riguroase ale datelor de intrare și utilizarea unui Web Application Firewall (WAF).

Componenta centrală a strategiei de securitate este un sistem granular de Management al Identității și Accesului (IAM), bazat pe modelul de control al accesului pe bază de roluri (Role-Based Access Control - RBAC). Administratorul platformei are capacitatea de a defini roluri specifice (de ex., "Administrator", "Operator de Teren", "Analist Date", "Nod") și de a asocia fiecărui rol un set strict de permisiuni. Aceste permisiuni dictează ce acțiuni poate efectua un utilizator și la ce seturi de date are acces. Astfel, un utilizator este limitat strict la funcționalitățile necesare pentru îndeplinirea sarcinilor sale, conform principiului privilegiului minim.

În cazul în care contul unui utilizator este compromis sau un utilizator acționează cu intenții maligne, modelul RBAC limitează în mod inerent daunele potențiale. Deoarece utilizatorul nu are drepturi administrative, acesta nu poate modifica reguli critice, șterge date istorice sau accesa configurația de bază a sistemului. Suplimentar, toate acțiunile efectuate în platformă, fie de către utilizatori, fie de către senzori, sunt înregistrate într-un jurnal de audit imutabil. Acesta este monitorizat în timp real de un sistem de detecție a anomaliilor, care poate alerta automat administratorii în cazul unor activități suspecte, permițând o reacție rapidă pentru investigarea și izolarea incidentului.

5.5 Motor de Evaluare Paralelă a Regulilor

Capacitatea de a reacționa în timp real la schimbările de mediu este dependentă de performanța motorului de reguli. Într-un sistem cu sute de reguli și mii de evenimente pe secundă, o evaluare secvențială ar introduce o latență inacceptabilă. Pentru a rezolva această provocare, platforma TROCI utilizează un motor de reguli cu procesare paralelă, optimizat pentru un flux masiv de date. Arhitectura acestuia este construită pe un model reactiv, *event-driven*, unde sosirea unei noi date de la un senzor declanșează evaluarea doar a regulilor care depind de acea dată.

Acest mecanism funcționează prin pre-compilarea regulilor într-o structură de date optimizată, adesea un graf de tip *Rete*. Atunci când o nouă valoare este recepționată, aceasta este propagată prin graf, activând simultan toate căile de evaluare relevante. Procesarea se realizează în fire de execuție (threads) paralele, permițând sistemului să evalueze zeci sau sute de reguli complexe în câteva milisecunde. Astfel, se garantează respectarea în timp util a restricțiilor software definite de utilizator și executarea promptă a acțiunilor automate necesare (de ex., închiderea unei valve în timp real[2] după detectarea unei scurgeri).

Un aspect critic al evaluării paralele este gestiunea conflictelor. Pot exista situații în care două reguli, ambele valide, dictează acțiuni contradictorii (de ex., una pornește o pompă, alta o oprește). Pentru a asigura un comportament determinist și sigur, motorul de reguli implementează o strategie de rezolvare a conflictelor. Aceasta se bazează pe un sistem de prioritizare, unde fiecare regulă are asociat un nivel de prioritate definit de operator. În caz de conflict, va fi executată doar acțiunea corespunzătoare regulii cu cea mai mare prioritate, în timp ce acțiunile conflictuale sunt anulate și înregistrate în jurnalul de sistem pentru o analiză ulterioară. Dacă cele două acțiuni au prioritate egală, acțiunile vor fi executate în ordine temporală, fiecare dintre ele având o întârziere și un mecanism de histerezis, pentru a se elimina zgomotul din sistem.

5.6 Arhitectură distribuită, bazată pe API-uri

Platforma TROCI este proiectată conform unei arhitecturi moderne, distribuite, în care comunicarea între componente se realizează prin intermediul unor Interfețe de Programare a Aplicațiilor (API-uri). Acest model presupune că un senzor (sau orice alt client) nu necesită o conexiune directă cu întregul sistem sau cunoștințe despre complexitatea sa internă (baze de date, motor de reguli, etc.). Singura sa responsabilitate este să trimită datele într-un format standardizat către un punct de acces central și securizat, cunoscut sub numele de Access Point (AP).

AP-ul acționează ca o "poartă de intrare" unică pentru toate datele care intră în sistem. Acesta este responsabil pentru sarcini critice precum autentificarea și autorizarea fiecărei cereri (verificând dacă senzorul are dreptul de a trimite date), validarea formatului datelor pentru a asigura integritatea acestora și protecția împotriva unui trafic excesiv

[2] Sintagma "în timp real" se referă la faptul că timpul este cunoscut, nu că acesta este zero.

(rate limiting). Odată ce o cerere este validată, AP-ul o direcționează către microserviciul intern corespunzător, cum ar fi serviciul de ingestie a datelor sau cel de configurare, fără ca senzorul să știe unde sau cum sunt procesate informațiile sale.

Această arhitectură API-centrică oferă avantaje majore în materie de securitate, scalabilitate și flexibilitate. Din punct de vedere al securității, suprafața de atac este redusă drastic, deoarece doar AP-ul este expus rețelelor externe. La nivel de scalabilitate, componentele interne ale platformei (de ex., baza de date) pot fi redimensionate sau chiar înlocuite complet fără a afecta în niciun fel senzorii, atâta timp cât "contractul" API rămâne neschimbat. De asemenea, această abordare facilitează integrarea cu sisteme terțe, care pot consuma date din platforma TROCI sau pot trimite comenzi către aceasta prin intermediul acelorași API-uri publice și bine documentate.

6 Rolul HOLISUN în cadrul proiectului

În anul al doilea al proiectului TROCI, HOLISUN și-a consolidat rolul esențial în proiectarea, dezvoltarea și integrarea componentelor software ale platformei digitale. Activitățile desfășurate în această perioadă au vizat maturizarea arhitecturii distribuite a sistemului, implementarea modulelor operaționale și definirea mecanismelor de securitate și interoperabilitate necesare funcționării unei platforme destinate infrastructurilor critice. Pe parcursul anului, HOLISUN a finalizat structura arhitecturală distribuită și mecanismele de comunicare API-centrice, asigurând un flux coerent de ingestie, validare și procesare a datelor provenite de la rețele extinse de senzori.

Contribuțiile tehnice ale echipei s-au concretizat în dezvoltarea dashboard-ului modular și personalizabil, în implementarea sistemului unificat de management al utilizatorilor și nodurilor, precum și în integrarea mecanismului de compunere și evaluare a regulilor. Tot în această etapă au fost dezvoltate procesul de înrolare automată a senzorilor, modelul de agregare contextuală a datelor și motorul de evaluare paralelă, capabil să proceseze în timp real un volum ridicat de condiții logice. În paralel, HOLISUN a contribuit la definirea și consolidarea modelului de securitate stratificat al platformei, integrând elemente precum controalele de acces granulare, jurnalizarea evenimentelor și validarea fluxurilor de date.

Pe partea de cercetare, echipa HOLISUN a continuat studiile aplicate privind procesarea distribuită a datelor, metodele de detectare a anomaliilor și fundamentarea modelelor de învățare automată ce urmează să fie integrate în etapele ulterioare. Aceste contribuții au fost susținute de o extindere semnificativă a bazei de date inteligente a proiectului, care include tehnologii NewSQL și reprezentări ontologice OWL, versiuni stabile și structurate săptămânal pentru gestionarea coerentă a cunoștințelor.

De asemenea, HOLISUN a participat activ la coordonarea activităților de proiect, la întâlnirile lunare cu partenerii și la workshopul fizic desfășurat la Cluj-Napoca, contribuind la asigurarea coerenței între componentele hardware, software și de cercetare. Activitatea de comunicare și diseminare a fost, de asemenea, consolidată prin administrarea site-ului oficial, dezvoltarea canalelor de social media și promovarea progresului proiectului în mediul profesional și academia internațională. Prin eforturile depuse în această etapă, HOLISUN a pus bazele tehnice necesare pentru integrarea algoritmilor avansați de analiză, securitate și reziliență, care vor fi dezvoltate în anul următor.

7 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

8 Rezultatele proiectului

8.1 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
D2.1	M14	Arhitectură software platformă, flux de date și co-proiectare hardware versiunea 1	Livrat
D2.1	M24	Arhitectură software platformă, flux de date și co-proiectare hardware versiunea 2	În lucru

8.2 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
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	Link articol
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	Link articol
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	Link articol
Emil Pașca, Daniela Delinschi, Rudolf Erdei, Iulia Baraian, Oliviu Matei, "**A Vulnerable-by-Design IoT Sensor Framework for Cybersecurity in Smart Agriculture**"	Agriculture MDPI	Link articol

9 Diseminare și exploatare

9.1 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 150 de vizitatori lunari
- pe pagina web a proiectului: https://troci.holisun.com/, având un număr de 20 de vizitatori lunari
- pe contul de LinkedIn: https://www.linkedin.com/company/holisun, cu peste 550 de adepți
- pe contul de LinkedIn al proiectului https://www.linkedin.com/company/troci2023/, cu 21 de urmăritori
- pe pagina de Facebook: https://www.facebook.com/Holisun.IT/, având peste 2400 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
CUNBM Research Workshop 2025	02.03.2025	—	Laura Andreica	Prezentare *TROCI*
International Mobility Days 2025	19.11.2025-21.11.2025	https://www.mobility-days.at/	Delinschi Daniela	Prezentare *TROCI*

9.1.1 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: 112
LinkedIn	https://www.linkedin.com/company/troci2023/	Urmăritori: 21

10 Concluzii

Anul al doilea al proiectului TROCI a reprezentat o etapă decisivă în evoluția platformei, în care componentele conceptuale definite anterior au fost transformate în module funcționale integrate într-o arhitectură distribuită coerentă. Dezvoltarea sistemului a avansat semnificativ, fiind implementate infrastructura de comunicare API-centrică, dashboard-ul modular și personalizabil, mecanismele de agregare contextuală a datelor, procesul de înrolare automată a senzorilor și motorul de evaluare paralelă a regulilor. Toate aceste elemente au fost validate în cadrul sistemului de testare și au demonstrat capacitatea platformei de a gestiona volume mari de date, de a reacționa în timp real și de a asigura continuitatea operațională în scenarii complexe specifice infrastructurilor critice.

Din punct de vedere științific, această perioadă a consolidat poziția proiectului prin publicarea și prezentarea de articole în conferințe și reviste de specialitate, contribuind la vizibilitatea și recunoașterea internațională a proiectului. Activitățile de diseminare desfășurate prin intermediul platformelor digitale, al workshopurilor și al rețelelor profesionale au sprijinit extinderea impactului proiectului și au facilitat conectarea cu comunități relevante din domeniul securității și rezilienței infrastructurilor critice.

La nivel de management, toate activitățile planificate pentru această etapă au fost realizate conform graficului, fără devieri, iar livrabilele au fost completate și predate conform cerințelor consorțiului. Proiectul a beneficiat de o colaborare eficientă între parteneri, ceea ce a permis integrarea coerentă a componentelor hardware, software și de cercetare.

Privind spre anul următor, accentul se va muta pe integrarea algoritmilor avansați de învățare automată, pe dezvoltarea mecanismelor de detecție și predicție a anomaliilor și pe validarea platformei în scenarii operaționale reale. Baza tehnică și conceptuală construită în anul al doilea asigură premise solide pentru finalizarea cu succes a platformei TROCI și pentru generarea unui impact semnificativ în domeniul protecției și optimizării infrastructurilor critice.

info@holisun.com
http://www.holisun.com
+4-0262-226.778
Versiune document: 1.0 din 24.11.2025