Soluții de securitate în sistemele de automatizare SCADA în contextul protecției infrastructurilor critice

Teză de doctorat – Rezumat

pentru obținerea titlului științific de doctor
Universitatea Politehnica Timișoara
în domeniul de doctorat Ingineria Sistemelor

autor: Alexandra-Ionela ȚIDREA (căs. Basso-Țidrea)
conducător științific: Prof. Univ. Dr. Ing. Ioan SILEA
Octombrie 2025

Sistemele de automatizare și SCADA sunt critice pentru buna funcționare a infrastructurilor critice, printre care se numără industria apei și a energiei, dar și sectorul medical și cel de transport. În acest context, un atac cibernetic lansat cu succes împotriva sistemelor din infrastructurile critice, care poate duce la perturbarea procesului de automatizare și control și chiar la daune fizice, reprezintă o amenințare asupra sectorului industrial și a securității naționale. Aceste sisteme au fost construite fără mecanisme de securitate incluse în designul lor cu scopul de a achiziționa și monitoriza date de la dispozitive prezente la nivelurile ierarhice inferioare (i.e., senzori, actuatori) și de a controla procesele industriale. Cu toate acestea, înainte de evoluția lor către conceptele Industriei 4.0 și IIoT (Industrial Internet of Things), o rețea izolată de tip "air-gaped" era considerată autosuficientă pentru a oferi protecție împotriva atacurilor cibernetice. Însă, în contextul evoluției acestor sisteme către a 4-a revoluție industrială, interconectarea lor cu alte rețele le face vulnerabile prin expunerea datelor către exterior. Mai mult de atât, introducerea securității și menținerea interconectării și a interoperabilității acestor sisteme reprezintă o provocare majoră care vine din numărul mare de dispozitive și protocoale de comunicație folosite, în special a sistemelor preexistente (legacy) cu resurse computaționale limitate și software specific, care nu suportă executarea unor operații complexe și administrarea unor cantități mari de date. Asigurarea unui schimb de date fără probleme este foarte important, considerând cerințele existente de operare în timp real și disponibilitate care sunt obligatorii și nenegociabile pentru infrastructurile considerate vitale. Prin urmare, securizarea sistemelor de automatizare SCADA în contextul protecției infrastructurilor critice este o provocare curentă și o problemă greu de rezolvat. În acest context, prinicipalul subiect de motivație al acestei teze îl consituie oferirea de soluții de securitate pentru sistemele de automatizare SCADA în contextul protecției infrastructurilor critice, luând în considerare provocările curente reprezentate de evoluția către conceptele IIoT. Motivația autorului acestei teze, precum și obiectivele de cercetare și contribuțiile majore ale tezei sunt adresate în Capitolul 1.

Stuxnet [1], atacul asupra centralei de tratare a apei din Florida [2] și pana de curent cauzată de atacul asupra unei centrale electrice din Ucraina [3], sunt doar câteva exemple de atacuri cibernetice asupra sistemelor de automatizare și SCADA cu implicații negative, care evidențiază nevoia urgentă de a implementa măsuri de securitate cibernetică pentru protejarea infrastructurilor critice. Mai mult, creșterea numărului de atacuri cibernetice asupra sistemelor de automatizare SCADA [4],[5] din ultimul deceniu,

împreună cu integrarea proceselor industriale fizice în arhitectura IIoT, au crescut gradul de conștientizare și au atras atenția în cadrul comunității de cercetare și a agențiilor guvernamentale (e.g., NIS 2 directive [6], USA National Security Memorandum on Critical Infrastructure and Resilience [7]) cu privire la importanța securizării sistemelor de control industriale și CPS (cyber-physical systems) [8], [9].

Cu toate acestea, industria este reticentă cu privire la înlocuirea sau actualizarea soluțiilor deja funcționale și operaționale care încorporează structuri preexistente (legacy) nesigure [10], din cauza costului și a ciclului de viață al dispozitivelor inteligente. Prin urmare, tendința este de a folosi o abordare non-invazivă, care presupune actualizări minime când sunt aplicate principiile Industriei 4.0 precum asigurarea interoperabilității. Interoperabilitatea verticală și orizontală este obținută de obicei prin gateway-uri sau structuri de tip wrapper care țintesc protocoalele de bază (e.g. cel mai răspândit protocol preexistent Modbus [11], IEC 61850 [12]), precum si Open Platform Communication Unified Architecture (OPC UA). Securizarea este obținută de obicei la nivelele ierarhice superioare prin implementarea OPC UA [13] sau prin diverse strategii bazate pe gateway [14]. Cu toate acestea, în multe cazuri, structurile preexistente (legacy) nu sunt supuse unor schimbări bruște pentru că ele asigură eterogenitatea protocoalelor de comunicație existente [15]. Mai mult decât atât, implementarea unor mecanisme de securitate pe dispozitive de la nivelele inferioare precum PLC-urile, care au limitări în ceea ce privește resursele computaționale și de memorie, fără a afecta funcționarea normală a procesului de control, este o provocare continuă. Prin urmare, securizarea comunicației la nivele inferioare ale unui sistem de automatizare și SCADA crește complexitatea și efortul pentru a obține comunicare în timp real fără erori sau întârzieri [16].

În plus, vulnerabilitățile sistemelor de automatizare SCADA sunt prezente la nivelul protocoalelor de comunicație, la nivelor componentelor hardware precum PLC-urile și în rândul componetelor software folosite la nivelul de control, după cum este concluzionat de studiul din [17], expunându-le la diverse atacuri cibernetice precum MITM, DoS sau hijacking-ul comunicației SCADA [18],[19],[20]. Mai mult, securizarea comunicației din cadrul sistemelor de automatizare și SCADA este vitală pentru asigurarea autenticității, integrității și confidențialității datelor vehiculate la diverse niveluri arhitecturale, îndeplinind în același timp obiectivele de securitate cu privire la disponibilitatea (availability) și actualitatea (timeliness) datelor. Cu toate acestea, protocoalele de comunicație preexistente (legacy) nesigure (e.g., Modbus TCP, DNP3) sunt foarte răspândite în zilele noastre, chiar dacă nu includ mecanisme de securitate. Chiar și pentru protocoalele noi de comunicație, precum OCP UA, devoltate cu mecanisme de securitate, un studiu realizat de către Oficiul Federal German pentru Securitatea Informațiilor identifică vulnerabilități pentru modurile de securitate suportate de OPC UA care, dacă sunt exploatate, ar putea permite unui atacator să execute atacuri precum eavesdropping, DoS și session hijacking [21].

Aceste vulnerabilități constituie motivația în vederea dezvoltării unor soluții de securitate eficiente pentru protejarea sistemelor de automatizare și SCADA. Metode bazate pe baza unei funcții keyed-hash (HMAC) [22] sau Adi Shamir [23] sunt doar câteva exemple propuse în literatura de specialitate pentru securizarea protocoalelor de comunicație clasice sau preexistente (legacy). Aceste propuneri sunt fie incomplete, sau introduc întârzieri în comunicație. O altă direcție de cercetare în contextul evoluției către IIoT se concentrează pe analiza introducerii unor mecanisme de securitate noi în cadrul infrastucturilor critice precum semnături digitale [24] sau blockchain [25]. Cu toate acestea, aceste propuneri nu oferă o analiză de securitate completă și nici studii de fezabilitate cu privire la aplicabilitatea lor pentru structurile clasice sau preexistente (legacy). De asemenea, alte studii arată ineficiența metodelor existente bazate pe RSA din cadrul protocolului OPC UA pentru dispozitivele cu limitări de resurse prezente la nivelurile ierarhice inferioare [26] a unui sistem de automatizare și SCADA, ceea ce evidențiază nevoia de a dezvolta soluții reziliente și eficiente pentru nivelurile ierahice inferioare ale acestor sisteme. Chiar dacă literatura de specialitate propune mai multe soluții pentru securizarea sistemelor de automatizare și SCADA, încă sunt o multitudine de lacune și provocări majore care necesită abordare. [27]. Începând cu lipsa metodelor de securitate non-intruzive pentru structurile preexistente (legacy), lipsa unor evaluări cu privire la implementarea acestor soluții pe dispozitivele cu memorie redusă și constrângeri computaționale folosite în industrie, urmate de lipsa unei analize detaliate cu privire la protecția împotriva atacurilor cibernetice și

finalizând cu mecanismele de securitate ineficiente care nu îndeplinesc cerințele de disponibilitate și operare în timp real, există încă o nevoie urgentă de a dezvolta soluții de securitate complete și reziliente pentru sistemele de automatizare și SCADA.

Obiectivele cercetării. În contextul menționat mai sus, considerând literatura de specialitate state-of-the art cu privire la vulnerabilitățile sistemelor de automatizare și SCADA, împreună cu propunerile existente pentru protejarea lor împotriva amenințărilor cibernetice, această teză propune următoarele obiective de cercetare denumite în continuare (RO), care sunt sumarizate astfel:

RO1. Analiză a literaturii de specialitate cu privire la provocările actuale pentru securizarea sistemelor de automatizare și SCADA cu focus pe lucrările conexe care au ca scop protocoalele de comunicație preexistente și soluții bazate pe curbe eliptice în contextul IIoT.

RO2. Proiectarea, implementarea și evaluarea soluțiilor de securitate pentru a asigura autenticitatea datelor și stocarea securizată a cheilor din cadrul protocoalelor de comunicație preexistente.

RO3. Definirea conceptului și implementarea soluțiilor de securitate pentru obținerea integrității datelor, autenticitatea datelor și confidențialitatea acestora bazate pe ECC în sisteme de automatizare și SCADA.

RO4. Implementarea și evaluarea performanței pentru securizarea comunicației OPC UA bazată pe pairings și alți algoritmi criptografici relevanți bazați pe ECC.

RO5. Implementarea și evaluarea soluțiilor de securitate bazate pe ECC pe dispozitive cu constrângeri de resurse utilizate în industrie pentru a demonstra fezabilitatea acestora.

Primul obiectiv de cercetare are ca scop studiul si identificarea provocărilor actuale cu privire la introducerea si îmbunătățirea securității din cadrul protocoalelor de comunicație, dispozitivelor IIoT și structurilor de automatizare și SCADA preexistente. Astfel, scopul următorului obiectiv este de a cerceta și defini soluții de securitate pentru asigurarea autenticității și stocarea sigură a cheilor criptografice în cadrul protocoalelor de comunicație clasice (i.e., Modbus TCP), țintind abordări criptografice non-invazive, folosind module-platformă sigure (TPM). În continuare, teza urmărește investigarea și dezvoltarea unor soluții criptografice reziliente care să asigure integritatea, autenticitatea și confidențialitatea datelor bazate pe criptografia cu curbe eliptice (ECC) pentru protecția sistemelor de automatizare și SCADA, luând în considerare constrângerile impuse de către industrie cu privire la cerințele de interoperabilitate și de timp. Un alt obiectiv acoperit de către teză are ca scop implementarea și evaluarea performanței metodelor criptografice pentru protocoale de comunicare recente (i.e., OPC UA) utilizate în Industria 4.0 bazate pe un subset al ECC, mai specific, metode bazate pe criptografia pairing-based (PBC). Ultimul obiectiv are ca scop implementarea și evaluarea unuia dintre conceptele de securitate propuse bazat pe curbe eliptice pe dispozitive cu constrângeri de resurse (i.e., PLCs) utilizate în industrie.

Contribuții majore. În această teză sunt propuse concepte referitoare la implementarea unor metode de securitate pentru sistemele de automatizare și SCADA. În particular, subiectele adresate sunt securitatea protocoalelor de comunicație preexistente, utilizând TPM-uri, definirea, evaluarea și implementarea unor metode criptografice de securitate bazate pe curbe eliptice în cadrul sistemelor de automatizare și SCADA, îmbunătățiri ale securității pentru protocolul de comunicție OPC-UA prin utilizarea ECC și pairings, respectiv integrarea și evaluarea conceptelor de securitate bazate pe ECC pe dispozitive utilizate în industrie. În particular, obiectivele de securitate sunt obținute prin intermediul următoarelor contribuții majore (MC), care fac parte din lucrările de cercetare ale autorului acestei teze:

MC1. Analiza și demostrarea vulnerabilităților din cadrul unui protocol de comunicație preexistent prin crearea și efectuarea unui atac de tip man-in-the-middle pe sistem local de automatizare și SCADA.

MC2. Conceperea, implementarea și evaluarea a două metode care să ofere autenticitatea datelor

vehiculate prin intermediul protocoalelor de comunicare preexistente utilizând TPM-uri.

MC3. Definirea conceptului, implementarea și evaluarea soluțiilor de securitate pentru Modbus TCP bazate pe semnături digitale și scheme de criptare hibridă utilizând ECC.

MC4. Implementarea și evaluarea performanței unei comunicații pe OPC UA, îmbunătățită din punctul de vedere al mecanismelor de securitate, bazată pe semnături digitale care utilizează curbe criptografice de diverse dimensiuni.

MC5. Definirea conceptului, implementarea și evaluarea metodelor bazate pe PBC pentru a securiza protocolul de comunicație OPC UA.

MC6. Integrarea și evaluarea soluțiilor de securitate bazate pe ECC pe un ansamblu (setup) compus din PLC-uri și dispozitive utilizate în industrie.

Protocoalele de comunicație preexistente sunt vast folosite în infrastructuri critice, chiar dacă datele sunt transmise fără a fi protejate de mecanisme de securitate, ori au mecanisme de securitate limitate. Astfel, în acest caz, scopul este de a evidenția vulnerabilitățile protocoalelor de comunicație nesigure și de a demonstra că dispozitivile utilizate în industrie, precum PLC-urile Siemens, sunt indirect vulnerabile prin prisma breșelor de securitate. Rezultatele arată că, având la dispoziție cunoștințe de specialitate, un cyber-attack reușit este posibil. Contribuția majoră MC1 e parte din lucrarea de specialitate a autorului, referențiată în [28].

Mai mult, detaliind MC2, o schemă de autentificare criptografică, utilizând TPM-uri, bazată pe două metode, e concepută și propusă spre a oferi integritatea și autenticitatea datelor în cadrul protocolului Modbus TCP care a fost ales ca reprezentativ al sistemelor de comunicație preexistente, fiind cel mai folosit. Cu toate acestea, soluția propusă poate fi extinsă și pentru alte protocoale de comunicație preexistente. Merită menționat că TPM-urile sunt integrate în arhitectura de sistem a conceptelor propuse pentru a le evidenția avantajele cu privire la introducera unor mecanisme de securitate și menținerea comunicației în timp real în cadrul sistemelor de automatizare și SCADA. Pentru implementarea software, cateva biblioteci (libraries) open-source sunt integrate și configurate. Mai mult, evaluarea conceptului propus arată conformitatea cu constângerile de timp impuse de către industrie asupra comunicației. Mai mult, atacul creat în MC1 este utilizat pentru a evalua securitatea conceptului implementat cu privire la atacurile de tip MITM. Contribuția majoră MC2 este parte din lucrarea de specialitate a autorului, referențiată în [28].

Evaluarea și implementarea metodelor criptografice bazate pe primitive ale curbelor eliptice e o metodă de abordare inovativă pentru multiple contribuții si soluții de securitate ale sistemelor de automatizare si SCADA prezentate în această teză. Astfel, implementarea și definirea conceptului, menționate în MC3, se bazează pe ECC care este aleasă deoarece respectă constrângerile sistemelor de la nivelele ierarhice inferioare ale rețelei de automatizare și SCADA, cât și pentru capabilitățile de securitate. Două metode pentru oferirea autenticității, integrității și confidențialității datelor transmise prin protocoale de comunicație nesigure sunt propuse. Soluția este implementată utilizând protocolul Modbus TCP ales ca reprezentativ pentru protocoalele preexistente nesigure, biblioteci de tip open-source care utilizează limbajul de programare C, care sunt integrate și configurate pentru a permite punerea în aplicare a soluției, și evaluarea ei pe setupul experimental compus din dispozitive utilizate în industrie precum PLC-uri cu constrângeri de memorie, care face parte din contribuția MC6. Evaluarea constă în măsurarea timpului de execuție al fiecărei operații criptografice pentru mai multe curbe ECC cu dimensiuni variate. Analiza de securitate concluzionează că ambele metode oferă protecție împotriva atacurilor de tip MITM și replay. Contribuția majoră MC3 este parte din lucrarea de specialitate a autorului referențiată în [29].

Integrarea unor soluții noi de securitate bazate pe metode criptografice în cadrul sistemelor de automatizare și SCADA este o provocare în prezent datorată resurselor limitate și cerințelor de a efectua operații în timp real. Când o soluție de securitate este propusă, trebuie analizată atât fezabilitatea implementării pe sistemul țintă fără a introduce întârzieri, cât și de a nu-i afecta modul de funcționare normal. Astfel, un sistem experimental a fost conceput, constituit din două PLC-uri de tip Industruino și

unul de tip MDUINO, ambele utilizate în cadrul sistemelor de automatizare și SCADA, fiind folosite în industria apei în cadrul stațiilor de tratare a apei, respectiv în cadrul sectorului energiei. Aceste dispozitive au incluse interfețe de comunicare utilizate în infrastructuri critice precum RS-232, I2C, Ethernet, RS-485 și suport pentru utilizarea protocolului de comunicație Modbus. Pentru fiecare PLC a fost considerat un controller de securitate Optiga Trust X care a acționat precum un procesor criptografic și ca un dispozitiv de stocare sigură a cheii criptografice pentru fiecare nod Modbus al comunicației. Pentru a putea implementa soluția propusă în contribuția MC3, biblioteci software de tip open-source cât și biblioteci personalizate care rulează pe PLC-uri sunt integrate și optimizate. Odată integrate pe ansamblul experimental, latența introdusă de soluția propusă din cadrul MC3 este măsurată, iar nivelul de securitate introdus pentru fiecare curbă ECC folosită este discutat. Rezultate evaluării arată că soluția de securitate implementată, bazată pe ECC pentru ambele metode, respectă cerințele de operare în timp real și este fezabilă pentru a fi implementată pe dispozitive cu constrângeri de memorie similare fără a cauza pierderea interoperabilității sistemelor țintă. Contribuția majoră MC3 este parte din lucrarea de specialitate a autorului referențiată în [29].

În tranziția către Industria 4.0 au fost dezvoltate protocoale de comunicație noi (i.e., OPC UA) care au integrate mecanisme de securitate. Totuși, din momement ce dispozitivele preexistente în majoritatea cazurilor nu au fost îmbunătățite, aceste mecanisme de securitate sunt inactivate deoarece necesită costuri computaționale mari. În acest context, un concept de îmbunătățire a protocolului de comunicație OPC UA folosind ECDSA este dezvoltat și implementat având ca țintă oferirea de date autentificate între un client și server. În scopul implementării, biblioteci de tip open-source au fost folosite pentru protocolul OPC UA și pentru operațiile criptografice necesare. Pentru evaluarea performanței, un ansamblu experimental care încorporează un PLC cu un server OPC UA și un Raspberry PI 4 acționând ca un client OPC UA este definit, facilitând implementarea conceptului și efectuarea unor măsurători de timpi. Performanța timpilor a fost analizată pe acest ansamblu experimental pentru curbe ECC de diverse dimensiuni începând de la 160 biți până la 446 biți în cadrul schemei de autentificare. Rezultatele obținute arată că pentru toate curbele evaluate de tip ECC, conceptul propus respectă cerințele de timp impuse de către protocolul de comunicație OPC UA. Contribuția majoră MC4 este parte din lucrarea de specialitate a autorului referențiată în [30].

În plus, în cazul integrării curbelor criptografice eliptice în cadrul protocolului de comunicație OPC UA, un concept pentru securizarea comunicației OPC UA client-server utilizând pairings, care sunt un subset al ECC, fiind parte din protocoalele de tip zero-knowledge și blockchain, este propus. Au fost selectate pairings deoarece au proprietăți unice precum agregare, și semnături de dimensiuni reduse. Două scheme criptografice pentru oferirea autenticității și integrității datelor bazate pe semnăturile digitale de dimensiuni reduse Boneh-Lynn-Shacham (BLS) și semnături BLS agregate definite pentru un scenariu personalizat sistemelor de automatizare și SCADA au fost concepute și implementate. În continuare protocolul de agreare a unei chei comune între trei părți numit tripartite Diffie Hellman (DH) bazat pe pairings este integrat și evaluat din perspectiva timpului de execuție pentru câteva curbe ECC pairing-friendly. În plus, algoritmul Elliptic-Curve Diffie-Hellman (ECDH), folosit pentru a obținerea unui secret comun între două părți și care poate fi utilizat pentru autentificarea mesajelor vehiculate în cadrul unui canal nesigur, este evaluat din aceeași perspectivă ca tripartite DH. Conceptul propus pentru implementarea tuturor schemelor criptografice este evaluat pe un ansamblu experimental prin măsurarea duratei fiecărei operații criptografice. Nivelul de securitate oferit de către fiecare curbă ECC de tip pairing-friendly este analizat în contrast cu numărul adițional de octeți introduși asupra canalului de comunicație ca rezultat al algoritmului pentru generarea semnăturii digitale. În plus, o comparație din perspectiva timpului de execuție între BLS și ECDSA este oferită considerând rezultatele obținute în [30] , care este baza contribuției majore MC4. Contribuția majoră MC5 este parte din lucrarea de specialitate a autorului referențiată în [31].

Aceste contribuții sunt parte din lucrările de cercetare ale autorului, fiind fie publicate în jurnale de specialitate, fie urmând a fi evaluate în jurnale, respectiv conferințe. Ca sumar, contribuțiile majore din această teză provin din următoarele lucrări de cercetare unde autorul acestei teze este prim-autor:

- [28] Tidrea, Alexandra, Adrian Korodi, and Ioan Silea. "Cryptographic considerations for automation and SCADA systems using trusted platform modules." Sensors 19.19 (2019): 4191
- [29] Tidrea, Alexandra, Adrian Korodi, and Ioan Silea. "Elliptic curve cryptography considerations for securing automation and SCADA systems." Sensors 23.5 (2023): 2686.
- [30] Tidrea, Alexandra, and Adrian Korodi. "ECC Implementation and Performance Evaluation for Securing OPC UA Communication." 2023 IEEE 22nd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). IEEE, 2023
- [31] Tidrea, Alexandra, and Adrian Korodi. "Pairing cryptography considerations for securing OPC UA communication within SCADA and automation systems." (**under submission)**.

Această teză propune diverse soluții de securitate aplicabile sistemelor de automatizare și SCADA în contextul protecției infrastructurii critice, considerând provocările curente din cadrul Industrial Internet of Things, și efectuează o analiză a lor care are ca scop evaluarea fezabilității implementării acestora pe dispozitive industriale. Ca și sumar al tezei, Capitolul 1 prezintă motivația, obiectivele de cercetare și contribuțiile majore ale tezei. Celelalte capitole ale tezei sunt structurate după cum urmează. Capitolul 2 prezintă o informație de bază a sistemelor de automatizare și SCADA necesară pentru contextul tezei și adresează lucrările de cercetare relevante pentru conținutul tezei cu privire la vulnerabilitățile existente și soluțiile de securitate propuse. Apoi, Capitolul 3 prezintă două metode pentru securizarea protocoalelor de comunicație preexistente utilizând TPM-uri, în timp ce evaluarea timpilor de execuție este discutată pentru toate operațiunile criptografice. În același capitol un atac de tip MITM este conceput și executat pe un sistem de automatizare și SCADA local. Capitolul 4 adresează conceptul, implementarea, integrarea și evaluarea ECC în cadrul infrastructurilor critice pentru asigurarea autenticității, integrității și confidențialității datelor. În primul rând, în acest capitol este prezentată o schemă de autentificare bazată pe ECDSA și o schemă hibridă de criptare bazată pe ECIES. Apoi urmează integrarea și evaluarea acestor soluții pe un ansamblu experimental care conține dispozitive folosite în industrie. În cele din urmă, o schemă de îmbunătățire a securității pe OPC UA bazată pe ECDSA este implementată și evaluată. Capitolul 5 introduce metode bazate pe pairings pentru securizarea comunicației pe OPC UA, prin implementarea semnăturilor digitale BLS pentru autentificarea datelor, semnăturilor agregate BLS, schemă customizată pentru un scenariu real OPC UA din cadrul unui sistem de automatizare și SCADA, precum și prin schema tripartite DH, pentru a stabili o cheie comună. Capitolul 6 încorporează concluziile tezei și prezintă posibile viitoare direcții de cercetare. Următoarele paragrafe sumarizează contribuțiile acestei teze și subliniază îmbunătățirile aduse soluțiilor de securitate actuale care există în industrie sau sunt prezentate ca state-of-the-art.

Capitolul 2 prezintă în primă fază informația de bază cu privire la evoluția și arhitectura sistemelor de automatizare și SCADA, urmată de aspectele teoretice ale criptografiei cu curbe eliptice împreună cu proprietățile de securitate ale primitivelor criptografice utilizate în conceptele de securitate propuse de această teză. În continuare, identifică provocările curente în securizarea SCADA și a sistemelor de automatizare, adresând informațiile relevante din lucrările de specialitate cu privire la subiectul acestei teze, începând cu vulnerabilitățile existente, urmate de soluțiile de securitate propuse în lucrările de cercetare state-of-the-art. Menținerea interoperabilității și efectuarea operațiilor în timp real prin introducerea mecanismelor de securitate în sistemele de automatizare și SCADA reprezintă una din provocările curente majore. Mai mult, metode ineficiente sau lipsa unor metode de securitate non-invazive pentru sistemele preexistente, precum și implementarea lor pe dispozitive cu constrângeri de resurse împreună cu o creștere de cost care provine din actualizarea sistemelor de control industriale funcționale cu dispozitive noi, mai sigure sunt doar câteva lacune care subliniază nevoia urgentă de dezvoltare a unor soluții de securitate reziliente pentru protecția infrastructurilor critice. Proiectarea acestui tip de soluții de securitate reprezintă motivația principală a acestei teze. Totuși, ținând cont de urgența protejării acestor sisteme, în afară de eforturile de cercetare pentru dezvoltarea algoritmilor criptografici și a conceptelor de securitate, furnizorii acestor dispozitive utilizate în sistemele de control industriale trebuie să considere evaluarea și încapsularea

primitivelor criptografice propuse de către literatura de specialitate în cadrul produselor concepute pentru infrastructurile OT.

Capitolul 3 prezintă două metode, parte a unei scheme criptografice de autentificare pentru securizarea protocoalelor de comunicație preexistente, folosind abilitățile TMP-urilor pentru a răspunde problemelor de securitate adresate de structurile preexistente și necesității de a dezvolta soluții de securitate reziliente pentru sistemele de automatizare și SCADA. Arhitectura sistemului, din perspectivă abtractă, a conceptului propus cu elementele logice de sistem este prezentată în Figura 1.

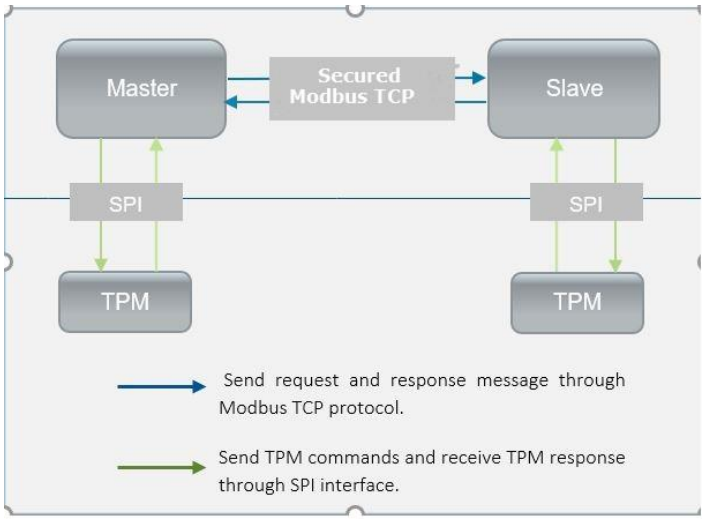

Figura 1: Arhitectura de sistem a conceptului propus - perspectiva abstractă [28]

În primul rând, un atac MITM asupra unui protocol de comunicație preexistent este proiectat și implementat pe un sistem local de automatizare și SCADA după cum este prezentat în Figura 2, care conține un PLC real (i.e., Siemens S7-1200) pentru a-i evidenția vulnerabilitatea împotriva amenințărilor cibernetice și, indirect, asupra vulnerabilităților de securitate a dispozitivelor folosite în industrie pe diferite niveluri arhitecturale. În al doilea rând, ca parte a schemei de autentificare care folosește TPM-ul, prima metodă utilizează primitivele HMAC-SHA-256, în timp ce a doua este bazată pe ECDSA ECC-256. Aceste metode sunt proiectate, implementate și evaluate pe un ansamblu (setup) experimental. Câteva biblioteci open-source scrise în limbaj C au fost optimizate, ajustate și integrate pentru a permite implementarea software a conceptului propus. Conceptul de securitate propus a fost evaluat pentru protecția împotriva atacurilor cibernetice MITM, utilizând același design ca cel folosit pe sistemul local de automatizare și SCADA. Rezultatele obținute prezintă cum conceptul de securitate propus este rezistent la acest tip de atac cibernetic și, în corelație cu rezultatele analizei de securitate, îndeplinește proprietățile de securitate propuse prin oferirea autenticității și a integrității schimbului de date prin intermediul protocolului de comunicație preexistent ales. În continuare, rezultatele de timp obținute prin măsurătorile efectuate pe setup-ul experimental arată îndeplinirea constrângerilor de timp impuse de industrie pentru ambele metode propuse. Mai mult, conceptul propus valorifică capabilitățile TPM-urilor de a stoca și genera o cheie criptografică într-un mod sigur, pentru a îmbunătăți nivelul de securitate. Acest avantaj constituie un caz solid pentru folosirea TPM-urilor ca parte a soluțiilor de securitate, în vederea protejării infrastructurilor critice. În continuare, toate operațiile criptografice necesare în cadrul schemei de autentificare au fost executate de către însuși TMP și accesate din aplicație prin intermediul unui wrapper. Rezultatele de timp obținute arată îndeplinirea cerințelor de disponibilitate și actualitate, evidențiind viabilitatea folosirii TPM-urilor pentru introducerea securității fără a afecta funcționarea normală a proceselor din cadrul structurilor de

automatizare și SCADA. Aceste aspecte fac din conceptul propus ”proof-of-concept” o temă de noutate fezabilă pentru a fi implementată și adoptată în industrie, în special pentru că oferă oportunitatea de reducere a interferențelor asupra sistemelor preexistente funcționale prin implementarea lui ca un strat de comunicație adițional. Această afirmație este susținută de către noul PLC Kunbus (disponibil din 2025) dezvoltat și proiectat cu un TMP inclus în cadrul hardware-ului său, accentuând aplicabilitatea conceptului propus pentru aplicațiile industriale reale de introducere a securității. Conținutul și rezultatele prezentate în acest capitol sunt bazate pe lucrarea de cercetare [28] a autorului acestei teze.

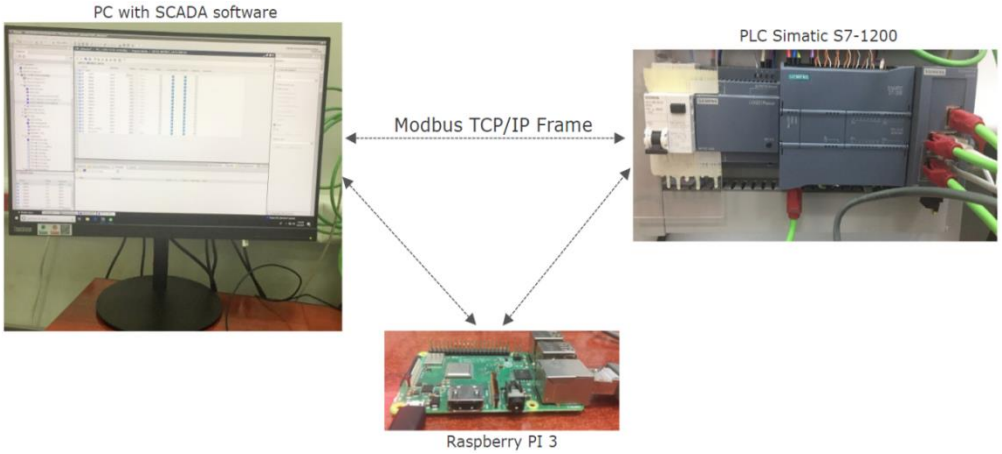

Figura 2: Setup fizic real pentru implementarea atacului MITM pe Modbus TCP [28]

Capitolul 4 prezintă două soluții de securitate funcționale bazate pe ECC pentru securizarea protocoalelor de comunicație preexistente și OPC UA, precum și pentru permiterea implementării pe dispozitive cu resurse limitate larg răspândite, dispersate la nivelele ierarhice inferioare a unui sistem de automatizare și SCADA real, atâta timp cât cerințele de timp impuse de industrie sunt îndeplinite. Prima soluție este bazată pe ECC pentru securizarea datelor vehiculate prin intermediul protocoalelor de comunicație preexistente cu Modbus TCP selectat ca reprezentativ, cu focus pe implementarea și integrarea ei pe dispozitive industriale de nivel ierarhic inferior cu constrângeri de resurse folosite în cadrul sistemelor de automatizare și SCADA reale. Ca parte a soluției propuse, două metode bazate pe ECC sunt implementate, proiectate și evaluate, cu focus pe integrarea și implementarea lor pe dispozitive de nivel ierarhic inferior cu constrângeri de resurse. Prima metodă bazată pe ECDSA oferă autenticitate și integritate a datelor, în vreme ce a doua soluție bazată pe ECIES oferă confidențialitate și integritate a datelor schimbate între două dispozitive industriale (ex. PLC-uri) prin intermediul protocolului de comunicație nesigur Modbus TCP. Adițional, un setup experimental format din PLC-uri folosite în sistemele de automatizare și SCADA reale, mai exact două dispozitive Industruino și un PLC MDUINO, este proiectat pentru a permite integrarea, implementarea și evaluarea celor două scheme criptografice propuse. Setup-ul experimental este prezentat în Figura 3. În continuare, o evaluare a performanței este efectuată pe setup-ul experimental pentru mai multe curbe eliptice cu diverse dimensiuni ale cheii folosite în cadrul schemei de autentificare considerând costul computațional, latența adăugată și nivelul de securitate. Ca element adițional al setup-ului experimental, un microprocesor de securitate Optiga Trust X este integrat cu succes pentru îmbunătățirea securității schemei de autentificare propuse ca o alternativă la o soluție bazată doar pe software. Pentru a finaliza setup-ul experimental, câteva biblioteci open-source scrise în limbajul de programare C sunt optimizate și ajustate în vederea permiterii implementării conceptului de securitate.

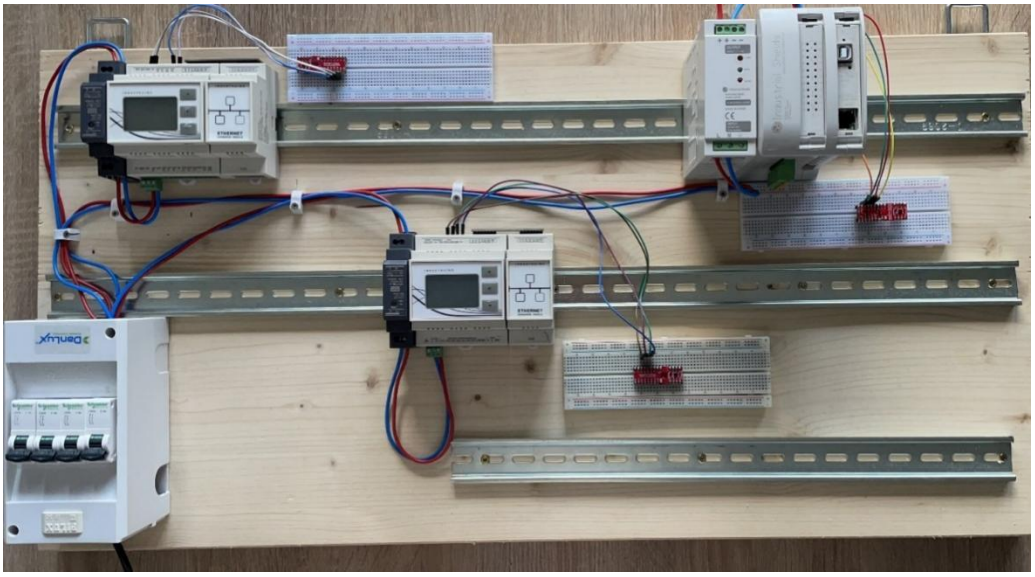

Figura 3: Setup experimental hardware cu PLC-uri și trei dispozitive Optiga Trust X [29]

Pentru ambele scheme criptografice propuse, rezultatele de timpi obținute prin efectuarea măsurătorilor pe setup-ul experimental arată coordonarea cu constrângerile de timp impuse de industrie în cadrul unei rețele reale de SCADA și automatizare referitoare la protocolul de comunicare preexistent Modbus TCP, în timp ce este integrat și evaluat pe dispozitivele PLC de nivel ierarhic inferior cu limitări de resurse Industruino și MDUINO. Mai mult decât atât, rezultatele obținute arată că Optiga Trust X oferă un cost computațional mai scăzut și un nivel mai ridicat de securitate decât soluția software ECDSA. Totuși, schema criptografică bazată pe ECDSA a fost implementată cu succes pe PLC-urile selectate fără a folosi cipuri de securitate, respectând constrângerile de timp impuse de industrie. În vederea unei soluții complete pentru a activa un canal securizat de încredere (trusted), schema de autentificare trebuie executată înaintea schemei de criptare hibridă. Cu toate acestea, cele două metode propuse sunt proiectate pentru a permite implementări diferite, ținând cont de obiectivele de securitate ale sistemelor de arhitectură vizate. După cum s-a prezentat anterior, analiza de securitate arată că ambele metode oferă protecție împotriva atacurilor de tip MITM și ”replay”, în timp ce adițional schema de criptare hibridă oferă rezistență împotriva atacurilor cu texte cifrate (cyphertext attacks). Aceasta întărește puterea soluției de securitate și susține obiectivele de securitate obținute cu privire la integritate, autenticitate și confidențialitate, după cum s-a prezentat în rezultatele experimentale. După cum s-a demonstrat prin măsurători, conceptul propus îndeplinește limitările de timp cu privire la protocolul de comunicare preexistent Modbus TCP a sistemelor reale SCADA și de automzatizare, în timp ce au fost implementate pe PLC-urile de nivel ierarhic inferior Industruino și MDUINO. În plus, aceasta demonstrează fezabilitatea integrării și implementării non-invazive a conceptului de securitate bazat pe ECC integrat pe dispozitive cu limitări de resurse care există deja în industrie fără necesitatea de a extinde structurile moștenite cu noi dispozitive sau înlocuirea lor cu dispozitive sigure prin design, care reprezintă o abordare costisitoare și invazivă. Aceste aspecte, în corelație cu rezultatele evaluării de securitate și durata de timp, cum de altfel și cu integrarea demonstrată pe dispozitivele folosite într-un sistem SCADA și de automatizare real, fac ca această soluție de securitate să fie o noutate cu potențial real de a fi preluată și implementată în industrie pentru a introduce securitate bazată pe ECC printre infrastructurile critice și extinsă către alt protocol nesigur de comunicare preexistent, vizând proprietăți de securitate similare. Ca o a doua soluție de securitate bazată pe ECC, a doua mare secțiune a acestui capitol prezintă un concept pentru securizarea comunicării client-server prin protocolul OPC UA bazat pe ECDSA ca o alternativă la soluția de securitate implementată existentă, bazată pe RSA, cu focus pe fezabilitatea de a fi integrată și implementată pe dispozitive de nivel ierarhic inferior, folosite

în industrie în contextul comunicării PLC cu SCADA sau PLC cu PLC. Principalii pași ai schemei de autentificare proiectată și implementată pentru a îmbunătăți securitatea OPC UA sunt prezentați în Figura 4.

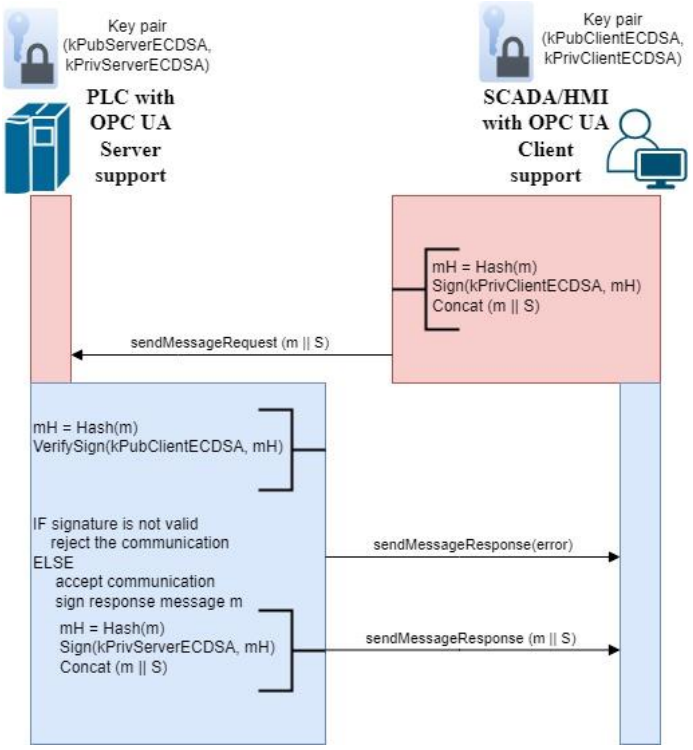

Figura 4: OPC UA mesaj de autentificare bazat pe ECDSA [30]

O evaluare de performanță a soluției de securitate bazată pe primitivele ECDSA și SHA256 este realizată pe setup-ul experimental, care include un PLC industrial real, pentru câteva curbe eliptice ECC cu diverse dimensiuni ale cheii. Pentru a permite implementarea conceptului de securitate pe setup-ul experimental, câteva biblioteci open-source scrise în limbajul de programare C sunt optimizate și ajustate. Rezultatele obținute prin măsurători arată că toate curbele eliptice selectate îndeplinesc cerințele de timp a comunicației pe OPC UA, care dovedește că soluția propusă este potrivită pentru implementarea pe dispozitive cu limitări de resurse. Adițional, măsurătorile de timp obținute și rezultatul analizei de securitate arată că profilele de securitate OPC UA pot fi extinse să adopte pe lângă NIST P-256 și NIST P-384 celelalte curbe eliptice selectate și evaluate care îndeplinesc constrângerile de timp impuse de către industrie. Mai mult decât atât, după cum s-a demonstrat prin măsurători, conceptul propus bazat pe ECDSA îndeplinește constrângerile de timp ale OPC UA pentru comunicația client-server în contextul sistemelor de automatizare și SCADA sau mediilor IoT, îndeplinind cerințele de disponibilitate (availability) și actualitate (timeliness), demonstrând astfel fezabilitatea pentru implementarea și adoptarea lor în aplicații industriale reale. Conținutul și rezultatele prezentate în acest capitol sunt bazate pe lucrările de cercetare [29] și [30] a autorului acestei teze.

Capitolul 5 prezintă un concept de securitate bazat pe PBC, care este un subset al ECC, pentru îmbunătățirea securității comunicării client-server pe OPC UA în contextul comunicării de tip PLC cu PLC și PLC cu SCADA, cu focus pe fezabilitatea acesteia de a fi integrată și implementată pe dispozitive industriale dispersate la nivelele ierarhice inferioare ale unui sistem de automtizare și SCADA real, atâta timp cât îndeplinește constrângerile de timp pe OPC UA și impuse de către industrie. Primele două scheme criptografice prezentate, mai exact schema de autentificare BLS și schema de agregare a semnăturilor BLS,

oferă autenticitate și integritate pentru mesajele de date schimbate prin canalul de comunicație OPC UA. Schema BLS de autentificare propusă pentru îmbunătățirea securității OPC UA a fost implementată ca o alternativă la semnăturile digitale bazate pe RSA folosite în versiunea standardizată actuală și implementată deja pe dispozitive folosite în industrie. Adițional, schema propusă de semnături agregate BLS pentru OPC UA a fost implementată ca o soluție de securitate pentru optimizarea și reducerea costului computațional necesar pentru verificarea unei semnături digitale din cadrul unei arhitecturi multi-server/client prezentate pentru un scenariu customizat, unde un server de agregare OPC UA este folosit în contextul unei arhitecturi reale a unui sistem de automatizare și SCADA. Scenariul customizat este prezentat în Figura 5. În acest context, schema propusă de semnături agregate BLS customizată pentru un scenariu real OPC UA dovedește fezabilitatea de a fi integrată în cadrul cazurilor de utilizare aplicabile infrastructurilor critice reale prin scalarea numărului de semnatari (signers) și verificatori (verifiers) la cel necesar, determinat de arhitectura OT avută în vedere. Ambele soluții sunt proiectate, implementate în OPC UA stack, și evaluate pe setup-ul experimental.

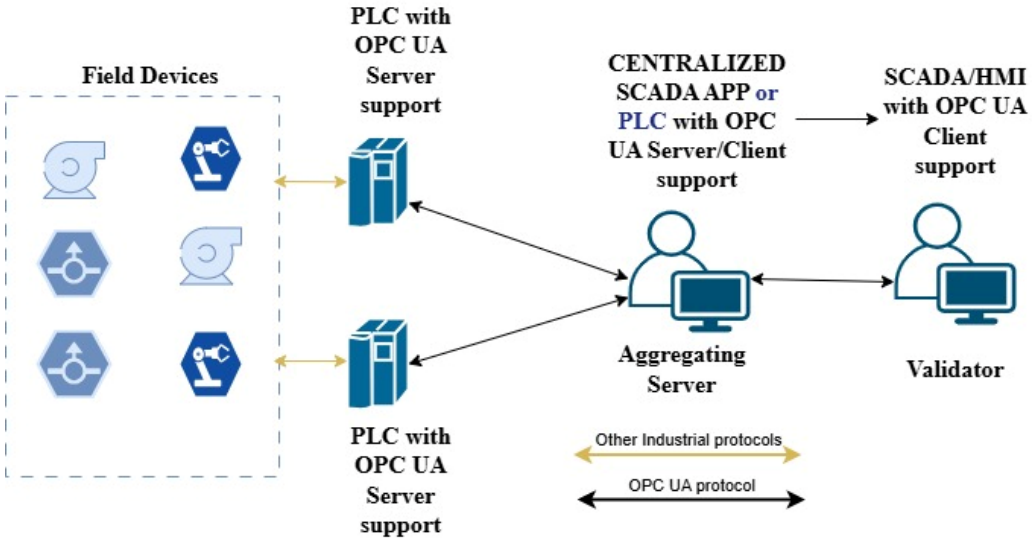

Figura 5: Descriere a cazului de utilizare a comunicației OPC UA pentru sistemele de automatizare și SCADA [31]

Schema tripartite DH a fost evaluată deoarece oferă un mecanism pentru stabilirea unei chei secrete comune între trei dispozitive și datorită utilizării sale ca bază pentru viitori algoritmi criptografici complexi care pot fi aplicați în cadrul aplicațiilor industriale OPC UA. Cu toate acestea, chiar dacă rezultatele arată îndeplinirea cerințelor de disponibilitate și actualitate ale sistemelor de automatizare și SCADA, schemă bazată pe tripartite DH necesită actualizări viitoare pentru a încorpora metode de autentificare, care să îi ofere rezistență împotriva atacurilor MITM. Toate schemele criptografice implementate sunt evaluate din punct de vedere al duratei de timp și al atenției adăugate pe canalul de comunicație OPC UA, pe un setup experimental, care este proiectat să emuleze un sistem real de automatizare și SCADA, ce include printre alte dispozitive embedded și un dispozitiv utilizat în industrie. Mai mult, rezultatele obținute arată că schemele propuse bazate pe semnături BLS oferă semnături digitale de dimensiuni mai mici cu un cost computațional mai mare, în comparație cu soluția bazată pe ECDSA din (61), considerând curbe eliptice ECC cu nivele de securitate similare. În continuare, dimensiunile semnăturilor digitale rezultate, reflectate în latența adăugată pe rețeaua de comunicație cresc împreună cu nivelul de securitate și costul computațional pentru toate curbele evaluate, când modul de securitate OPC UA este setat pe None. Pentru celelalte două moduri de securitate disponibile în cadrul protocolului de comunicație OPC UA, când semnăturile digitale bazate pe RSA sunt folosite, lățimea de bandă a rețelei este mai mare pentru același nivel de securitate față de conceptul propus bazat pe semnături BLS. Mai mult de atât, bazat pe rezultatele de timp obținute, profilele de securitate OPC UA pot fi actualizate să includă toate curbele ”pairing

friendly" evaluate care oferă un nivel de securitate mai mare decât 100 și mai mic sau egal cu 256, împreună cu algoritmii propuși bazați pe BLS, ca protocoale noi de securitate. Munca realizată în acest capitol demonstrează, prin măsurătorile de timp efectuate pe setupul experimental, că conceptul propus de securitate îndeplinește constrângerile de timp impuse de către industrie pentru comunicația client-server OPC UA din cadrul sistemelor de automatizare și SCADA reale pentru toate schemele criptografice implementate, bazate pe PBC (pairing based criptography) și pentru toate curbele ECC (pairing friendly). În continuare, rezultatele de timp obținute prin măsurători efectuate pe setupul experimental, asociate cu schemele criptografice propuse și implementate, bazate pe BLS, arată îndeplinirea cerințelor de disponibilitate (availability) și actualitate (timeliness), accentuând potențialul real de a fi implementate independent sau împreună în industrie, în cadrul infrastructurilor critice, la nivelele ierarhice inferioare ale unui sistem real de automatizare și SCADA, fără a-i afecta modul de funcționare normal. Conținutul și rezultatele prezentate în acest capitol sunt bazate pe lucrarea de cercetare a autorului acestei teze, trimisă spre publicare, din [31].

Capitolul 6 redă rezultatele de cercetare revendicate în capitolele anterioare, care au fost validate prin intermediul a patru lucări de cercetare, unde autorul acestei teze este prim-autor.

Sumarizând, această teză prezintă diverse metode bazate pe ECC și PBC pentru securizarea sistemelor de automatizare și SCADA în contextul protecției infrastructurilor critice și efectuează evaluarea lor cu focus pe posibilitatea de a fi implementate pe dispozitive industriale. Contribuțiile acestei teze permit, în cele din urmă, activarea unor mecanisme de securitate care pot fi introduse de către industrie pentru a securiza sistemele de automatizare și SCADA în contextul protecției infrastructurilor critice, depășindu-le limitările cu privire la constrângerile de timp, dispozitive cu resurse limitate și cerințe de disponibilitate (availability), atâta timp cât oferă interoperabilitate fără a perturba procesele de control.

Referințe

[1] Folgado, Francisco Javier, et al. "Review of Industry 4.0 from the perspective of automation and supervision systems: Definitions, architectures and recent trends." Electronics 13.4 (2024): 782, https://doi.org/10.3390/electronics13040782

[2] New Jersey Cybersecurity & Communications Integration Cell (NJCCIC). Cybersecurity for Critical Infrastructure: Water and Wastewater. State of New Jersey, 6 March 2023, Internet Archive. [Online]. Archive: https://web.archive.org/web/20240716093218/https:/www.cyber.nj.gov/threat-landscape/cybersecurity-for-critical-infrastructure/water-and-wastewater (accessed: 2024-10-22)

[3] Whitehead, David E., et al. "Ukraine cyber-induced power outage: Analysis and practical mitigation strategies." 2017 70th Annual conference for protective relay engineers (CPRE). IEEE, 2017, https://doi.org/10.1109/CPRE.2017.8090056

[4] Gerrikagoitia, Jon Kepa, et al. "Digital manufacturing platforms in the industry 4.0 from private and public perspectives." Applied Sciences 9.14 (2019): 2934, https://doi.org/10.3390/app9142934

[5] Müller, Julian Marius. "Antecedents to digital platform usage in Industry 4.0 by established manufacturers." Sustainability 11.4 (2019): 1121. https://doi.org/10.3390/su11041121

[6] Cyber Risk GmbH, "The NIS 2 Directive", https://www.nis-2-directive.com/

[7] United States, The White House. National Security Memorandum on Critical Infrastructure Security and Resilience. 30 Apr. 2024. The White House, Internet Archive. [Online]. Archive: https://web.archive.org/web/20250118023435/https:/www.whitehouse.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience/ (accessed: 2024-11-27)

[8] Gao, Xueqin, et al. "Quantitative risk assessment of threats on SCADA systems using attack countermeasure tree." 2022 19th annual international conference on privacy, security & trust (Pst). IEEE, 2022, https://doi.org/10.1109/PST55820.2022.9851965

[9] United States Government Accountability Office, "CRITICAL INFRASTRUCTURE PROTECTION. EPA Urgently Needs a Strategy to Address Cybersecurity Risks to Water and Wastewater Systems", August 2024, https://www.gao.gov/assets/gao-24-106744.pdf (accessed: 2024-10-27)

[10] Hurst, William, and Nathan Shone. "Critical infrastructure security: Cyber-threats, legacy systems and weakening segmentation." Management and Engineering of Critical Infrastructures. Academic Press, 2024. 265-286. https://doi.org/10.1016/B978-0-323-99330-2.00010-6

[11] Korodi, Adrian, and Ioan Silea. "Achieving interoperability using low-cost middleware OPC UA wrapping structure. Case study in the water industry." 2017 IEEE 15th International Conference on Industrial Informatics (INDIN). IEEE, 2017. https://doi.org/10.1109/INDIN.2017.8104949

[12] Cavalieri, Salvatore, and Alessio Regalbuto. "Integration of IEC 61850 SCL and OPC UA to improve interoperability in Smart Grid environment." Computer standards & interfaces 47 (2016): 77-99., https://doi.org/10.1016/j.csi.2015.10.005

[13] Salhaoui, Marouane, et al. "Smart industrial iot monitoring and control system based on UAV and cloud computing applied to a concrete plant." Sensors 19.15 (2019): 3316. https://doi.org/10.3390/s19153316

[14] De Araújo, Paulo Régis C., et al. "Infrastructure for integration of legacy electrical equipment into a smart-grid using wireless sensor networks." Sensors 18.5 (2018): 1312. https://doi.org/10.3390/s18051312

[15] Jaloudi, Samer. "Communication protocols of an industrial internet of things environment: A comparative study." Future Internet 11.3 (2019): 66. https://doi.org/10.3390/fi11030066

[16] Yadav, Geeta, and Kolin Paul. "Architecture and security of SCADA systems: A review." International Journal of Critical Infrastructure Protection 34 (2021): 100433. https://doi.org/10.1016/j.ijcip.2021.100433

[17] Irmak, Erdal, and İsmail Erkek. "An overview of cyber-attack vectors on SCADA systems." 2018 6th international symposium on digital forensic and security (ISDFS). IEEE, 2018, https://doi.org/10.1109/ISDFS.2018.8355379

[18] European Cyber Security Organisation WG3. "INDUSTRY 4.0 AND ICS SECTOR REPORT - Cyber security for the industry 4.0 and ICS sector." European Cyber Security Organization (ECSO), March 2018. https://ecs-org.eu/ecso-uploads/2022/10/5fdb2628a0318.pdf

[19] Nelson, Trent and Chaffin, May. "Common Cybersecurity Vulnerabilities in Industrial Control Systems." U.S. Department of Homeland Security, May 2011, (DHS), https://www.cisa.gov/sites/default/files/recommended_practices/DHS_Common_Cybersecurity_Vulnerabilities_ICS_2010.pdf

[20] Xu, Yikai, et al. "Review on cyber vulnerabilities of communication protocols in industrial control systems." 2017 IEEE Conference on Energy Internet and Energy System Integration (EI2). IEEE, 2017. https://doi.org/10.1109/EI2.2017.8245509

[21] vom Dorp, Johannes, Sven Merschjohann, David Meier, Florian Patzer, Markus Karch, and Christian Haas. OPC UA Security Analysis. Federal Office for Information Security (BSI), Version 1.2, June 2022. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/OPCUA/OPCUA_2022_EN.pdf (accessed: 2024-12-11)

[22] Hayes, Garrett, and Khalil El-Khatib. "Securing modbus transactions using hash-based message authentication codes and stream transmission control protocol." 2013 third international conference on communications and information technology (ICCIT). IEEE, 2013. https://doi.org/10.1109/ICCITechnology.2013.6579545

[23] Ádámkó, Éva, and Gábor Jakabóczki. "Proposal of a secure modbus RTU communication with adi shamir's secret sharing method." International Journal of Electronics and Telecommunications (2018). https://doi.org/10.24425/119357

[24] Marian, Marius, et al. "Experimenting with digital signatures over a DNP3 protocol in a multitenant cloud-based SCADA architecture." IEEE Access 8 (2020): 156484-156503.. https://doi.org/10.1109/ACCESS.2020.3019112

[25] Yeasmin, Samira, and Adeel Baig. "Permissioned blockchain-based security for IIoT." 2020 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS). IEEE, 2020. https://doi.org/10.1109/IEMTRONICS51293.2020.9216343

[26] Post, Olli, Jari Seppälä, and Hannu Koivisto, H. "The Performance of OPC UA Security Model at Field Device Level". In Proceedings of the 6th International Conference on Informatics in Control, Automation and Robotics, Volume Robotics and Automation, Milan, Italy,2–5 July 2009; Volume 2, pp. 337–341. https://doi.org/10.5220/0002249103370341

[27] Altaleb, Haya, and Rajnai Zoltán. "A Comprehensive Analysis and Solutions for Enhancing SCADA Systems Security in Critical Infrastructures." 2024 IEEE 11th International Conference on Computational Cybernetics and Cyber-Medical Systems (ICCC). IEEE, 2024. https://doi.org/10.1109/ICCC62278.2024.10582956

[28] Tidrea, Alexandra, Adrian Korodi, and Ioan Silea. "Cryptographic considerations for automation and SCADA systems using trusted platform modules." Sensors 19.19 (2019): 4191. https://doi.org/10.3390/s19194191

[29] Tidrea, Alexandra, Adrian Korodi, and Ioan Silea. "Elliptic curve cryptography considerations for securing automation and SCADA systems." Sensors 23.5 (2023): 2686. https://doi.org/10.3390/s23052686

[30] Tidrea, Alexandra, and Adrian Korodi. "ECC Implementation and Performance Evaluation for Securing OPC UA Communication." 2023 IEEE 22nd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). IEEE, 2023. https://doi.org/10.1109/TrustCom60117.2023.00232.

[31] Tidrea, Alexandra, and Adrian Korodi. "Pairing cryptography considerations for securing OPC UA communication within SCADA and automation systems." 2025 **(under submission).**