IOSUD – Politehnica University of Tmișoara
Doctoral School for Engineering Studies

Security solutions for SCADA and automation systems in the context of protecting critical infrastructures

PhD Thesis – Summary

for obtaining the Scientific Title of PhD in Engineering at
Politehnica University of Timișoara
in the field of Systems Engineering
by

Author: Alexandra-Ionela ȚIDREA (căs. Basso-Țidrea)
PhD Supervisor: Prof. Univ. Dr. Ing. Ioan SILEA

October 2025

Supervisory Control and Data Acquisition (SCADA) and automation systems are critical for the well-functioning of critical infrastructures such as medical and transportation sectors as well as for energy and water industries. In this context, successful cyber-attacks against critical infrastructures systems, which may lead to disruption of the controlled process and even physical damage, pose a threat to the industrial sector and national security. They were built without including security mechanisms within their design with the purpose of acquiring and monitoring data from field level devices (i.e., sensors, actuators) and controlling industrial processes. However, before their evolution towards Industry 4.0 and Industrial Internet of Things (IIoT) concepts, an air-gaped network was considered self-sufficient for ensuring protection against cyber-attacks. Nevertheless, in the context of their evolution towards the 4th industrial revolution, interconnection of these systems with other networks makes them vulnerable to cyber threats by exposing data to the outside world. Moreover, introducing security while maintaining interconnection and interoperability represents a major challenge which comes from the multitude of devices and communication protocols used, especially legacy systems with limited computation resources and proprietary software, which are unable to support complex operations and management of a large amount of data. Ensuring seamless data exchange is highly important considering real-time operation and availability requirements, which are mandatory to be fulfilled and non-negotiable for vital infrastructures. Therefore, securing SCADA and automation systems in the context of protecting critical infrastructures is a nowadays challenge and a difficult problem to solve. In this context, the main motivation topic for this thesis is to provide security solutions for SCADA and automation systems in the context of protecting critical infrastructures considering current challenges posed by evolution towards IIoT. The motivation of the author of this thesis, as well as the research objectives and major contributions are addressed in Chapter 1 of the thesis.

Stuxnet [1], Florida Water treatment plant attack [2] and Ukraine electric power utility outage [3], are just several examples of cyber-attacks against SCADA and automation systems with negative implications which have emphasized the urgency of implementing cybersecurity measures for protecting critical infrastructures. Moreover, the increased number of cyber-attacks against SCADA and automation systems [4],[5] in the last decade along with the integration of physical industrial processes within IIoT,

have raised awareness among the research community and government agencies (e.g., NIS 2 directive [6], USA National Security Memorandum on Critical Infrastructure and Resilience [7]) in respect to the importance of securing cyber-physical and industrial control systems [8], [9].

However, the industry is reluctant to replace or update already operation and functional solutions which are incorporating insecure legacy structures [10], due to cost and intelligent devices lifecycle. Therefore, the tendency is to employ a non-invasive approach, which requires minimum updates, when applying interoperation and other Industry 4.0 principles. Vertical and horizontal interoperation is being obtained usually through gateways or wrappers responsible for vehiculating and translating data of legacy communication protocols (e.g., Modbus [11], IEC 61850 [12]) towards a unified standardized communication protocol Open Platform Communication Unified Architecture (OPC UA). Security is achieved at higher levels through implementation of OPC UA [13] or through various gateway-based strategies [14]. However, in many cases legacy structures are not subject to sudden changes since they assure the heterogeneity of existing communication protocols [15]. Moreover, deploying security mechanisms on low-level resource constrained devices such as PLCs without affecting the normal operation of the control process is a continuous challenge. Therefore, securing communication between lower levels of a SCADA and automation system increases complexity and effort in achieving real-time communication without faults or delays [16].

Furthermore, the vulnerabilities of SCADA and automation systems are present at communication protocol level, within hardware devices such as PLCs and among the software components used across control level as stated by a research study [17] exposing them to various cyber attacks such as MITM, DoS or SCADA communication hijacking [18],[19],[20]. Moreover, secure communication within SCADA and automation systems is vital for ensuring the authenticity, integrity and confidentiality of the data vehiculated within different architectural levels while fulfilling availability and timeliness security objectives. However, insecure legacy communication protocols (e.g., Modbus TCP, DNP3) are widely used nowadays, despite their lack of security mechanisms. Even for the newer communication protocol with built-in security, i.e., OPC UA, a research study conducted by the German Federal Office for Information Security identifies several vulnerabilities for the supported security modes which could allow an intruder to perform eavesdropping, DoS and session hijacking attacks [21].

These vulnerabilities are the incentive for developing efficient security solutions for SCADA and automation systems. Employing keyed-hash functions (HMAC) [22] or Adi Shamir method [23] are just several examples for securing legacy communication protocols addressed in literature. These proposals are either incomplete, or they introduced delays in communication. Another research direction with respect to evolution towards IIoT focuses on the analysis of introducing new security mechanisms within critical infrastructures such as digital signatures [24] or blockchain [25]. However, these approaches do not provide a complete security analysis and feasibility studies in respect to their applicability to legacy structures. Moreover, other studies show the inefficiency of RSA-based exiting security mechanisms of OPC UA for lower-level devices [26], which emphasizes the need of resilient and efficient security solutions for lower architectural levels of SCADA and automation systems. Even though several security solutions are presented in the literature for securing SCADA and automation systems there are still a multitude of security gaps and open challenges that need to be addressed properly [27]. Starting with the lack of non-intrusive security solutions for legacy structures, missing evaluation of their deployment on low memory resourced and computationally constrained devices used in industry, followed by lack of an in-depth effectiveness analysis for protection against cyber-attacks and ending up with inefficient security mechanisms for communication protocols that do not fulfill the need for availability and real-time operation, there is still an urgent need of developing resilient and complete security solutions for SCADA and automation systems.

Research objectives. In the aforementioned context, considering the state-of-the art research with respect to vulnerabilities of SCADA and automation systems along with the existing proposals for protecting them against threat actors, this thesis sets out several research objectives (RO), which can be summarized as follows:

RO1. Literature review on nowadays challenges for securing SCADA and automation systems with focus on related work targeting legacy communication protocols and elliptic curve-based solutions in the context of IIoT.

RO2. Design, implementation and evaluation of security solutions for ensuring data authenticity and secure key storage within legacy communication protocols.

RO3. Concept definition and implementation of security solutions for achieving data integrity, data authenticity and confidentiality based on ECC within SCADA and automation systems communication network.

RO4. Implementation and performance evaluation of securing OPC UA communication based on pairings and other relevant ECC-based cryptographic algorithms.

RO5. Deployment and evaluation of the proposed security solutions based on ECC on resource constrained devices used within industry for feasibility demonstration purposes.

The first research objective aims to study and identify the open challenges with respect to introducing or enhancing security within communication protocols, IIoT devices and legacy SCADA and automation structures. Then, the goal of the following objective is to research and define security solutions for ensuring authenticity and secure key storage within classical communication protocols (i.e., Modbus TCP) targeting non-invasive cryptographic approaches using trusted platform modules. Further, the thesis pursues the investigation and development of resilient cryptographic solutions to ensure data integrity, authenticity and confidentiality based on elliptic curve cryptography (ECC) for protecting SCADA and automation systems considering the constraints imposed by industry with respect to interoperation and timing requirements. Another research objective covered by this thesis targets implementation and performance evaluation of cryptographic methods for newer communication protocols (i.e., OPC UA) used in Industry 4.0 based on subset of ECC, more specifically methods based on pairing-based cryptography (PBC). The last research objective is related to deployment and evaluation of one of the proposed ECC-based security concepts on resource constrained devices (i.e., PLCs) used in industry.

Major contributions. In this thesis, several concepts are proposed for implementing security for SCADA and automation systems. In particular, the topics addressed are the security of legacy communication protocols using TPMs, design, evaluation and implementation of elliptic curve cryptographic methods within SCADA and automation systems, security enhancement of OPC UA communication protocol using ECC and pairings and integration and evaluation of the ECC-based security concepts on devices used by industry. In particular, the defined security objectives are achieved via the following major contributions (MC), which are part of peer-reviewed publications*:*

MC1. Analysis and demonstration of weaknesses within a legacy communication protocol by designing and conducting a man-in-the-middle attack on a local SCADA and automation system setup.

MC2. Design, implementation and evaluation of two methods for providing authenticity of the data vehiculated through legacy communication protocols using TPMs.

MC3. Concept definition, implementation and evaluation of security solutions for Modbus TCP based on digital signatures and hybrid encryption scheme using ECC.

MC4. Implementation and performance evaluation of an enhanced OPC UA communication based on digital signatures using various elliptic curve sizes.

MC5. Design, implementation and evaluation of pairings for securing OPC UA communication protocol

MC6. Integration and evaluation of security solutions based on ECC on a setup composed of PLCs and devices used within industry

Legacy communication protocols are widely used within critical infrastructures even though they carry data in plain text or with limited security mechanisms. Therefore, the goal in this case is to emphasize the weaknesses of insecure classical communication protocols and to demonstrate that devices used within industry such as Siemens PLCs are indirectly vulnerable to security breaches. The results show that with expert knowledge a successful cyber-attack is possible. The MC1 contribution is part of the author's research paper from [28].

Furthermore, detailing MC2, a cryptographic authentication scheme using TPMs based on two methods is designed and proposed for providing data integrity and authenticity within Modbus TCP protocol, which was chosen as a representative of legacy communication protocols since it is the most used. Nevertheless, the proposed solution can be extended to other legacy communication protocols. Worth mentioning is that TPMs are integrated within the system architecture of the proposed concepts to emphasize their advantages for achieving security and maintaining real-time communication of SCADA and automation systems. For software implementation purposes several open-source libraries are integrated and configured. Moreover, the evaluation of the proposed concept shows compliance with the communication timing constraints imposed by the industry. In addition, the attack designed in MC1 is used to evaluate the security of the implemented concept with respect to protection against MITM attacks. The MC2 contribution is part of the author's research paper from [28].

The evaluation and implementation of cryptographic methods based on elliptic curves primitives is a predominant novel approach for multiple contributions and security solutions for SCADA and automation systems presented in this thesis. Therefore, concept design and implementation stated in the contribution MC3, relies on ECC which is chosen since it fits the constraints of low-level devices of a SCADA/automation network and due to its security capabilities. Two methods for providing authenticity, integrity and confidentiality of the data exchanged through insecure communication protocols are proposed. The solution is implemented using Modbus TCP protocol as selected insecure communication protocol, open-source C language-based libraries which are integrated and configured accordingly in order to allow deployment on the evaluation setup composed of devices used within industry - low memory PLCs, part of MC6 contribution. The evaluation consists of measuring the timing execution of each cryptographic operation for multiple ECC curve sizes. The conducted security analysis concludes that both methods offer protection against MITM and replay attacks. The MC3 contribution is part of the author's research paper from [29].

Integration of novel cryptographic solutions within SCADA and automation systems is a nowadays challenge due to limited resources and real-time operation requirements. When proposing a security solution, one must analyze the feasibility of implementation on the targeted system without introducing delays or affecting its normal operation. Therefore, an experimental system setup is designed consisting of two Industruino PLCs devices and one MDUNIO PLC, both used within SCADA and automation systems in industries like water treatment and energy sector. These devices have embedded communication interfaces used within critical infrastructures such as RS-232, I2C, Ethernet, RS-485 and support Modbus protocol communication. For each PLC was considered a security controller Optiga Trust X which acted as a crypto processor and secure key device storage for each Modbus node part of the communication. For being able to deploy the security solution proposed in the contribution MC3, open-source software libraries and custom-made libraries running on the PLCs are integrated and optimized. Once integrated on the experimental setup, the latency introduced by the proposed solution from MC3 is measured and the security level introduced for each ECC curve used is discussed. The evaluation results show that the implemented security solution based on ECC for both methods fits the real-time operation requirements and it is feasible to be deployed on devices with similar memory constraints without causing disruption or affecting the interoperability of the targeted systems. The MC3 and MC6 contribution is part of the author's research paper from [29].

In transition to Industry 4.0, newer communication protocols (e.g., OPC UA) have been developed with built-in security mechanisms. Nevertheless, since the legacy devices were not upgraded in many cases,

these security mechanisms are left inactive because they require high computational resources. In this context, an OPC UA protocol enhancement with ECDSA is designed and implemented in order to provide data authenticity between a client and a server. For implementation purposes open-source software libraries for OPC UA protocol and for cryptographic operations are used. In respect to the performance evaluation, an experimental setup incorporating a PLC with an OPC UA server and a Raspberry PI 4 acting as an OPC UA client is defined, enabling concept deployment and time measurements. The timing performance on the experimental setup for various ECC curve sizes used within the authentication scheme starting from 160 bits up to 446 bits is evaluated. The obtained results show that for all evaluated ECC curves, the implemented concept complies with the timing requirements imposed for OPC UA communication. The MC4 contribution is part of the author's research paper from [30].

Furthermore, following the thread of integrating elliptic curve cryptography within OPC UA communication protocol, a concept for securing OPC UA client-server communication using pairings, which are a subset of ECC and are employed in zero-knowledge protocols and blockchain, is designed and implemented. Pairings were selected due to their unique properties, such as aggregation and small signature sizes. Two cryptographic schemes for providing data authenticity and integrity based on Boneh-Lynn-Shacham short signatures (BLS) and BLS aggregated signatures tailored for a SCADA and automation system scenario are designed and implemented. Further, a tripartite Diffie Hellman (DH) key agreement protocol based on pairings is integrated and evaluated from a timing perspective for several ECC pairing friendly curves. In addition, the Elliptic-curve Diffie-Hellman (ECDH) algorithm employed for obtaining a shared secret and which can be used afterwards for message authentication over an insecure channel is evaluated from the same perspective as tripartite DH. The proposed concept for all implemented cryptographic schemes is evaluated on an experimental setup by measuring the duration of each cryptographic operation. The security level provided by each selected ECC pairing friendly curve in contrast to additional bytes introduced on the communication channel as a result of signature algorithm steps is analyzed. In addition, a comparison from timing execution perspective between BLS and ECDSA is provided considering the results from [30] which is the basis of MC4 contribution. The MC5 contribution is part of the author's research paper from [31].

These contributions are part of this author's peer-reviewed research papers published or under submission in journals and conference proceedings. As a summary, the major contributions of this thesis originate from the following research papers where the author of this thesis is the first author:

- [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)**.

This thesis proposes various security solutions suitable for SCADA and automation systems in the context of protecting critical infrastructures considering current challenges posed by Industrial Internet of Things and conducts their evaluation with focus on the feasibility to deploy them on industrial devices. As a summary of the thesis outline, Chapter 1 presents the motivation, research objectives and major contributions. The remaining chapters of the thesis are structured as follows. Chapter 2 introduces a required background for the context of this thesis and discusses the relevant related work starting with the identified vulnerabilities and followed by proposed security solutions. Then, Chapter 3 presents two methods for securing legacy communication protocols using TPMs while the timing evaluation is performed and discussed for all cryptographic operations. In the same chapter, a MITM attack is designed and conducted

on a local SCADA and automation system. Chapter 4 addresses design, implementation, integration and evaluation of elliptic curve cryptography within critical infrastructures for ensuring data authenticity, data integrity and data confidentiality. First, in this chapter, is presented a cryptographic authentication scheme based on ECDSA and a hybrid encryption scheme based on ECIES. Then, follows the integration and evaluation of these solutions on an experimental setup with devices used by industry. Lastly, an enhanced security OPC UA protocol based on ECDSA is implemented and evaluated. Chapter 5 introduces pairing-based cryptography as a cryptographic approach for securing OPC UA communication by implementing BLS for message authentication, BLS aggregated signatures for a tailored SCADA and automation system scenario and tripartite DH for key agreement. Chapter 6 incorporates the conclusions of this work and addresses future research possibilities. The following paragraphs summarize the contributions of this thesis and highlight the improvements brought to current security solutions existing in the industry or presented in the state of the art.

Chapter 2 presents first the background information with respect to SCADA and automation systems evolution and their architecture, followed by the theoretical aspects of elliptic curve cryptography along with the security properties of the cryptographic primitives used within the proposed security concepts of this thesis. Then, it identifies existing open challenges in securing SCADA and automation systems and addresses the relevant related work for the subject of this thesis starting with the vulnerabilities followed by the proposed security solutions within state-of-the-art research studies. Maintaining availability and real-time operation while introducing security mechanisms within SCADA and automation systems represents one of the major open challenges. Moreover, inefficient or lack of non-invasive security methods for legacy structures and their deployment on resource constrained devices along with additional costs stemmed from updating the well-functioning industrial control systems with newer, more secure devices, are several identified gaps which emphasize the urgent need for developing resilient security solutions for protecting critical infrastructures. Designing such security solutions constitutes the ultimate motivational paramount of this thesis. However, in order to respond to the urgency of protecting these systems, besides the research efforts for developing cryptographic algorithms and security concepts, the vendors of devices used in industrial control systems must consider evaluating and encompassing forms of cryptographic primitives proposed by literature within their products intended for OT environments.

Chapter 3 presents two methods, part of an authentication cryptographic scheme for securing legacy communication protocols using the capabilities of TPMs, in order to respond to the security issues raised by the legacy structures and to the need to develop resilient security solutions for SCADA and automation systems. The system architecture, abstract view, of the proposed concept with the logical system elements is shown in Figure 1. First, a MITM attack on a legacy communication protocol is designed and deployed on a SCADA and local automation system as shown in Figure 2, which contains a real PLC (i.e., Siemens S7-1200) for emphasizing its vulnerability against cyber threats and indirectly the security weakness of devices used in industry across different architectural levels. Secondly, as part of the authentication scheme which uses TPMs, the first method employs HMAC-SHA-256 primitives while the second one is based on ECDSA ECC-256. These methods are designed, implemented and evaluated on an experimental setup. Several open-source C language libraries were optimized, updated and integrated in order to allow the software implementation of the proposed concept. The proposed security concept was evaluated for protection against MITM cyber-attacks using the same design as the one used on the local SCADA and automation system. The results obtained show that the proposed security concept is resistant to this type of cyber-attack and in conjunction with the results of the security analysis achieves the targeted security properties by providing authenticity and integrity of the data exchanged through the selected legacy communication protocol. Furthermore, the timing results obtained through measurements conducted on the experimental setup show compliance with the timing constraints imposed by industry for both proposed methods. Moreover, the proposed concept leverages the capability of TPMs to store and generate a cryptographic key in a secure manner, for enhancing the level of security. This advantage constitutes a strong case for employing TPMs as part of security solutions for protecting critical infrastructures.

Furthermore, all cryptographic operations required within the authentication scheme were performed by the TPM itself and accessed from the application through a wrapper. The timing results obtained showed compliance with timeliness and availability requirements, emphasizing the suitability of using TPMs for introducing security without affecting the normal operation process within automation/SCADA structures. These aspects make the proposed proof-of-concept a subject of novelty suitable for being implemented and adopted by industry, especially since it provides the opportunity of reducing the interference on well-functioning legacy systems by deploying it as an extra communication layer. This statement is supported by newly developed Kunbus PLC (i.e., released in 2025) designed with a TPM included within its hardware emphasizing the applicability of the proposed concept within real industrial applications for introducing security. The content and results presented in this chapter are based on the author's research paper [28].

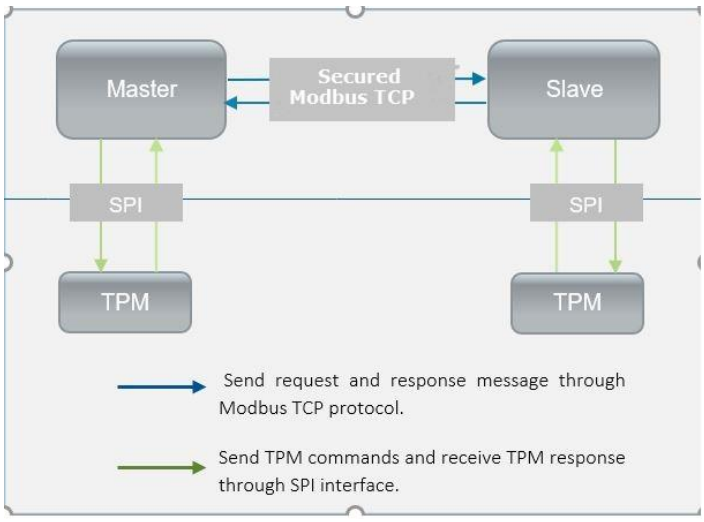

Figure 1: System architecture of the proposed concept - abstract view [28]

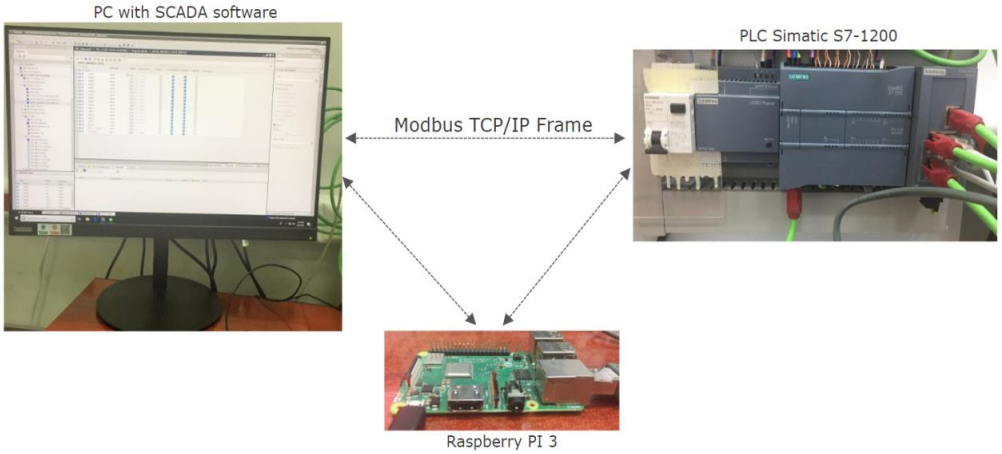

Figure 2. Real physical setup for deploying Modbus TCP MITM attack [28]

Chapter 4 presents two working security solutions based on ECC for securing legacy communication protocols and OPC UA, as well as for allowing deployment on widely spread resources

constrained devices dispersed at lower architectural levels of a real SCADA and automation system while complying with the timing constraints imposed by industry. The first solution is based on ECC for securing the data vehiculated through legacy communication protocols with Modbus TCP selected as representative, with focus on its implementation, integration and deployment on lower-level resources constrained industrial devices used within real SCADA and automation systems. As part of the proposed solution, two methods based on ECC are implemented, designed and evaluated with focus on their integration and deployment on lower-level resource constrained devices. The first method based on ECDSA provides data authenticity and integrity while the second one based on ECIES provides data confidentiality and integrity of the messages exchanged between two industrial devices (e.g., PLCs) through insecure Modbus TCP communication protocol. In addition, an experimental system setup composed of PLCs used in real SCADA and automation systems, more specifically two Industruino devices and one MDUINO PLCs, is designed for allowing integration, deployment and evaluation of the two proposed cryptographic schemes. The experimental setup is presented in Figure 3. Furthermore, a performance evaluation is conducted on the experimental setup for several ECC curves with various key sizes employed within the proposed message authentication scheme considering the computational cost, added latency and security strength. As additional element to the experimental setup, a security microprocessor Optiga Trust X is integrated successfully for enhancing the security of the proposed authentication scheme as an alternative to a software-based solution only. For completing the experimental setup, several open-source C language libraries are optimized and adapted to support the deployment of the security concept.

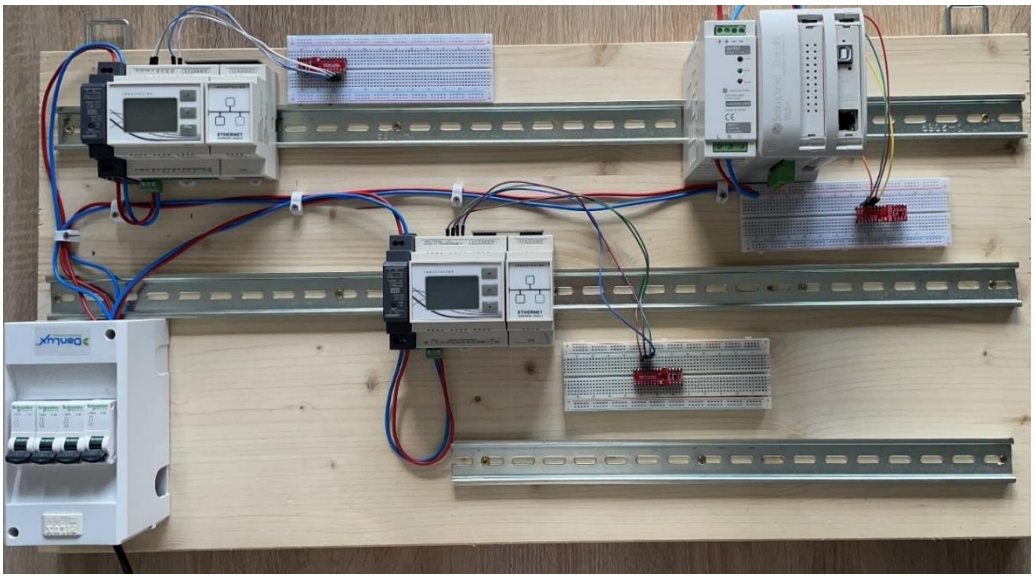

Figure 3 Experimental hardware setup with PLCs and three Optiga Trust X devices [29]

For both proposed cryptographic schemes, the timing results obtained by conducting measurements on the experimental setup show compliance with the time constraints imposed by industry within a real SCADA and automation network with respect to the legacy communication protocol Modbus TCP while being integrated and evaluated on lower-level constrained Industruino and MDUINO PLCs. Moreover, the results obtained show that Optiga Trust X provides a lower computational cost and a higher security level than the software-based ECDSA. However, the ECDSA-based cryptographic scheme was deployed successfully on the selected PLCs without employing security chips by complying with the timing constraints imposed by industry. In order to have a complete solution for enabling a secure trusted channel, the authentication scheme must be executed first followed by the hybrid encryption scheme. However, the two proposed methods are designed to allow independent deployment considering the security goals of the targeted

system architecture. As presented, the security analysis shows that both methods are offering protection against MITM and replay attacks, while in addition the hybrid encryption scheme provides resistance against cyphertext attacks. This enforces the strength of the security solution and sustains the achieved security targets with respect to integrity, authenticity and confidentiality, as presented in the experimental results. As demonstrated through measurements, the proposed concept fulfills the timing constraints with respect to legacy Modbus TCP communication protocol of real SCADA and automation systems while being deployed on lower-level constrained PLCs Industruino and MDUINO. Additionally, it proves the suitability of integrating and deploying noninvasively the proposed security concept based on ECC on resource constrained devices already existing in industry without the need of extending the legacy structures with newer devices or replacing them with secure by design devices which represents a costly and invasive approach. These aspects, in conjunction with the results of the security evaluation and timing duration, as well as proven integration on devices used in a real SCADA and automation systems, make this security solution a novelty with real potential to be adopted and deployed in industry for introducing security based on ECC among critical infrastructures and extended to other insecure legacy communication protocol targeting similar security properties. As second security solution based on ECC, the second main section of this chapter presents a concept for securing client-server communication over OPC UA protocol based on ECDSA as an alternative to the existing deployed security solution based on RSA, with focus on its feasibility of integration and deployment on lower-level resource constrained devices used in industry in the context of PLC-to-SCADA or PLC-to-PLC communication. The main steps of the designed and implemented authentication scheme for enhancing OPC UA security are shown in Figure 4.

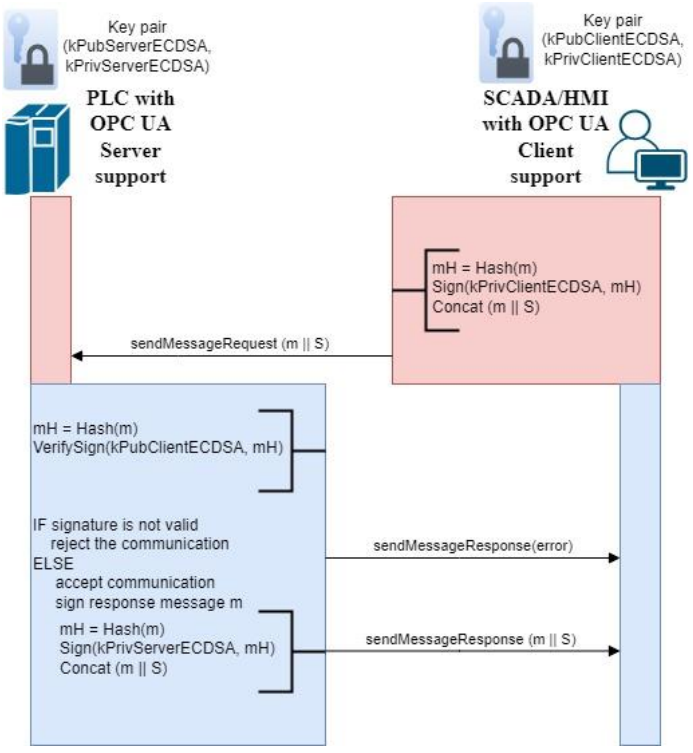

Figure 4: OPC UA message authentication based on ECDSA [30]

A performance evaluation of the security solution based on ECDSA and SHA256 primitives is conducted on the experimental setup, which includes a real industrial PLC, for several ECC curves with various key sizes. For allowing deployment of the security concept on the experimental setup, several open-source C language libraries are optimized and adapted. The results obtained through measurements show that all

selected ECC curves fit the OPC UA communication timing requirements which proves that the proposed solution is suitable for deployment on resource constrained devices. In addition, the obtained time measurements and the outcome of the security analysis show that the OPC UA security profile can be extended to adopt besides NIST P-256 and NIST P-384 the other selected and evaluated ECC curves, which fit the timing constraints imposed by industry. Furthermore, as demonstrated through measurements, the proposed concept based on ECDSA complies with OPC UA timing constraints for client-server communication in the context of SCADA and automation systems or IoT environments while fulfilling availability and timeliness requirements, proving its suitability for deployment and adoption in real industrial applications. The content and results presented in this chapter are based on the author's research papers [29] and [30].

Chapter 5 presents a security concept based on PBC, which is a subset of ECC, for enhancing the security of OPC UA client-server communication in the context of PLC-to-PLC and PLC-to-SCADA communication, with focus on its feasibility of integration and deployment on industrial devices spread at lower architectural levels of a real SCADA and automation system while complying with timing constraints of OPC UA and imposed by industry. The first two presented cryptographic schemes, more specifically BLS authentication scheme and BLS aggregated signatures scheme, provide authenticity and integrity for the data messages exchanged over the OPC UA communication channel. The proposed BLS authentication scheme for enhancing OPC UA security was implemented as an alternative to digital signatures based on RSA employed within OPC UA current standardized version and deployed already on devices used in industry. In addition, the proposed OPC UA BLS aggregated signatures scheme was implemented as a security solution for optimizing and reducing the required computational cost for the verification of a digital signature in a multi-server/client architecture presented for a tailored use case, where an OPC UA aggregating server is used within the context of a real SCADA and automation system architecture. The tailored scenario is shown in Figure 5. In this context, the proposed OPC UA BLS aggregation scheme tailored for a real OPC UA use cases proves the suitability of integrating it within real critical infrastructure uses-cases by scaling the number of the signers and verifiers to the one required by the targeted OT architecture. Both solutions are designed, implemented within OPC UA stack and evaluated on the experimental setup.

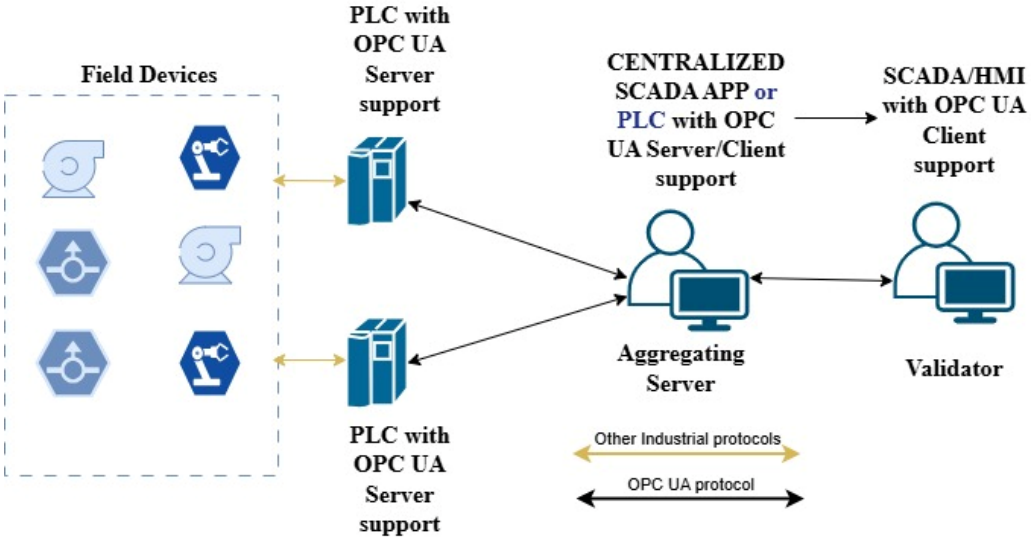

Figure 5: Description of OPC UA communication use case for SCADA and automation systems [31]

The tripartite DH scheme was evaluated since it provides a mechanism for establishing a common secret key between three devices and due to its usability as basis for further complex cryptographic

algorithms which can be applied in OPC UA industrial applications. However, even if the results show compliance with the availability and timeliness requirements of SCADA and automation systems, the scheme based on tripartite DH requires further updates to incorporate authentication methods in order to be resistant against MITM attacks. All implemented cryptographic schemes are evaluated with respect to timing duration and added latency on the OPC UA communicational channel on an experimental setup, which is designed to emulate a real SCADA and automation system, which include among other embedded devices a PLC used in industry. In addition, the obtained results show that the proposed schemes based on BLS signatures provide digital signatures with smaller sizes and higher computational cost when compared with the solution based on ECDSA from [61] considering ECC curves with similar security levels. Moreover, the output sizes reflected in added latency on the communication network increases along with the security level and computational cost for all evaluated curves when the OPC UA security mode is set to None. For the other two security modes available within OPC UA protocol, when digital signatures based on RSA are used, the network bandwidth is higher for the same security level than the proposed concept which employs BLS signatures. Furthermore, based on the timing results obtained, the OPC UA security profiles can be updated to include all evaluated pairing friendly curves which provide an estimated security level higher than 100 and lower or equal with 256 along with the proposed algorithms based on BLS as new security policies. The work conducted in this chapter demonstrates through timing measurements conducted on the experimental system setup, that the proposed security concept complies with the timing constraints imposed by industry for OPC UA client-server communication within real SCADA and automation systems for all implemented cryptographic schemes based on pairing based cryptographic algorithms and for all evaluated ECC pairing friendly curves. Moreover, the timing results obtained through measurements on the designed experimental setup associated with the implemented proposed cryptographic schemes based on BLS, show compliance with timeliness and availability requirements, emphasizing the real potential of deploying them independently or together in industry within critical infrastructures at lower architectural levels of a real SCADA and automation system without affecting its normal operation. The content and results presented in this chapter are based on the author's research paper under submission [31].

Chapter 6 summarizes the research results presented in previous chapters which were validated through four research papers where the author of this thesis is the first author.

To summarize, this thesis presents various methods based on ECC and PBC for securing SCADA and automation systems in the context of protecting critical infrastructures and conducts their evaluation with focus on the feasibility to deploy them on industrial devices. The contributions of this thesis ultimately enable security mechanisms which can be introduced by industry to secure SCADA and automation systems in the context of protecting critical infrastructures, overcoming their limitations with respect to timing constraints, devices with limited resources and availability requirements while providing interoperation without disrupting the control process.

References

[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).**