Security-Gateway for SCADA-Systems in Critical Infrastructures

Tobias Frauenschläger and Jürgen Mottok
Laboratory for Safe and Secure Systems (LaS³)
Technical University of Applied Sciences Regensburg
93053 Regensburg, Germany
{tobias.frauenschlaeger, juergen.mottok}@oth-regensburg.de

2022 International Conference on Applied Electronics (AE) | 978-1-6654-9482-3/22/$31.00 ©2022 IEEE | DOI: 10.1109/AE54730.2022.9920070

***Abstract*—Supervisory Control and Data Acquisition (SCADA) systems are used to control and monitor components within the energy grid, playing a significant role in the stability of the system. As a part of critical infrastructures, components in these systems have to fulfill a variety of different requirements regarding their dependability and must also undergo strict audit procedures in order to comply with all relevant standards. This results in a slow adoption of new functionalities. Due to the emerged threat of cyberattacks against critical infrastructures, extensive security measures are needed within these systems to protect them from adversaries and ensure a stable operation. In this work, a solution is proposed to integrate extensive security measures into current systems. By deploying additional security-gateways into the communication path between two nodes, security features can be integrated transparently for the existing components. The developed security-gateway is compliant to all regulatory requirements and features an internal architecture based on the separation-of-concerns principle to increase its security and longevity. The viability of the proposed solution has been verified in different scenarios, consisting of realistic field tests, security penetration tests and various performance evaluations.**

***Keywords*—Security, Dependability, Critical Infrastructure, Supervisory Control and Data Acquisition, Certification**

I. Introduction

In recent years, the share of renewable energies within the energy mix increased rapidly [1]. The decentralization of power generation and the volatility of renewables increases the efforts of providers to stabilize the system by controlling and monitoring each component. Therefore, large wide-area *Supervisory Control and Data Acquisition* (SCADA) systems are created, requiring numerous communication links between a central control station and the different decentral nodes. Over those links, proprietary protocols, specifically created for these use-cases, are deployed to exchange control commands and monitoring data. However, mostly commodity hardware and software is used to build the necessary underlying communication networks, resulting in the usage of standard network protocols like TCP/IP to transmit the actual payload.

Due to the long mission time of the devices in operation and the resulting slow progression related to the adaption of new technologies, there are currently only a few measures deployed regarding the emerged necessity of protection against cyberattacks. As the energy grid is part of the critical infrastructure, this lack can cause tremendous damage in case of an attack, as already happened in Ukraine in 2015 [2], where a cyberattack caused a large power outage. Therefore, it is very important to integrate security measures into the existing systems as soon as possible to prevent such attacks in the future and ultimately ensure a stable power grid.

The context of critical infrastructure impedes the deployment of available security measures. Thus, security solutions specifically created for these environments are required. The general approach is to add additional security-gateways into the communication systems to integrate the new measures. Such devices, however, have to fulfill the same regulatory requirements as the existing monitoring and control components within the systems. This work presents such a security-gateway designed for the deployment in the SCADA-systems of the German power grid. Its main characteristics are:

- Full compliance with all relevant standards and certifications.
- Designed for longevity to support the expected operation lifetime of these systems.
- Achieving a high level of security and safety due to a modular hardware and software architecture based on the separation-of-concerns principle.

In Section II, the context for our work and its implications on the created security-gateway are explained. Thereafter, Section III presents related work. Based on these preliminaries, Section IV introduces the design of our security-gateway, with Section V shortly describing the implementation of the current prototype. Section VI presents evaluation results regarding the viability of our solution. In Section VII, the work is concluded.

II. Context

In this section, the context of critical infrastructures is presented in more detail to understand its implications on our proposed security-gateway. At first, the regulatory background of the SCADA-systems is described that a device has to be compliant with. In addition, a threat analysis is outlined to explain the different security measures of the device. Finally, further aspects derived from the context are presented to be considered for the device.

A. Regulatory Background

Due to their importance for society, systems within critical infrastructures are subject to many regulations to guarantee their functionality and dependability over a long operation lifetime. On the one hand, the actual **communication** between the nodes in a system is defined in various standards (e.g., IEC 61850 [3] and IEC 60870-5-104 [4]). A comprehensive overview of relevant SCADA protocols can be found in [5]. Most of them only define the message flow on the application layer and rely on established network protocols for the underlying transmission of data, e.g., the TCP/IP protocol stack. On the other hand, a set of standards regulates the requirements regarding **functional safety** (e.g.,

978-1-6654-9482-3/22/$31.00 ©2022 IEEE

IEC 61508 [6]). In these, so-called *Safety Integrity Levels* (SIL) are defined to classify required dependability specifications, e.g., allowed failure rates. In Section IV, we present the classification of our gateway into the appropriate SIL.

Due to the emerged importance of security in recent years, there are also now standards and laws regarding proper **security measures** for these systems. The most important one for our work is the standard IEC 62351 [7], which covers an extensive set of measures for each part of the relevant SCADA-systems. Most relevant for the communication within the systems, part 3 of the standard prescribes the usage of the Transport Layer Security (TLS) protocol for all connections based on TCP/IP. Other parts cover topics like key-management (part 9) or secure event logging (part 14). Further relevant documents containing security regulations or recommendations are published in Germany and in the United States. For example, the German law regarding the security of IT-systems [8], which also covers critical infrastructures, or the document TR-02102 [9] from the German Federal Office for Information Security (BSI) covering the secure deployment of TLS, are relevant for the proposed security-gateway. From the US, Special Publications from the National Institute for Standards and Technology (NIST), covering topics like key-management (SP 800-57 [10]) or security for Industrial Control Systems (SP 800-82 [11]), also have been considered.

In addition, there are different **certification and audit procedures** a product must pass in order to allow its deployment in critical infrastructure (e.g., Common Criteria EAL levels [12] or the 140 series of the Federal Information Processing Standards [13]). These certification programs are very time-consuming and cost-intensive, resulting in only a few available products and a slow adoption of new features.

B. Threat Analysis

To define a proper set of security measures for the proposed security-gateway, a threat analysis has been performed, complemented with other work from the literature [14], [15]. The main conclusions of all these works are the following four attack scenarios:

- **Loss of availability:** Through a *Denial-of-Service* attack, an adversary disrupts the message flow and thus interferes with the proper functionality of a single component or the whole SCADA-System.
- **Loss of confidentiality:** An attacker is able to obtain information worth protecting about the state of the SCADA-system. This may not directly influence the system, but could lead to sociopolitical or financial damage.
- **Loss of integrity:** If an attacker can manipulate transmitted messages, he directly influences the operation of the SCADA-system, potentially leading to huge damage within the system.
- **Loss of authenticity:** In case an adversary can impersonate a valid communication partner of the system, he has full access to the systems' communication. Hence, all previous scenarios apply in this case.

Another consistent result of works regarding possible threats is the general acknowledgement of the new regulations regarding security measures (see Section II-A). The proposed measures achieve a thorough level of security and approach all described attack scenarios.

However, as the works of Schlegel et al. [16] and Wright et al. [17] show, the prescribed measures only add security without decreasing dependability and functional safety when applied and configured correctly. Due to many legacy features supported, and various features recommended in different parts that do not interoperate with each other, the integration of features may also lead to a decrease in system performance.

By incorporating additional gateways for the security measures, as the solution presented in this work, such pitfalls are well manageable due to the sole focus on security. However, the **security of the device** itself is still a concern and must therefore also be considered in the threat analysis. Hence, not only the communication but also the devices must incorporate measures to approach the above attack scenarios. Such measures for the device are currently not prescribed within the regulatory context and are therefore part of ongoing research activity (see related work in Section III).

C. Further Aspects

Another problem regarding the adoption of security features in the relevant SCADA-systems is the long operation lifetime of devices. Typical lifespans of these components are around 15 to 25 years. Therefore, it takes a long time to replace devices in the field and hence to deploy new features. This is especially relevant for security measures that all nodes in the system must support in order to create an overall protection against cyberattacks. This problem can be addressed by the incorporation of additional security-gateways, as these devices are also a viable option to retrofit security measures to legacy devices.

However, the gateways themselves also have to fulfill such **long operation lifetimes**. This is especially problematic regarding the time horizon of the currently used public-key cryptography. As, for example, indicated in part 2 of the already mentioned document TR-02102 [9] from the German BSI, the current algorithms based on RSA and ECC are only valid for the next 5 to 10 years. After that, new algorithms have to be deployed, especially due to the rising threat caused by the development of the quantum computer. Currently, there is a standardization process ongoing at the NIST [18] to find new, quantum-safe algorithms, called *Post-Quantum Cryptography*. These new algorithms possess new performance and memory requirements, leading to currently deployed devices potentially not being able to execute them. Hence, although the devices are typically able to perform software updates, the hardware of many of them is not powerful enough to run these futuristic security features. Therefore, additional measures must be integrated to increase the longevity of the devices.

III. Related Work

There are many approaches and solutions within the literature proposing security-gateways for critical infrastructures or similar contexts. The most relevant of them are presented in the following.

Khan et al. [19], propose an architecture using security-gateways to add Virtual Private Network (VPN) tunnels to

the SCADA-systems in the smart grid, mainly to enable secure communication with new cloud-based systems. These so-called *Cloud Connectivity Kits* are placed in front of an existing device to only provide the newly secured communication as an interface to the device. Internally, they consist of three functional blocks, to perform Firewall and VPN tasks, to handle the required network connections, and to add internal monitoring and secure storage possibilities. However, no further implementation of the gateway is presented, but the general viability of the architecture with the additional devices is evaluated and confirmed using a proof-of-concept setup.

In another work of the same authors [20], such a security-gateway is actually presented. It is based on Linux running on a Raspberry Pi 2. The application of this device is very similar to the one proposed in this work (see Section IV-A), as there are two gateways deployed within a SCADA-system of a power grid to create a secure communication channel, one in a Substation and one in the Control Center. Each gateway handles the communication with both the existing components and the other security-gateway. Another feature of the proposed device is protocol translation to also integrate security measures for messages that are based on legacy protocols without built-in security measures.

The presented approach, however, still has two main drawbacks considering the context of this work. On the one hand, the proposed measures are not compliant with the current regulatory background. On the other hand, the bigger problem is the monolithic design of the gateway. Using a Raspberry Pi as a foundation, the security-gateway only enables software-updates as a way to increase its longevity, which is not sufficient as shown in Section II-C. Furthermore, the lack of specially designed security features or additional cryptographic hardware within the device results in an increased attack surface for cyberattacks. Therefore, a more thorough approach is necessary for the SCADA-systems considered in this work.

The integration of additional cryptographic hardware into devices and their usage within protocols to increase the security level is well known today. Kehret et al. [21], for example, examined the integration of different available solutions, namely secure elements in the form of smartcards, Trusted Platform Modules (TPMs), and Hardware Security Modules (HSMs), into the TLS implementation of embedded systems. They confirm the viability and the improved security, but also note that the additional hardware dependability may decrease flexibility and longevity due to the fixed scope of functionality.

One example for a security-gateway integrating an additional cryptographic hardware solution is presented in a work of Matischek et al. [22]. They created a gateway with a secure element that performs cryptographic operations and securely stores all keys. Another example is the work of Bienhaus et al. [23], showing a security-gateway with a TPM as an additional hardware module. With this extra component, they are able to guarantee the integrity of the entire gateway and also only permit the usage of securely stored keys when the device is in a known validated system state.

These two examples demonstrate the increased security level of using additional security components, but also depict some remaining drawbacks. Firstly, the longevity of the gateways is bound to the lifetime of the cryptographic algorithms the additional modules support. Once these are considered insecure, the complete device is obsolete due to a lack of update abilities. Secondly, the mostly slow interfaces between the additional modules and the host devices may result in potential performance penalties of a gateway under high load. Finally, the integration of cryptographic hardware does not deal with the security goal of availability. All presented solutions are still susceptible to DoS-attacks, potentially resulting in a damaging influence on the system behavior in case of such an attack.

The last solution to be named in this context is the security architecture created by Eckel et al. [24] for the railway infrastructure. By integrating a TPM and an operating system based on a *Multiple Independent Levels of Safety and Security (MILS) Separation Kernel (SK)*, a device can be developed that is able to run safety-critical applications in a secured environment with additional security features (e.g., secure key-storage, secure software-updates). This design achieves a high level of safety and security, as individual applications or low-level components can only communicate in limited and strictly defined ways. However, to run the MILS SK with all available safety and security features, powerful hardware with special features (e.g., hardware redundancy) is required. This results in a very expensive device that is not suited for a wide deployment or as a retrofit solution. Furthermore, the longevity of the solution is only based on software-updates due to no further hardware update capabilities.

Based on the presented related solutions with their drawbacks and problems, we present the design of our security-gateway in the next section.

IV. Design

Based on the context and the related work described in the previous sections, the design of our security-gateway for the SCADA systems of critical infrastructure is presented in the following. For that, the integration of the gateway into the system and the resulting network topology is described first in Subsection IV-A. Thereafter, in Subsection IV-B, the internal design of the gateway is presented.

A. System Setup

In the SCADA systems considered in this work, it is possible to abstract the whole communication network to many independent wide-area point-to-point connections between a central control station and a single end node in the field (1-to-many star topology). The end nodes can either be actual devices, often called *Remote Terminal Units* (RTU), or a gateway in a substation aggregating the local traffic to a single outbound connection. Considering the threats mentioned in Section II-B, these wide-area connections are rated to be significantly more threatened compared to, e.g., local connections within an inaccessible substation due to the easier access for an attacker. Therefore, our solution focuses on these type of communication paths.

Furthermore, as there are many more nodes in the field than central control stations based on the 1-to-many relationship, and due to the more stringent requirements of the field compared to the enterprise context of control stations, our

security-gateway has been designed for deployment in the harsh environment of, for example, a substation. The gateway itself is designed to be integrated into a communication path as a bump-in-the-wire device, with one port to the existing component and another port to provide the newly secure interface to the outside. This setup facilitates a retrofit of the gateway. In future devices, however, it is also possible to directly integrate the technologies of the gateway to avoid the additional device.

Within the control station, a corresponding counterpart to the security-gateway is necessary to complete the integration of the security measures. By design, this could be any solution supporting the proper security features (see below). However, as we designed our gateway to flexibly support different network setups, it is possible to also use it within the control station as a counterpart. But, due to the 1-to-many topology and the intended deployment in the field, this is merely a proof-of-concept setup, as our gateway is not designed to scale with the increased number of connections within a control station.

The security measures are integrated into the communication path in form of the *Transport Layer Security* (TLS) protocol atop the TCP/IP protocol stack, as prescribed by the regulatory context introduced in Section II-A. This integration is completely done by the security-gateways, requiring no change of the existing devices at all. With a proper configuration of TLS (mutual authentication, cipher suites with perfect forward secrecy and authenticated encryption) and an additional firewalling functionality (whitelist based filtering of incoming traffic) in the gateway, all threats of Section II-B are resolved.

The integration of TLS into the communication path at the transport layer results in an application-protocol agnostic and completely transparent deployment of the security measures. To achieve all goals we had set for the security-gateway, a modular internal design has been created, which is introduced in the next subsection.

B. Internal Architecture

Our goal for the security-gateway was to create a device that achieves a high level of security and safety over the complete operation lifetime of the SCADA-systems. Furthermore, it should be low cost to enable an easy retrofit of existing systems, and it should be compliant to all regulatory standards. For that, a modular internal architecture based on the separation-of-concerns principle has been created.

In a previous work [25], we showed that a separation of cryptographic functions from the communication interface onto different functional hardware units increases the overall security level of a device. Adapted to our security-gateway, this resulted in distinct processors for handling the TCP/IP protocol stack and for performing all TLS related tasks. Thus, all cryptographic data and operations are isolated from the outside and therefore protected.

As the related work in Section III showed, additional security components can further increase the security level. Therefore, we also added two supplemental security components. A pluggable smartcard to store all long term cryptographic keys in a tamper-proof storage and a true random number generator (TRNG) with high entropy for the creation of ephemeral keys. The resulting internal architecture of the gateway is depicted in Figure 1.

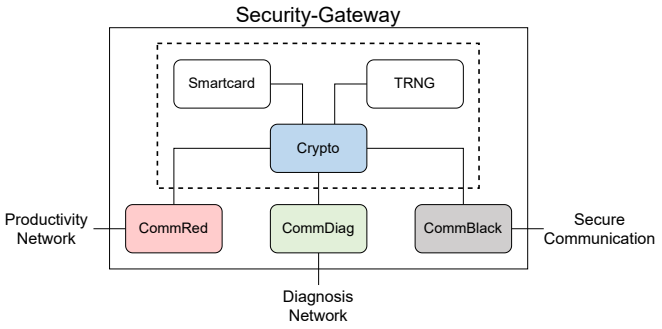

Fig. 1. Internally, the security-gateway consists of four independent functional units with separate tasks (marked with different colors). The three processors in the lower area are responsible for the communication with external devices using TCP/IP (*CommRed* with the legacy device; *CommBlack* with the counterpart of the secure channel; *CommDiag* provides an interface to a second diagnosis network not relevant for this work). The central *Crypto* processor handles all TLS tasks with the support of the *Smartcard* and the *TRNG*. The dashed line indicates a modular design based on two hardware boards.

During an evaluation of potential hardware solutions for the different required processors, we concluded that simple and low-cost microcontroller units (MCUs) with bare-metal software result in a more secure design compared to more powerful processors running embedded Linux. Such MCUs do not have recent security flaws based on complex processor designs (e.g., side-channels due to out-of-order execution like Spectre [26]). Furthermore, due to the separation of tasks onto many functional units, the individual software on each MCU is much simpler and does not require a complex operating system, further decreasing the attack surface and also simplifying a future auditing procedure.

The diagnosis interface provided by CommDiag is not part of the main functionality of the security-gateway and thus not in focus of this work. However, the non-participation of CommDiag in the primary operation allows it to perform additional functional safety tasks, increasing the reliability of the device. This is also necessary due to the regulatory context (see Section II-A). Based on a *Failure Mode and Effects Analysis* (FMEA), a single security-gateway has been classified to be in SIL 2, which is only achieved with the additional tasks performed by CommDiag within the Multi-MCU design.

In order to increase the longevity of the device, the hardware is built modularly: the three communication MCUs (CommRed, CommBlack and CommDiag) are placed on a *Mainboard*, the security related components (Crypto MCU, smartcard and TRNG) on an exchangeable *Cryptoboard* (indicated by the dashed line in Figure 1). This enables a partial hardware upgrade of the Cryptoboard without replacing the whole security-gateway in case new cryptographic algorithms must be supported, which require more powerful hardware. Furthermore, the pluggable smartcard enables an easy upgrade with new functionality of solely the card, too. More information about the exact separation of tasks onto the different MCUs and more details about the architecture can be found in [27].

In addition to the security measures to protect the communication channel, the design has many other features to further improve the overall system security. To update the software of the MCUs while maintaining the integrity of it, there are secure-boot and secure-software-update mechanisms. Furthermore, functionalities to integrate the device into a Public-Key-Infrastructure (PKI) for certificate and key management (via the Enrollment-over-Secure-Transport EST protocol) and for status verification of peer-certificates (via Certificate Revocation Lists CRL and the Online Certificate Status Protocol OCSP) are integrated. Finally, all system events within the gateway are logged in a cryptographically secure audit-trail that fulfills the security goal of non-repudiation. That way, the system behavior is traceable in case of an incident.

The created internal architecture fulfills all set requirements of Section II. To verify its viability, a proof-of-concept prototype has been created for evaluation. In the next section, the implementation of this prototype is briefly introduced.

V. Implementation

The current prototype implements all features to integrate TLS into the application traffic between the existing device and the secure counterpart. Furthermore, all mentioned additional security features are implemented, too.

The hardware is based on Cortex-M7 MCUs from STMicroelectronis, namely STM32H743 for the communication MCUs and STM32H753 for the Crypto-MCU. The Crypto-MCU features additional hardware accelerators for symmetric cryptographic algorithms (e.g., AES and SHA) to boost the performance of the gateway. The smartcard is an Infineon SLE78 chip with software from Atos, certified to EAL5+. For the TRNG, we use the PTG.3 certified module PRG270 from Ingenieur-Büro Bergmann. To implement the modular hardware design, we created two PCBs for the Cryptoboard and the Mainboard, connected using standard pin-headers. The communication between the MCUs is done over SPI for the high-throughput payload data and over UART for all remaining data (e.g., maintenance, logging, functional safety).

For the software on the MCUs, we created a common base firmware for all four controllers, using the FreeRTOS kernel and custom drivers. On the three communication MCUs, the Lightweight IP (LWIP) stack is used for network functionality, together with a custom Ethernet driver that incorporated the firewall. To implement TLS on the Crypto MCU, we use the WolfSSL library in combination with drivers for the smartcard and the TRNG.

VI. Results

Using the current prototype, the viability of our gateway has been confirmed in several field tests within realistic laboratory setups, consisting of a simulated control center and a substation with real RTUs and automation devices as end nodes. In all tests, they showed no difference in their behavior with our gateways incorporated. Therefore, we conclude that our approach works as intended and is indeed a viable option to add security measures into the SCADA-systems.

In additional performance measurements, we characterized the behavior of a single security-gateway and also of the complete setup consisting of two gateways. Summarizing these results, we measured an average connection setup-time (including the TLS handshake between the two gateways) of below two seconds. The latency added to the communication channel for actual messages is between 0.5 ms and 1.5 ms, depending on the load of the gateway. Finally, the maximum capable throughput is between 30 Mbps and 50 Mbps. However, this throughput and its variability is currently limited by the internal half-duplex SPI connection between the MCUs, which is a bottleneck to be removed in a future revision of the prototype.

Furthermore, first penetration tests and preliminary audit procedures of the gateway and of the smartcard in particular have been performed to test the conformance to the relevant standards, to find potential vulnerabilities and to harden the device against various attack scenarios. The current hardware costs are around $200 for a single device, leading to an attractive solution to retrofit the communication paths within the current SCADA-systems and to deploy it in new installations.

The biggest limitation of the current prototype is the support for only a single TCP stream. Hence, if the communication between the two existing devices is based on multiple streams, the current prototype does not work. However, all considered SCADA protocols are based on a single TCP stream, making this limitation less significant. Nevertheless, it is part of future work to remove this limitation by extending the software of the prototype to support more streams and hence more use cases.

VII. Conclusion and Outlook

To protect the SCADA-systems of critical infrastructure from cyberattacks, comprehensive security solutions are necessary that comply with the extensive set of requirements within that field. In this work, we presented a security-gateway to be deployed into the communication path between two nodes to add the TLS protocol and firewall functionality as security measures. In order to make the device comply with all requirements and prescriptions, and to keep the high level of dependability of the overall system while integrating the security measures, a modular internal architecture for the gateway has been designed. Based on the separation-of-concerns principle, a Multi-MCU system consisting of four microcontrollers and two additional security modules form the complete gateway. This setup achieves the isolation of cryptography from the communication interfaces and therefore increases the level of security while also improving the longevity of the device.

The current proof-of-concept prototype has been thoroughly evaluated to confirm the viability of the design. The results are very promising and conclude that the proposed solution is a viable option to integrate security measures into the SCADA-systems of critical infrastructures.

Acknowledgment

The presented work is part of the research project *Energy Safe and Secure System Module* (ES^{3}M), which is funded by the Project Management Jülich (PtJ) and the German Federal Ministry for Economic Affairs and Energy (BMWi) under funding code 0350042A.

REFERENCES

[1] IEA. (2021) Global Energy Review 2021. IEA. Accessed: Sep 29th, 2021. [Online]. Available: https://www.iea.org/reports/global-energy-review-2021/renewables

[2] A. Greenberg. (2017, June) How an entire nation became russia's test lab for cyberwar. Article. WIRED. Accessed: Sep 23th, 2021. [Online]. Available: https://www.wired.com/story/russian-hackers-attack-ukraine/

[3] *IEC 61850: Communication networks and systems for power utility automation*, International Electrotechnical Commission Std.

[4] *IEC 60870-5-104: Telecontrol equipment and systems - Part 5-104: Transmission protocols - Network access for IEC 60870-5-101 using standard transport profiles*, International Electrotechnical Commission Std.

[5] O. Vuković, "Data Integrity and Availability in Power System Communication Infrastructures," 2013, Publisher: KTH Royal Institute of Technology.

[6] *IEC 61508: Functional safety of electrical / electronic / programmable electronic safety-related systems*, International Electrotechnical Commission Std.

[7] *IEC 62351: Power systems management and associated information exchange – Data and communications security*, International Electrotechnical Commission Std.

[8] Bundesamtes für Sicherheit in der Informationstechnik. (2021, May) Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0). Publication.

[9] ——. (2022, January) Technische Richtlinie TR-02102 - Kryptographische Verfahren: Empfehlungen und Schlüssellängen. Publication.

[10] National Institute for Standards and Technology. (2020, May) Sp 800-57: Recommendation for key management. Publication.

[11] ——. (2015, May) Sp 800-82: Guide to industrial control systems (ics) security. Publication.

[12] International Organization for Standardization, "Information technology — Security techniques — Evaluation criteria for IT security," Standard ISO/IEC 15408-1/2/3, December 2009.

[13] M. Cooper and K. Schaffer, "Security requirements for cryptographic modules," 2019-03-22 2019.

[14] E. Irmak and I. Erkek, "An overview of cyber-attack vectors on SCADA systems," in *2018 6th International Symposium on Digital Forensic and Security (ISDFS)*, March 2018, pp. 1–5.

[15] C. K. G. Ang and N. P. Utomo, "Cyber Security in the Energy World," *2017 Asian Conference on Energy, Power and Transportation Electrification, ACEPT 2017*, vol. 2017-Decem, pp. 1–5, 2017.

[16] R. Schlegel, S. Obermeier, and J. Schneider, "A security evaluation of IEC 62351," *Journal of Information Security and Applications*, vol. 34, no. June 2018, pp. 197–204, 2017.

[17] J. G. Wright and S. D. Wolthusen, "Limitations of IEC62351-3's Public Key Management," *Proceedings - International Conference on Network Protocols, ICNP*, vol. 2016-Decem, pp. 1–6, 2016.

[18] National Institute for Standards and Technology. Post-Quantum Cryptography. NIST. Accessed: March 10th, 2022. [Online]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography

[19] R. Khan, K. McLaughlin, B. Kang, D. Laverty, and S. Sezer, "A Seamless Cloud Migration Approach to Secure Distributed Legacy Industrial SCADA Systems," in *2020 IEEE Power Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, 2020, pp. 1–5.

[20] R. Khan, K. Mclaughlin, D. Laverty, and S. Sezer, "Design and Implementation of Security Gateway for Synchrophasor Based Real-Time Control and Monitoring in Smart Grid," *IEEE Access*, vol. 5, pp. 11 626–11 644, 2017.

[21] O. Kehret, A. Walz, and A. Sikora, "INTEGRATION OF HARDWARE SECURITY MODULES INTO A DEEPLY EMBEDDED TLS STACK," *International Journal of Computing*, vol. 15, pp. 22–30, 2016.

[22] R. Matischek and B. Bara, "Application Study of Hardware-Based Security for Future Industrial IoT," in *2019 22nd Euromicro Conference on Digital System Design (DSD)*, 2019, pp. 246–252.

[23] D. Bienhaus, A. Ebner, L. Jäger, R. Rieke, and C. Krauß, "Secure gate: Secure gateways and wireless sensors as enablers for sustainability in production plants," *Simulation Modelling Practice and Theory*, vol. 109, p. 102282, 2021.

[24] M. Eckel, D. Kuzhiyelil, C. Krauß, M. Zhdanova, S. Katzenbeisser, J. Cosic, M. Drodt, and J.-J. Pitrolle, "Implementing a Security Architecture for Safety-Critical Railway Infrastructure," in *2021 International Symposium on Secure and Private Execution Environment Design (SEED)*, 2021, pp. 215–226.

[25] T. Frauenschläger, S. Renner, and J. Mottok, "Security Improvements by Separating the Cryptographic Protocol from the Network Stack onto a Multi-MCU Architecture," in *Architecture of Computing Systems – ARCS 2020*. Cham: Springer International Publishing, 2020, pp. 185–199.

[26] P. Kocher, J. Horn, A. Fogh, D. Genkin, D. Gruss, W. Haas, M. Hamburg, M. Lipp, S. Mangard, T. Prescher, M. Schwarz, and Y. Yarom, "Spectre attacks: Exploiting Speculative Execution," *Communications of the ACM*, vol. 63, no. 7, pp. 93–101, 2020.

[27] T. Frauenschläger, M. Dentgen, and J. Mottok, "Systemarchitektur eines Sicherheitsmoduls im Energiesektor," in *2. Symposium Elektronik und Systemintegration: Intelligente Systeme und ihre Komponenten: Forschung und industrielle Anwendung*, April 2020.