# Assessment of a MACsec-based security system for use in critical Infrastructure Communication

Lukas Füreder
*Technical University of Applied Sciences Regensburg (OTH)*
*Laboratory for Safe and Secure Systems (LaS³)*
Regensburg, Germany
lukas.fuereder@oth-regensburg.de

Supervisor: *Prof. Dr. Jürgen Mottok*

**Abstract**

Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis at vero eros et accumsan et iusto odio dignissim qui blandit praesent luptatum zzril delenit augue duis dolore te feugait nulla facilisi. Lorem ipsum dolor sit amet,

***Keywords*— MACsec, IEC61850, IEC62351, GOOSE, Secure Communication**

## I. Introduction

Companies that are classified as critical infrastructure as for example water supply facilities, power plants and their corresponding distribution systems, can constitute a vulnerability which may be exploited to disrupt the supply of basic resources to entire countries. For this reason, laws such as the Network and Information Security Act (NIS-2) [1] of the European Union or the IT Act 2.0 [23] of the German Federal Office for Information Security (BSI) demand a unified level of cybersecurity for these entities. In these regulations, the councils prescribe that the companies will be required to implement security features to detect and prevent intrusions, as well as remove faults caused through intrusion attempts during system runtime [23, §11 (1d)]. Additionally the extension of this paragraph dictates, that these companies are obliged to provide proof of compliance with the safety requirements in a two year period [23, §11 (1e)]. This decision is intended to ensure the future working of the security systems with respect to adapting changes of the latest technologies.

In addition to measures for detecting and handling attacks, these laws mandate the compliance with security standards to ensure the protection of confidential information [23, §2 (2a)]. The main objectives of these security standards is the ensurance of security goals as for instance authenticity, integrity and confidentiality of the internal mode of operation [23, §2 (13)]. Organizations such as the International Electrotechnical Commission (IEC) or the Institute of Electrical and Electronics Engineers (IEEE) develop standards that specify the implementation of these abstract security goals. This paper evaluates the currently established implementation of protection systems securing communication in Substation Automation Systems (SASs) and thereby provides a brief overview of the communication standard used in these facilities. Following this we propose a Media Access Control Security (MACsec) based security system and evaluate, wether this implementation fulfills the requirements of the security goals specified in the IEC 62351 security standards.

The further course of the paper is structured as follows: Chapter II clarifies the technical background of this paper and thereby provides a general overview of the IEC 61850 communication standard and the associated message types. Building on this, the further part of this chapter presents the current state of message security mandated by the IEC 62351 security standard. Following this a brief introduction into the MACsec security standard is provided, which presents the relevant features used in the implementation later on. Chapter III displays relevant information presented by related work assessing the current state of technology in this topic. In the further course of the paper Chapter IV explains the test setup used to measure the efficiency of the MACsec-based security system. Lastly the data gathered from this is then evaluated in chapter V and is placed in the context of the mandated safety requirements.

## II. Background

### A. Overview of the IEC 61850 Standard

Among other standards used for communication is industrial applications, power systems primarily utilize the IEC 61850 standard [4], which is published and maintained by the International Electrotechnical Comission (IEC) [16]. This standard specifies the transmission of diagnostical information, measurement values or control signals among devices structured in a three level architecture [19], as displayed in Figure 1. The major advantage here consists of the object-oriented data structure defined in this standard, which makes the integration of various components developted by different vendors possible [3, p. 5643].

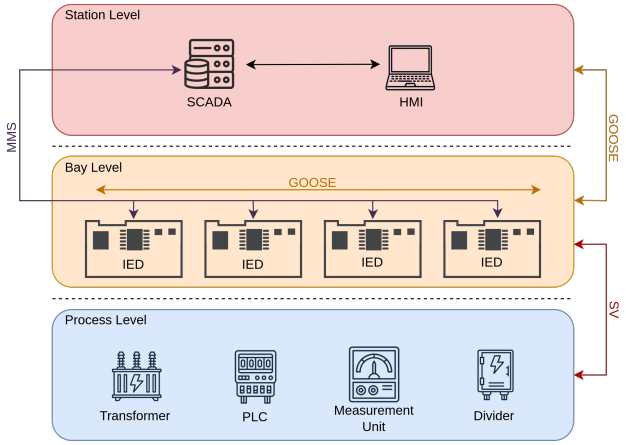


Fig. 1. Overview of the three architecture levels in IEC 61850 [19]

At the lowest point, the process level contains devices tasked with the actual power management. Examples for these are: transformers, circuit breakers, Programmable Logic Controllers (PLCs) and measurement units [19]. Upon configuration, Process Level components periodically publish measurement information to all subscribing communication partner in the Bay Level via Sampled-Value (SV) packets [20]. This communication involves LAN-internal multicast packets, which take place exclusively on the second layer (=Data Link Layer) of the Open System Interconnection (OSI) model [20].

The Bay Level above contains the Intelligent Electronic Devices (IEDs), each of which represents a transformation field in the substation [6, p. 39]. The IEDs gather the measurement data from the process level and initially processes them. The resulting information is then communicated through Manufacturing Message Specification (MMS) packets to other IEDs and the Station Level components [9, p. 44]. Simultaniously the IEDs receive control signals from the Station Level, which are also transmitted via MMS packets [13]. As the Station Level components are not necessarily located in the same LAN as the IEDs, the MMS messaging is implmented through TCP packets on the fourth layer (=Transport Layer) of the OSI model [9, p. 45]. In addition to the MMS messaging, the IEDs use Generic Object Oriented Substation Events (GOOSE) to send time-critical information to surrounding IEDs. Simmilar to SV, GOOSE messages are implemented through broadcast Ethernet packets in the LAN [2].

The devices located in the Station Level of the architecture are responsible for controlling the SAS. This is achieved through MMS packets adressed to specific IEDs and the presentation of the processed information in graphical illustrations to the user [19]. For this, the Station Level components typically consist of a Supervisory Control and Data Acquisition (SCADA) component and a Human-Machine-Interface (HMI). Lastly, as displayed in Figure 1, it is possible to transmit GOOSE messages to the Station Level components. For this the IEC 61850-90-5 standard [10] defines a routable version of the layer two GOOSE frame. For this purpose, the Ethernet packets are extended by adding network and transport layer headers to form a UDP packet, which is routable throughout a Wide Area Network (WAN) [21].

### B. Message Security according to IEC 62351

Building on the IEC 61850 message types described in Chapter II-A, the IEC 62351 standard [11] dictates security goals and requirements for cybersecurity solutions. In order to evaluate the proposed MACsec solution for industrial applications correctly, we need to assess the proposed security functions according to the demands of this standard.

With regard to MMS messaging, the standard divides the security requirements according to the layers of the OSI reference model. The upper three layers are summarized in the application profile and the lower four layers in the transport profile [22]. Based on this, the standard specifies that the security system shall verify the authenticity of the communication partner and the

integrity of the transmitted messages during the handshake phase of the transport profile [3]. Following this the system shall provide confidentiality for the outgoing messages in the data transfer phase [22]. With respect to the upper three layers, the standard specifies two possible implementations in the application profile: peer-to-peer security and End-to-End security [3]. The primary difference between them consists in the data origin authentication and message integrity checks, which are only verified during the association establishment in the peer-to-peer implementation, whereas the End-to-End implementation also ensures them in the following data transfer [3].

For GOOSE messages the standard argues, that the strict real-time requirement of a maximum of 3 ms [2] outweighs the safety requirements and for this reason state, that security measures, which affect the trasnmission rates are not acceptable [14]. Building on this the IEC 62351 standard advises against the encryption of GOOSE messages and only proposes the use of digital signatures to verify the authenticity of the GOOSE publisher and the integrity of the message. As simmilar restrictions arise for SV messages, the standard equally advises the usage of digital signatures for SV packets [3].

### *C. Fundamentals of the MACsec Security Standard*

MACsec poses an information security standard, which protects messages on the second layer (=Data Link Layer) of the OSI model. In contrast to security standards operating in higher layers of the TCP/IP stack (e.g. Transport Layer Security (TLS)), which provide End-to-end encryption, MACsec verifies the integrity and authenticity of a packet within each hop of the transmission [17]. However, this lower layer implementation close to the PHY enables MACsec to secure communication, which takes place exclusively in Ethernet packets (e.g. SV & GOOSE). The following paragraph explains the most important aspects of the MACsec standard, which are responsible for ensuring the authenticity, integrity and confidentiality of the transmitted packets.

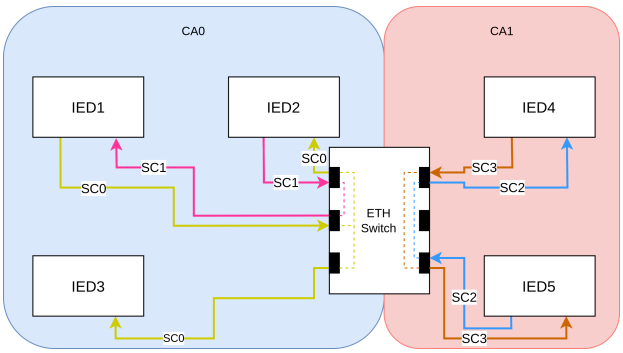


Fig. 2. Schematic representation of the MACsec entities [12]

As displayed in Figure 2, the communicating devices are initially grouped in Connectivity Associations (CAs), which represent the logical separation of secured communication areas [12, p. 35]. Each member of a CA possesses the associated Connectivity Association Key (CAK), which is later used to generate the individual session keys. Simmilar to other encryption systems, the CAK acts as a shared secret between the individual parties and is therefore used to verify the authenticity of incoming MACsec frames. In the IEEE 802.1AE standard the distribution of the CAK among the participants is only specified as a brief overview of the established methods [12, p. 230]. In our case, we utilize pre-shared keys to configure the CA in the test set up explained in chapter IV.

Within a CA, the connections between the communicating devices are referred to as Secure Channels (SCs). As displayed in Figure 2, a SC is a unidirectional connection from a transmitter to one or more receivers. Each SC can be identified by the Secure Channel Identifier (SCI), which is added to the MACsec specific field in the secured frame [12, p. 43]. During transmission on a SC, the packets are sent within Security Associations (SAs). These are time intervals in which a single Secure Association Key (SAK) is valid [12, p. 44]. The SAK is the session key, which is derived from the previously described CAK and is only valid for up to $(2^{32} - 1)$ packets, after which a new SAK needs to be generated [12, p. 66]. To be able to monitor the number of transmitted packets in an SA, the MACsec frame contains a packet number field, which is incremented with each subsequent packet. This field aditionally ensures, that no replay attacks can be carried out on the network [12, p. 145].

To ensure confidentiality and integrity of the transmitted frames, MACsec utilizes Authenticated Encryption with Associated Data (AEAD) cipher suites. These encryption system typically consist of a symmetric block cipher, wich provides the option to encrypt the payload of the message and simultaniously generates a Message Authentication Code (MAC) over the entire message [2]. For usage the IEEE 802.1AE standard specifies four variations of the Advances Encryption System in Galois/Counter Mode (AES-GCM) [12, p. 143ff].

## III. Related Work

To assess the operating principal of a MACsec-based security system in IEC 61850 compliant communication it is necessary to understand both the working method of the communication inside a substation as well as the corresponding functionality of the MACsec security standard. The following related work display these important aspects and are therefore relevant for the implementation of an experimental set up for MACsec secured industrial communication.

Mackiewicz [16] describes the overall usage of the IEC 61850 protocol by displaying key features as well as the general aspects of IEC 61850 compliant communication. Since this standard represents a core part of the communication inside of power grid systems, it is vital to understand the corresponding aspects such as communication paths, model structures or data addressing in order to design a representative test environment.

Hussain *et al.* [3] published a paper assessing the IEC 62351 standard and its security mechanisms towards IEC 61850 compliant messaging. The publication initially describes the basic values and security goals of the safety standard and, building on this, which attacks can potentially be carried out on IEC 61850 messages to manipulate the internal workings of a SAS. At this point the paper primarily focuses on the Ethernet-based message types GOOSE and SV and the associated decision not to encrypt them due to strict time delivery requirements.

Lackorzynski *et al.* [15] proposed modifications of the IEEE 802.1AE standard to improve MACsec for usage in industrial applications. In particular, the fragmentation of Ethernet frames was considered. This procedure is necessary, if messages exceed the Maximum Transmission Unit (MTU) and are thus possibly discarded by the recipient of the message. The presented implementation ensures this parameter and spits messages into multiple frames, if it is exceeded. Additionally the authors discuss the usage of different cipher suits instead of the AES-GCM 128/256 specified in the MACsec standard. The evaluation of their study shows that the ChaCha20-Poly1305 cipher is a promising alternative for industrial applications.

Moreira *et al.* [17] evaluate various approaches to introduce cyber security in SASs. Initially, a brief outline of the communication structures in substations is presented. Building on this, various established security approaches are explained and evaluated based on the protection objectives of the IEC 62351 standard. The authors also point out possible implementation problems, such as incompatibilities between the security systems and the communication protocols or the handling of redundant packets inside ring-topology networks. In the further course of the paper, they present the idea of MACsec based communication security in SASs and the associated advantages and challenges that arise with it.

Hussain *et al.* [2] analyzed possible GOOSE security implementations based on their preceding review of the IEC 62351 standard [3]. Especially concerning the decision to abstain from implementing confidentiality in GOOSE messages, the authors argue, that the critical payload of these messages demand encryption to provide efficient protection against attacks. However, in order to meet the real-time requirements of the protocol, they suggest replacing the RSA signature with encryption using an AEAD cipher. In the further course of the paper they compare encryption and signature times between different AEAD ciphers and conclude based on the measurement results, that these encryption systems pose a promising solution, which provides the opportunity to encrypt the message while simultaniously meeting the 3 ms timing requirement.

Building on the theoretical proposition of Moreira *et al.* [17], we formulate our evaluation of MACsec carried out for use in substations and other power systems based on the IEC 61850 standard. Along with this, we consider the findings of Hussain *et al.* [2] in relation to the usage of Encrypt-then-MAC AEAD ciphers in the implementation of our MACsec test environment. From this, our experimental setup enables us to discuss the advantages and disadvantages of MACsec in comparison with the security goals of the IEC 62351 standard.

## IV. Implementation

To test the mode of communication in a SAS, we implement a test environment consisting of three Bay Level components. As the IEDs take part in all forms of message exchange inside the Substation Architecture, they are perfectly suitable for testing the communication in conjunction with MACsec.

In order to ensure the reproducibility of this study, we decided to use the Raspberry Pi 4 as hardware plattform for all devices in the setup. With respect to the software used in the applications, we utilize the open source library libiec61850[1] to establish the different communication types and data structures of the IEC 61850 standard. To integrate MACsec into the communication, we utilize the MACsec Linux kernel module[2], which establishes a configurable virtual interface on top of an existing network interface [18]. For the implementation of time measurement in chapter IV-C,

The remainder of this chapter is structured as follows: Chapter IV-A initially explains the overall structure of the test environment. Building on this, Chapter IV-B describes the overall MACsec configuration and the corresponding entities of the security standard. Lastly Chapter IV-C elaborates on the subsequent test executions.

[1]source: https://libiec61850.com/

[2]source: https://github.com/torvalds/linux/blob/master/drivers/net/macsec.c

### A. Structure of the Test Environment

As displayed in Figure 3, we configure IED1 as a publishing server and IED2 and IED3 as communication clients. Furthermore the implementation of IED1 contains a XML data structure compliant to the specification of the Substation Configuration Language (SCL) in IEC 61850-6 [5]. This file contains the communication and processing information of the IED itself [16].

In our case, we integrated a measurement unit (MMXU) [8, p. 268] and a control unit (LLN0) [8, p. 164] into the SCL file. During runtime, IED1 continuously populates the data points of the measuring unit with sampled values of a sinusoidal function. In addition to the actual measurement, each sampled value contains a time stamp and a quality index [7, p. 61ff]. These values can then be requested by IED2 and IED3 via MMS messages.

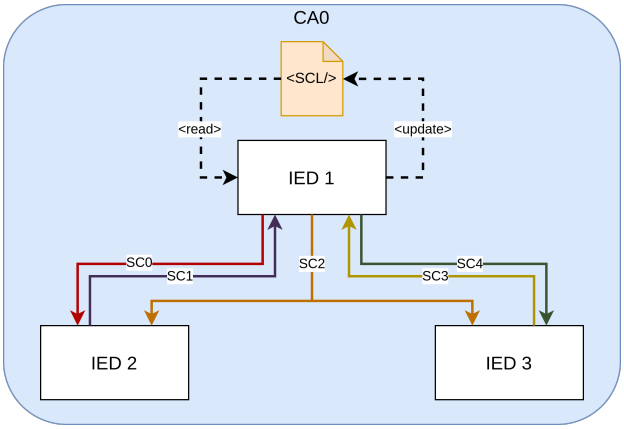


Fig. 3. Component Structure of the Test Setup

In addition to the TCP request-response communication via MMS messages, IED1 periodically publishes GOOSE and SV messages in a configurable interval containing the current value of the measurement. The configuration of the GOOSE messages, which contains the corresponding broadcast MAC address, VLAN Id and VLAN Priority are equally stored in the control unit of the SCL file [9, p. 189]. For the transmission of the SV packets, an Application Protocol Data Unit (APDU) is configured during the initialization phase of the server. This object contains the floating point number value of the measurement and a message time stamp. As the application progresses, the content of the APDU is periodically updated and published.

On the client side, the subscription to the corresponding events (in this case GOOSE and SV) is implemented in software in the form of asynchronous handler functions, which subsequently log the incoming information.

### B. MACsec integration in the Test Environment

Building on the general structure described in chapter IV-A, the implementation of MACsec into the test setup can now be explained. In doing so, we primarily integrated all devices in the same CA by distributing a pre-shared CAK. Based on this key, the various SCs and SAs can be established as shown in Figure 3.

For bidirectional MMS communication between two IEDs, one SC is required for each communication direction. Using the example of packet exchange between IED1 and IED2, we have configured the secure channels SC1 and SC2 for this purpose. Each of these channels derives its own SAK from the CAK and establishes a secure connection for the duration of the SA. The establishment of SC3 and SC4 is carried out identically for MMS communication between IED1 and IED3. Consequently, if IED2 and IED3 are also ment to send secure multicast messages, two additional SCs must be configured.

With regard to the secure publication of GOOSE and SV packets, we established an additional SC (displayed in Figure 3 as SC2), which is connected to both IED2 and IED3. This configuration enables us to broadcast the messages while simultaniously securing the payload and ensuring authenticity and integrity. Since this configuration only allows the publication of GOOSE and SV packets originating from IED1, we only need one SC to secure them in MACsec.

### C. Definition of the Test Procedures

To evaluate whether this MACsec implementation fulfills the requirements of the IEC 62351 standard, we conduct a measurement of the transmission times for each of the different package types. In order to achieve a precise time measurement, we expanded the implementation of the server and the client application to toggle a General Purpose Input/Output (GPIO) pin during transmission and reception of the associated frame type.

By using an external logic analyzer, the times between the voltage level shifts can be measured in the next step. Since the measurement is performed by an external device, we do not need clock synchronization between the communication participants, which significantly reduces the implementation efforts of the measurement.

## V. Evaluation

## VI. Conclusion

## References


[1] Council of the European Union. *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)*. L 333, p. 80. Dec. 2022.

[2] S. M. Suhail Hussain, Shaik Mullapathi Farooq, and Taha Selim Ustun. "A method for achieving confidentiality and integrity in IEC 61850 GOOSE messages". In: *IEEE transactions on Power Delivery* 35.5 (2020), pp. 2565–2567.

[3] S. M. Suhail Hussain, Taha Selim Ustun, and Akhtar Kalam. "A review of IEC 62351 security mechanisms for IEC 61850 message exchanges". In: *IEEE Transactions on Industrial Informatics* 16.9 (2019), pp. 5643–5654.

[4] *IEC 61850:2023 SER Series – Communication networks and systems for power utility automation – ALL PARTS*. International Standard. Geneva, CH: International Electrotechnical Comission, 2023.

[5] *IEC 61850:2023 SER Series – Communication networks and systems for power utility automation – Part 6 Configuration description language for communication in power utility automation systems related to IEDs*. International Standard. Geneva, CH: International Electrotechnical Comission, 2010.

[6] *IEC 61850:2023 SER Series – Communication networks and systems for power utility automation – Part 7-1 Basic Communication Structure – Principles and Models*. International Standard. Geneva, CH: International Electrotechnical Comission, 2011.

[7] *IEC 61850:2023 SER Series – Communication networks and systems for power utility automation – Part 7-3 Basic Communication Structure – Common data classes*. International Standard. Geneva, CH: International Electrotechnical Comission, 2010.

[8] *IEC 61850:2023 SER Series – Communication networks and systems for power utility automation – Part 7-4 Basic Communication Structure – Compatible logical node classes and data object classes*. International Standard. Geneva, CH: International Electrotechnical Comission, 2010.

[9] *IEC 61850:2023 SER Series – Communication networks and systems for power utility automation – Part 8-1 Specific communication service mapping (SCSM) – Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3*. International Standard. Geneva, CH: International Electrotechnical Comission, 2011.

[10] *IEC 61850:2023 SER Series – Communication networks and systems for power utility automation – Part 90-5: Use of IEC 61850 to transmit synchrophasor information according to IEEE C37.118*. International Standard. Geneva, CH: International Electrotechnical Comission, 2012.

[11] *IEC 62351:2024 SER Series – Power systems management and associated information exchange - Data and communications security - ALL PARTS*. International Standard. Geneva, CH: International Electrotechnical Comission, 2024.

[12] *IEEE Std 802.1AE-2018 – IEEE Standard for Local and metropolitan area networks – Media Access Control (MAC) Security*. International Standard. New York, USA: The Institue of Electrical and Electronics Engineers, Inc., 2018.

[13] Jakub W. Konka et al. "Traffic generation of IEC 61850 sampled values". In: *2011 IEEE First International Workshop on Smart Grid Modeling and Simulation (SGMS)*. 2011, pp. 43–48. DOI: 10.1109/SGMS.2011.6089025.

[14] Nishchal Singh Kush et al. "Poisoned GOOSE: Exploiting the GOOSE protocol". In: *Proceedings of the Twelfth Australasian Information Security Conference (AISC 2014)[Conferences in Research and Practice in Information Technology, Volume 149]*. Australian Computer Society. 2014, pp. 17–22.

[15] Tim Lackorzynski et al. "Enabling and optimizing MACsec for industrial environments". In: *IEEE Transactions on Industrial Informatics* 17.11 (2020), pp. 7599–7606.

[16] Ralph E. Mackiewicz. "Overview of IEC 61850 and Benefits". In: *2006 IEEE Power Engineering Society General Meeting*. IEEE. 2006, 8–pp.

[17] Naiara Moreira et al. "Cyber-security in substation automation systems". In: *Renewable and Sustainable Energy Reviews* 54 (2016), pp. 1552–1562.

[18] Sabrina Dubroca. *ip-macsec(8) – Linux manual page*. https://man7.org/linux/man-pages/man8/ip-macsec.8.html. Accessed: 2024-05-13.

[19] SGRWin - Network Solutions Suite. *Basic understanding of IEC 61850*. https://www.sgrwin.com/goose-mms-and-sv-protocols/. Accessed: 2024-04-30.

[20] Typhoon HIL Inc. *IEC 61850 Sampled Values protocol*. https://www.typhoon-hil.com/documentation/typhoon-hil-software-manual/References/iec_61850_sampled_values_protocol.html. Accessed: 2024-04-30.

[21] Taha Selim Ustun, Shaik Mullapathi Farooq, and S. M. Suhail Hussain. "Implementing secure routable GOOSE and SV messages based on IEC 61850-90-5". In: *IEEE Access* 8 (2020), pp. 26162–26171.

[22] Taha Selim Ustun and S. M. Suhail Hussain. "IEC 62351-4 security implementations for IEC 61850 MMS messages". In: *IEEE Access* 8 (2020), pp. 123979–123985.

[23] “Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme*”. In: *Bundesgesetzblatt, ausgegeben zu Bonn* (2021). Teil I Nr. 25, pp. 1122–1138.