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

***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.**

***Index Terms*—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 [16] 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. [16, §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. [16, §11 (1e)] This decision is intended to ensure the future working of the security systems with respect to adapting changes of the latest technologies.

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 with the security goals set for these applications. The further course of the paper is structured as follows: Chapter II provides a general overview of the IEC 61850 communication standard and the associated message types. 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 works assessing the current state of technology in this topic. 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.

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) [11]. This standard specifies the transmission of diagnostical information, measurement values or control signals among devices structured in a three level architecture [13], 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].

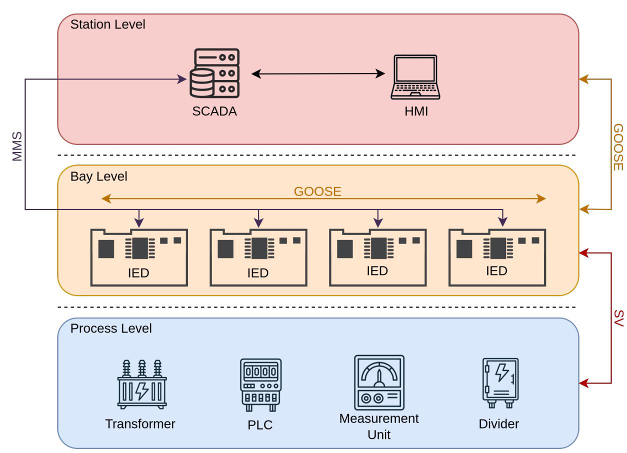

Fig. 1. Overview of the three architecture levels in IEC 61850 [13]

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 [13]. Upon configuration, Process Level components periodically publish measurement information to all subscribing communication partner in the Bay Level via Sampled-Value (SV) packets [14]. 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 [14].

The Bay Level above contains the Intelligent Electronic Devices (IEDs), each of which represents a transformation field in the substation [5, 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 [6, p. 44]. Simultaniously the IEDs receive control signals from the Station Level, which are also transmitted via MMS packets [9]. 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 [6, 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 [13]. 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 [7] 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) [15].

B. 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 [12]. 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.

As displayed in Figure 2, the communicating devices are initially grouped in Connectivity Associations (CAs), which represent the logical separation of secured communication areas [8, 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. 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 [8, p. 230]. In our case, we utilize pre-shared keys to configure the CA in the test set up explained in chapter IV.

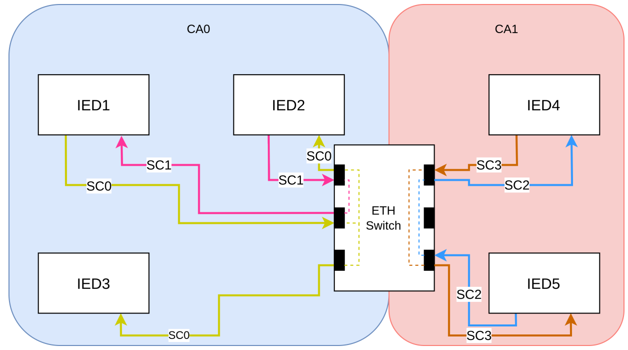

Fig. 2. Schematic representation of the MACsec entities [8]

Within a CA, the connections between the communicating devices are referred to as Secure Channels (SCs). An 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 header of the MACsec secured frame [8, p. 43].

III. Related Works

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 works display these important aspects and are therefore relevant for the implementation of an experimental set up for MACsec secured industrial communication.

Mackiewicz [11] 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 1850 messages to manipulate the internal workings of a SAS. At this point the paper primarily focuses on the Ethernet-based message types Generic Object Oriented Substation Event (GOOSE) and Sampled Values (SV) and the associated decision not to encrypt them due to strict time delivery requirements.

Moreira *et al.* [12] 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 and the associated advantages and challenges that arise with it.

Lackorzynski *et al.* [10] 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.

Building on the findings of Moreira [12] and Lackorzynski [10] we formulate the evaluation of MACsec carried out for use in substations and other power systems based on the IEC 61850 standard. Along with this, we discuss the advantages and disadvantages of MACsec in comparison with the security goals of the IEC 62351 standard based on our findings.

IV. Implementation

V. Evaluation

VI. Conclusion

References

[1] Council of 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 7-1 Basic Communication Structure – Principles and Models*. International Standard. Geneva, CH: International Electrotechnical Comission, 2011.

[6] *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.

[7] *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.

[8] *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.

[9] 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.

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

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

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

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

[14] 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.

[15] Taha Selim Ustun, Shaik Mullapathi Farooq, and SM Suhail Hussain. "Implementing secure routable GOOSE

and SV messages based on IEC 61850-90-5”. In: *IEEE Access* 8 (2020), pp. 26162–26171.

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