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 [4] 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. [4, §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. [4, §11 (1e)] This decision is intended to ensure that the security systems will continue to work with adapting changes of the latest technologies in the future.

This paper evaluates the currently established implementation of protection systems securing communication in Substation Automation Systems (SASs). Following this ... . Among other stadards used for communication is SASs, the facilities utilize the IEC 61850 standard, which is published and maintained by the International Electrotechnical Comission (IEC). This standard is used to transmit diagnostical information, measurement information or control signals between Supervisory Control and Data Acquisition (SCADA) entities and the associated substation components. The major advantage here consists of the object-oriented data structure specified in this standard, which enables the integration of various components developted by different vendors [2, p. 5643].

`-- HIER NOCH WEITER MIT MACSEC`

`-- HIER NOCH WEITER MIT PAPER STRUKTUR`

II. 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 associated security standard IEC 62351 and 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.

Moreira et al. [3]

III. Fundamentals of the IEC Standards

`-- HIER NOCH WEITER MIT IEC61850`

`-- HIER NOCH WEITER MIT IEC62351`

IV. Implementation

V. Evaluation

VI. Conclusion

References

[1] “DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL 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)”. In: *Journal of the European Union* (2022), pp. 1–60.

[2] SM 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.

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

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