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 electricity grids, power plants and their corresponding distribution systems, constitute a vulnerability which can 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.

`-- HIER NOCH WEITER ZU IT 2.0 UND NIS-2`

As basis for communication predominantly used in substations and later on in smartgrids, the International Electrotechnical Comission (IEC) publishes and maintains the IEC 61850 standard [3], which 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].

II. Related Works

III. Implementation

IV. Evaluation

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

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