END-TO-END SECURITY OF SMART METER INFRASTRUCTURE–BASED CONTROL CHAINS

A STRIDE Analysis of Residual Risks Beyond the Smart Meter Gateway

Julian Britz[1], Julian Maximilian Behrensen[2], **Sascha Kaven[1]**, Felix Scholl[1],
Kolja Eger[1], Milena Zachow[2] and Volker Skwarek[1]
[1]Hamburg University of Applied Sciences
[2]Technical University of Applied Sciences Lübeck
21.04.2026

SASCHA KAVEN

SASCHA.KAVEN@HAW-HAMBURG.DE

Experience

- M. Sc. industrial engineering
- PhD candidate at HAW Hamburg

Areas of Research

- Smart Grid
- Co-Simulation
- Cybersecurity

TOPICS OF RESEARCH INTEREST & CURRENT PROJECTS

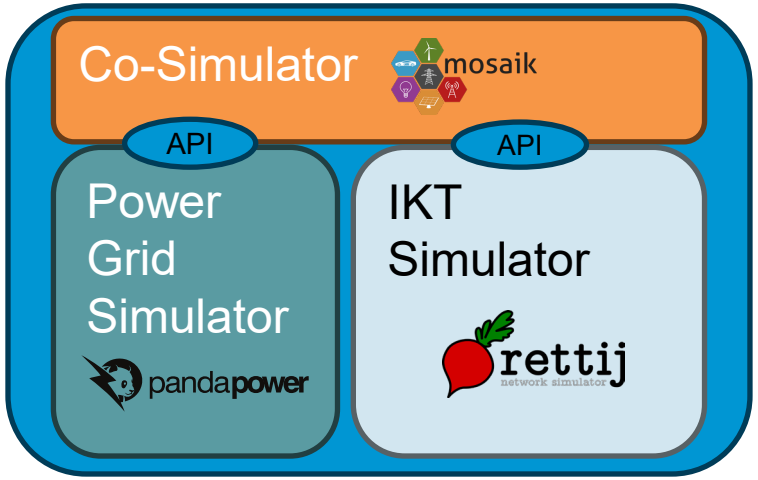
SimCyberGrid

Overview:

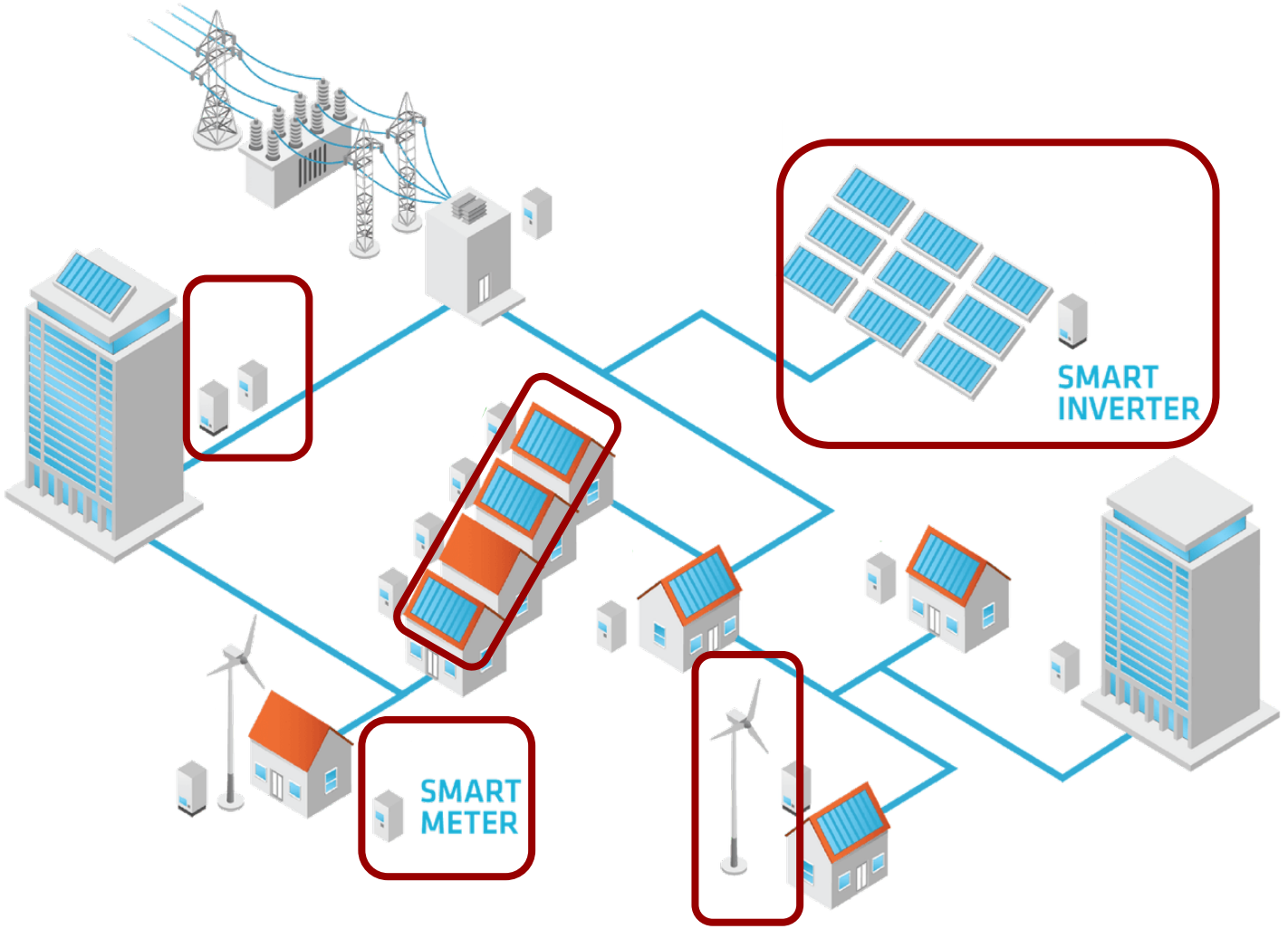
- Building a simulator for cyberattacks on distributed electrical microgrids
- Focus on prosumer-based low-voltage grids of the future
- Increasing integration of renewable energy → volatility & decentralization

Approach:

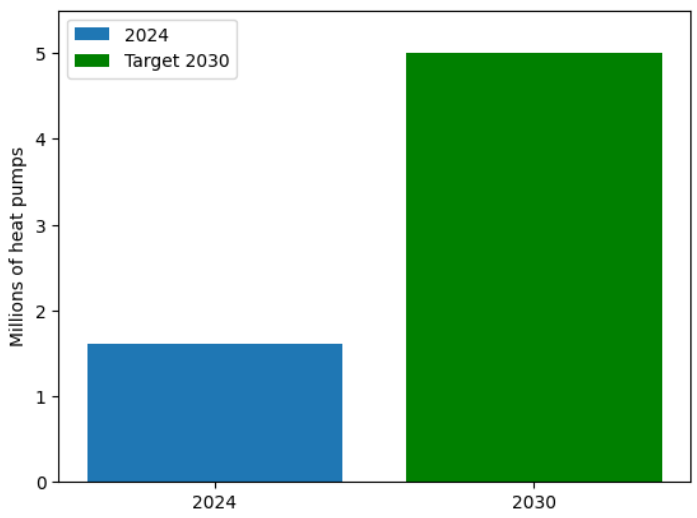
- Development of a co-simulation framework combining:
  - Electrical microgrid simulation
  - Internet-based communication network
- Execution of realistic cyberattacks in a virtual environment



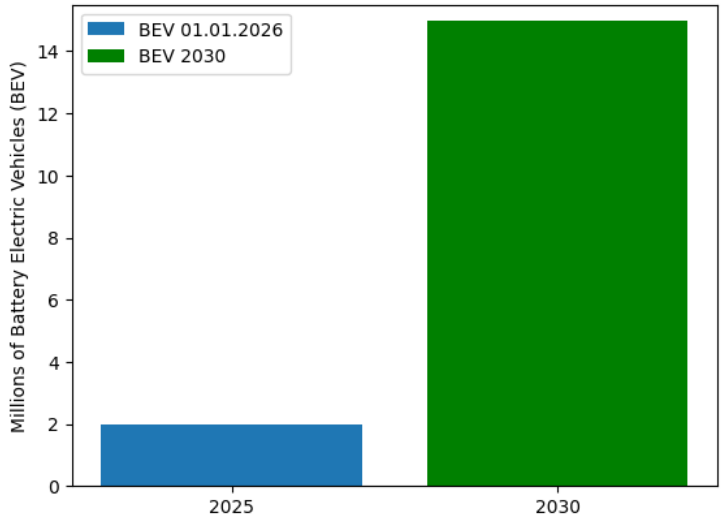
WHAT EXACTLY IS THIS SMART GRID?



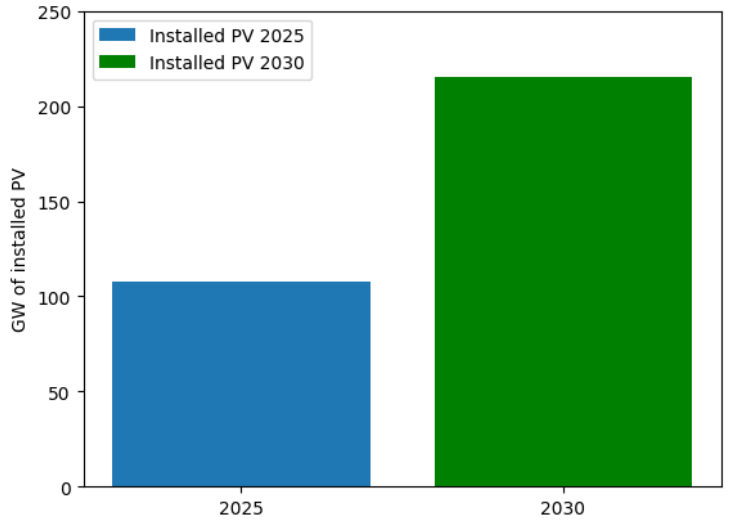
SIGNIFICANCE OF §14A OF THE ENERGY INDUSTRY ACT (ENWG) AND § 9 OF THE RENEWABLE ENERGY ACT (EEG)



Heat pump development in Germany (2024 vs 2030) [5]



Battery Electric Vehicle development in Germany (2025 vs 2030) [6]

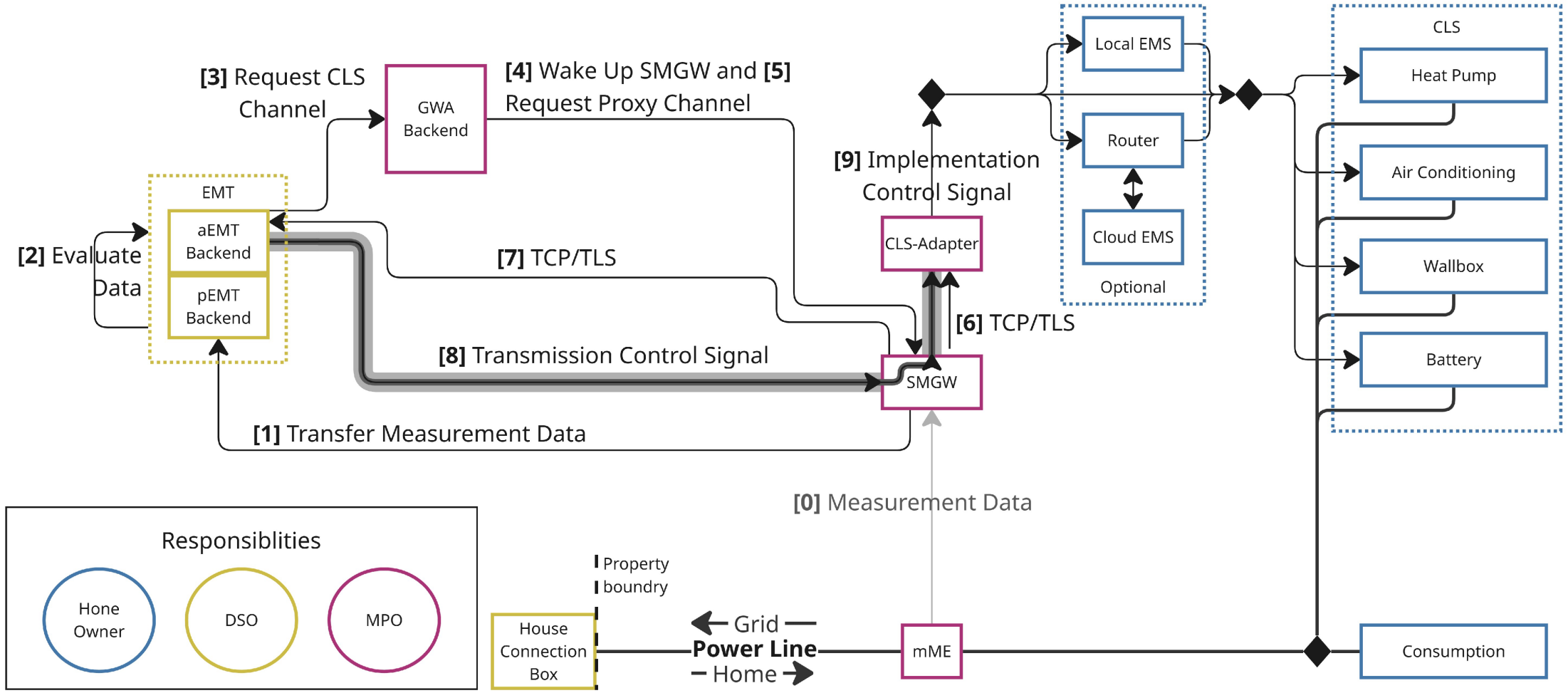


Installed PV development in Germany (2025 vs 2030) [7]

Amendment to the Energy Network Act: In future, network operators will no longer be permitted to refuse or delay the connection of new heat pumps, air conditioning units, electricity storage systems or private charging points for electric cars on the grounds of potential local network overload [8]

→ Network operators are granted control over the installations

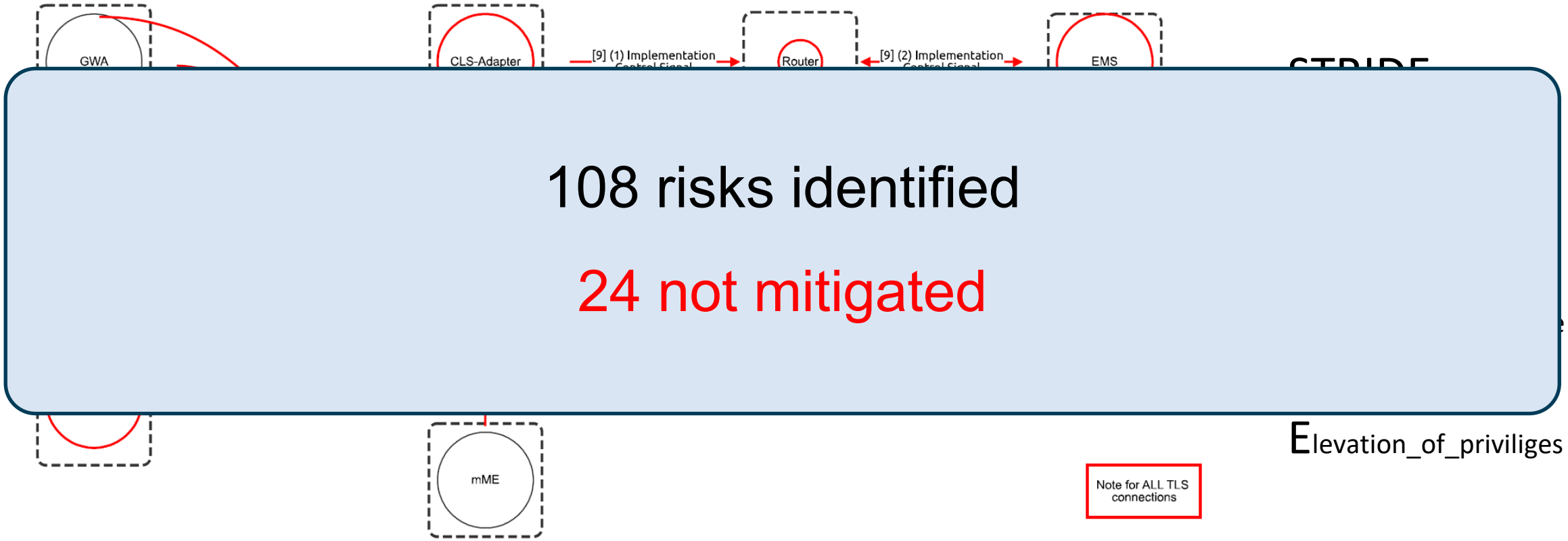
CONTROL PROCESS



References: [9]

STRIDE ANALYSIS

End-to-end analysis using OWASP Threat Dragon

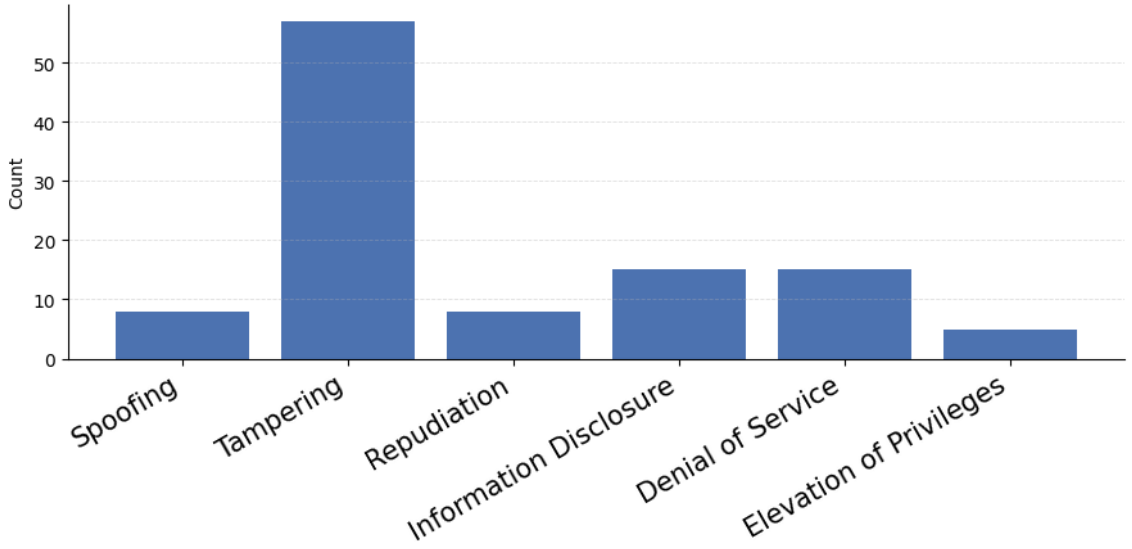


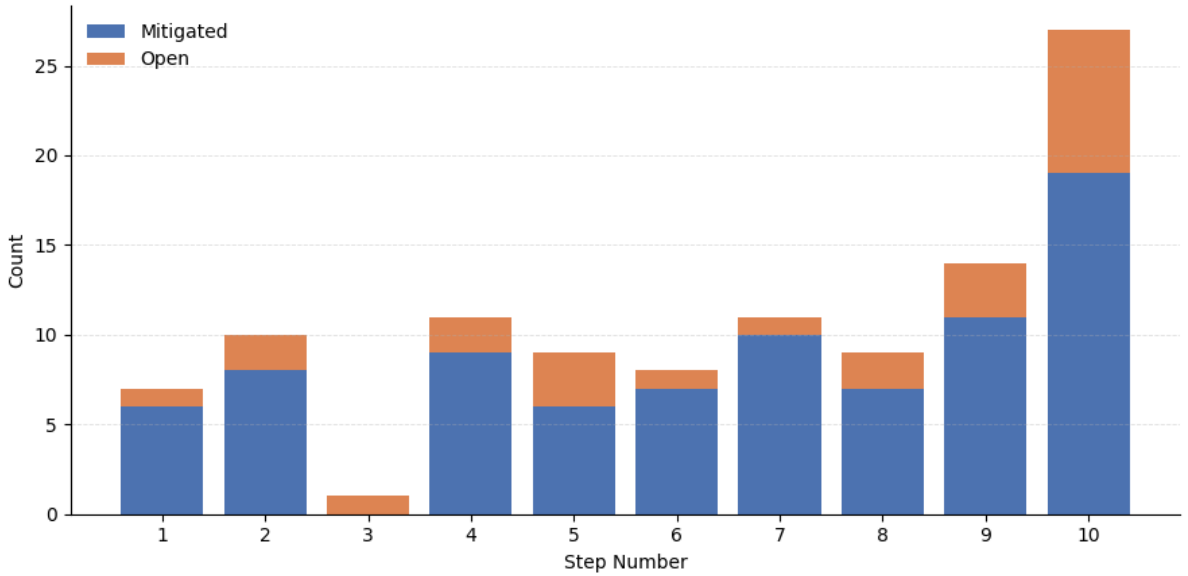
108 risks identified

24 not mitigated

References: [10]

RESULTS OF THE STRIDE ANALYSIS





SMGW WAKING-UP RISKS

- Wake-up message is an unencrypted UPD message
- Attackers may observe, record and replay structurally valid messages
- number of valid messages per minute is bound to 10

→ replayed messages can result in a denial of service by triggering the rate limit

REPUDIATION RISKS DUE TO MISSING END-TO-END ACKNOWLEDGMENTS

- MPO does not explicitly acknowledge DSO requests to initiate CLS communication
- SMGW does not confirm the receipt of wake-up messages
- Neither EMS nor SMGW confirm the successful execution of control commands

→ As SMGW are not required to have a separate mME, it is also not possible to determine from the counter values whether the control signal has been carried out or not. This offers the possibility for home owners to actively prevent the realization of control signals.

MITIGATIONS

- Risk mitigation in relation to the SMGW wake-up mechanism
  - Wake-up messages received by the SMGW must be filtered promptly and with minimal effort before computationally intensive cryptographic checks are performed

- Reducing the risk of disputes through explicit confirmations
  - To prevent disputes, explicit acknowledgements of receipt and execution must be provided for in the §14a control process
  - CLS adapters must provide execution feedback so that a clear correlation can be established between issued control commands and the observed system behavior

FUTURE WORK

- Implementation of the control chain in our Co-Simulation
- Analysis of risks in the VDE FNN Implementation Guide for Control Systems with Verification in the SMGW
- Implementation of PQC algorithms

REFERENCES

(1) European Union. Directive 2009/72/EC of the European Parliament andof the Council of 13 July 2009 concerning common rules for the internalmarket in electricity and repealing Directive 2003/54/EC. EuropeanParliament and Council of the European Union, 2009. Accessed: 2026-03-03

(2) Deutsche Energie-Agentur GmbH (dena). The introduction of smart meters in Germany: an analysis of roll-out scenarios and their regulatory implications (dena Smart Meter Study). Report 9092, Deutsche Energie-Agentur GmbH (dena), Berlin, Germany, 2014. Accessed: 2026-03-03

(3) Deutscher Bundestag. Act on Metering Point Operation and Data Communication in Smart Grids, 2023. Last amended 2025. Accessed: 2026-03-03

(4) Bundesnetzagentur. Procedure for determining the integration of controllable consumption devices and controllable grid connections pursuant to Section 14a of the Energy Industry Act (BK6-22-300). Decision of 27 November 2023, Bundesnetzagentur, Bonn, Germany, 2023. Accessed: 2026-03-22

(5) Bundesverband Wärmepumpe (BWP) e. V. Branchenstudie 2025: Development of the heat pump market in Germany. Report, Bundesverband Wärmepumpe (BWP) e. V., Berlin, Germany, 2025. Accessed: 2026-03-23

(6) Kraftfahrt-Bundesamt (KBAThe number of fully electric vehicles registered in Germany has exceeded the two-million mark for the first time. Pressemitteilung Nr. 08/2026, Kraftfahrt-Bundesamt, Flensburg, Germany, 2026. Accessed: 2026-03-23 (https://www.kba.de/DE/Presse/Pressemitteilungen/Allgemein/2026/pm08_2026_elektro_pkw.html)

(7) Enkhardt, Sandra. Half of the target for new photovoltaic capacity of 215 gigawatts by 2030 has been achieved. pv magazine Deutschland, 4 July 2025. Accessed: 2026-03-23 (https://www.pv-magazine.de/2025/07/04/haelfte-des-photovoltaik-zubauziels-von-215-gigawatt-bis-2030-erreicht/)

(8) Bundesnetzagentur. Controllable consumption devices in accordance with Section 14a of the Energy Industry Act (EnWG). Informationsportal, Bundesnetzagentur, Bonn, Germany, Accessed: 2026-03-23 (https://www.bundesnetzagentur.de/DE/Vportal/Energie/SteuerbareVBE/start.html)

(9) Bundesnetzagentur, “BK6-22-300”, 2023, Accessed: Mar. 13,2026. [Online]. Available: https://www.bundesnetzagentur.de/DE/Beschlusskammern/1_GZ/BK6- GZ/2022/BK6- 22-300/Beschluss/BK6-22-300_Beschluss_20231127.pdf.

(10) J. Britz, J. M. Behrensen, and S. Kaven, “OWASP ThreatModel”, 2026, Accessed: Mar. 13, 2026. [Online]. Available:https://github. com / SimCyberGrid / STRIDE_14a_EnWG_Control_Chain.

THANK YOU FOR YOUR ATTENTION

HAW HAMBURG