Enhancing Situational Awareness in Smart Grids through Event Correlation for ATT&CK Mapping

Sine Canbolat Kaya
Karlsruhe Institute of Technology (KIT)
Eggenstein-Leopoldshafen, Germany
sine.canbolat@kit.edu

Ghada Elbez
Karlsruhe Institute of Technology (KIT)
Eggenstein-Leopoldshafen, Germany
ghada.elbez@kit.edu

Veit Hagenmeyer
Karlsruhe Institute of Technology (KIT)
Eggenstein-Leopoldshafen, Germany
veit.hagenmeyer@kit.edu

Abstract

The increasing complexity and connectivity of Smart Grids (SGs) have made them vulnerable to cyber-physical threats, highlighting the need for improved situational awareness in the energy domain. To meet this need, we present ECAM (Event Correlation for ATT&CK Mapping), an approach that uses the Industrial Control Systems (ICS)-specific MITRE ATT&CK framework to support the correlation and interpretation of security events. We outline a workflow for implementing and testing ECAM, aimed at strengthening the security of future power grids. The approach successfully maps the conducted attacks to techniques T0814 (Denial of Service) and T0830 (Adversary-in-the-Middle), demonstrating its effectiveness in improving situational awareness. Therefore, we propose the ECAM approach along with a workflow to guide future research and advancements.

CCS Concepts

• **Security and privacy**; • **Hardware → Power and energy**;

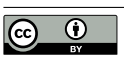
Keywords

Contextual understanding, Smart Grid (SG), MITRE ATT&CK matrix, Industrial Control Systems (ICS)

ACM Reference Format:
Sine Canbolat Kaya, Ghada Elbez, and Veit Hagenmeyer. 2025. Enhancing Situational Awareness in Smart Grids through Event Correlation for ATT&CK Mapping. In *The 16th ACM International Conference on Future and Sustainable Energy Systems (E-ENERGY '25), June 17–20, 2025, Rotterdam, Netherlands.* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3679240.3734689

1 Introduction

Modern energy systems are dynamic and interconnected systems that integrate advanced communication and control technologies to ensure a reliable, efficient and resilient energy supply. However, this complexity increases the grid vulnerability to various security concerns [1, 3]. Without security event correlation, the huge number of events from various assets can overwhelm operators, making it difficult to distinguish between benign events and threats. The work of Sen et al. [7] focuses on a subset of techniques from the MITRE ATT&CK framework, mapping the adversary's tactics, techniques and procedures to the kill-chain phases to form their multi-stage attack model. Our approach directly maps observed adversary behaviors to known MITRE Industrial Control Systems (ICS) Matrix [5], aiding in threat identification without relying on the Cyber Kill Chain. We focus on the MITRE framework, as it can be integrated into risk management. This work presents the Event Correlation for ATT&CK Mapping (ECAM) approach, which examines the effectiveness of MITRE ATT&CK-based correlation in identifying threats within Smart Grids (SGs) and highlights the benefits of integrating asset information. Key contributions include proposing a MITRE-based security event correlation approach, incorporating a dynamic asset inventory database and evaluating the approach using the available upon request dataset of Mumrez et al. [6].



E-ENERGY '25, Rotterdam, Netherlands

ACM ISBN 979-8-4007-1125-1/25/06
https://doi.org/10.1145/3679240.3734689

2 Event Correlation for ATT&CK Mapping (ECAM)

According to [4], correlation techniques are classified into similarity-based, step-based and mixed approaches. Similarity-based methods analyze event attributes, timestamps or other features of group-related alerts. Step-based methods identify sequential relationships and causality between events. Mixed methods combine elements of both, leveraging the strengths of attribute matching and scenario reconstruction. Figure 1 illustrates our workflow for security event correlation in ICS, focusing on mapping events to the MITRE ATT&CK framework. The novelty lies in demonstrating the application of security event correlation with targeted asset mapping and security requirements, which supports risk prioritization for SGs.

(1) **Test phase** generates security event data by selecting tactics and techniques of ATT&CK, creating adversary profiles, and executing realistic attack scenarios. In this study, attack scenarios are based on [6], and the corresponding ATT&CK tactics and techniques were selected manually after analyzing the executed scenarios.
(2) **Correlation phase** focuses on two processes: Preprocessing, which ensures data normalization and filtering, and contextual correlation, which links individual events to broader attack scenarios, facilitating their alignment with specific tactics and techniques. The correlation phase is designed to map events to techniques and tactics by using a combination of graph-based, scenario-based and filtering-based techniques. Graph-based correlation is performed by constructing a directed graph from the network traffic that incorporates data, such as asset details (e.g., MAC addresses, asset types), interaction protocols (e.g., ARP, TCP, ICMP), and temporal information (e.g., timestamps) to provide contextual

understanding. Next, the approach applies scenario-based correlation to map specific attack patterns. For instance, in the case of an Adversary-in-the-Middle (AiTM) attack, the system duplicate ARP packets, indicative of ARP spoofing, with subsequent ICMP Redirect packets, suggesting traffic redirection. These predefined scenarios serve as templates, enabling the system to correlate sequences of events into meaningful patterns related to malicious activity. To enhance precision, the system employs filtering-based correlation.

(3) **Evaluation phase** assesses the effectiveness of the correlation process to ensure it provides reliable and actionable insights for enhancing cyber-security in ICS environments.

Results. To evaluate the proposed approach, we use a dataset in pcapng format, along with descriptions of attack scenarios and their impact on confidentiality, integrity, or availability, from [6]. Using the information on the scenarios and affected components, these attacks were manually mapped to the corresponding MITRE techniques and targeted assets. This mapping was carried out by cross-referencing the MITRE ATT&CK ICS Matrix, focusing on the technique descriptions and the identified targeted assets. The results of the selection are presented in the *MITRE Technique* column of Table 1. In energy systems, ensuring the availability of the data is of greater importance than integrity and confidentiality [2]. The results of the correlation phase - ECAM show that the approach mapped the attack-related, *T0814 Denial of Service* and *T0830 Adversary-in-the-Middle*, events to the relevant techniques as shown in Table 1.

Adversary	MITRE Technique	Security Requirement
Motivation - Denial of Service (DoS): The attacker is assumed to cause the termination of active connections. **Attack:** TCP SYN Flooding Attack involves flooding the channel with TCP packets originating from a high volume of invalid IP addresses.	T0814 Denial of Service	Availability
Motivation - Data modification Attack: The attacker is expected to obtain Man-in-the-Middle (MITM) position, enabling them to intercept the real time flow of network traffic. **Attack:** ARP spoofing to poison the cache of the Programmable Logic Controller (PLC) and Photovoltaic (PV) model by impersonating the switch between them.	T0830 Adversary -in-the-Middle	Integrity

Table 1: Attack Scenarios mapped to the MITRE Techniques.

3 Conclusion and Outlook

We propose the Event Correlation for ATT&CK Mapping (ECAM) approach to enhance situational awareness in Smart Grids (SGs) by mapping adversary behaviors to specific techniques. The results demonstrate the relevance of structured framework for enhancing cyber-security. Future work includes evaluating false positive and negative rates, correlation performance under varying scalability, and adaptability to evolving threats. We plan to extend the attack scenarios using a threat emulation tool at the KASTEL Security Lab Energy to automate the test phase.

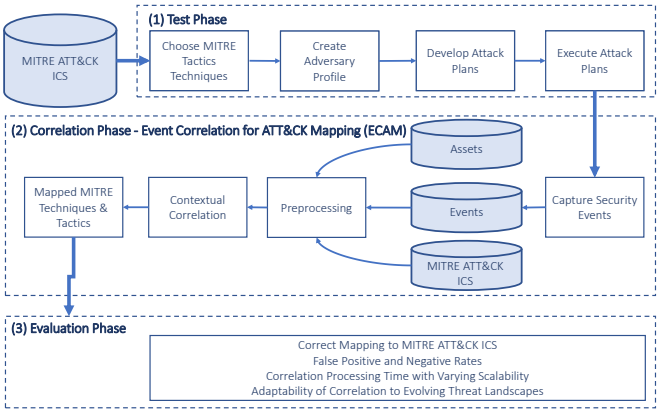


Figure 1: Workflow for implementing and testing Event Correlation for ATT&CK Mapping (ECAM)

Acknowledgments

This work was supported by funding from the topic Engineering Secure Systems of the Helmholtz Association (HGF) and by KASTEL Security Research Labs (structure 46.23.02).

References

[1] Ghada Elbez, Hubert B. Keller, and Veit Hagenmeyer. 2018. A new classification of attacks against the cyber-physical security of smart grids. In *Proceedings of the 13th International Conference on Availability, Reliability and Security*. 6 pages. https://doi.org/10.1145/3230833.3234689

[2] Ghada Elbez, Klara Nahrstedt, and Veit Hagenmeyer. 2022. Early Detection of GOOSE Denial of Service (DoS) Attacks in IEC 61850 Substations. In *2022 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids*. 367–373. https://doi.org/10.1109/SmartGridComm52983.2022.9961042

[3] Mohammad Ghiasi, Taher Niknam, Zhanle Wang, Mehran Mehrandezh, Moslem Dehghani, and Noradin Ghadimi. 2023. A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: Past, present and future. *Electric Power Systems Research* 215 (2023), 108975. https://doi.org/10.1016/j.epsr.2022.108975

[4] Igor Kotenko, Diana Gaifulina, and Igor Zelichenok. 2022. Systematic Literature Review of Security Event Correlation Methods. *IEEE Access* 10 (2022), 43387–43420. https://doi.org/10.1109/ACCESS.2022.3168976

[5] MITRE. 2025. Industrial Control Systems (ICS) Matrix. https://attack.mitre.org/matrices/ics/.

[6] Aneeqa Mumrez, Gustavo Sánchez, Ghada Elbez, and Veit Hagenmeyer. 2023. On Evasion of Machine Learning-based Intrusion Detection in Smart Grids. In *2023 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*. 1–7. https://doi.org/10.1109/SmartGridComm57358.2023.10333966

[7] Ömer Sen, Dennis van der Velde, Katharina A. Wehrmeister, Immanuel Hacker, Martin Henze, and Michael Andres. 2022. On using contextual correlation to detect multi-stage cyber attacks in smart grids. *Sustainable Energy, Grids and Networks* 32 (2022), 100821. https://doi.org/10.1016/j.segan.2022.100821