Research Article

On Process Awareness in Detecting Multi-stage Cyberattacks in Smart Grids

Ömer Sen[1,2], Yanico Aust[2,1], Simon Glomb[2], Andreas Ulbig[1,2]

1. Digital Energy, Fraunhofer Institute for Applied Information Technology, Sankt Augustin, Germany; 2. IAEW, RWTH Aachen University, Germany

This study delves into the role of process awareness in enhancing intrusion detection within Smart Grids, considering the increasing fusion of ICT in power systems and the associated emerging threats. The research harnesses a co-simulation environment, encapsulating IT, OT, and ET layers, to model multi-stage cyberattacks and evaluate machine learning-based IDS strategies. The key observation is that process-aware IDS demonstrate superior detection capabilities, especially in scenarios closely tied to operational processes, as opposed to IT-only IDS. This improvement is notable in distinguishing complex cyber threats from regular IT activities. The findings underscore the significance of further developing sophisticated IDS benchmarks and digital twin datasets in Smart Grid environments, paving the way for more resilient cybersecurity infrastructures.

Corresponding authors: Ömer Sen, oemer.sen@fit.fraunhofer.de; Andreas Ulbig, andreas.ulbig@fit.fraunhofer.de

I. Introduction

The transformation of traditional power grids into smart grids has brought significant advancements and challenges, particularly in the realm of cybersecurity due to enhanced connectivity[1]. The integration of Information and Communication Technology (ICT) components, while beneficial, has exposed these grids to cyber threats, making robust cybersecurity measures essential.

One of the primary tools in combating these threats is the use of intrusion detection systems, which have traditionally relied heavily on ICT data, potentially overlooking critical underlying processes. The development of process-aware IDSsrepresents a significant enhancement in this field, focusing on domain-specific knowledge to detect anomalies accurately within the unique operational context of SGs[2]. These systems are designed to recognize abnormal behavior patterns and cybersecurity threats effectively.

Despite advancements in IDSs, challenges remain, such as improving detection accuracy, reducing false positives, and coping with novel attack vectors. Machine learning techniques have emerged as a promising solution to enhance the capabilities of IDSs through their ability to learn and adapt to new threats[3]. However, the application of these methods still struggles with high false positive rates and unclear alert mechanisms, which complicates their deployment in critical infrastructure[4].

The need for an effective anomaly detection system is paramount, particularly one that offers high precision and clear, explainable alerts. This is crucial for reducing the effort required to process alerts and for improving the speed and accuracy of responses to potential threats.

In environments like Industrial Control Systems (ICS) and SGs, detecting anomalies in process data is critical. Techniques employed in machine learning-driven IDSs include allowlisting and blocklisting, which help identify deviations from normal operations and focus on predefined abnormal behaviors. These capabilities are essential for detecting various issues like cyberattacks, system errors, or configuration mistakes, which may manifest as protocol anomalies or communication disruptions.

This paper addresses several challenges:

- Leveraging domain knowledge inherent to electrical grid operations for detecting cyber threats and enhancing IDScapabilities.
- Integrating indicators from diverse domains such as Information Technology (IT), Operational Technology (OT), and Energy Technology (ET) to improve attack detection in SGs.
- Employing process-aware detection techniques to understand the impact of different domains on attack detection.

Our research explores the effectiveness of process-awareness in identifying complex, multi-stage cyberattacks in SGs, combining SG knowledge with traditional ICT intrusion detection methods. We utilize a detailed simulation environment that reflects all aspects of SG operations, including IT, OT, and ET components. A layered approach is employed where sensors monitor the grid for anomalies and relay information to a central system that integrates domain knowledge for enhanced process awareness. This system analyzes both ICT traffic and process data from Supervisory Control and Data Acquisition (SCADA) systems, correlating different data types to form a comprehensive understanding of potential cyber incidents.

Our contributions include investigating the effectiveness of process-aware IDSs, employing comprehensive simulation environments, and implementing a layered approach to enhance grid security through improved anomaly detection.

II. Process Awareness in IDS

In this section, we develop an understanding of IDS, elaborate on the characteristics of process awareness, and analyze machine learning-based methods for anomaly detection.

doi.org/10.32388/KDSNLM

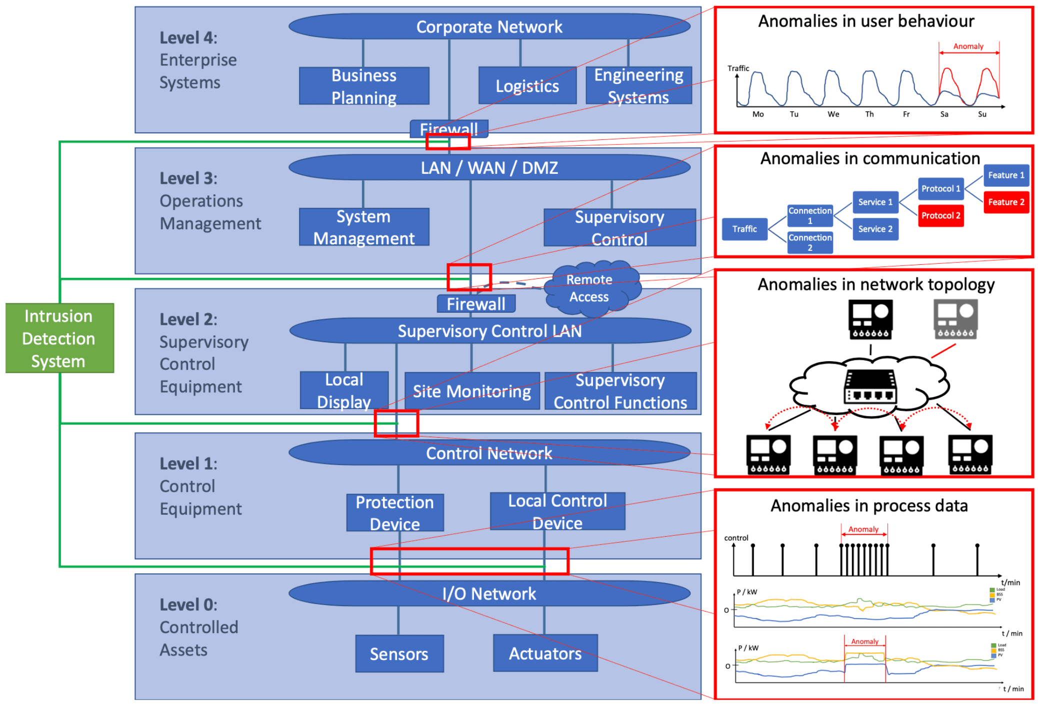

Figure 1. Illustration of IDS integration into SG industrial control architecture and anomalies in the environment

A. Intrusion Detection Systems

An IDS is designed to monitor network or system activities to detect cyber threats, such as unauthorized access or misuse, through both software and hardware solutions. IDSs are vital in ICS environments, particularly SG, due to their capability to monitor device logs, network traffic, and process data, identifying suspicious activities[5]. Host-based IDSs focus on internal device activities, while network-based IDSs analyze external network traffic. Process-aware IDSs in SG are crucial for detecting anomalies by analyzing process data, including measurements or control commands.

Machine learning methods in IDSs include allowlisting and blocklisting, which identify deviations from normal operations or recognize predefined abnormal behaviors, respectively. These methods are essential for detecting various anomalies, such as protocol errors and misconfigurations. Explainability in these systems helps in understanding the basis of alerts and maintaining system trust[6].

Machine learning in IDSs involves significant preprocessing steps like data cleaning, transformation, and reduction. Ensemble learning, particularly stacking methods, is employed to improve classification performance by combining multiple learning algorithms. These models are evaluated based on detection accuracy, runtime efficiency, and explainability, with a focus on minimizing false positives and enhancing system trust[3].

B. Process Awareness

Process-awareness in IDS utilizes domain-specific knowledge to enhance anomaly detection, particularly in SGenvironments (cf. Figure 1). This approach leverages confirmed communication patterns and network structures to detect anomalies, focusing on unknown devices, new connections, or altered communication functions. Anomalies can arise from cyberattacks or system faults, manifesting as protocol errors or delayed messages. Network-based interactions and the traffic's special information aid in detecting anomalies and assessing the legitimacy of system components.

The Purdue Model of Purdue Enterprise Reference Architecture (PERA) categorizes ICS architecture into operational (OT) and informational (IT) zones, further divided into six levels from physical hardware to enterprise network integration[7]. This framework helps in selecting datasets for benchmarking IDSs across different ICS levels, focusing on anomalies that affect both physical components and control systems.

Datasets that mirror real-world scenarios at various ICS levels are crucial for evaluating IDSs effectiveness in detecting and classifying network-based threats. This comprehensive approach ensures IDSs are tested against diverse attack types, enhancing their robustness and applicability in ICS environments.

C. Related Work

The research landscape has been actively exploring the development of benchmark environments to evaluate the performance of various machine learning algorithms in detecting anomalies and intrusions within ICS. Approaches like the Penn Machine Learning Benchmark[8] and the Scientific Machine Learning Benchmark suite[9] provide vital resources for testing and comparing algorithm performance. Researchers have also emphasized the creation of datasets from real ICS environments, such as the Cyber-kit datasets[10] and the Numenta anomaly benchmark[11], to evaluate unsupervised anomaly detection techniques or IDSs in ICS. Specific focus has been given to datasets related to SGs to assess the performance of machine learning algorithms in detecting anomalies in these systems[12][13][14]. However, there exists a need for more specialized and comprehensive approaches, particularly in considering the unique characteristics and constraints of ICS and SGs, such as explainability of algorithms and statistical confidence of findings[15][16].

In addition, research works have investigated process-aware IDSs in ICS, focusing on evaluating the criticality of ICSdevices and identifying potential adversary traces[17][18]. Advanced approaches include the replication of program states in digital twins[19], cyber-attack classification[20], and modeling ICS/SCADA communication using probabilistic automata[21][22]. Anomaly detection methods for IEC 60870-5-104 (IEC104) have also been explored using multivariate access control and outlier detection approaches[23][24][25]. However, these proposed approaches require additional analytical resources for their functionality, such as infrastructure specifications, attack target understanding, statistical data, or technical specifications[26][27][28]. Process awareness in IDShas not been systematically investigated, particularly in terms of its specific contribution to the general detection of cyberattacks and the added value it provides across different domain spaces of ICS.

This paper aims to delve into the realm of process awareness in IDS, particularly focusing on how domain knowledge from the operation of electrical grids can be leveraged to enhance these systems. A key aspect of our investigation is the identification of significant domain knowledge inherent to grid operation that could be crucial for detecting cyberattacks.

 doi.org/10.32388/KDSNLM

This includes an in-depth analysis of the plausibility of process data, a critical factor in discerning legitimate operations from potential security breaches. We also explore the integration of relevant indicators from diverse domains, specifically IT, OT, and ET. This involves identifying domain-specific attributes of the indicators with regard to detecting multi-stage cyber attacks impacting several domains in the ICS layer hierarchy.

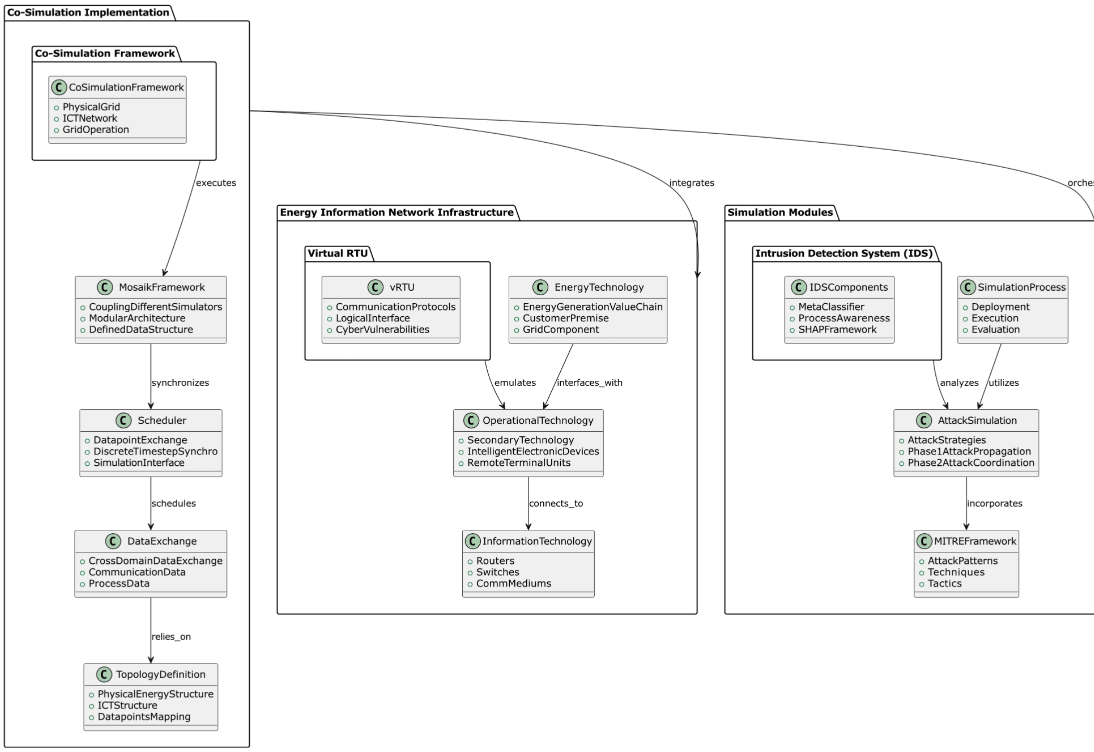

Figure 2. Overview of the class diagrams of the co-simulation for the investigation of process-aware IDS

III. Investigation Framework

This section outlines our research framework developed to investigate how process-awareness can enhance IDS, especially within SG environments.

A. Overview

The framework emphasizes the integration of domain knowledge from both IT and OT sectors, aiming to detect and differentiate cyber threats from genuine operational activities. By analyzing process data, the approach not only distinguishes between normal and anomalous activities but also considers that system faults may not always indicate cyberattacks.

It involves a detailed correlation and combination of indicators across IT and OT domains, enhancing the effectiveness and proactivity of IDS in managing grid security. The visual representation in Figure 2 highlights the dynamic interplay between energy technologies and operational technologies within a co-simulation environment. This illustration depicts

 doi.org/10.32388/KDSNLM

the complex interactions essential for realistic security investigations and the framework used to evaluate the plausibility of detected activities.

Reproducibility is critical for scientific validation and requires well-documented methodologies encompassing datasets, data preprocessing, model training, and evaluation[29][30]. This study utilizes domain-specific, balanced datasets based on the Purdue Model[7]. Preprocessing includes data cleaning, transformation, reduction, and labeling[31]. We emphasize the use of ensemble learning techniques to enhance detection accuracy and employ robust evaluation metrics like detection rate, runtime efficiency, and explainability[32][3].

B. Investigation Environment

Our work focuses on developing a comprehensive co-simulation framework for energy information networks, merging Distribution System Operator (DSO) infrastructure across ET, OT, and IT domains. The ET domain manages essential elements like switches and transformers for efficient electricity distribution, while the OT domain features Intelligent Electronic Devices connecting primary units to support crucial functions like control and measurement, primarily communicating via IEC104 protocols to the SCADA system. The IT domain handles remote maintenance and external communications, with the SCADA system playing a critical role, linking the OT network with the office network via a Demilitarized Zone (DMZ).

The simulation emphasizes a component-based, modular approach, accommodating diverse network characteristics. It is designed to provide a realistic depiction of component behaviors and communication within IT and OT domains, crucial for representing ICT failures and cyberattacks. This modular simulation supports varied investigative scenarios, enhancing the resilience of energy information networks.

The co-simulation process comprises three phases: Deployment, involving network topology setup and environment establishment; Execution, managing synchronized data transfer; and Evaluation, focusing on result analysis, especially the impact of cyberattacks.

Utilizing the Mosaik framework, our co-simulation facilitates central initialization, scheduling, and data exchange among simulators[33], supporting large-scale scenarios and integration with real-time labs and software-in-the-loop systems. The ”rettij” simulator integrates into this environment to emulate realistic ICT communication networks, using real network stacks and standard Linux tools to create complex network topologies[34].

For modeling attacks, we apply the MITRE ATT&CK Framework, which categorizes attack modalities and patterns. Our cyberattack simulation stages include Initial Access, Execution, Privilege Escalation, Credential Access, Lateral Movement, Collection, Command and Control, and Impact, each reflecting specific attack objectives and techniques.

This co-simulation framework provides a robust platform for scrutinizing and enhancing the security of energy information networks, focusing on genuine scenarios and comprehensive vulnerability evaluations.

C. Multistage Attack Implementation

The implementation of multistage cyberattacks across the main domains ET, OT, and IT is detailed in this section. These attacks are essential for a comprehensive coverage of the network infrastructure and are reused in various multistage

doi.org/10.32388/KDSNLM

scenarios due to their efficacy.

The setup includes an additional node simulating the attacker, equipped with a suite of adversarial tools, allowing for prolonged surveillance and deep insight into network operations such as Remote Terminal Units, Master Terminal Units, and switches. Initial network access is assumed, setting the stage for a series of coordinated attacks.

One of the primary techniques employed is Address Resolution Protocol (ARP) Spoofing/Poisoning. The attacker manipulates the ARP protocol to redirect legitimate IP addresses to their machine, effectively camouflaging malicious activities. This facilitates Man-in-the-Middle (MITM) attacks, where traffic between specific devices is rerouted through the attacker, enabling packet sniffing and modification.

Network connection enumeration is another critical strategy, utilizing subnet scanning and port scanning to identify and exploit vulnerabilities within the network.

Specific attacks include: (i) A Denial of Service (DoS) attack targeting the network's MTU, using a TCP 3-way handshake to disrupt service to 26 RTU, maximizing the impact on network operations. (ii) The IEC104 Value Modification attack, initiated once a MITM position is established, involves intercepting and altering IEC104 protocol traffic. This attack can be precise, targeting specific system commands to cause disruption or confusion. (iii) The Replay Attack, which captures legitimate traffic patterns between the MTU and RTUs, later replaying altered packets to simulate normal activities, thus masking the intrusion.

These simulated multistage attacks demonstrate complex strategies to exploit network vulnerabilities, emphasizing the need for robust security measures in power grids.

D. IDS Implementation

This section elaborates on the classifier used in our evaluations, employing the One-Vs-All (OVA) technique for multi-class classification[35]. Here, N binary classifiers are trained for N classes, with each classifier differentiating its class from all others. Predictions from these classifiers are integrated by a meta-classifier, which selects the most confident output, enhancing multi-stage cyberattack detection.

The meta-classifier employs a windowing technique to analyze segments of data for potential attack patterns, utilizing the softmax function to convert classifier outputs into a probability distribution. This nuanced approach allows for detecting and sequencing multi-stage attacks, essential for recognizing deviations from expected attack patterns.

Real-time capabilities are crucial for IDSs, hence a windowing mechanism is employed to analyze data within specific time frames, focusing on sequential detection of attack stages, which may include typical sequences like initial access followed by execution and persistence.

The SHAP framework is implemented to determine the impact of individual features on predictions, applied to each base classifier within our architecture[36]. This helps in understanding the decision-making process by elucidating how each classifier's outputs contribute to the final decision. If the combination process lacks transparency, SHAP can reassess the influence of each base classifier.

In our setup, data from ”unified2” files is parsed into a DataFrame, preprocessed to remove redundant columns and encode categorical data, with labels binarized for use with the meta-classifier. The analysis involves supervised, unsupervised, and mixed learning techniques to detail feature contributions using the SHAP framework, visualized through bar and beeswarm plots.

Our methodology, combining a meta-classifier with the SHAP framework, provides a robust system for real-time detection of multi-stage cyberattacks. This holistic approach ensures precise and clear threat detection, leveraging varied data inputs to enhance intrusion detection accuracy and reliability in complex environments like smart grids.

Our IDS approach utilizes an ensemble stacked meta-learner approach, where different base learners are associated with different phases of the attack, while the overarching meta-learner is responsible for determining the overall attack classification. Particularly, we associate the MITRE ATT&CK Matrix for ICS with the different base learners, where we traditionally distinguish between IT and OT related phases. Table I describes the mapping of the MITRE ATT&CK phases to the IT and OT stages.

Phase	IT Attacks	OT Attacks
Initial Access	Phishing, System exploits	Physical, Workstation exploits
Execution	Malware, Scripting	Through HMIs, Field devices
Persistence	Account, Registry keys	Firmware, Device replacement
Privilege Esc.	Exploits, Rootkits	Bypass security controls
Defense Evasion	Obfuscation, Log deletion	Logic tampering, State changes
Credential Access	Credential dumping, Sniffing	Credential compromise in controllers
Discovery	Service scanning, System discovery	Sniffing, ICS network scanning
Lateral Movement	Pass the Hash, Pivoting	Interconnected system compromise
Collection	Local and network data	Process system, Historian data
C2	Port use, Encryption	Server comms, Tunneling
Exfiltration	Compression, Scheduled transfer	Over C2 channels, Replication
Impact	Data destruction, Disruption	Process manipulation, Sabotage

Table I. Simplified MITRE ATT&CK Phases for IT and OT in ICS

To provide process-awareness, we segregated the relevant fields into their fitting categories. The structured overview of the used fields is provided in Table II, listing each indicator according to their operational significance, categorizing them into their specific domains (IT, OT, and ET), and facilitating the efficient interpretation of dissected traffic data. This structured approach leads to a comprehensive interpretation of industrial protocol traffic within a cyber-physical environment for IDS purposes. Finally, process-awareness is incorporated into the IDS with the capability of Deep Package Inspection (DPI), where fields related to IT, OT, and ET in the industrial protocol traffic are dissected and interpreted accurately. We modified our IDS, such that it would provide seven different categorical types of results by providing each possible combination from IT, OT, and ET. The IDS creates security events according to Table I and masks out only the required fields that fit in the corresponding category. Since our approach tests and evaluates all possible combinations, the best possible combination of categories is created and gives insights into the importance of process-awareness.

Field Name	Description	Category
timestamp	Event timestamp	Global
categorization	Event categorization	Global
priority	Event priority level	Global
phase	Phase in MITRE ATT&CK	Global
ttp	Tactics, techniques, procedures	Global
id	Unique event identifier	Global
IP Data	Various IP Layer protocol fields	IT
TCP Data	Various TCP Layer protocol fields	IT
rtt	Packet round-trip time	IT
frequency_general	General event frequency	IT
frequency_proto	Protocol-specific event frequency	IT
throughput	Network throughput	IT
iec104_frame	IEC 104 frame format	OT
diff_tx	TX difference between two packages	OT
diff_rx	RX difference between two packages	OT
iec104_type_id	IEC 104 type identification	OT
iec104_oa	IEC 104 origin address	OT
iec104_numix	IEC 104 number of objects	OT
iec104_coa	IEC 104 common ASDU address	OT
iec104_ioa	IEC 104 information object address	OT
iec104_cot	IEC 104 cause of transmission	OT
iec104_value_sigma	Sigma between IEC 104 IO values	OT
iec104_io_value	IEC 104 protocol IOA value	ET
iec104_control	IEC 104 control signals	ET
iec104_status	IEC 104 status notification	ET

Table II. Fields of event describing indicators

doi.org/10.32388/KDSNLM

IV. Investigation

In this section, we present our findings on the effectiveness of process-aware IDS. The investigation involves a scenario to simulate a multi-stage cyberattack, enabling a detailed analysis of detection capabilities across different network layers.

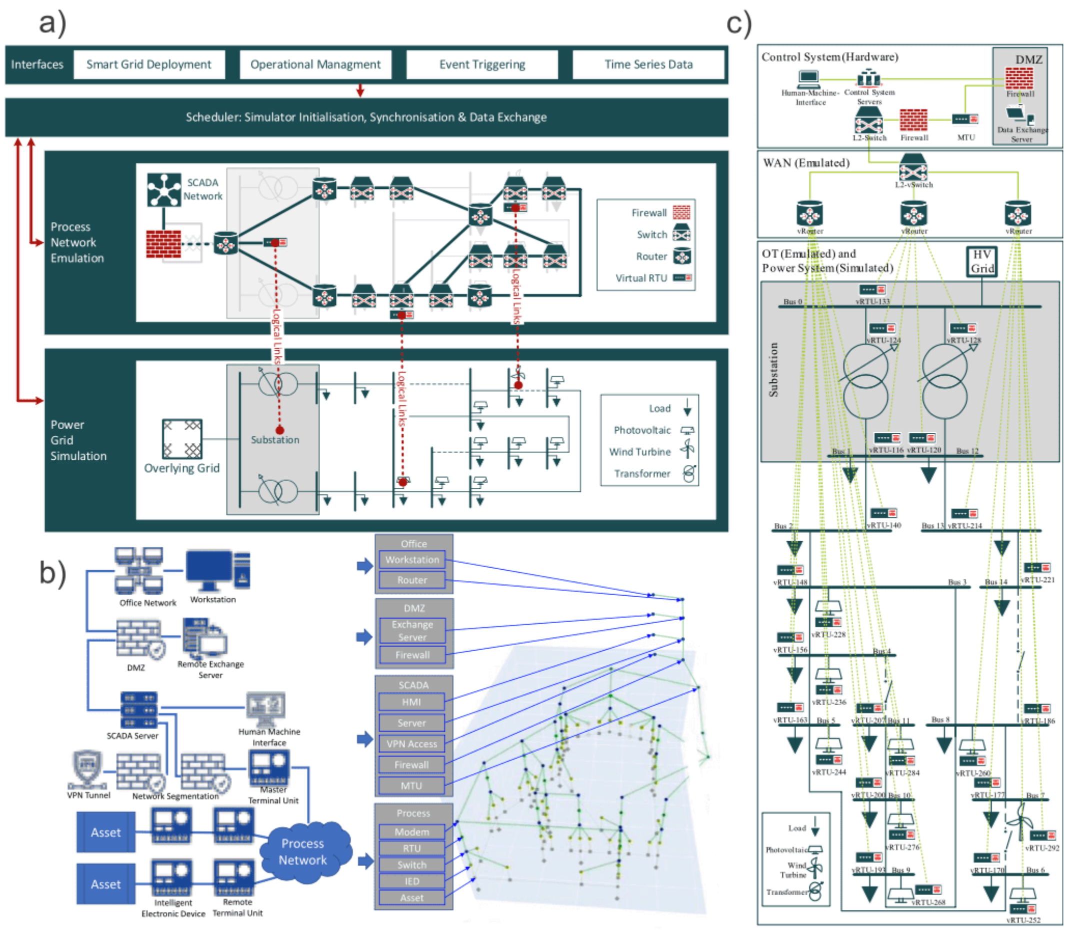

Figure 3. Overview of the cigre-based scenario simulated in the co-simulation for the study: a) the co-simulation architecture and the components involved, b) the infrastructure model of the scenario and c) the specific network model for the case

A. Scenario

In this study, we utilize the CIGRE grid model to simulate a distribution grid with integrated decentralized power generation[37] (cf. Figure 3). This scenario features an OT communication infrastructure comprising routers, switches, firewalls, SCADA systems, and RTUs, all interconnected to ensure control compliant with IEC104 standards, facilitating the simulation of power flow and communication within a smart grid framework.

Our multi-stage cyberattack employs MITRE ATT&CK recommended techniques in a sequenced manner. Initially, ARPspoofing between RTUs and an MTU establishes a MITM link, allowing packet manipulation including alteration and dropping. During the first 10% of the simulation, Transmission Control Protocol (TCP) RST flags are manipulated, followed by modifications to IEC104 transmission causes and information object values between 20% and 80% of the simulation time.

The final 20% features an SSH brute-force attack on a non-spoofed RTU, carefully executed to avoid triggering alarms. Post-attack, an IDS processes PCAP files to detect anomalies, analyzing traffic and matching specific patterns to improve accuracy. This IDS categorizes events into seven groups corresponding to IT, OT, and ET layers, each undergoing separate classification to ensure balanced representation of all attack techniques.

Additionally, the simulation can replicate normal operational scenarios where no attacks occur but ICT failures like communication link breakups are present. The IDS analysis is performed using PCAP files that record all network traffic, focusing on pattern matching and attack detection across the IT, OT, and ET layers. Each network event is categorized and analyzed for its relevance to detection, with a category classification process for balanced representation.

B. Case Studies

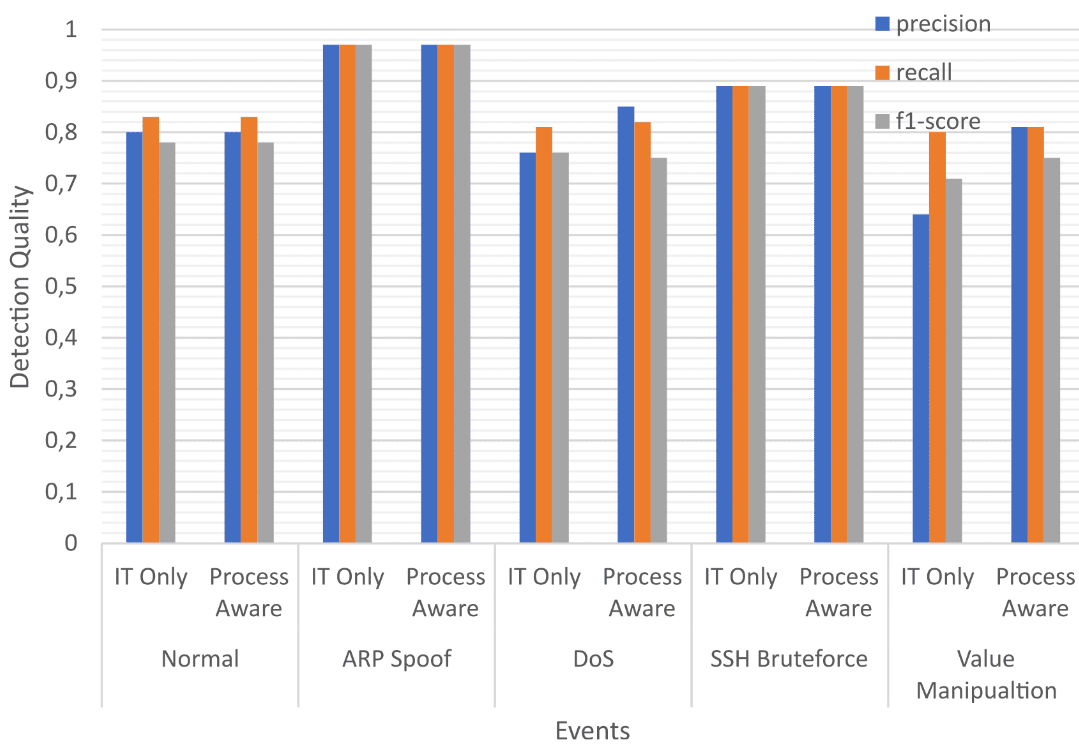

Figure 4. Comparison between the IT-only and process-aware IDS in various scenarios

doi.org/10.32388/KDSNLM

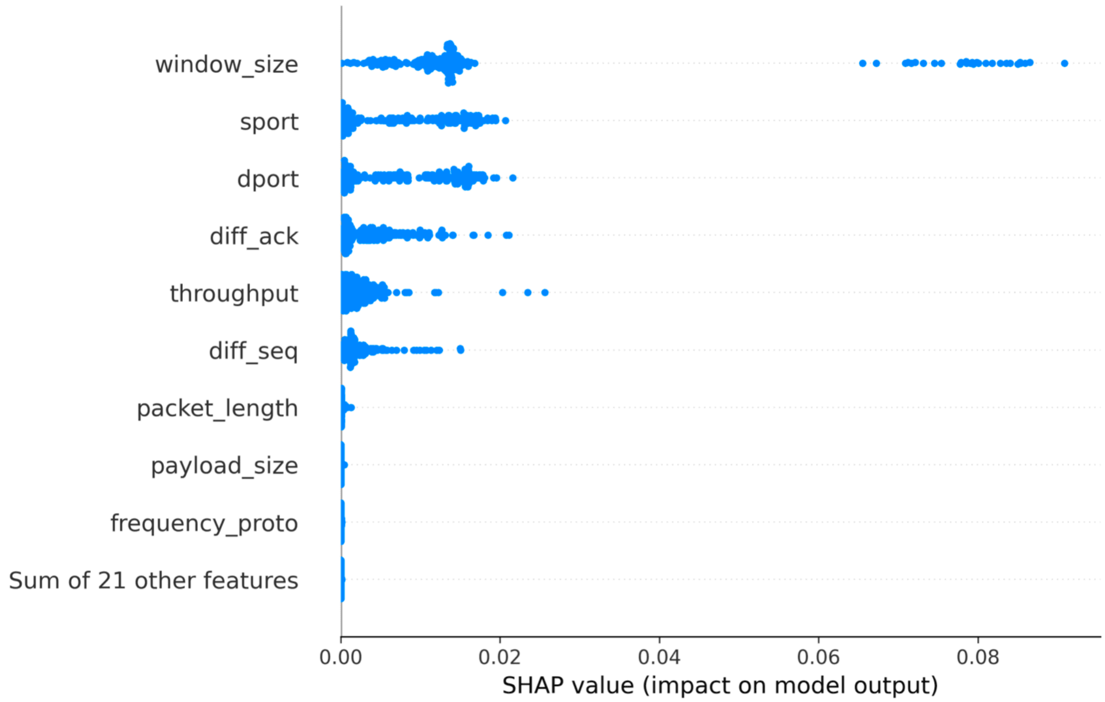

Figure 5. Feature analysis with a focus on IT layer-specific attributes, representing the DoS attack

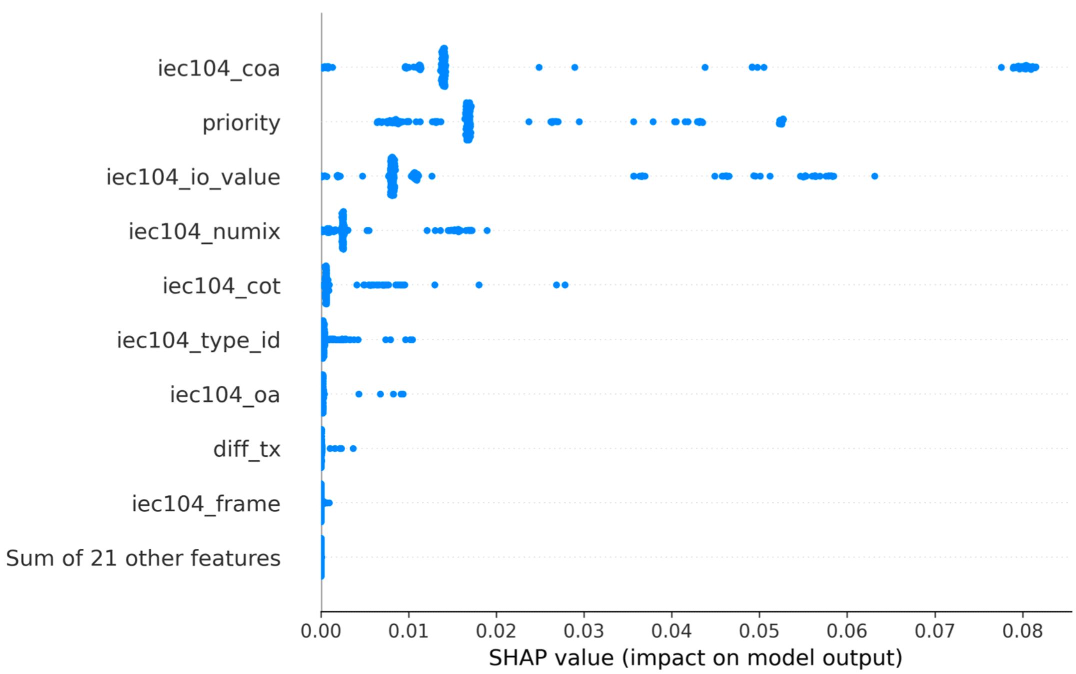

Figure 6. Feature analysis focusing on the process layer-specific attributes, specifically illustrating the DoSattack

doi.org/10.32388/KDSNLM

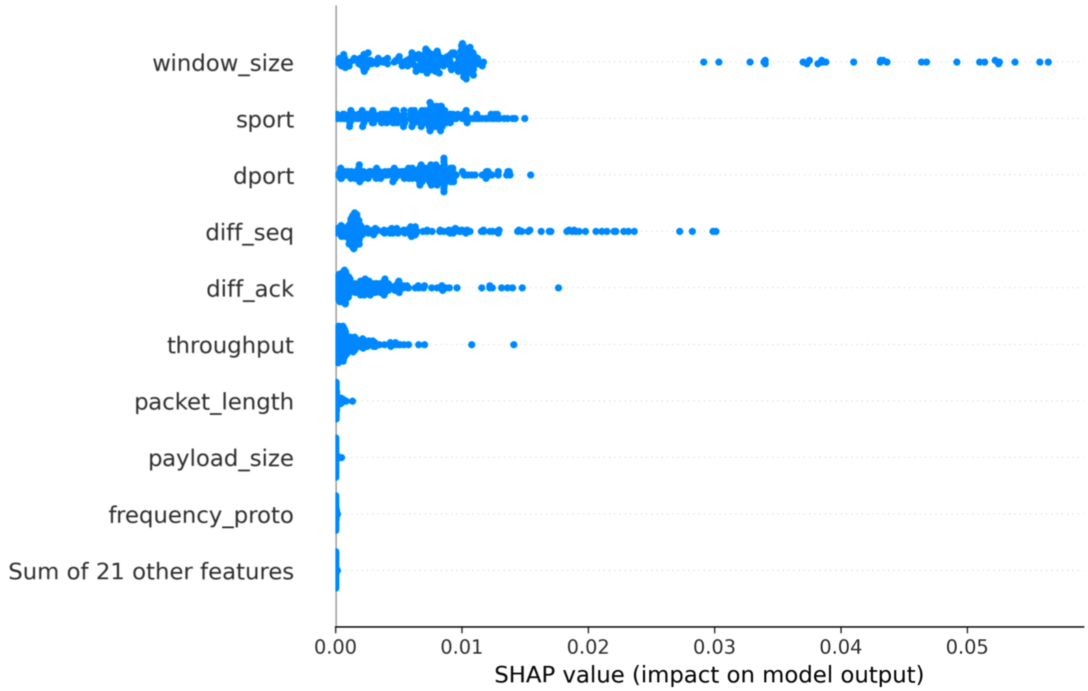

Figure 7. Feature analysis concentrating on the IT layer-specific attributes, showcasing the IEC104manipulation

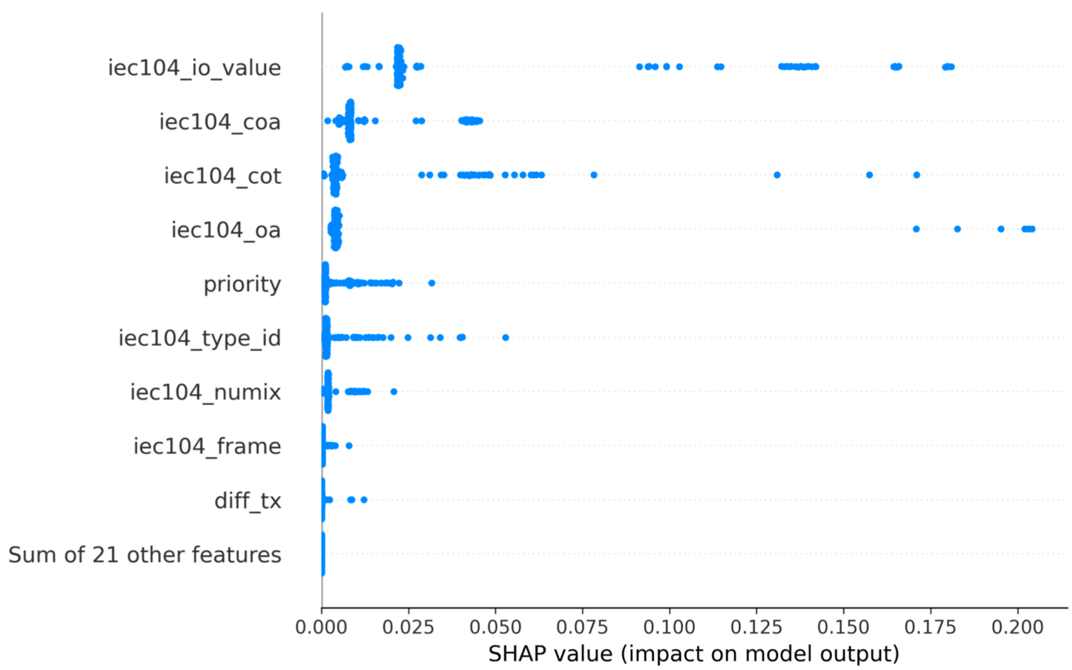

Figure 8. Feature analysis concentrating on the process layer-specific attributes, showcasing the IEC104manipulation

doi.org/10.32388/KDSNLM

In examining the significance of features in detection, we analyze both IT and process-focused events. Our focus includes multiple IT attacks (e.g. DoS) and IEC104-based manipulation attacks, to understand the impact of domain-specific knowledge on detection effectiveness. The observation within this investigation offer valuable insights into cyberattack detection across IT, OT, and ET layers.

Direct comparison of detection quality between IT-only and process-aware IDS reveals notable differences in their performance across scenarios (cf. Figure 4). While both systems perform similarly in IT-focused events, process-aware IDS significantly excels in detecting process-focused events, particularly IEC104 manipulation attacks, more accurately than IT-focused IDS.

Figure 6 depicts an attack scenario in the OT and ET layers, highlighting general and SYN DoS attacks. However, the lack of IT data renders DoS attacks undetectable in this setup. Instead, the focus is on IEC104 common object address and information object value details, inadvertently missing the real attack. Priority values are less critical here as they indicate the alert level specified by the MITRE ATT&CK framework, crucial for real-time IDS.

Contrastingly, Figure 5 presents an IT-oriented attack, including general and SYN DoS. The window size's bifurcation suggests simplicity in sent packets and limited recipient response. source ports and destination port features imply consistent host involvement, while ack and seq number variations suggest packet loss and disrupted connections in the DoS scenario. Figure 7 returns to the IT level, adding IEC104 manipulations. This demonstrates the inadequacy of window size alone for attack indication, underscoring the necessity for OT and ET specific data. Lastly, Figure 8 explores an attack across OT and ET layers, focusing on IEC104 manipulation. The impact of IO value manipulation on system control is significant, and the recurrence of similar IEC104 common addresses of ASDUs within an attack highlights their importance. The figure also indicates a correlation of IEC104 object address with value changes, often seen in attacks executed via the same spoofed line.

C. Discussion

The comparative performance analysis of IT-only and process-aware IDS demonstrates that integrating OT and ETinformation significantly enhances the detection capabilities of IDS systems. This integration allows for a more nuanced detection of complex attacks, particularly those involving subtle manipulations in control systems such as IEC104 value changes. The inclusion of process-specific data not only improves the accuracy of cyber threat detection but also aids in the understanding of attack dynamics across different network layers, as depicted in Figure 4.

Both systems exhibit comparable precision, recall, and F1-score in detecting normal activities and ARP spoofing attacks, yet differ markedly in their ability to detect DoS and value manipulation attacks. The process-aware IDS outperforms the IT-only system in these scenarios, indicating its superior capability in environments prone to sophisticated cyber threats.

Overall, the findings underscore the necessity of process awareness in IDS design, particularly in environments where the integrity and stability of control systems are paramount. The advanced capabilities of process-aware IDS in detecting and responding to cyber threats affirm their critical role in safeguarding modern cyber-physical systems.

V. Conclusion

The integration of ICT in power grids elevates both opportunities and cybersecurity risks. This paper underscores the importance of process awareness in IDS, specifically within the power grid's IT, OT, and ET layers. We developed a prototype machine learning-based IDS, evaluated through multi-stage cyberattack simulations based on the MITRE ATT&CK Matrix. The findings reveal that process-aware IDS significantly enhance detection capabilities for process-centric cyberattacks compared to IT-only IDS. While both types of IDS are effective for IT layer threats such as DoS and SSH brute-force attacks, process-aware systems demonstrate superior precision by utilizing domain-specific indicators. Future research should focus on advancing IDS benchmark environments and generating comprehensive datasets from co-simulations to better mirror individual infrastructure setups.

Acknowledgments

This work has received funding from the BMBF under project no. 03SF0694A (Beautiful).

References

1. ^ *Pan S, Morris T, Adhikari U (2015). "Developing a hybrid intrusion detection system using data mining for power systems". IEEE Transactions on Smart Grid.*
2. ^ *Shun J, Malki HA (2008). "Network intrusion detection system using neural networks." In: IEEE ICNC.*
3. a, b, c *Liu H, Lang B (2019). "Machine learning and deep learning methods for intrusion detection systems: A survey." applied sciences.*
4. ^ *Samrin R, Vasumathi D (2017). "Review on anomaly based network intrusion detection system." In: IEEE ICEECCOT.*
5. ^ *Hu J, Yu X, Qiu D, Chen HH (2009). "A simple and efficient hidden Markov model scheme for host-based anomaly intrusion detection". IEEE Network. 2009.*
6. ^ *Islam SR, Eberle W, Ghafoor SK (2020). "Towards quantification of explainability in explainable artificial intelligence methods." In: FLAIRS-32.*
7. a, b *Williams TJ (1996). "An overview of PERA and the Purdue Methodology". Architectures for Enterprise Integration. Springer.*
8. ^ *Olson RS, La Cava W, Orzechowski P, Urbanowicz RJ, Moore JH (2017). "PMLB: a large benchmark suite for machine learning evaluation and comparison." BioData mining.*
9. ^ *Thiyagalingam J, Shankar M, Fox G, Hey T (2022). "Scientific machine learning benchmarks". Nature Reviews Physics. 2022.*
10. ^ *Mubarak S, Habaebi MH, Islam MR, Khan S (2021). "ICS Cyber Attack Detection with Ensemble Machine Learning and DPI using Cyber-kit Datasets." In: IEEE ICCCE.*
11. ^ *Lavin A, Ahmad S (2015). "Evaluating real-time anomaly detection algorithms--the Numenta anomaly benchmark." In: IEEE ICMLA.*
12. ^ *Bernieri G, Conti M, Turrin F (2019). "Evaluation of machine learning algorithms for anomaly detection in industrial networks." In: IEEE M&N.*

13. ^Liyakkathali S, Furtado F, Sugumar G, Mathur A (2020). "Validating anomaly detection mechanisms in industrial control sys tems." In: Proceedings of TMCE.
14. ^Mohammadpourfard M, Weng Y, Tajdinian M (2019). "Benchmark of machine learning algorithms on capturing future distr ibution network anomalies." IET Generation, Transmission & Distribution.
15. ^Japkowicz N. "Why question machine learning evaluation methods." In: AAAI workshop on evaluation methods for machine learning; 2006.
16. ^Tufan E, Tezcan C, Acartürk C (2021). "Anomaly-based intrusion detection by machine learning: A case study on probing att acks to an institutional network". IEEE Access.
17. ^Cook A, Janicke H, Smith R, Maglaras L (2017). "The industrial control system cyber defence triage process". Computers & Se curity. Elsevier.
18. ^Escudero C, Sicard F, Zamaï É (2018). "Process-aware model based IDSs for industrial control systems cybersecurity: approac hes, limits and further research." In: ETFA. IEEE.
19. ^Eckhart M, Ekelhart A (2018). "A specification-based state replication approach for digital twins." In: CPS-SPC. 2018.
20. ^Mohan SN, Ravikumar G, Govindarasu M. Distributed intrusion detection system using semantic-based rules for SCADA in s mart grid. In: T&D. IEEE; 2020.
21. ^Matoušek P, Havlena V, Holík L (2021). "Efficient modelling of ics communication for anomaly detection using probabilistic automata." In: IM. IEEE.
22. ^Almseidin M, Piller I, Al-Kasassbeh M, Kovacs S (2019). "Fuzzy automaton as a detection mechanism for the multi-step atta ck". IJASEIT.
23. ^Grammatikis PR, Sarigiannidis P, Sarigiannidis A, Margounakis D, Tsiakalos A, Efstathopoulos G (2020). "An anomaly detec tion mechanism for IEC 60870-5-104." In: MOCAST. IEEE.
24. ^Burgetová I, Matoušek P, Ryšavý O (2021). "Anomaly Detection of ICS Communication Using Statistical Models." In: CNSM. I EEE.
25. ^Anwar M, Borg A, Lundberg L (2021). "A Comparison of Unsupervised Learning Algorithms for Intrusion Detection in IEC 10 4 SCADA Protocol." In: ICMLC. IEEE.
26. ^Scheben F, Genzmer K, Mohrdieck JM, Möller J (2017). "Status of the National Implementation of the NC RfG in Germany." I n: NEIS Conference 2016. Springer.
27. ^Dang QV (2021). "Improving the performance of the intrusion detection systems by the machine learning explainability". IS O4. Emerald Publishing Limited.
28. ^Holzinger A, Carrington A, M\uoofcller H (2020). "Measuring the quality of explanations: the system causability scale (SC S)." KI-K\uoofcnstliche Intelligenz. Springer.
29. ^Tatman R, VanderPlas J, Dane S (2018). "A practical taxonomy of reproducibility for machine learning research". openrevie w.net.
30. ^Uetz R, Hemminghaus C, Hackländer L, Schlipper P, Henze M. "Reproducible and Adaptable Log Data Generation for Sound Cybersecurity Experiments." In: ACSAC, 2021.
31. ^Davis JJ, Clark AJ (2011). "Data preprocessing for anomaly based network intrusion detection: A review." computers & securit y. Elsevier.

32. ^*Zhou ZH. Ensemble methods: foundations and algorithms. CRC press; 2012.*

33. ^*Schütte S, Scherfke S, Tröschel M. "Mosaik: A framework for modular simulation of active components in smart grids." In: SGMS. IEEE; 2011.*

34. ^*Niehaus F, Fraune B, Gritzan G, Sethmann R. "A Modern ICT Network Simulator for Co-Simulations in Smart Grid Applications." In: International Conference on Cyber Warfare and Security. Academic Conferences International Limited; 2022. p. 227-236.*

35. ^*Rifkin R, Klautau A (2004). "In defense of one-vs-all classification." The Journal of Machine Learning Research. 5: 101–141.*

36. ^*Chen H, Janizek JD, Lundberg S, Lee S-I (2020). "True to the model or true to the data?" arXiv preprint arXiv:2006.16234. arXiv:2006.16234.*

37. ^*pandapower Development Team. pandapower CIGRE Networks Documentation [Internet]. 2020 [cited 2024 Feb 2]. Available from: https://pandapower.readthedocs.io/en/v2.4.0/networks/cigre.html.*

Declarations

Funding: This work has received funding from the BMBF under project no. 03SF0694A (Beautiful).

Potential competing interests: No potential competing interests to declare.