

TESTBED AND SOFTWARE ARCHITECTURE FOR ENHANCING SECURITY IN INDUSTRIAL PRIVATE 5G NETWORKS

A PREPRINT

 **Song Son Ha**

Electrical Measurement Engineering
Helmut-Schmidt-University
Hamburg, Germany
song.ha@hsu-hh.de

 **Florian Foerster**


Institute for Innovative Safety and Security
Technical University of Applied Sciences Augsburg
Augsburg, Germany
florian.foerster@tha.de

 **Thomas Robert Doebbert**

Electrical Measurement Engineering
Helmut-Schmidt-University
Hamburg, Germany
thomas.doebbert@hsu-hh.de

Tim Kittel

ipoque GmbH
A Rohde & Schwarz company
Leipzig, Germany
tim.kittel@rohde-schwarz.com

 **Dominik Merli**

Institute for Innovative Safety and Security
Technical University of Applied Sciences Augsburg
Augsburg, Germany
florian.foerster@tha.de

Gerd Scholl

Electrical Measurement Engineering
Helmut-Schmidt-University
Hamburg, Germany
gerd.scholl@hsu-hh.de

July 28, 2025

ABSTRACT

¹ In the era of Industry 4.0, the growing need for secure and efficient communication systems has driven the development of fifth-generation (5G) networks characterized by extremely low latency, massive device connectivity and high data transfer speeds. However, the deployment of 5G networks presents significant security challenges, requiring advanced and robust solutions to counter increasingly sophisticated cyber threats. This paper proposes a testbed and software architecture to strengthen the security of Private 5G Networks, particularly in industrial communication environments.

Keywords Security, Private 5G, DPI, Machine Learning

1 Introduction

The rapid development of industrial automation, driven by the Industry 4.0 revolution, has significantly increased the need for secure and reliable communication networks. The 5G technology, characterized by ultra-low latency and high reliability, also sets a focus on data security requirements, addressing the special needs of industrial environments [1, 2]. While offering high flexibility, wide-area connectivity, and rapid deployment [2], these properties also increase the attack surface, posing risks to industrial operations, data integrity, and system availability [3]. This risk becomes particularly critical in environments with functional safety applications, where any irregularity could threaten both operational availability and human, machine, and environmental safety [4, 5]. To secure conventional networks, firewalls and traditional Intrusion Detection Systems (IDS) are commonly employed. Nevertheless, their protection is often insufficient against advanced and evolving threats [6]. In modern industrial environments such as Private 5G Networks,

¹This is the author's version of a paper that has been accepted for presentation at the 30th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA 2025), to be held in Porto, Portugal, on September 9–12, 2025.

there is a critical need to develop more sophisticated and adaptive security solutions. In this context, several publications studied the integration of Deep Packet Inspection (DPI) with Machine Learning (ML) as a promising approach for monitoring and analyzing network traffic [7, 8]. However, the effectiveness of this approach in securing industrial Private 5G Networks has still to be proven. Moreover, the limited availability of real-world network traffic datasets from industrial environments poses a significant challenge for training and evaluating ML models [9]. Therefore, it is essential to develop a testbed and software architecture that enables both the development of advanced DPI- and ML-based security solutions and the generation of high-quality, tailored industrial datasets.

This paper is structured as follows: Section 2 provides related work. Section 3 outlines the proposed architecture, while Section 4 describes its testbed implementation in detail. In Section 5, the current results of testbed experiments are presented. Finally, Section 6 concludes the paper and outlines future work.

2 Related Work

Wen et al. [10] introduce a virtual testbed (VET5G) for 5G security research using OpenAirInterface and Android emulators to simulate end-to-end networks, although their emulation-only approach limits applicability to industrial environments. Baccar et al. [11] propose a testbed for real-time 5G packet generation and injection for security evaluation with a focus on deploying attacks to facilitate fuzzing-based vulnerability detection rather than implementing an intrusion detection approach. Similarly, Almazyad et al. [12] present a 5G testbed that combines open-source software and hardware, focusing solely on simulating and analyzing cyberattacks such as DoS and database exploits. Storm et al. [13] design a test environment for evaluating existing industrial IDS solutions, but do not include a custom implementation, unlike our tailored approach.

Yang et al. [7] propose a DPI- and ML-based method for monitoring and identifying encrypted or unknown traffic. However, their work is limited to algorithm-level evaluation without deployment in realistic testbeds or relevance to industrial Private 5G Networks. Stein et al. [8] propose a transformer-based DPI algorithm for malicious traffic detection, while Bindra et al. [14] develop an IDS for OPC UA traffic focusing on DoS attacks. However, both studies rely on public datasets and lack a real-world test environment. Similarly, Jonghoon et al. [15] apply deep learning to 5G traffic intrusion detection using public datasets and evaluate their solution in a model factory, but the lack of a dataset tailored to their environment limits its specificity and suitability.

While prior studies offer valuable contributions to 5G security through testbed designs, DPI- and ML-based techniques, they typically either remain confined to simulated environments, focus solely on attack deployment, or rely on public datasets without validation of realistic industrial 5G settings. To address these gaps, our work presents an testbed and software architecture that supports the development of advanced IDS based on DPI and ML, along with the generation of customized datasets tailored to industrial Private 5G Networks.

3 Proposed Architecture

The proposed architecture, as shown in Fig. 1, consists of three main components: the IDS, the 5G Network Environment, and the Model Training Environment. The IDS utilizes advanced DPI integrated with ML models to enhance network security. DPI performs a detailed inspection of network packets, extracting essential data and traffic features, which can be leveraged by ML algorithms to accurately detect abnormal network behavior and malicious activity with high accuracy, offering more effective and adaptive protection for modern industrial communication systems. The 5G Network Environment, based on a real-world 5G Standalone Campus Network, enables seamless industrial application deployment while supporting more realistic attack simulations. It enables customizable attack scenarios and application behaviors, essential for training ML models with diverse datasets. By utilizing a real Private 5G Network instead of a simulated environment, the architecture ensures that the network traffic accurately reflects real world conditions, generating high quality and realistic datasets to enhance the accuracy and resilience of trained ML models. Meanwhile, the Model Training Environment includes advanced training servers for developing and optimizing detection models. Additionally, user-plane traffic is captured and forwarded from the Private 5G Network to the IDS via a dedicated mirror interface of the 5G core, or it can be securely transmitted unidirectionally to the Public 5G Network via a self-developed data diode [16, 17] for further analysis or monitoring purposes. The architecture also includes a Database and Data Engineering node, which processes and structures the collected traffic, and a Visualization node that provides graphical insights into the detected results.

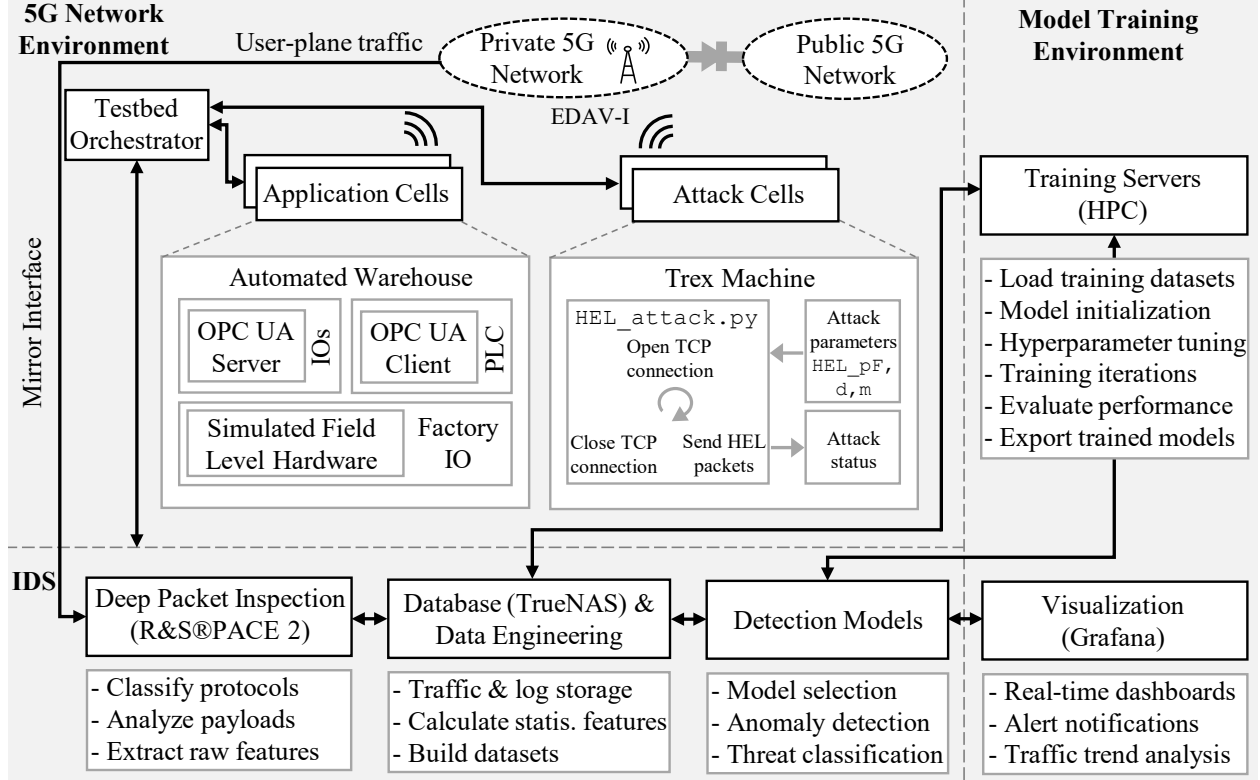


Figure 1: Overview of the proposed architecture with key functions and selected implementations

4 Testbed Implementation

This section presents the testbed designed to validate the proposed architecture in detail.

4.1 Application Cell using OPC UA Protocol

The widely adopted industrial communication protocol OPC UA is selected for initial application deployment within the testbed. The Application Cell represents an automated warehouse, where packets are loaded onto and unloaded from shelves automatically. The Factory IO application is used to simulate hardware components at the field level, while the logic control program and OPC UA instances are deployed on industrial Programmable Logic Controllers (PLCs), called Revolution Pi (RevPi). The first RevPi module is connected to Factory IO through IO modules (IOs) to collect input data from and send output commands to the simulated field level components. An OPC UA server integrated into the RevPi module acts as a gateway, ensuring data accessibility for control programs and monitoring applications. The PLC program on the second RevPi is responsible to remotely control the warehouse application through an OPC UA client connected to the OPC UA server. Two 5G HAT modems equipped with SIM8200EA-M2 multi-band modules are employed to connect the RevPi devices to the Private 5G Network, ensuring high reliability and low latency communication for the application.

4.2 Attack Cell

The Attack Cell generates attack traffic using TRex, an open source packet generator from Cisco, installed on a Dell Precision 3630 workstation equipped with an 10Gb X550-T2 network card. TRex provides high-performance traffic generation capabilities and is well-suited for simulating complex attack scenarios. Meanwhile, the 5G router Scanlance M800 connects the Attack Cell to the Private 5G Network, enabling efficient transmission of attack traffic within the testbed.

4.3 Private 5G Network

A Standalone Private 5G Network, installed by Telekom Deutschland GmbH on the campus of Helmut Schmidt University – University of the Federal Armed Forces in Hamburg, serves as the backbone of the testbed. The network is based on the EDAV-I solution developed by Ericsson, which is compliant with 3GPP Release 16 and operates in the 3.7 – 3.8 GHz frequency band [5]. The integrated mirror interface in EDAV-I captures and provides user-plane traffic with a bandwidth of up to 10 Gb/s, enabling robust and comprehensive data collection for further analysis.

4.4 IDS

The IDS is implemented on a cluster consisting of a R750xs and a R660xs Dell server, installed with the R&S@PACE 2 library to enable real time protocol classification and packet analysis up to OSI Layer 7. Additionally, an external tool has been developed and integrated into the library to extract and enrich traffic features used for training and evaluation of detection models. These processes are performed on the campus High Performance Computing (HPC) cluster [18], ensuring efficient handling of large datasets and accelerating processing. Furthermore, a Grafana dashboard is implemented to provide intuitive visualization of traffic patterns and detection results.

5 Evaluation

In this section, HEL flooding attacks that exploit the connection handshake mechanism of the OPC UA protocol are implemented as representative attack scenarios within the testbed. These attacks are carried out over untrusted, unencrypted packet streams and are based on findings from the Federal Office for Information Security (BSI) report [19] and the study by Neu et al. [20]. Statistical features calculated from network traffic generated within the testbed are also analyzed to assess their suitability for ML-based security solutions.

5.1 Attack Simulation

The attack can be executed with adjustable attack parameters: HEL packets per flow HEL_pF, flow multiplier m, and flow creation duration d, using the command `start -f HEL_attack.py -m X -d Y`. The HEL_pF parameter can be modified in the HEL_attack.py script. Upon execution, the TRex server attempts to generate X attack flows per second for Y seconds, resulting in $X \times Y$ total attack flows. Using the HEL_attack.py script, each flow follows three steps: (1) establishing a TCP connection to the OPC UA server with a unique source port, (2) sending HEL_pF HEL packets, and (3) closing the connection after transmission. The implemented attack operates in a stateful traffic context, meaning its duration may vary depending on network quality and OPC UA server processing capacity.

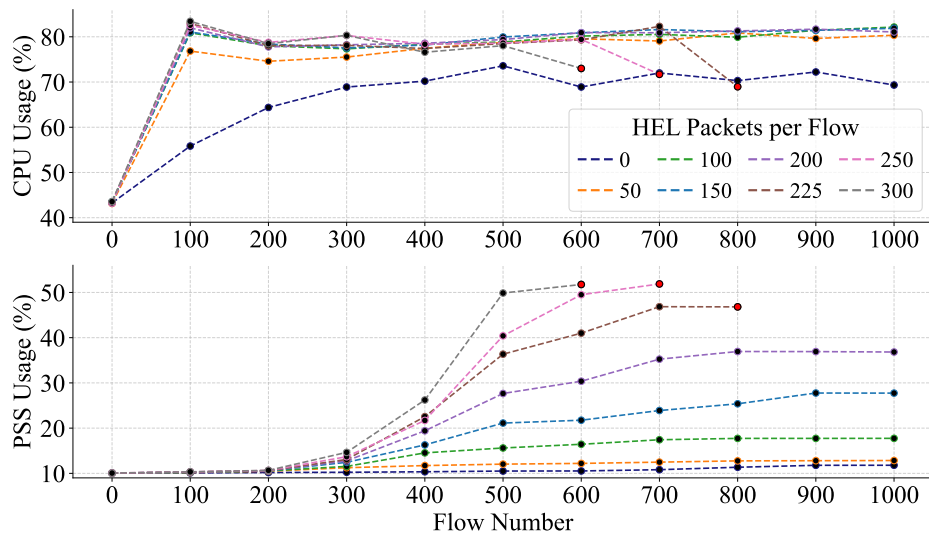


Figure 2: Impact of HEL flooding on OPC UA server resource utilization. Red points indicate termination of the server. Each data point represents the average of measurements from three independent attacks with identical attack parameters.

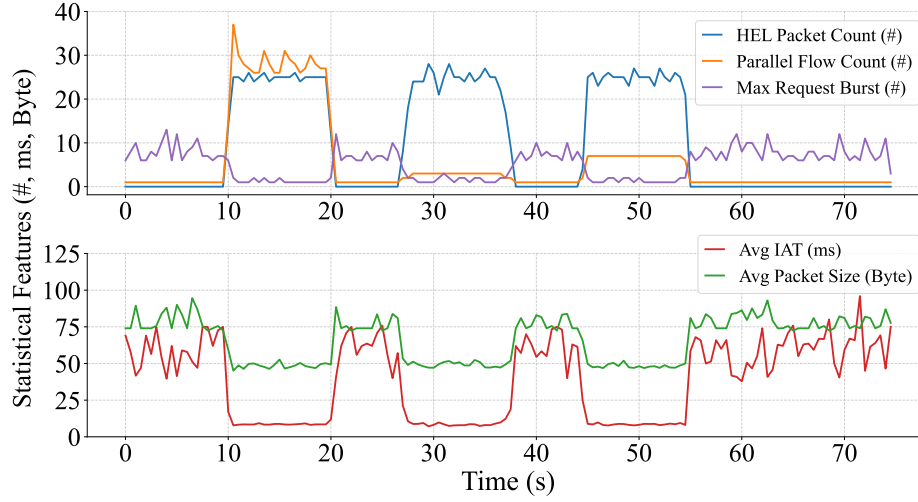


Figure 3: Statistical features were calculated in 500 ms time windows during three example DoS attacks against the OPC UA server. The first attack (≈ 9 s – ≈ 21 s) uses $\text{HEL_pF} = 1$, $m = 50$; the second (≈ 26 s – ≈ 38 s) uses $\text{HEL_pF} = 50$, $m = 1$; and the third (≈ 44 s – ≈ 55 s) uses $\text{HEL_pF} = 5$, $m = 10$.

Fig. 2 demonstrates the attack impact on OPC UA server resource utilization across varying attack parameters, with the flow creation duration d set to 1 s. CPU utilization metric represents the average CPU load, while PSS utilization metric indicates the peak Proportional Set Size (PSS) memory allocation, both measured either during the attack or about a 10 s interval, when no attack is performed (at Flow Number = 0). During each execution, measurements are taken every 200 ms within the measured intervals. As shown in Fig. 2, CPU utilization increases significantly with the flow number and stabilizes around 80%, except when no HEL packets are sent, until the OPC UA server is terminated. Meanwhile, PSS utilization rises sharply as both the flow number and HEL packets per flow increase. These results validate the testbed capability to effectively simulate the attack scenarios within an industrial Private 5G Network. They also indicate that the combination of application- and transport-layer message flooding can significantly amplify the attack impact, emphasizing the need for DPI-based security solutions to deeply inspect network traffic and effectively detect application-layer threats.

5.2 Traffic Evaluation

To further analyze network traffic characteristics, 5G traffic of the testbed is forwarded to the IDS, where packets are thoroughly inspected and statistical features reflecting flow- and packet-level behavior were calculated. Fig. 3 presents five selected features, based on insights from the study by Hindy et al. [9], Panigrahi et al. [21] and observations of OPC UA traffic, namely HEL Packet Count, Parallel Flow Count, Max Request Burst, Average Inter-Arrival Time (IAT), and Average Packet Size. These features are computed from 5G traffic under both normal conditions and simulated DoS attacks using three representative attack parameter configurations. As illustrated, the extracted features reflect clear differences in traffic behavior between normal and attack scenarios, indicating their potential to support the development of ML-based security solutions. However, some features are more effective for specific attack strategies, while others are broadly applicable but sensitive to the context. For example, Parallel Flow Count is primarily effective in detecting DoS attacks that involve many concurrent flows, while Average IAT is sensitive to sudden bursts in traffic and is potentially less reliable under stealthy attacks or in the presence of network jitter. This underscores the importance of combining multiple features to increase the robustness and reliability of ML-based anomaly detection within an industrial Private 5G Network. By leveraging flow-based data, malicious and normal traffic are accurately labeled, facilitating the creation of a high-quality dataset for training and evaluating ML models in future work.

6 Conclusions and future work

This paper presents a testbed and software architecture for enhancing security in industrial Private 5G Networks. It enables the development and evaluation of advanced DPI- and ML-based security mechanisms, while also supporting the generation of realistic traffic datasets for training and validating ML models. The implemented testbed demonstrates

the feasibility of simulating attack scenarios within an industrial Private 5G Network. The DPI module can deeply analyze network traffic, extract data from individual packets, and compute statistical features within predefined time windows. Other architectural components have also been tested, exhibiting expected operation. These results provide an initial validation of the proposed design under controlled conditions, confirming their readiness for further development.

In future work, we will scale up the OPC UA Application Cell and implement a wider range of attacks, as outlined in the BSI report [19] and the study by Neu et al. [20]. The testing process will include untrusted, unencrypted and trusted, encrypted packet streams to evaluate the OPC UA application under different security configurations. Beyond OPC UA, the testbed will be extended to incorporate additional industrial communication protocols and a diverse range of attack scenarios in industrial environments. Consequently, DPI will be applied more extensively in the next phase to support this broader testing scope. Additionally, ML model training will leverage HPC to accelerate processing, enable large dataset training and improve model accuracy. Finally, the architecture will be validated in real-world environments for robustness and effectiveness in securing industrial Private 5G Networks.

Acknowledgment

The authors would like to thank ipoque GmbH, H. Beuster, K. Tebbe, J. Jockram and F. Mueller for their valuable support.

Funding

This research is funded by dtec.bw – Digitalization and Technology Research Center of the Bundeswehr. dtec.bw is funded by the European Union – NextGenerationEU (project “Digital Sensor-2-Cloud Campus Platform” (DS2CCP), <https://dtecbw.de/home/forschung/hsu/projekt-ds2ccp>).

References

- [1] Xiongfeng Zhang, Seonjo Lim, Changdae Lee, Won Seok Song, Yu Chul Kim, Mengmeng Yu, Seung Ho Hong, Nam Hyun Yoo, and Min Wei. Integration of 5G and OPC UA for Smart Manufacturing of the Future. In *2023 IEEE/SICE International Symposium on System Integration (SII)*, pages 1–6, 2023. doi:10.1109/SII55687.2023.10039191.
- [2] Adnan Aijaz. Private 5G: The Future of Industrial Wireless. *IEEE Industrial Electronics Magazine*, 14(4): 136–145, 2020. doi:10.1109/MIE.2020.3004975.
- [3] Ashutosh Dutta and Eman Hammad. 5G Security Challenges and Opportunities: A System Approach. In *2020 IEEE 3rd 5G World Forum (5GWF)*, pages 109–114, 2020. doi:10.1109/5GWF49715.2020.9221122.
- [4] Thomas Robert Doebbert, Henry Beuster, Gerd Scholl, Florian Fischer, and Dominik Merli. Testbed for Functional Safety-Relevant Wireless Communication Based on IO-Link Wireless and 5G. In *dtec. bw-Beiträge der Helmut-Schmidt-Universität/Universität der Bundeswehr Hamburg*, pages 147–152. 2022.
- [5] Henry Beuster, Kevin Tebbe, Thomas Robert Doebbert, and Gerd Scholl. Measurements of the Safety Function Response Time on a Private 5G and IO-Link Wireless Testbed. In *2024 IEEE 29th International Conference on Emerging Technologies and Factory Automation (ETFA)*, pages 1–4, 2024. doi:10.1109/ETFA61755.2024.10710762.
- [6] Merve Ozkan-Okay, Refik Samet, Omer Aslan, and Deepti Gupta. A Comprehensive Systematic Literature Review on Intrusion Detection Systems. *IEEE Access*, 9:157727–157760, 2021. doi:10.1109/ACCESS.2021.3129336.
- [7] Bowen Yang and Dong Liu. Research on Network Traffic Identification based on Machine Learning and Deep Packet Inspection. In *2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC)*, pages 1887–1891, 2019. doi:10.1109/ITNEC.2019.8729153.
- [8] Kyle Stein, Arash Mahyari, Guillermo Francia, and Eman El-Sheikh. A Transformer-Based Framework for Payload Malware Detection and Classification. In *2024 IEEE World AI IoT Congress (AIIoT)*, pages 105–111, 2024. doi:10.1109/AIIoT61789.2024.10579000.
- [9] Hanan Hindy, Ethan Bayne, Miroslav Bures, Robert Atkinson, Christos Tachtatzis, and Xavier Bellekens. Machine Learning based IoT Intrusion Detection System: An MQTT case study (MQTT-IoT-IDS2020 dataset). In *the 12th International Networking Conference*, pages 73–84. Springer, 2020.
- [10] Zhixin Wen, Harsh Sanjay Pacherkar, and Guanhua Yan. VET5G: A Virtual End-to-End Testbed for 5G Network Security Experimentation. In *Proceedings of the 15th Workshop on Cyber Security Experimentation and Test*, pages 19–29, 2022.

- [11] Karim Baccar and Abdelkader Lahmadi. An Experimental Testbed for 5G Network Security Assessment. In *NOMS 2023-2023 IEEE/IFIP Network Operations and Management Symposium*, pages 1–6, 2023. doi:10.1109/NOMS56928.2023.10154283.
- [12] Ibrahim Almazyad, Safwan Elmadani, and Salim Hariri. A 5G and Beyond Testbed for Cybersecurity Research and Education. In *2024 IEEE/ACS 21st International Conference on Computer Systems and Applications (AICCSA)*, pages 1–6. IEEE, 2024.
- [13] Jon-Martin Storm, Siv Hilde Houmb, Pallavi Kaliyar, Laszlo Erdodi, and Janne Merete Hagen. Testing Commercial Intrusion Detection Systems for Industrial Control Systems in a Substation Hardware in the Loop Testlab. *Electronics*, 13(1):60, 2023.
- [14] Sandeep Singh Bindra and Alankrita Aggarwal. Deep Learning-based Enhanced Security in Cyber-Physical Systems: A Multi-Attack Perspective. In *2024 International Conference on Computational Intelligence and Computing Applications (ICCICA)*, volume 1, pages 347–352. IEEE, 2024.
- [15] Jonghoon Lee, Hyunjin Kim, Chulhee Park, Youngsoo Kim, and Jong-Geun Park. AI-based Network Security Enhancement for 5G Industrial Internet of Things Environments. In *2022 13th International Conference on Information and Communication Technology Convergence (ICTC)*, pages 971–975, 2022. doi:10.1109/ICTC55196.2022.9952490.
- [16] Song Son Ha, Henry Beuster, Thomas Robert Doebbert, and Gerd Scholl. An FPGA-based Unidirectional Gateway Proposal for OT-IT Network Separation to Secure Industrial Automation Systems. In *2023 IEEE 21st International Conference on Industrial Informatics (INDIN)*, pages 1–6, 2023. doi:10.1109/INDIN51400.2023.10218126.
- [17] Song Son Ha, Henry Beuster, Thomas Robert Doebbert, and Gerd Scholl. A New Approach to Secure Industrial Automation Systems Based on Revolution Pi Modules. In *2022 IEEE 27th International Conference on Emerging Technologies and Factory Automation (ETFA)*, pages 1–4, 2022. doi:10.1109/ETFA52439.2022.9921668.
- [18] HPC Portal. HPC Technical Specifications, 2024. [Online]. Available: <https://portal.hpc.hsu-hh.de/documentation/>. Accessed: Apr. 3, 2025.
- [19] BSI. OPC UA Security Analysis, 2017. [Online]. Available: <https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/OPCUA/OPCUA.html?nn=132646>. Accessed: Mar. 26, 2025.
- [20] Charles Varlei Neu, Ina Schiering, and Avelino Zorzo. Simulating and Detecting Attacks of Untrusted Clients in OPC UA Networks. In *Proceedings of the Third Central European Cybersecurity Conference (CECC)*, pages 1–6, 2019.
- [21] Ranjit Panigrahi. Cicans2017, 2025. URL <https://dx.doi.org/10.21227/akxq-9v09>. Accessed: May. 23, 2025.