AARMS Vol. 23, No. 3 (2024) 5–19.

10.32565/aarms.2024.3.1

Building an OT Security Microgrid Testbed

Gergő GYEBNÁR[1]

This paper introduces the development of an Operational Technology (OT) security microgrid testbed. The testbed is aligned with the IEC 62443 standard and structured to simulate and mitigate potential security risks within OT systems. It serves as a platform for evaluating cybersecurity strategies through test scenarios and cases, aimed at enhancing the resilience and responsiveness of OT environments to cyber threats. The work described here lays the foundational framework for subsequent research, focusing on cybersecurity measures, including MITRE ATT&CK-based methodologies and detection strategies using machine learning. This initial exploration emphasises the importance of creating a versatile, realistic testing environment to understand and address the unique security challenges faced by OT systems.

Keywords: *Operational Technology, cybersecurity, microgrid, testbed, IEC 62443, MITRE ATT&CK, security testing, feasibility study, simulation, cyber threat intelligence*

Introduction

Operational technology (OT) refers to the use of hardware and software for controlling industrial equipment, primarily interacting with the physical world. This collective term encompasses SCADA, DCS, PLC, SYS, CNC and other equipment utilised by critical infrastructures and the military.

The rise in OT security concerns is mainly attributed to IT–OT convergence. This convergence often requires accessing data from sites that were previously engineered to remain disconnected from the internet. Consequently, the cyber resilience of these control systems is notably compromised. Essentially, adversaries can achieve significantly greater impacts with minimal resource investments. Another significant concern regarding OT security is that since the emergence of Stuxnet, the development and research of OT vulnerabilities have followed an exponential trend. This applies to both exploit development and vulnerability research in the field of OT, with an increasing focus on the creation of "killware" – malware designed with the intention of potentially harming or even killing people.

[1] PhD student, Ludovika University of Public Service, Faculty of Military Sciences.

Given the unique nature of OT systems in the field of cybersecurity, it is advisable to establish a testbed to better model cybersecurity test cases. Many industries have digital twins, which are digital models of planned or actual physical products, systems, or processes that serve practical purposes such as simulation, integration, testing, monitoring and maintenance. However, in cases where a digital twin is not available, it is worthwhile to create a testbed. This paper examines this possibility and proposes building one testbed through a Microgrid project.[2]

A microgrid is a local energy system capable of generating, distributing and controlling electrical energy as a single controllable unit. When connected to the main grid, microgrids can operate in island mode or be sufficiently regulated to fulfil their tasks, thereby revolutionising energy management. Microgrids can be beneficial in industrial parks, commercial zones such as shopping centres, critical infrastructures, or even within smaller residential communities, supplying local energy needs and, if necessary, promoting the stability of the local electrical grid.[3]

The microgrid is a topic that enables the creation of a heterogeneous environment. However, to better prepare the environment for future test cases, it is advisable to examine the relevant frameworks and their recommendations. The testbed considers the NIST SP 800-82 Rev. 3, IEC 62443-4-2 and MITRE ATT&CK frameworks, considering the ICS (Industrial Control Systems) and Enterprise matrices in the latter case.[4]

The purpose of this paper is to develop a testing environment that might be suitable for emulating cybersecurity attacks, detecting them, automating the investigation of detections and automating the management of entire incident response scenarios. It is important to examine the methodology to perform the most complete and realistic simulation possible so that the attacks and their defences correspond as closely as possible to reality. The environment must be modularly developed for both the OT and IT aspects, along parameters that are currently given on both the attacking and defensive sides.

Test cases

IEC 62443-4-2

To model IEC 62443-4-2 test cases in a microgrid testbed, it is needed to create specific test scenarios that address the key security requirements outlined by the standard. Given the criteria and the detailed security measures within each category, below is a structured approach to modelling test cases for a microgrid testbed:

- CR: Component requirement which is common to all types of components
- SAR: Software application requirement
- EDR: Embedded device requirement
- HDR: Host device requirement
- NDR: Network device requirement

[2] Hexagon AB 2024.
[3] Szabó 2022.
[4] MITRE ATT&CK 2024.

Identification and authentication control

One of the fundamental aspects of securing any cyber–physical system is the assurance that each human and/or system user is uniquely identified and authenticated with multi-factor where it is possible. In this context, a test scenario and case focusing on the user identification and authentication process as prescribed by IEC62443 standards are presented.[5]

- *Test scenario: Validate unique identification and authentication for creating user accounts (CR) using a registration process*
  The establishment of a mechanism for user identification and authentication is essential to ensure that each user accessing the microgrid system is properly authorised. This test scenario is designed to validate the process of creating user accounts, involving a registration process that must guarantee the uniqueness and security of user identifiers.
- *Test case: Simulate user account creation (e.g. "Create Account, T1136") and verify the uniqueness of user identifiers*
  In this corresponding test case, the process of user account creation is simulated. The key objective is the verification of the uniqueness and security of the user identifiers assigned during the registration process. Through this, it is aimed to demonstrate the efficacy of the system's ability to prevent unauthorised access and ensure that each account is uniquely linked to an authorised user.
- *Test scenario: Implement multi-factor authentication for accessing microgrid services*
  In this scenario, multi-factor authentication is mandated for all human users attempting to access the system, ensuring that multiple pieces of evidence are provided before access is granted.
- *Test case: Conduct simulated login attempts with multi-factor authentication requirements (e.g. "Multi-Factor Authentication Interception, T1111")*
  In this test case, simulated login attempts incorporating multi-factor authentication requirements are conducted. The primary objective is to assess the multi-factor authentication system in preventing unauthorised access.
- *Test scenario: Ensure unique identification and authentication for software processes and devices (EDR)*
  This test scenario is crafted to ensure that all software and devices interacting with the microgrid system are uniquely identified and authenticated, thereby safeguarding the integrity and confidentiality of the microgrid operations.
- *Test case: Validate the identification and authentication process for microgrid software and embedded devices*
  In this corresponding test case, the identification and authentication process for microgrid software and embedded devices is validated. The focus is on verifying the uniqueness and security of the identifiers assigned to each component involved in the system. The process is designed to demonstrate the system's capability to identify and authenticate nearly all software processes and devices accurately, thereby preventing any unauthorised or malicious activities within the microgrid system.

[5] International Society of Automation 2024.

Use control

Other aspects of securing in any cyber–physical system is ensuring that both authorisation enforcement and the recording of auditable events are rigorously applied according to predefined security policies. This involves not only verifying that each user's activities and access rights align with their designated roles – using mechanisms such as supervisor overrides and dual approval processes where necessary – but also ensuring that all significant actions within the system are traceable and verifiable through meticulous recording and storage of auditable events. This enhances the ability to perform thorough security audits and maintain accountability. In this context, test scenarios and cases focusing on both authorisation enforcement and the management of auditable events, as prescribed by IEC62443 standards, are presented.

- *Test scenario: Test authorisation enforcement by mapping user permissions to specific roles (CR)*
  In this scenario, the permissions are mapped to specific roles to ensure that each user is granted access according to their role's privileges. This methodical mapping is crucial to maintaining operational integrity and compliance with security policies.
- *Test case: Validate supervisor override and dual approval functionalities within the microgrid system*
  During the test case, the functionalities of supervisor override and dual approval within the microgrid system are validated. The objectives are to confirm that the supervisor override can effectively alter control settings during critical situations.
- *Test scenario: Ensure auditable events are logged and stored within the microgrid environment (SAR)*
  The logging and storage of auditable events within the microgrid environment are crucial for tracking and reviewing activities to ensure security and to be able to run further queries to define alerts and investigations and compliance. This scenario is designed to ensure that all significant actions and decisions are recorded, providing a trail that can be audited to detect any unauthorised or inappropriate activities.
- *Test case: Generate auditable events and verify proper storage capacity and response to audit processing failures*
  In this test case, auditable events are generated, and it is verified whether they are properly stored with adequate capacity and whether the system correctly responds to audit processing failures. The aim is to evaluate the system's ability to record and maintain an accurate and comprehensive log of all auditable events, ensuring that data integrity and availability are upheld in case of system audits.

System integrity

Maintaining system integrity is crucial in securing cyber–physical systems, therefore, the testbed as well. This encompasses ensuring the integrity of both communications and the software and information they carry.

- *Test scenario: Authenticate communication channels (HDR)*
  In this scenario, communication channels are authenticated to ensure that data transmitted across them is intact and secure from unauthorised access. Authenticating these channels is vital to maintaining the overall security of the infrastructures, protecting it against potential intrusions and data breaches.
- *Test case: Generate a malicious network traffic injection, conduct communication integrity tests to detect and/or prevent*
  Here, a simulated scenario involving the injection of malicious PCAP into the system is used to test the security of the communication integrity measures. The test aims to challenge the implementation of authentication and detection or prevention mechanisms of the communication security protocols.
- *Test scenario: Validate software and information authenticity (CR)*
  This scenario involves validating the authenticity of software and information within the system through automated integrity checks. It ensures that the software and data have not been tampered with and remain reliable and accurate for operational needs.
- *Test case: Implement automated notification mechanisms for integrity violations during normal operations*
  The corresponding test case focuses on the implementation of automated notification mechanisms that alert operators to any integrity violations. This proactive approach is designed to quickly address and mitigate any issues that arise, thereby maintaining the operational integrity of the microgrid.

Data confidentiality

Preserving data confidentiality is a paramount concern in cyber–physical systems, where sensitive information must be safeguarded against unauthorised access.

- *Test scenario: Test the erasure and verification of shared storage resources (EDR)*
  This scenario addresses the challenge of maintaining information confidentiality by focusing on the erasure and verification of shared storage resources. The aim is to ensure that once data is no longer needed or when it is imperative to prevent unauthorised access, it can be securely and effectively erased, leaving no remnants that could be exploited.
- *Test case: Execute data erasure procedures and verify successful and secure erasure of sensitive information*
  In this test case, data erasure procedures are executed to demonstrate the system's ability to remove sensitive information securely and completely from shared storage resources. The process includes verification steps to ensure that the data is irrecoverable, thereby upholding the strict confidentiality requirements necessary for the integrity and security of the microgrid operations.

Restricted data flow

Effectively managing the flow of information within systems is critical for enhancing security and operational efficiency. Network segmentation plays a one of the core roles in this by isolating various components and restricting data flow between them.

- *Test scenario: Evaluate network segmentation (NDR)*
  This scenario focuses on evaluating network segmentation within the microgrid to ensure that data flows are properly restricted according to security policies. The aim is to prevent unauthorised access and mitigate potential cyber threats by dividing the network into distinct segments that operate independently.
- *Test case: Test zone boundary protection mechanisms to deny all, permit by exception, or operate in island mode when necessary*
  In this test case, the effectiveness of zone boundary protection mechanisms is tested. These mechanisms are designed to "deny all" access by default, "permit by exception" based on predefined security criteria or allow components to "operate in island mode" when isolation is necessary for security or operational reasons. The test evaluates how well these mechanisms enforce the segmentation policies and protect sensitive areas from unauthorised access or data breaches.

Timely response to events

The capability to respond promptly to security incidents will be the most examined test case in the future of this lab environment. This involves ensuring that audit logs are accessible and secure and queried by certain risk tolerance thresholds, providing the necessary data to analyse and respond to events effectively.

- *Test scenario: Access to audit logs (SAR) and continuous monitoring capabilities*
  This scenario aims to guarantee that audit logs are not only accessible, but also monitored continuously. Ensuring programmatic access allows for automated systems to analyse log data efficiently, facilitating quick detection of anomalies and security incidents. Continuous monitoring ensures that these systems are always aware of the current state of the microgrid, ready to respond at any moment.
- *Test case: Validate the accessibility and security of audit logs during and after simulated events*
  In this test case, the accessibility and security of the audit logs are validated during and after simulated security events. The test involves generating events and then verifying that the logs can be accessed and analysed to understand what occurred.

Resource availability

Ensuring the availability of resources is fundamental for maintaining the operational continuity and *safety,* especially under adverse conditions such as cyberattacks. Denial of Service (DoS) protection is a critical aspect of safeguarding these systems against disruptions that could compromise their functionality.

- *Test scenario: Manage communication load (NDR) to protect against Denial-of-Service attacks on microgrid components*
  This scenario focuses on managing the communication load across microgrid components to protect against potential Denial-of-Service attacks. The goal is to prevent such attacks from overwhelming the system, which can disrupt operations and reduce the availability of critical resources.
- *Test case: Test resource management and emergency power systems to ensure continuous availability during critical operations*
  In this test case, the robustness of resource management is tested to ensure they provide continuous availability and functionality during critical operations. The test evaluates the systems' ability to handle increased loads and maintain operational stability, even under potential DoS attack conditions. It ensures that essential services and components remain functional, demonstrating the system's resilience and reliability.[6]

Through these exemplary test cases, compliance with IEC62443 standards can be assessed, and areas needing enhancement may be identified to strengthen the overall security posture of the microgrid testbed.

MITRE ATT&CK

The value of threat intelligence lies in its capacity to thwart cyberattacks through effective countermeasures. An illuminating framework for understanding this concept is David Bianco's Pyramid of Pain.[7]

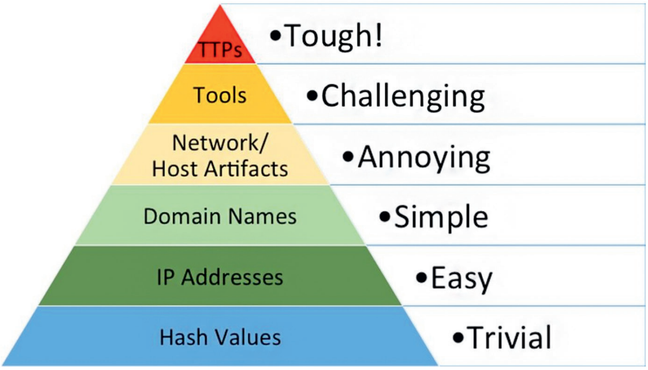

Figure 1: David J. Bianco's Pyramid of Pain
Source: AttackIQ Enterprise 2022

[6] Fritsch 2021.
[7] AttackIQ Enterprise 2022.

This model illustrates how various indicators used to detect adversary activities correlate with the level of difficulty or "pain" it inflicts upon them when those indicators are rendered ineffective. By detecting and mitigating Tactics, Techniques and Procedures (TTPs), we address the entirety of adversary behaviours rather than just their tools. This holistic approach maximises effectiveness, as it compels adversaries to expend considerable effort adapting to new strategies. Consequently, timely prevention or response to adversary TTPs compels them to undertake the most arduous task: acquiring new skills. By amalgamating the outcomes of this evaluation with an analysis of sector specific TTPs, actionable insights emerge, guiding efforts towards areas where they can inflict the greatest obstacles for potential attackers.[8]

Hence, establishing TTP-driven test cases as robust constants within security operations is imperative. Exemplary blueprints for both Operational Technology (OT) and Enterprise realms can be formulated and validated within the microgrid framework available at: https://github.com/blackcellltd/Heatmaps

In military jargon, a heatmap can be interpreted as an RCP (Recognized Cyber Picture), which requires specialised threat intelligence.

By structuring test scenarios and corresponding test cases based on the specific IEC 62443-4-2, and MITRE ATT&CK security criteria and requirement categories, there is an opportunity to effectively model and evaluate the security posture of a microgrid testbed. These test cases should be executed in a controlled environment that mirrors real-world microgrid operations to accurately assess security controls and identify potential vulnerabilities or weaknesses. Continuously refine and iterate on test scenarios based on test results to enhance the overall security of the microgrid infrastructure.

Architecture and design

Printed circuit board (PCB)

One central component and visualisation element of a microgrid is the printed circuit board (PCB), on top of which the components are applied using a screen-printing technique. Essentially, there are three input units: the grid supply, the wind turbine and the solar panel. Each is connected to a main switch, a power unit and a power meter. The three sources charge the central battery unit, which supplies electricity to the lighting of two barracks, illustrated with two conventional bulbs to represent understandable consumption.

[8] Black Cell Ltd. 2023.

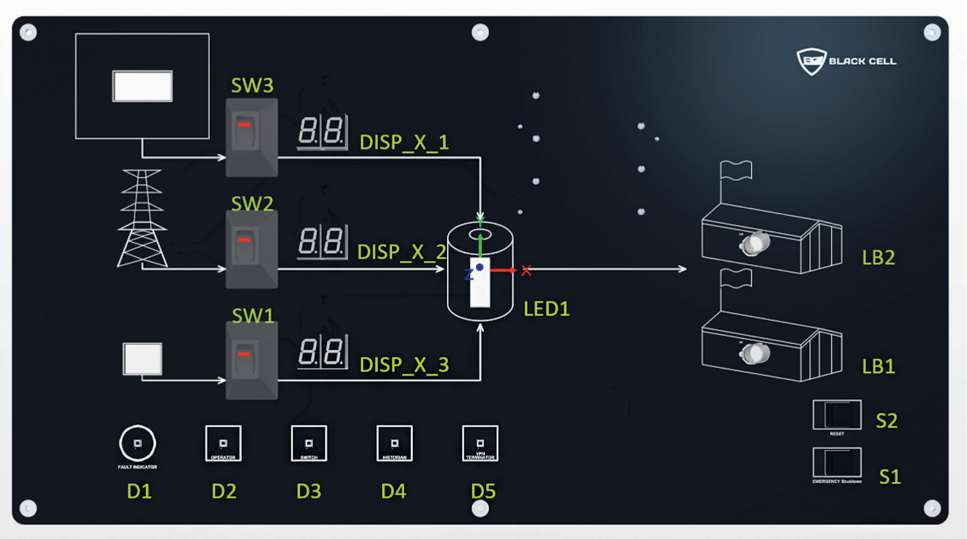

Figure 2: Printed circuit board by Gergo Gyebnar
Source: compiled by the author

IED

A microcontroller at the heart of a microgrid's power unit plays a pivotal role in orchestrating the charging process and overall energy management. It is an Intelligent Electronic Device (IED) as defined by the IEC 62443 standard, which focuses on the security for industrial automation and control systems. This microcontroller is equipped with software designed to manage inputs from diverse energy sources, such as solar panels, wind turbines and grid supplies, ensuring optimal charging of the central battery unit.

As an IED, the microcontroller performs real-time monitoring and control of the power flow, dynamically adjusting to changes in energy production and consumption. It integrates various functions such as data acquisition, automatic control and communication with other IEDs in the network to ensure seamless operation and efficiency. By leveraging advanced algorithms, it can predict energy needs, manage storage and even perform tasks like demand response and load balancing.

In compliance with IEC 62443, this microcontroller incorporates robust security features to protect against cyber threats. These features include secure communication protocols, authentication and authorisation mechanisms, and regular security updates to safeguard the microgrid's operations. This ensures that the microgrid not only operates efficiently but also securely, preventing unauthorised access and ensuring the integrity and availability of the power supply.

Through its advanced capabilities and adherence to international security standards, the microcontroller epitomises the evolution of power management systems into smart, autonomous and secure components of the modern energy landscape.[9]

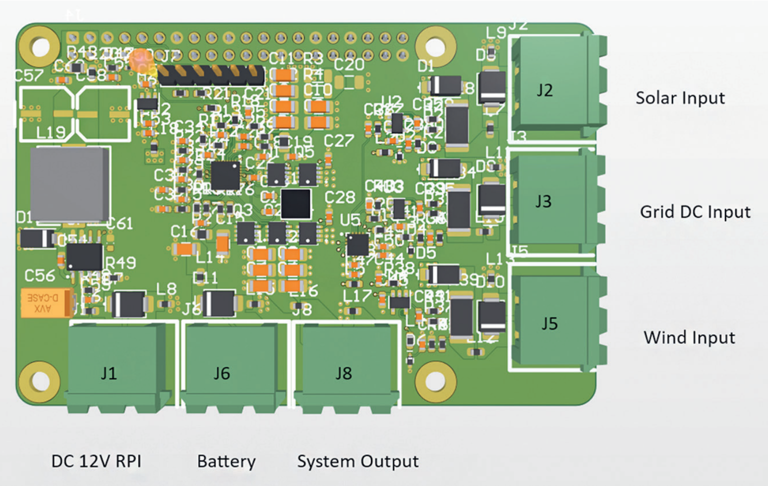

Figure 3: Raspberry Pi based microcontroller (IED) by Gergo Gyebnar
Source: compiled by the author

PLC

The Click Programmable Logic Controller (PLC), equipped with both digital and analogue cards, serves as a versatile and efficient component in a microgrid testbed environment. Its primary function is to provide reliable control and automation of the microgrid's operations, enabling the integration and management of various energy sources, storage solutions and load demands. With its ability to handle both digital (on/off) signals and analogue (variable) signals, the Click PLC can monitor and control a wide range of devices and parameters, from simple switches to complex sensors measuring voltage, current, or temperature.[10]

Integration into microgrid testbed

In a microgrid testbed, the Click PLC can perform several critical functions:

- Energy management: By analysing inputs from solar panels, wind turbines and grid connections, the PLC can optimise the charging of battery storage units and manage the distribution of power to meet the demands efficiently.

[9] Nabidoust 2024.
[10] Crestani Tasca et al. 2020: 21–22.

- Load control: The PLC can prioritise and control various loads within the microgrid, implementing strategies like load shedding or demand response to maintain stability and efficiency.
- Interfacing with IEDs: As part of a broader network of Intelligent Electronic Devices, the Click PLC can communicate and coordinate actions, enhancing the microgrid's resilience and adaptability.
- Data acquisition and monitoring: Collecting data from both digital and analogue sources, the PLC provides valuable insights into the performance and health of the microgrid, enabling predictive maintenance and system optimisation.

IEC 62443 test case opportunities

The incorporation of IEC 62443 standards into the operation of the Click PLC within a microgrid testbed offers numerous opportunities for enhancing security and reliability:

- Security by design: Implementing IEC 62443 from the design phase ensures that the PLC is equipped with necessary cybersecurity measures, such as secure authentication, encrypted communications and access control.
- Anomaly detection: Through continuous monitoring of network traffic and device behaviour, the PLC can help identify potential security threats or anomalies, enabling proactive responses to mitigate risks.
- Resilience testing: Leveraging the IEC 62443 framework, the microgrid testbed can simulate cyberattack scenarios to test the resilience of the PLC and the microgrid's response mechanisms, ensuring that operations can be maintained even under adverse conditions.

Historian

An integrated SQL Server acting as a Historian Server in a microgrid setup plays a crucial role in data management, analysis. This specialised database system is designed to efficiently collect, store and retrieve vast amounts of time-series data generated by the microgrid's various components, including energy production units (like solar panels and wind turbines), consumption data and operational logs from devices like the Click PLC.

Functionality in a microgrid

In the context of a microgrid, the SQL Historian Server's primary functions include:

- Data aggregation and storage: It collects and archives real-time and historical data on energy generation, usage, system performance and events across the microgrid. This data is vital for operational analysis, optimisation and regulatory compliance.
- Trend analysis and reporting: By analysing historical data, the server can identify patterns, predict future energy needs and optimise the balance between energy

supply and demand. It supports decision-making processes related to energy trading, maintenance scheduling and infrastructure investment.

- Performance monitoring: The server monitors the health and efficiency of the microgrid, providing alerts for anomalies or failures. This enables predictive maintenance, reducing downtime and extending the life of equipment.

Other components

Linux web server: Acts as the backbone for data management and user interface, hosting applications that collect, process and display data from across the microgrid. It facilitates remote monitoring, control and optimisation of the testbed operations.[11]

- Operator workstation: The central hub for human operators, equipped with software tools for system monitoring, data analysis and decision-making. It is where strategies are formulated and deployed, leveraging data served by the Linux web server.
- Switch: Manages data flow within the microgrid network, ensuring that communications between devices, sensors and the control systems are efficiently routed. It supports the segmentation of networks for better performance and security.
- Firewall: Protects the microgrid's digital infrastructure from external threats and unauthorised access, ensuring that only legitimate communication and control commands pass through to the microgrid components.[12]
- Human Machine Interface (HMI): Provides a graphical interface for real-time interaction with the microgrid systems, offering a visual overview of operations, alarm status and control options for quick adjustments and interventions.
- Load simulator: LED: Simulates electrical loads within the microgrid to test how well the system can manage and distribute power under various demand scenarios. LEDs represent energy consumption patterns, helping to analyse the efficiency of power distribution.
- Emergency shutdown button: A critical safety feature allowing immediate cessation of all microgrid operations in case of an emergency, helping to prevent damage to equipment or hazards to personnel.
- Reset button: Enables the quick restoration of system operations following tests, faults, or after emergency shutdowns, ensuring the microgrid testbed is readily brought back to its operational state.
- Fault indicators: Visual or auditory signals that alert operators to system abnormalities or failures, facilitating rapid diagnosis and troubleshooting of issues within the microgrid.
- Power supply: Provides stable and reliable electrical power to the testbed components, ensuring that all devices and systems are operational for testing and simulation purposes.

[11] Thompson 2024.

[12] GnosisX 2023.

- Battery: Acts as energy storage within the microgrid, simulating how real-world systems store excess energy for later use, contributing to the efficiency and resilience of the grid.
- Renewable energy source simulator: Comprising Solar Panel and Air Turbine simulators, these components mimic the behaviour of actual renewable energy sources, allowing the testbed to evaluate how well the microgrid integrates and utilises renewable energies in various conditions.

Conclusion

In conclusion, this paper presents the development of an Operational Technology (OT) security microgrid testbed, interpreted as a feasibility study. This testbed is structured around the IEC 62443 standard through the opportunity for testing of tailored use cases of the OT environment's specific vulnerabilities and threat landscape but fit for the purpose for MITRE ATT&CK based research and development. The testbed offers an approach to identifying, analysing and mitigating potential security risks,[13] and provides the ability for essential security prerequisites for in-depth research into specialised security strategies. By integrating defined technical test cases, the resilience and responsiveness of the proposed systems against cyber threats could be effectively evaluated.

This paper is the first part of a series that forms the foundation of my research. Its purpose was to present, as a kind of feasibility study, how to build an OT testbed for defining cybersecurity test cases. Subsequent parts of the series will focus on presenting and analysing the military recognised cyber picture (RCP). This part will centre on the military interpretation and adoptability of the MITRE ATT&CK, utilising Cyber Threat Intelligence and SIEM. The latter is related to designing, automating and incorporating Detection as code within an Elastic stack.[14]

Due to the characteristics of OT systems' cybersecurity, it is necessary to deal with mirrored traffic, where a network IDS (Intrusion Detection System, Suricata) and the Zeek network querying language will play a central role. The latter is essential for interpreting OT protocols and for inventory purposes, highlighting that not only detection coverage but also log source analysis is extremely important. Further advanced detections will be introduced, such as passive vulnerability scanning and the exploration of honeypots as an option.[15]

In the fourth part, the necessary dataset and the appropriate alert system will be available, thus the construction of the attack environment will be based on MITRE CALDERA foundations. This will create a central repository for attackers, where attack campaigns can be easily orchestrated.[16]

[13] Wesley 2022.

[14] French 2023.

[15] Satta–Bennacer 2023.

[16] Nachaat 2022: 55–57.

Following this, the key part of my research focuses on the investigation of alerts and the management of events, including the modelling and comparison of tracing processes by machine models against human performance. This will be done using real-world SOC metrics, via TTP IDs. The main hypothesis of my research is: Can machine learning perform more effectively and reliably than a SOC Level 1 analyst? The final and in my opinion most useful part of the series will focus on attacking and defending machine learning within the framework of MITRE ATLAS. The outcome of this concluding section will be a comprehensive offensive and defensive capability, specifically within the AI dimension.[17]

References

AttackIQ Enterprise (2022): *What is the Pyramid of Pain?* Online: www.attackiq.com/glossary/pyramid-of-pain/

Black Cell Ltd. (2023): *Sector Specific MITRE ATT&CK Heatmaps for Detection Engineering.* Online: https://github.com/blackcellltd/Heatmaps

Crestani Tasca, Laurence – Pignaton de Freitas, Edison – Rech Wagner, Flávio (2020): A Study on the Performance Impact of Programmable Logic Controllers Based on Enhanced Architecture and Organization. *Microprocessors and Microsystems,* 76, 21–22. Online: https://doi.org/10.1016/j.micpro.2020.103082

French, David (2023): *From Soup to Nuts: Building a Detection-as-Code Pipeline.* Online: https://medium.com/threatpunter/from-soup-to-nuts-building-a-detection-as-code-pipeline-28945015fc38

Fritsch, Sebastian (2021): *IEC 62443-4-2 Use Case Industrial Firewall.* Online: www.teletrust.de/fileadmin/user_upload/2021-TeleTrusT-IEC_62443-4-2_Use_Case_Industrial_Firewall.pdf

GnosisX (2023): *pfSense.* Online: https://medium.com/@contact_45426/pfsense-3616ceb0ded0

Hexagon AB (2024): *Digital Twin Solution for Projects and Operations.* Online: https://exploreali.hexagon.com/interactive/digital-twin-solution-for-projects-and-operations

International Society of Automation (2024): *ISA/IEC 62443 Series of Standards.* Online: www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

Liaghati, Christina (2024): *MITRE ATLAS Overview.* Online: www.dau.edu/sites/default/files/2024-03/MITRE%20ATLAS%20Overview%20for%20sharing.pdf

MITRE ATT&CK (2024): *Enterprise Matrix.* Online: https://attack.mitre.org/matrices/enterprise/

Nabidoust, Fatemeh (2024): *EMI Filter and PFC (Power Factor Control) Schematic #AltiumDesigner.* Online: www.researchgate.net/publication/379861549_EMI_Filter_and_PFC_Power_Factor_Control_Schematic_hashtagAltiumDesigner

Nachaat, Mohamed (2022): Study of Bypassing Microsoft Windows Security Using the MITRE CALDERA Framework. *F1000Research,* 11, 55–57. Online: https://doi.org/10.12688/f1000research.109148.3

[17] Liaghati 2024.

Satta, Abdelwahhab – Bennacer, Samir (2023): *Industrial Control Systems Security with Elastic Security and Zeek.* Online: www.elastic.co/blog/industrial-control-systems-elastic-security-zeek

Szabó, Gergely Gábor (2022): *Mit jelent a mikrogrid és mire használható?* Online: https://szgg.hu/mit-jelent-a-mikrogrid-es-mire-hasznalhato/

Thompson, Katrina (2024): *The 10 Most Common Website Security Attacks (and How to Protect Yourself).* Online: www.tripwire.com/state-of-security/most-common-website-security-attacks-and-how-to-protect-yourself

Wesley, Lee (2022): *Developing OT Security Monitoring Use Cases.* Online: www.linkedin.com/pulse/developing-ot-security-monitoring-use-cases-wesley-lee/?trk=public_post