2023 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm) | 978-1-6654-5556-5/23/$31.00 ©2023 IEEE | DOI: 10.1109/SmartGridComm57358.2023.10333902

Comparative Study on Smart Grid Security Testbeds Using MITRE ATT&CK Matrix

Aneeqa Mumrez*, Muhammad M. Roomi†, Heng Chuan Tan†, Daisuke Mashima†,
Ghada Elbez*, Veit Hagenmeyer*
* Institute for Automation and Applied Informatics, KASTEL Security Research Labs, Karlsruhe Institute of Technology
† Illinois Advanced Research Center at Singapore (IARCS)
Email: {aneeqa.mumrez, ghada.elbez, veit.hagenmeyer}@kit.edu, {roomi.s, hc.tan, daisuke.m}@iarcs-create.edu.sg

***Abstract*—The increasing use of information and communication technologies has led to increasing threats on critical infrastructure like smart grids. Owing to confidentiality issues and difficulties in experimenting cyberattacks on a real environment, testbeds reflecting the characteristics of smart grids have been developed to enable attack experiments and cybersecurity research. In fact, different implementations of smart grid testbeds exist, each with its own challenges and limitations. The comparative study we present here justifies the usability of each type of testbed for different experiments. We begin our study with a selection of state-of-the-art smart grid testbeds, which can be classified into physical, hybrid, and virtual. We then present an evaluation based upon several qualitative metrics and MITRE ATT&CK matrix to demonstrate the coverage of all tactics and techniques to guide about the selection of testbed according to security needs. Finally, we explain applicable tactics and techniques for one of the testbeds through an attack case study to highlight current cybersecurity challenges faced by smart grids.**

***Index Terms*—Smart Grids, Cybersecurity Testbeds, Industrial Control Systems (ICS), MITRE ATT&CK Matrix.**

I. Introduction

Smart grids are integral parts of the energy infrastructure. They leverage advanced communication technologies to enable real-time monitoring and control of the electrical grid [1]. Due to the integration of communication technologies, smart grids have become increasingly vulnerable to cyberattacks. Thus, measures are necessary to improve smart grid security [2], [3]. However, securing them is nontrivial due to their complex interconnection and the necessity for continuous operation to avoid downtimes and unnecessary disruptions. To overcome these challenges, researchers have developed various types of smart grid testbeds for cybersecurity research and training. These testbeds integrate hardware and software components according to standardized network infrastructure. Such testbeds exist in different forms, ranging from physical and hybrid to virtual implementations. They allow researchers to evaluate the impact of cyberattacks (e.g., in terms of grid stability, operation disruptions, and quality of service) and the effectiveness of security measures in a high-fidelity setting. Furthermore, they provide valuable hands-on exercise and training resources for the research community. Since the configurations of each testbed is different, it is important to understand its capabilities and key differences to make informed decisions about its use for experiments.

In this paper, we conduct a comparative study on testbeds to understand their practicality and readiness for cybersecurity research. Our evaluation is based on qualitative analysis and utilizes the MITRE ATT&CK matrix for industrial control systems (ICS) [4]. The qualitative measures aim to identify the strengths and weaknesses of each testbed to justify their practicality, while the MITRE ATT&CK matrix for ICS (hereafter MITRE ICS matrix) is used to systematically categorize adversarial tactics and techniques that can be used to exploit them. To the best of our knowledge, there is no previous work on characterizing cybersecurity testbeds based on their mapping to MITRE ICS matrix. By applying this matrix, we aim to assess how well the testbeds can support realistic simulation of attack experiments, as opposed to using the MITRE framework for threat intelligence/detection [5], risk assessment or developing tools for attack emulation [6]. For our evaluation, we have selected three state-of-the-art testbeds, particularly a physical Electrical Power and Intelligent Control (EPIC) testbed [7] at the Singapore University of Design and Technology (SUTD) which is accessible with some associated applicable cost. Another is a recently developed hybrid testbed, KASTEL Security Lab Energy (hereafter KASTEL Lab) [8] by the Karlsruhe Institute of Technology (KIT) which is accessible upon approval of lab management. Lastly an open-sourced virtual environment that emulates the physical and cyber characteristics of a modern grid, called Smart Grid Cyber Range (SGCR), for conducting interactive cybersecurity experiments is developed by Illinois Advanced Research Center at Singapore [9]. By evaluating these testbeds, we provide a focal guide for the selection of testbeds. The main contributions of this paper can be summarized as follows.

- We provide a comprehensive description of each selected testbed by highlighting its architecture, configuration, integrated components, limitations, and advantages.
- We define qualitative metrics to evaluate the testbeds' suitability for cybersecurity experimentation and use the MITRE ICS matrix to demonstrate the feasibility and coverage of tactics and techniques for assessing practicality.
- We discuss an attack implementation on EPIC testbed and map the tactics/techniques to the MITRE ICS matrix to demonstrate potential vulnerabilities in the EPIC testbed.

In the remainder of this paper, we first briefly present

related literature in Section II before describing the selected testbeds and comparing them based upon different metrics in Section III. Subsequently, we provide insights using MITRE ICS matrix to identify potential techniques and tactics for all testbeds. Then, we present a case study for an attack scenario implemented at EPIC and map it onto the MITRE ICS matrix in Section IV. All findings are discussed in Section V along with the future work. Finally, Section VI concludes the paper.

II. Overview of Selected Smart Grid Testbeds

There are diverse practices to implement smart grid testbed architectures engaging advanced communication technologies. At high level, such testbeds are categorized into physical, hybrid, and virtual testbeds. Physical testbeds comprise of the hardware (e.g., generators) that is actually used in the production environment. One such physical testbed is the National SCADA Testbed (NTSB) built by Idaho National Laboratory [10]. It comprises of seven substations, thousands of monitoring sites and 61-mile 138 kV transmission lines. Another one is EPIC [7] built at SUTD, being used extensively for educational and training platform for researchers to launch different attacks [11]. Conversely, several hybrid implementations of testbeds, integrating hardware and simulators have also been developed. A testbed at Washington State University is used to investigate communication networks and cybersecurity research areas [12]. Different hardware components including Phasor Measurment Units (PMUs), Remote Terminal Units (RTUs) and relays have been integrated with network simulators and Real Time Digital Simulators (RTDS). A recently developed hybrid testbed is KASTEL Lab [8] comprising of control and protection hardware in addition to generation part as simulated models. Similarly, virtual testbeds are implemented as integrated cyber-physical co-simulators using virtualization and simulation technologies. Few implementations utilize commercial simulator software while the others only utilize open-source technologies. An example is Cost-efficient IEC 61850 Substation Testbed developed for the cyberphysical security analysis of a modern electrical substation [13]. It integrates various open source tools like GNS3, and libIEC61850 library etc. to simulate different components like Intelligent Electronic Devices (IEDs) etc. Another virtual testbed, SGCR [9], uses Smart Grid Modelling Language (SG-ML) processor and virtual elements like IEDs, PLCs etc.

Each of the aforementioned testbeds introduces different security challenges and limitations depending on whether they are implemented with physical, virtual components or a combination of both. The suitability of testbed highly depends on the developed use case. Therefore, criteria or guideline need to be defined in this direction. As a result, we present an evaluation of smart grid testbeds based on qualitative metrics and MITRE ICS matrix, highlighting the type of applicable tactics and techniques that are directly related to the type of cyberattacks. This is to justify their practicality for security assessment. An accurate testbed evaluation also depends on the availability of all technical details and their accessibility

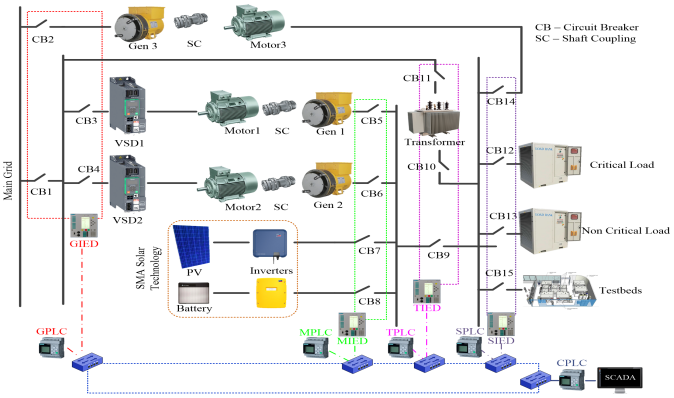

Fig. 1. Single Line Diagram - EPIC [14]

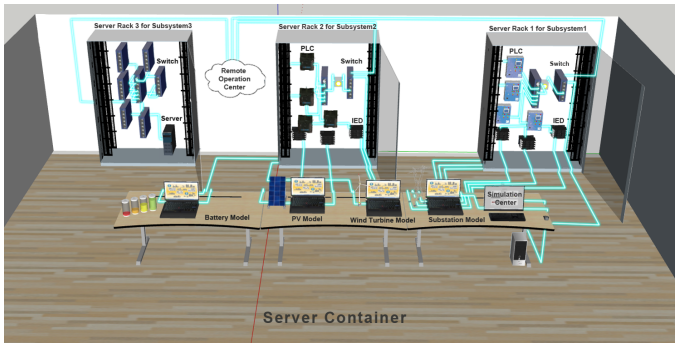

Fig. 2. Projection of KASTEL Security Lab Energy [8]

for experimentation. To the best of our knowledge, EPIC, KASTEL Lab, and SGCR were the only ones with necessary technical details accessible for us. Thus, we chose them as representative testbeds for each category (i.e., physical, hybrid, virtual). Detailed description of each testbed is provided below.

A. Electric Power and Intelligent Control (EPIC)

EPIC is a full-fledged power grid testbed that mimics a modern-day smart grid system [7]. The physical layout of the testbed is divided into four sectors: generation, transmission, microgrid and smart homes. The generation sector contains Variable Speed Drives (VSDs) and generators. An autotransformer is incorporated in the transmission sector to either step up or step down the voltage. The microgrid sector comprises of Photovoltaic (PV) and batteries, and finally, programmable loads form the smart homes sector. Each sector is equipped with IEDs, protective and switching equipment, and Advanced Metering Infrastructure (AMI). The communication network in the testbed include segmented, wired and wireless communications. IEC 61850 services [15] such as Generic Object-Oriented Substation Events (GOOSE) and Manufacturing Message Specification (MMS) are employed in the ring network to enable communication between the IEDs and Supervisory Control and Data Acquisition (SCADA).

B. KASTEL Security Lab Energy

The KASTEL Lab tackles the challenge of securing critical infrastructures [8]. The testbed is composed of three sub-

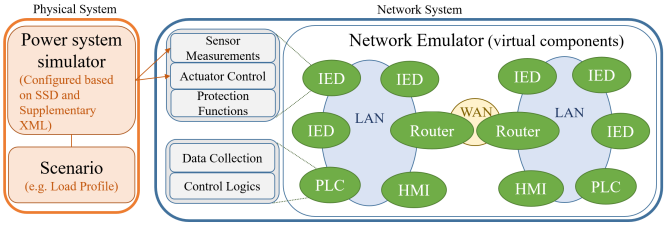

Fig. 3. High-level Architecture of SGCR [9]

systems: microgrid, transmission/distribution substation and Software-Defined Network (SDN) as shown in Fig. 2. Microgrid is the homogeneous subsystem with devices like PLCs and IEDs from Siemens to control the simulated energy generation models while taking corrective actions. Transmission/distribution substation is implemented in three levels: 1) station level with a Substation Automation System (SAS) and Human Machine Interface (HMI) solution for control and monitoring; 2) bay level with control and protection devices and; 3) process level with injection test set for simulating the physical system. It is a heterogeneous subsystem with devices such as IEDs, MUs etc. multi-sourced from various manufacturers. This allows studying the interoperability of the communication between different components. Both subsystems have physical as well as virtual (simulated) components. KASTEL Lab utilizes IEC 61850 as a general communication standard together with protocols like Modbus TCP, Profinet, and IEC 60870-5-104. Finally, the SDN subsystem, including different Network Function Virtualization (NFV) servers, serves to investigate the applicability and potential advantages of software-defined networking in energy communication networks. The focus is on increasing the security and resilience of future energy communication networks. By leveraging machine learning techniques, i.e., reinforcement learning, SDN-based ingress filtering is conducted in order to achieve adaptation to evolving traffic situations. The lab also allows implementation of experiments to analyze vulnerabilities in energy control components including hardware, network protocols, and the communication structure. The main goal is to develop adequate solutions to secure the energy systems.

C. Smart Grid Cyber Range (SGCR)

Cyber ranges for smart grids are virtual environments allowing cybersecurity research and training. Numerous efforts have been made to develop different kinds of cyber ranges. Fig. 3 illustrates the high-level architecture of SGCR. It consists of two main components, physical system and network system. The physical system consists of the power system simulator. The System Specification Description (SSD) and the Supplementary XML file are used as inputs to the SG-ML processor to generate the power system topology while power flow is simulated using the power system simulator. Similarly, the network system in SGCR consists of the virtual elements in the cyber range such as IEDs, PLCs and SCADA HMI. The sensor measurements and the actuator status can be obtained from the power system simulator. These values are stored in the database and used by the IEDs to control the operation of the system. The protection functions are also implemented in the IEDs. Communication with other IEDs, PLCs and SCADA is achieved through IEC 61850 protocols [15]. The SGCR supports MMS for measurements and GOOSE control for a single substation model. Conversely, Routable-GOOSE (R-GOOSE) and Routable-Sampled Value (R-SV) are used for inter-substation communication. The detailed SG-ML implementation is explained in [9].

III. Comparative Study of Selected Testbeds

In this section we present an evaluation of the selected testbeds from two different perspectives: qualitative metrics and MITRE ICS matrix.

A. Qualitative Metrics

For qualitative comparison, we selected cost, accessibility, fidelity, flexibility, and reproducibility to compare the three testbeds. As these metrics impose high impact on the testbed's effectiveness, they can help researchers to determine suitability of testbed for specific research or experiment.

Mimicking the behaviour of real smart grid by integrating actual hardware and software components, communication protocols, and compliance standards etc. is defined as fidelity. Given that EPIC and KASTEL Lab comprise of real hardware components (i.e. PLCs, and IEDs etc.), they have very high fidelity. One benefit of high fidelity is that it eradicates the need to add noise factor synthetically to the measurements, but it also comes with a drawback of high implementation cost. In contrast, for SGCR, implementation costs are minimum as compared to physical and hybrid testbeds, but fidelity is compromised in this case. Another important requirement for the testbeds is flexibility, which is the ability to scale the physical and network architecture to support different cyber attack experiments without extensive reconfiguration and redesign. In this regard, EPIC has low flexibility because it requires intensive domain knowledge and resources to configure the system topology, upgrade devices, and update configuration changes. Consequently, conducting attack experiments in EPIC is limited. As KASTEL Lab is a hybrid testbed that combines hardware devices and a simulation environment, it provides medium flexibility. In fact, the simulation environment supports experiments for investigating interoperability, cyber-attack detection, mitigation and impact analysis together with dynamic SDN configuration. On the other hand, SGCR is highly flexible as the system can be scaled up or scaled down without much effort and it allows a wide range of cyber attack experiments to be conducted without impacting any real device.

One major limitation of EPIC is its limited accessibility. One has to pay a physical visit to use the testbed, while SGCR is easily accessible over the internet. In the case of KASTEL Lab, remote access is possible over VPN but access is limited to only authorized users. Another important metric for testing and validating testbeds is reproducibility. It refers to

TABLE I
ARCHITECTURAL DIFFERENCES AMONG THE SELECTED TESTBEDS

Testbed	Type	Configuration	Components	Supported Protocols	No. of Physical ICS Devices
EPIC	Physical	Hardware	Generation, Transmission, Microgrid, Smart Homes	IEC 61850 - GOOSE, MMS, Modbus TCP	5 x PLCs, 11 x IEDs, 1 x SCADA, 3 x Workstations, 16 x network switches
KASTEL Lab	Hybrid	Hardware & Matlab/Simulink Models	Microgrid, Substation, SDN infrastructure	IEC 61850, IEC 60870-5-104, Modbus TCP, S7 Comm, PTP	4 x PLCs, 6 x IEDs, 2 x RTU, 3 x MUs, 14 x network switches, 4x NFV/SDN servers, 2 HMIs
SGCR	Virtual	Software	Single-/Multi-substations	IEC 61850 (MMS, GOOSE, R-GOOSE, R-SV), Modbus TCP	None

TABLE II
QUALITATIVE ANALYSIS OF THE SELECTED TESTBEDS

Testbed	Cost	Accessibility	Fidelity	Flexibility	Reprod.
EPIC	High	Low	**High**	Low	Low
KASTEL	High	Medium	**High**	Medium	Medium
SGCR	**Low**	**High**	Medium	**High**	**High**

the creation of realistic experimental environment to yield consistent results upon repetition. Considering the fact that SGCR only have software-based components, consistent results could be achieved by repeating the experiments multiple times. On contrary, for EPIC and KASTEL Lab, where hardware components are involved, it is hard to achieve similar results even after repeating the same experiment due to noise or ageing physical components. Table II presents this comparison with desirable values for the metrics highlighted in bold.

B. MITRE ATT&CK matrix

The MITRE ICS matrix [4] models the causalities in a cyber kill chain and allows practitioners to construct attack paths that represent how a malicious adversary can attack the ICS. The framework comprises of 12 tactics describing where the attack vector originates in the network, how it pivots into the OT systems, what vulnerabilities it exploits, and what impact it has on the target system. For each tactic, it also provides detailed techniques to explain how an attacker might target ICS networks and components. The framework helps ICS operators analyze potential cyber threats so they can prioritize security needs to improve the overall security of their systems.

We use the matrix to describe tactics and techniques that can be experimented on the EPIC, KASTEL Lab, and SGCR testbeds. A collective mapping for all testbeds is provided in Fig. 4 with color distinction to make it easier to navigate for each testbed. Our goal is to assess the completeness of selected testbeds for cybersecurity experimentation by identifying exploitable vulnerabilities in each of them. For ease of comparison, tactics and techniques that are common to two or more testbeds are discussed, followed by those that are unique for each testbed.

1) Common Tactics and Techniques:

Initial Access: Exploitation of remote services, external remote service, remote services - Include techniques that could be used as entry points to the ICS network. As the remote services are available for both EPIC and KASTEL Lab, there is always a potential for an adversary to gain an initial foothold to the OT (Operational Technology) network by exploiting them. To activate the remote services at EPIC, an attacker would first have to exploit some programming errors or OS while for KASTEL Lab, remote services are usually not disabled.

Execution: Command Line interface (CLI), execution through API, Graphical User Interface (GUI), Modify Controller Tasking - Include techniques that could be used by an adversary to manipulate parameters or functions of the systems. Availability of Application Programming Interfaces (APIs) and their vulnerabilities when identified by malicious attacker could result in execution of malicious commands. For example, at KASTEL Lab, adversary can leverage CLIs to execute arbitrary commands while an attacker at EPIC can also manipulate physical processes by taking advantage of the SCADA's GUI apart from manipulating through CLIs.

Persistence: Modify Program - To maintain the presence in the network, an adversary can modify controller codes or firmware. To remain stealthy for longer periods of time, another method could be to embed malware into existing PLC code and program it to execute only under certain conditions [16]. This holds for the Wago PLCs in EPIC and OpenPLC in SGCR.

Evasion: Spoof reporting message - Communication of devices over unauthenticated protocols such as MMS, Modbus TCP allow adversaries to spoof the messages before they reach the operator. This holds for all three testbeds.

Discovery: Network connection enumeration, network sniffing, remote system discovery, remote system information discovery - Tools like *NMAP* could be used to map out the network, determine which hosts to target, and search for exploitable vulnerabilities for subsequent lateral movement within the OT network. As all three testbeds have some part of communication implemented over unauthenticated and unencrypted protocol, this holds for all of them.

Lateral Movement: Default credentials, exploitation of remote services, remote services - The attacker leverages exploitable vulnerabilities to control remote targets, particularly the field devices on the network. Those vulnerabilities may include harvested credentials and remote services that allow the attacker to access file systems on field devices.

Collection: Adversary in the middle, data from local system, detect operating mode, I/O image, monitor process state, point and tag identification, Screen capture - This step is similar to the "discovery" tactic in which the attacker gathers information about the network, devices, and topology. The main difference is that after data collection, the data is exfiltrated for further analysis. As mentioned earlier, using

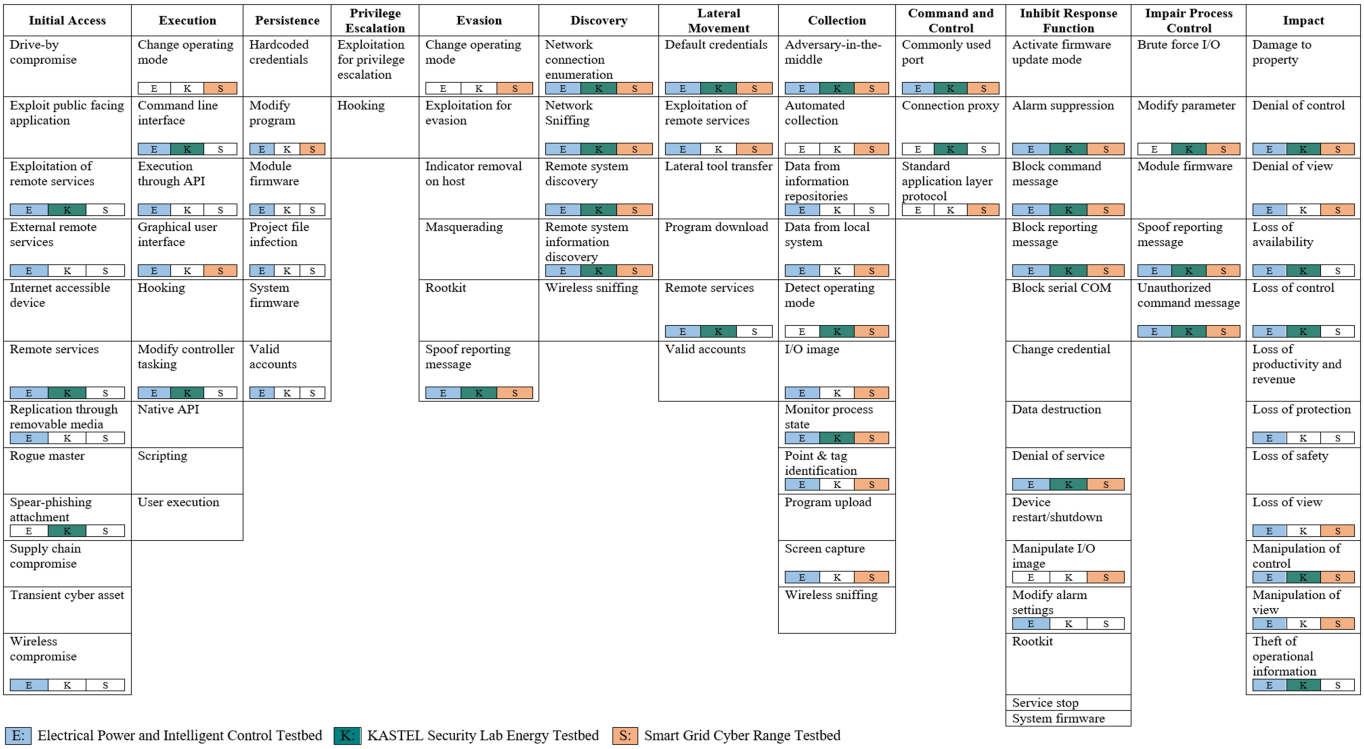

Fig. 4. Potential Tactics and Techniques that can be demonstrated on EPIC, KASTEL Lab, and SGCR testbeds.

unauthenticated protocols allow traffic interception. This becomes the first step to plan further attacks such as process data collection, False Data Injection (FDI) or modification in real-time. On the other hand, data which includes configuration files, logs, standard based mappings or I/O image could be collected by targeting a local system. For example, the EPIC historian server that records all traffic or events could be targeted. Likewise, the SGCR database that stores the physical measurements and the control status of the system.

Command and Control: Commonly used port - The attacker can establish itself as a man-in-the-middle between two target hosts and start modifying MMS and Modbus TCP packets on the fly. The attacker may use legitimate ports such as port 102 associated with MMS and port 502 associated with Modbus TCP to blend in with normal network activity at EPIC, KASTEL Lab or SGCR to avoid detection.

Inhibit Response Function: Alarm suppression, block command message, block reporting message, denial of service - The adversary seeks to prevent protection and safety logic from execution, including operators from responding to any failure after an attack. This is possible by suppressing alarms, blocking command/reporting messages or modifying settings for the alarms. These actions, regarded as multistage attacks, are possible in all three type of testbeds where attacker targets multiple nodes to hide his activity.

Impair Process Control: Modify parameter, spoof reporting message, unauthorized command message - This step examines an attacker's ability to interfere with control processes and can be broadly classified into deny, disrupt, and deceive in the context of the power grid. Target of interests include taking advantage of the active parameters/procedures, which harms the physical environment. For example, at KASTEL Lab, changing the run time from infinity to a specific value for the models simulating renewable energy generation would halt the physical process completely after defined time. Specific to EPIC, spoofing reporting messages and issuing unauthorized command messages can disturb the physical process.

Impact: Denial of control, denial of view, loss of availability, loss of control, loss of view, manipulation of control, manipulation of view, theft of operational information - Extent of damage and after-effects that occur after a successful attack is regarded as an impact. Attacks on any of the four sectors of EPIC testbed would lead to loss of control and theft of operational data apart from raising security concerns. Same would be applicable to KASTEL Lab, where attacks on one subsystem would also affect other subsystems due to logical dependency among all. For SGCR, depending on the number of substations involved, the impact can lead to a chain of events. The adversary can manipulate control commands to disrupt the normal operation of the substation and simultaneously spoof the SCADA to hide the disruption.

As the hardware and software component varies for all the three testbeds, the exploitable vulnerabilities in each of them also varies. This explains why some tactics and techniques hold only for one testbed while cannot be exploited in other testbed. We now present unique techniques for each testbed.

2) Common Tactics and Distinctive Techniques:

Initial Access: External Remote Services, Removable Media, Wireless Compromise - Attacker can gain initial access

to the network in many ways depending upon integrated hardware and software components. For instance, at EPIC, the attacker may use removable media injected with malware or exploit compromised wireless access points to gain initial access. Similarly, engineering workstation in EPIC is configured with remote access capability to facilitate management tasks. An attacker can also harvest VPN credentials to gain access into the SCADA Network.

Spear-phishing - While KASTEL Lab provides remote services over VPN connection to specific VLANs, adversaries who manage to obtain the necessary VPN configuration will still be unable to connect to the VLAN without entering authorized user credentials. Social engineering tactics such as spear-phishing could be used by an attacker, to first gain an authenticated user credentials and then connect to VLAN.

Execution: Execution through API - Execution refers to the manipulation of system in different ways. For a testbed like EPIC, both hardware or software vulnerabilities can be exploited. For example, at EPIC, the programming software (i.e., CoDeSys) for Wago PLCs could be exploited to enable the attacker to interface with the real PLC.

Change operating mode - In SGCR, the adversary can change the operating modes of OpenPLC61850, leading to reset of memory address.

Persistence: Module Firmware, Project file infection, Valid Accounts - An attacker can exploit vulnerabilities in CoDeSys to upload malicious PLC codes and firmware to achieve persistent control over the physical processes at EPIC. By embedding logic bombs within PLC code and programming it to execute only under certain conditions, attackers can remain stealthy for longer periods of time. Device configuration files including user credentials can also be modified to provide a means of backup access for persistence.

Collection: Data from information repositories - PLC and IED configuration files (e.g., IID and ICD files) contain sensitive data, such as network settings and mappings specific to the IEC 61850 standard. These data can be exfiltrated for further intelligence about the system topology, identify potential vulnerabilities, and plan advanced attacks in EPIC.

Automated collection - In SGCR, the state of the system at every instance is recorded and stored in a historian database. By gaining access to the database, the attacker can collect the information about the connected devices, the communication protocols, message exchange details, etc. Subsequently, these information can be used by the attacker to launch preferred attacks on the system.

Command and Control: Connection Proxy - As KASTEL Lab has physical devices like PLCs, adversaries can manipulate their configurations as well, apart from manipulating the protocol. For instance, an insider with enough knowledge about PLC configuration could make some amendments by changing server configuration of controller to client. It is then possible to use a proxy server to connect the controller and the client indirectly and intercept all traffic. A compulsion is to have proxy server in the VLAN.

Standard Application Layer Protocol - In SGCR, OpenPLC61850 uses Modbus to communicate with the ScadaBR [17]. These protocols can be manipulated by the adversary to breach the network communication and send false control commands to the controller.

Inhibit Response Function: Modify Alarm Settings- The IEDs in EPIC monitor the power grid and communicate the status with the SCADA via report control blocks described in SCL (System Configuration Language) files. The SCADA then raises alarms, if necessary, based on the received information. An attacker can establish a connection to the IEDs to modify report control blocks in SCL files and thereby modify alarm parameters to inhibit the SCADA's response functions.

Manipulate I/O image - For SGCR, a mapper tool in OpenPLC61850 maps measurements from the physical simulator into the memory address of the OpenPLC61850. These inputs and outputs of the programmable controller can be modified through attack manipulation [18]. As a result, fake measurements could be reported to the SCADA HMI which falsely triggers the protection function to destabilize the system.

Impact: Loss of protection - In EPIC, when reverse power flow is detected, one of the PLCs will send a Modbus command to regulate the VSD speed of the affected generator. By spoofing an incorrect value in a Modbus packet, an attacker can deny reverse power prevention, causing malfunction or severe damage to the generator. On the other hand, such issues are not reported for KASTEL Lab or SGCR.

In reference to the details and comparison presented in this section, we provide, as a validating example, an attack scenario mapped on the MITRE ICS matrix to illustrate identified tactics and techniques.

IV. Map An Example Attack to MITRE ICS Matrix

In this section, we related the mapping on MITRE ICS matrix for EPIC testbed after implementing an attack on the physical testbed. Our attack scenario targets reverse power prevention logic in the generator [14] and is defined as follows: when reverse power flow is detected, the PLC sends a Modbus TCP command to increase the speed of the VSD. We modify the Modbus TCP command to instruct the VSD to underspin. This action causes the generator to draw more reverse power and eventually trip, causing a blackout. The above attack scenario can be mapped to the following tactics and techniques:

Initial Access: Replication through removable media - We mimick an insider attack by physically connecting a laptop to a network switch where the PLC and VSDs are located. This attack corresponds to replication through removable media where a contractor's laptop is infected with malware and brought into the ICS network. *Collection:* Monitor process state, Data from local system - On our laptop, we ran Wireshark to capture the Modbus message formats and the relationship between the PLC and the speed of the VSD. This technique corresponds to monitoring the process state and gathering data from the local system. *Discovery:* Network sniffing - We sniff network traffic and launch ARP spoofing to redirect Modbus TCP packets to our laptop for analysis.

Command and Control: Commonly used port - On knowing which Modbus register to manipulate, we execute a man-in-the-middle attack script to intercept and modify Modbus TCP command values on the fly through Modbus TCP port 502. *Impair Process Control:* Unauthorized command message - By sending unauthorized Modbus TCP commands to underspin the VSD, the generator tripped, impairing the normal process control. *Impact:* Loss of availability - The plant was forced to shut down, resulting in power outage and a loss of availability.

V. Discussion & Future Work

The comparison of testbeds highlights the importance of using different qualitative metrics to evaluate testbed feasibility. For example, physical testbeds provide a better visualization of the impact of cyberattacks but can be limited in usability due to high costs. This is where virtual testbeds offer a viable alternative despite lacking the physical dynamics of real systems. Moreover, in developing defense mechanisms, an approach developed for the virtual testbeds may not be directly applicable to other types of testbeds. In this case, hybrid testbed offers a convenient trade-off since it combines the advantages of both physical and virtual testbeds. Separately, the evaluation based on MITRE ICS matrix presents the exploitable vulnerabilities in each testbed from initial access to final impact. Some tactics and techniques are only applicable to EPIC, KASTEL Lab, or SGCR based on the type of integrated software and hardware components. This implies that one should also be aware of components (as presented in Section II) to implement realistic attack case studies. As our MITRE ICS matrix mapping covers the feasibility and coverage of adversarial tactics and techniques, hence future work will focus on planning defense mechanisms to mitigate the identified techniques. In particular, the implementation and validation of security solutions such as Intrusion Detection System (IDS) on the selected testbeds to rule out several techniques and tactics from the presented mapping will be considered. Additionally, due to space limitation, the current study only provides attack mapping for the EPIC testbed. In future, we plan to map similar attacks on the other two testbeds.

VI. Conclusion

Smart grid testbeds provide a platform to study and evaluate the impact of cyberattacks. Physical, hybrid, and virtual implementations exist for these platforms. The present study provides a comparative analysis of these implementations to aid the selection of testbeds for conducting different experiments. We selected three testbeds to conduct an evaluation based upon different qualitative metrics such as cost, fidelity, and flexibility etc. to address their advantages and limitations. Additionally, we used MITRE ICS Matrix to investigate the potential security challenges and vulnerabilities within each testbed by mapping common/unique tactics and techniques. To the best of our knowledge, this is the first time that such characterization is presented. Hence from cybersecurity perspective, this study helps to understand better the adversarial abilities which could be leveraged within each testbed.

Acknowledgement

This research is supported in part by funding from the topic Engineering Secure Systems of the Helmholtz Association (HGF) and by KASTEL Security Research Labs (structure 46.23.02). It is also supported by the National Research Foundation, Prime Minister's Office, Singapore under its Campus for Research Excellence and Technological Enterprise (CREATE) programme.

References

[1] G. Dileep, "A survey on smart grid technologies and applications," *Renewable energy*, vol. 146, pp. 2589–2625, 2020.

[2] M. Ghiasi, T. Niknam, Z. Wang, M. Mehrandezh, M. Dehghani, and N. Ghadimi, "A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: Past, present and future," *Electric Power Systems Research*, vol. 215, p. 108975, 2023.

[3] H. C. Tan, C. Cheh, B. Chen, and D. Mashima, "Tabulating cybersecurity solutions for substations: Towards pragmatic design and planning," in *2019 IEEE Innovative Smart Grid Technologies-Asia (ISGT Asia)*. IEEE, 2019, pp. 1018–1023.

[4] MITRE, "Mitre-att&ck matrix for ics," Available at https://attack.mitre.org/matrices/ics/ (accessed Aug. 17, 2023).

[5] Z. Jadidi and Y. Lu, "A threat hunting framework for industrial control systems," *IEEE Access*, vol. 9, pp. 164 118–164 130, 2021.

[6] R. Alford, D. Lawrence, and M. Kouremetis, "Caldera: A red-blue cyber operations automation platform," *MITRE: Bedford, MA, USA*, 2022.

[7] iTrust, Available at https://itrust.sutd.edu.sg/testbeds/electric-power-intelligent-control-epic/.

[8] KASTEL, "Kastel - security and privacy for future energy systems," Available at https://www.kastel.kit.edu/english/energie.php (accessed Aug. 17, 2023).

[9] D. Mashima, M. M. Roomi, B. Ng, Z. Kalbarczyk, S. Hussain, and E.-C. Chang, "Towards automated generation of smart grid cyber range for cybersecurity experiments and training," in *Proceedings of Dependable Systems and Networks 2023 (Industry Track)*, 2023.

[10] M. Zeller, "Common questions and answers addressing the aurora vulnerability," in *DistribuTECH Conference*, 2011.

[11] M. R. Saifuddin, L. Wei, H. C. Tan, and B. Chen, "Coordinated network attacks on microgrid dispatch function: An epic case study," in *European Symposium on Research in Computer Security*. Springer, 2022, pp. 26–45.

[12] M. H. Cintuglu, O. A. Mohammed, K. Akkaya, and A. S. Uluagac, "A survey on smart grid cyber-physical system testbeds," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 1, pp. 446–464, 2016.

[13] G. Elbez, H. B. Keller, and V. Hagenmeyer, "A cost-efficient software testbed for cyber-physical security in iec 61850-based substations," in *2018 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*. IEEE, 2018, pp. 1–6.

[14] M. M. Roomi, S. M. S. Hussain, D. Mashima, E.-C. Chang, and T. S. Ustun, "Analysis of false data injection attacks against automated control for parallel generators in IEC 61850-based smart grid systems," *IEEE Systems Journal*, pp. 1–12, 2023.

[15] R. E. Mackiewicz, "Overview of IEC 61850 and benefits," in *2006 IEEE Power Engineering Society General Meeting*. IEEE, 2006, pp. 8–pp.

[16] N. Govil, A. Agrawal, and N. O. Tippenhauer, "On ladder logic bombs in industrial control systems," in *Computer Security: ESORICS 2017 International Workshops, CyberICPS 2017 and SECPRE 2017, Oslo, Norway, September 14-15, 2017, Revised Selected Papers 3*. Springer, 2018, pp. 110–126.

[17] M. M. Roomi, W. S. Ong, D. Mashima, and S. S. M. Hussain, "OpenPLC61850: An IEC 61850 MMS compatible open source PLC for smart grid research," *SoftwareX*, vol. 17, p. 100917, 2022.

[18] M. M. Roomi, W. S. Ong, S. M. S. Hussain, and D. Mashima, "IEC 61850 Compatible OpenPLC for Cyber Attack Case Studies on Smart Substation Systems," *IEEE Access*, vol. 10, pp. 9164–9173, 2022.