IEEE Access
Multidisciplinary : Rapid Review : Open Access Journal

Received 24 January 2024, accepted 22 February 2024, date of publication 11 March 2024, date of current version 15 March 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3375401

RESEARCH ARTICLE

Multidomain Cyber-Physical Testbed for Power System Vulnerability Assessment

DENYS MISHCHENKO[1], (Member, IEEE), IRINA OLEINIKOVA[1], LÁSZLÓ ERDŐDI[2], AND BASANTA RAJ POKHREL[1], (Member, IEEE)

[1]Department of Electric Energy, Norwegian University of Science and Technology, 7491 Trondheim, Norway
[2]Department of Information Security and Communication Technology, Norwegian University of Science and Technology, 7491 Trondheim, Norway

Corresponding author: Denys Mishchenko (denys.mischenko@ntnu.no)

This work was supported by the Department of Electric Energy, Norwegian University of Science and Technology, Trondheim, Norway.

ABSTRACT The rapid digitalization of power systems involves enhanced interconnectivity, intelligence, and cost-efficiency across all components. In the era of Industry 5.0, the criticality of energy supply makes power systems prime targets for attacks, highlighting the need for the creation and evaluation of solutions against cyber-physical threats. Testbeds have emerged as essential tools for these purposes by representing real-world power systems in controlled environments and simulating cyber-physical attack-defense experiments. This paper introduces a Cyber-Physical Security (CPS) testbed rooted in the Smart Grid Architecture Model (SGAM) and developed adversary setup within the National Smart Grid Laboratory at the Norwegian University of Science and Technology. By adhering to the SGAM framework, this study delves into the classification and assessment of threats within the structure of the CPS testbed, examining vulnerabilities at distinct structural levels. Significantly, the strategic placement of the adversary setup within these levels enables a comprehensive evaluation of cyber-physical vulnerabilities in simulated systems, thereby facilitating the assessment of protective measures. Furthermore, this research presents case studies using three data sources as an aggregated dynamic power system model simulated in the real-time digital simulator OPAL-RT, real power grid, and playback of previously recorded data frames using virtual phasor measurement units functionality. The focus of this work is on the analysis of the five most common cyberattacks on power systems, such as passive and active reconnaissance, interruption in communication, TCP packet injection, and men-in-the-middle attacks utilizing the C37.118.2-2011 protocol. The results of the case studies illustrate the framework for the adversary setup and provide proof-of-concept attack scenarios for evaluation purposes. As part of future work, we intend to expand upon this research with a defender setup and implement more sophisticated, stealthy attacks.

INDEX TERMS Power system, cyber-physical security, testbed, smart grids, threats.

I. INTRODUCTION

The digitalization of power systems is proceeding rapidly as all components like generation, distribution, and consumption become more interconnected, intelligent, and cost-effective [1]. The integration of digital technologies such as modern sensors, real-time communication, the Internet of Things (IoT), and data analytics is taking place. Additionally, it's essential to acknowledge the numerous industrial control systems (ICS) that monitor, control, and protect elements of power systems. These technologies allow to ensure reliable, secure, and sustainable operation of the power system.

However, digitalization also brings new risks and challenges. Cyber-physical threats are one of these problems. The purpose of attackers may be possible power outages, collection, and data manipulation. Such actions are aimed at causing physical and economic damage to critical infrastructure [2]. Despite the implementation of standards, conducting regular testing and training, and application of new measures that aim to protect power system elements against physical and cyber threats, new cases of attacks are recorded every year [3].

The associate editor coordinating the review of this manuscript and approving it for publication was Arash Asrari.

In the period of Industry 5.0 [4] dependence on energy supply has never been greater. That makes power system components one of the main targets for attacks, especially with zero-day exploits – undisclosed vulnerabilities until launched by attackers. Therefore, it is important to create a secure and realistic environment to test, evaluate, and validate the effectiveness of the solutions developed against cyber-physical threats. For these purposes, cybersecurity testbeds provide a golden mean platform.

A cybersecurity testbed is an isolated and controlled environment designed for evaluating and testing the security of physical and cyber components of power systems elements that can fully cover realistic digital power grid operating scenarios on a laboratory scale. The first task of the testbed is to recreate processes that accurately mimic the power system behavior. The next task is to model physical and cyber threats and evaluate system component resilience in real-world scenarios. The general aim of testing is to assess vulnerabilities, evaluate security measures, and develop strategies to protect critical infrastructure and systems.

A. RELATED WORK

Various types of testbeds for testing cyber-physical threats in power systems have been created. Yohanandhan et al. in [5] and [6] presented an extensive review that described 72 cyber-physical power system testbeds in academia and national laboratories. In these papers, testbeds are divided into type, targeted research area, domain, and communication infrastructure with the fusion of physical and cyber systems. That makes it possible to evaluate existing testbeds from the functional and technical side.

In the literature reviews on cyber-physical testbeds for power systems presented in [7], [8], [9], [10], and [11] their functionality assessed and presented below in accordance with the type: physical, virtual, and cyber-physical.

The main advantage of the physical testbeds is the most realistic representation of the power system processes. The physical testbeds allow to achieve high fidelity of results, observe real-time responses and interactions. However, the main disadvantage of such systems is the very high cost of implementation, lack of scalability, and as a result testing flexibility. An example of a physical testbed is the National SCADA Testbed (NSTB) built by Idaho National Lab [12]. This testbed has its own substations and power grid allowing them to test and analyze system processes more realistically.

Unlike physical, virtual testbeds offer high configuration flexibility of the power system components. Software modeling is used instead of physical power system equipment. That allows to reduce time and costs of implementation and maintenance. However, the results depend on the accuracy of the models, which may not fully mimic the behavior of an entire physical system. For example, the Cyber Security Testbed at Karlsruhe Institute of Technology (KIT) [13] is a virtual testbed mostly with open-source software that was designed and implemented to study the cyber-physical security (CPS) of IEC 61850-based electrical substations.

The most widely implemented type is cyber-physical testbeds. Such testbeds provide real-time interaction between physical components and digital systems. These testbeds have the advantages of two previous types. On the one side, such testbeds are more cost-effective than physical testbeds. At the same time, cyber-physical testbeds provide quite realistic testing and validation of CPS in power systems, unlike virtual ones. One of them is the PowerCyber testbed at Iowa State University [14]. The authors describe the architecture and capabilities of the testbed, specifically highlighting the communication, control, and physical system simulation components. The testbed currently utilizes an array of real, emulated, and simulated components to provide a realistic cyber and physical environment.

The testbed presented in this work is characterized as a cyber-physical. A comparative analysis will be conducted against similar types of testbeds currently in existence. This comparison will highlight the differences and illuminate the advantages that this cyber-physical testbed holds over others. Through this comprehensive exploration and comparison, a clear understanding of the value and potential applications of this particular cyber-physical testbed is expected to emerge.

B. CONTRIBUTION

The existing types of testbeds mentioned above and their functionality allow to investigate all known cyber-physical threats. However, modeling is carried out using typical physical and digital components for the testbed region. Hardware and software that are used in different areas or systems have their own advantages and limitations that it is necessary to investigate against physical and cyber threats. For example, authors in [15], [16], [17], and [18] used Distributed Network Protocol 3 (DNP3) which is one of the most popular communication protocols but is widespread only for power systems components located in the United States of America (USA). Despite this, nowadays exist a lot of other types of modern and legacy protocols [19]. In response to this, the CPS testbed and the adversary setup, presented in this work, are created in the National Smart Grid Laboratory (NSGL) [20] at the Norwegian University of Science and Technology (NTNU), Trondheim, Norway with the main scope to explore and evaluate measures against threats that typical for power system components in the Nordic and Europe Union (EU) regions.

Researchers in [21], [22], [23] have explored CPS testbeds aligning with Supervisory Control And Data Acquisition (SCADA) systems to assess vulnerabilities. However, the SCADA capabilities are limited and do not meet the new operational requirements of modern and intelligent power grids, such as the need for high-rate sampled data, accuracy, and synchronized measurements. Consequently, global grid congestion and disruptions have prompted the need to upgrade power grids, leading to the emergence of cost-effective Wide Area Monitoring, Protection, and Control (WAMPAC) systems [24]. These systems improve grid design, operation, maintenance, and monitoring using advanced Information Technology (IT) and Operational Technology (OT) components. Considering this, we explored and analyzed the CPS testbed in this work in alignment with a WAMPAC system. Evaluating measures against cyber-physical vulnerabilities becomes crucial for implementing advanced WAMPAC applications within a secure and cyber-resilient environment.

A number of authors [8], [21], [25] offer a set of criteria for the testbed implementation and evaluation that consider one position of attacker in the power system structure and don't provide an assessment of threats for each power system structural level that could be explored using testbed facilities. Unlike them, this paper explores threats in the CPS testbed structure according to the Smart Grid Architecture Model (SGAM). The analysis will encompass a range of vulnerabilities that vary depending on the structural level. Changing the position of created adversary setup among layers and zones, allows to stress each of them with cyber-physical vulnerabilities in simulated systems and evaluate protection measures. A list of the most probable and unique cyber-physical threats for each component layer of the energy system that is possible to evaluate using the CPS testbed and the adversary setup will be shown. Introduced CPS testbed structure and adversary setup have been evaluated with five cyberattacks in a smart grid operating scenario using physical and cyber components of the NSGL.

Furthermore, another objective of the cyber-physical testbed and the adversary setup is to facilitate training within the field of electrical engineering, specifically focused on enhancing the resilience of cyber-physical power systems against cyberattacks. Through hands-on training and experimentation, the created facility helps to advance the knowledge, skills, and capabilities of electrical engineers in protecting and strengthening the security of cyber-physical power systems. This objective aligns with the revised Network and Information Security 2 (NIS2) Directive [26], the latest EU cybersecurity legislative document, mandating training for entity management in cyber protection, fostering cooperation between member states, and promoting communication and information exchange among entities.

In summary, the main contributions of the paper are as follows:

- Evaluation of measures against threats specific to power system components in the Nordic and EU regions;
- Exploration and analysis of the CPS testbed in alignment with WAMPAC applications;
- Consideration of hardware and software in the CPS testbed according to the SGAM to assess cyber-physical vulnerabilities across structural levels;
- Leveraging the CPS testbed and the adversary setup to offer cyber-physical protection training.

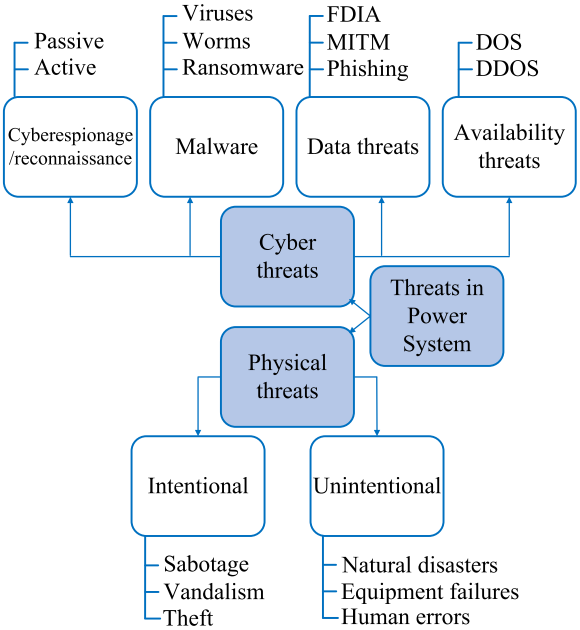


FIGURE 1. Power system threats structure.

C. ARTICLE STRUCTURE

The paper is organized as follows. Section II explores cyber-physical threats, their implications for power systems components, and the classification of existing measures. The vulnerability assessment of the CPS testbed architecture based on the SGAM shown in Section III. This assessment concentrates on the components that can be applied within the NSGL at NTNU. Section IV introduces the concept of the adversary setup for testing and describes five attack scenario details. The results, findings, and measures against explored attacks are discussed in Section V. Finally, Section VI contains conclusions and outlines for future work.

II. CYBERSECURITY IN POWER SYSTEM

With the increased digital transformation, the number of threats is growing every year. Only for the second quarter of 2023, 151 malicious activities were detected among critical infrastructures [27]. The energy sector is one of the components of a critical infrastructure that includes IT and OT making them potential targets for threats. In the report of cybersecurity incidents for 2022, the energy sector accounted for 15 % of all cybersecurity incidents related to critical sectors [28]. Furthermore, a study conducted by Kaspersky Lab [29] showed that the most vulnerable ICS components that were widespread among power systems were connected with Human Machine Interfaces (HMI), electric devices, and SCADA systems. Despite this, all components of the power system should be considered as targets for attacks that are feasible to divide into two main categories as physical and cyber threats that shown in Figure 1.

A. PHYSICAL THREATS

Physical threats against power systems can have severe consequences, impacting the reliability of electricity supply and potentially disrupting critical infrastructure. These threats can arise from intentional or unintentional actions, posing risks to the functioning of power generation, transmission, distribution, and consumption systems.

Common types of intentional actions can be sabotage, vandalism, or theft with a lot of techniques. Among the known and previously well-studied threats it is necessary to emphasize one of the new challenges against the power system that has emerged in 2022 [30]. This new threat takes the form of drone attacks, where drones have the capability to transport various explosive devices and deploy them onto critical power system components. Consequently, these attacks have led to widespread and significant blackouts across the country. Deploying anti-drone technologies that can detect, track, and neutralize unauthorized drones within restricted airspace can be challenging and have an impact on normal operation IT and OT components of power systems.

On the other hand, natural disasters, equipment failures, and human errors are related to unintentional actions. For the 2022 year in Europe, it was reported about earthquakes, floods, and forest fires. Climate change is expected to increase the amount and frequency of hazards in the future, so losses and the number of people affected will also rise around the world. Unintentional equipment failures within power systems can also pose threats. Aging infrastructure, inadequate maintenance, or manufacturing defects can lead to component malfunctions or system failures. Last but not least are human mistakes in system operation, maintenance procedures, or decision-making processes.

B. CYBER THREATS

Cyber threats to power systems are diverse and can be classified into various categories based on their nature, intent, and potential impact. According to the report [27] in Q2 2023 the main motive of the attackers with 63% of the cases was cyberespionage. Cyberespionage can involve passive and active reconnaissance techniques. This helps attackers gather intelligence, understand the target power system's infrastructure, and identify potential vulnerabilities and weaknesses that can be exploited in later stages of the espionage operation.

As regards initial access, the observed and three most popular techniques detected in 2022 were malware, threats against data, and availability [28]. The first is malicious software, such as viruses, worms, and ransomware, that can infect computers, servers, or digital systems within a power grid. Malware can disrupt operations, compromise system integrity, steal sensitive information, or enable unauthorized access. The second type is attacks against availability with the aim to interrupt operation between power system elements by flooding them with excessive traffic or requests. Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) typical representatives of this type of attack can lead to service disruptions, system unavailability, and hindered response capabilities. Furthermore, threat actors can manipulate data within power system networks to deceive operators, disrupt control processes, or cause system malfunctions. Data manipulation attacks such as false data injections (FDIA) using Men in the Middle (MITM) attacks can lead to inaccurate monitoring, protection, and control errors, or compromised decision-making.

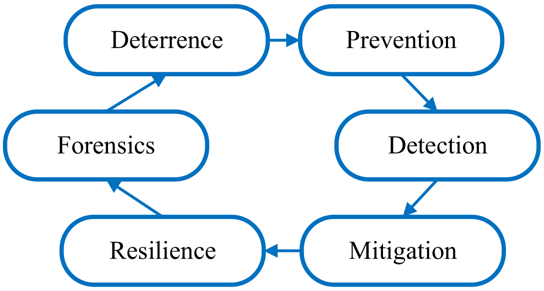


FIGURE 2. Power system defence structure [31].

Despite currently known attacks, there may also be unknown attacks called zero-day exploits. This type of attack targets an unknown vulnerability or weakness in software, hardware, or digital systems. Such attacks are highly effective due to the lack of countermeasures. The discovery and sale of zero-day vulnerabilities can have ethical and legal implications, as they can be used for both offensive and defensive purposes.

The occurrence of cyber and physical threats in the power system has resulted in extensive and substantial outages, damages, and blackouts. This underscores the critical need for implementing effective measures to overcome these threats.

C. EXISTING MEASURES AGAINST THREATS

Implementing measures against threats is a main requirement to ensure reliable, secure, and sustainable power system operations. The key to reaching a high level of cybersecurity is through the consolidation of technical, operational, and organizational measures against physical and cyber threats. Authors in [31] showed an end-to-end security life cycle for attack-resilient WAMPAC applications in the power grid. This comprehensive security lifecycle is illustrated in Figure 2 and categorizes existing research according to their alignment with different stages of this cycle. This work emphasizes deterrence, prevention, detection, mitigation, and resilience that can be further evaluated with the introduced CPS testbed within a WAMPAC system.

The initial phase of this approach involves "deterrence" which reduces risks by implementing regulations and possessing defensive capabilities. In recent years, different security standards guidelines, and laws have been developed that help to overcome existing threats [32]. These documents provide structured requirements and guidelines that cover all existing domains and components in the power system. Adhering to standard requirements in power systems is instrumental in mitigating threats. Consequently, aligning testbed components with these standard requirements enables realistic experiments, testing physical and cyber threats, the analysis of their impacts, and the development of effective countermeasures.

To enhance protection against threats, the subsequent step is "prevention," which aims to thwart attacks through risk assessment, penetration testing, and implementing advanced techniques. Regular risk assessment ensures the identification of vulnerabilities, potential weaknesses and offers an effective reaction to threats. In [33] authors proposed a risk assessment framework to systematically evaluate the vulnerabilities of SCADA systems that also could be applied to the CPS testbed considered in this work. Penetration test plans are detailed in [34], offering specific guidelines for different smart grid sectors. The authors identified various components and layers of WAMPAC systems that should be subjected to penetration tests and also presented the procedure for conducting these tests. In [35], advanced techniques are discussed, including the moving target defense, which periodically modifies the system's configuration, and physical watermarking, which introduces specific noise into the measurements and control commands.

If the initial two preventive measures prove to be ineffective, the following steps, "detection" and "mitigation," are implemented. These steps aim to identify and tackle ongoing attacks while ensuring the stability of the grid. They primarily address two types of threats: data integrity and data availability. To counter data threats, Model-Based Detection which utilizes estimation-based detection algorithms, and Data-Driven Detection, which is detailed using machine learning algorithms in [36], are explored. Regarding availability threats, one of the referenced studies is [37], where various technical solutions for DoS attacks are examined.

In situations where attacks are undetectable or cannot be mitigated, the "resilience" of the system becomes a critical factor, ensuring that operations continue even in compromised states. Undetectable attacks often involve the use of zero-day exploits thereby evading traditional security measures. Creating a power grid that is resilient to such threats involves designing elements with redundancy. This concept is exemplified in [38], where the authors provide an attack-resilient measurement design methodology. This methodology involves the optimal placement of sensors to ensure the overall system observability, even under possible contingencies and loss of measurements. Another approach to improve resilience involves the segmentation of the power system elements. In [39], the authors propose architectures consisting of a multitude of geographically dispersed phasor measurement units (PMU) and phase data concentrators (PDC). These architectures help to overcome challenges such as large data volumes, security issues, communication overhead, and failures to meet real-time deadlines.

The presence combination of measures at every structural level of the CPS testbed facilitates the implementation of a comprehensive security life cycle for solutions resilient to attacks. This comprehensive approach is further enhanced when the CPS testbed is considered with the SGAM. This consideration enables the analysis of the attacker's actions and the development of countermeasures tailored to each level, thereby strengthening the overall security framework.

III. ASSESSMENT OF CYBER-PHYSICAL TESTBED

The NSGL is connected to the NTNU control center infrastructure, smart house, photovoltaic facilities, and charging/energy storage infrastructure. From these functionalities, the simulations are sent through a network to the control center. A specific feature of the laboratory is the opportunity to integrate real-time simulations and physical power system assets (hardware in-the-loop) with ratings up to 200 kVA, 400 V AC, or 700 V DC. Therefore, the CPS testbed harnesses these state-of-the-art facilities to conduct cyber-physical tests, systematically assessing vulnerabilities and evaluating measures aimed at fortifying the security and resilience of modern power systems.

A. COMPONENTS FOR PENETRATION TESTING AND MODELING OF CYBERATTACKS

Penetration testing and modeling of cyberattacks performed using the adversary setup. It is a workstation with a set of tools for launching cyber threats and exploiting security vulnerabilities such as Kali Linux [40], Wireshark [41], tcpdump [42], and scripts written in the Python programming language [43].

Kali Linux is a powerful and comprehensive operating system that provides a wide range of tools and resources for security professionals, penetration testers, and cybersecurity enthusiasts. Its extensive toolset, regular updates, and active community make it a valuable resource for assessing and enhancing the security of computer systems and networks.

Wireshark and tcpdump are two powerful network analysis tools commonly used by network administrators, security professionals, and IT enthusiasts. They both serve the purpose of capturing and inspecting network traffic. Wireshark is known for its comprehensive graphical user interface and deep protocol analysis capabilities, making it suitable for detailed network troubleshooting and analysis. Tcpdump, on the other hand, is a command-line tool favored for its efficiency and scriptability, making it ideal for quick network captures and automation tasks.

Python is a versatile programming language widely used in penetration testing and cybersecurity due to its simplicity and extensive libraries. Developed scripts used only for ethical and legal purposes, such as assessing penetration vulnerabilities and ethical hacking.

B. THE STRUCTURE OF THE CPS TESTBED

The design of the CPS testbed was conceived to be adaptable to a wide range of ICS spanning across different domains, including Generation, Transmission, Distribution, Distributed Electrical Resources (DER), and Customer Premises [44]. Each structural level is a set of physical and cyber components that provide flexibility and allow to achieve high fidelity of results. Levels of the CPS testbed

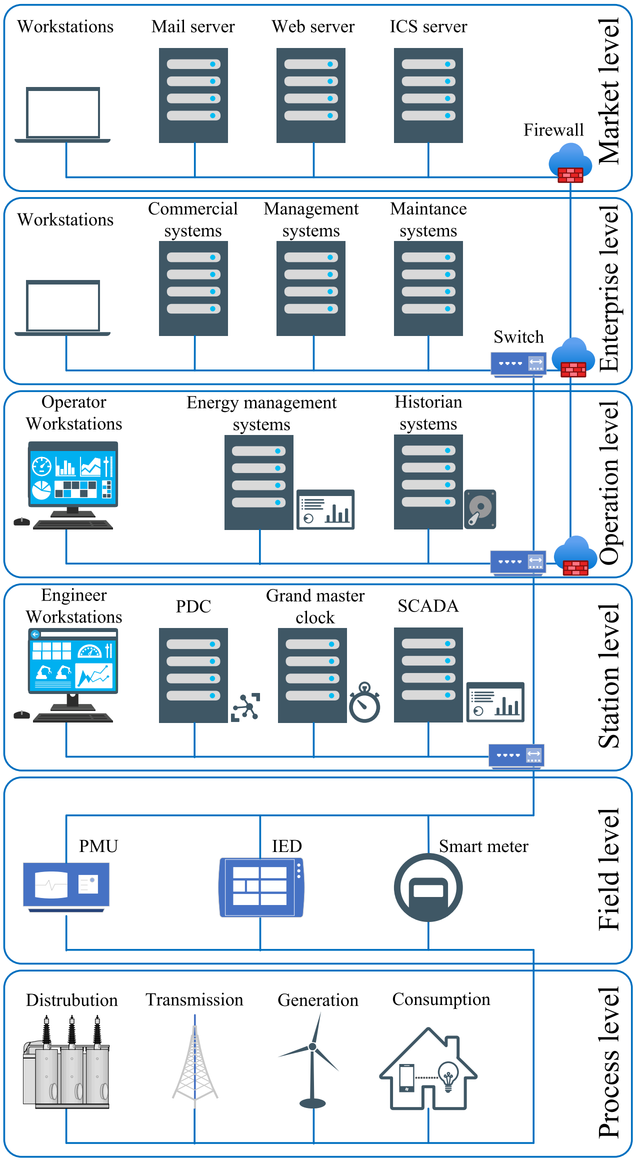


FIGURE 3. Testbed structure.

can interact with each other, which corresponds to a real environment, or can be isolated for testing specific threats. This is achieved by properly configuring network switches, routers, and firewalls. A demilitarized zone (DMZ) has been created inside the CPS testbed, allowing cyber threats to be safely implemented without affecting the rest of the network.

The structure of the CPS testbed, which is a power system divided by levels, is shown in Figure 3, along with the components listed in Table 1. This model takes into consideration all SGAM levels. The construction of the attacks is established according to the CPS testbed structure, which is a hierarchical representation of different attack paths that an attacker could follow to exploit vulnerabilities and reach a specific goal. Start with the primary goal, such as compromising monitoring, protection, control systems, or disrupting power supply, and break it down into sub-goals and attack steps. Considering factors such as system complexity, existing security measures, and the attacker's position helps to create risk scenarios and assess the probability of each attack.

TABLE 1. Physical and cyber components of the NSGL in the NTNU explored by the CPS testbed.

Level Structure	Physical/Hardware layer	Cyber/Protocol layer
Process	Physical power system assets with up to 200 kVA, 400 VAC or 700 VDC	Real-time simulators OPAL-RT represent power system in MATLAB (Simulink)
Field	Local and remote controllers, sensors, and actuators	Virtual controllers, sensors, and actuators
Operation	Grandmaster clock	SEL-5073 PDC and OpenPDC
Station	Workstations	SEL-5702 Synchrowave Operation
Enterprise	NTNU client devices	NTNU local network, software applications
Market	Workstations	Data exchange via network (email, market protocols)

The following sections describe each level in the hierarchical structure of the CPS testbed. These descriptions include information about the characteristics of the level, the cyber and physical components of the CPS testbed, as well as the most potential and unique threats for each level that can be tested and analyzed within the adversary setup.

C. PROCESS LEVEL

This level represents the primary equipment of the power system (switchers, transformers, measuring elements, etc.) as well as physical energy conversion (electricity, solar, heat, water, wind). Equipment of this level can be first subject to physical attacks with the aim to tamper equipment, compromise operation, and safety processes.

NSGL physical equipment was used to study and test threats at the CPS testbed. When physical equipment reaches its limitations in terms of scalability, the replication of power system processes becomes achievable through the utilization of real-time simulators. CPS testbed delves into the capabilities of real-time simulators offered by OPAL-RT [45]. This simulator enables the creation of a virtual power system through the use of applications like MATLAB (Simulink). A virtual environment provides a flexible and efficient platform for conducting power system simulations, effectively overcoming the constraints posed by physical hardware limitations.

Currently, the created adversary setup is not utilized for exploring vulnerabilities at this level. This is because physical threats are the primary concern at this level, and mitigating these threats primarily involves implementing physical security measures [46].

D. FIELD LEVEL

Physical components of the field level are directly connected to the power system infrastructure. It is equipment that protects, controls, and monitors the processes of the power system, mainly through controllers, sensors, and actuators.

Devices at this level receive information about physical processes in the power systems, transmit it to the higher system levels for processing and decision-making. Furthermore, control commands from higher levels are transmitted down to devices at the field level to regulate and control processes.

On the physical side, the CPS testbed in the NSGL at this level used local and remote PMUs, smart meters, and intelligent electronic devices (IED). Considering remote PMUs that are connected using VPN technology allows testing of additional vulnerabilities related to WAMPAC applications. The cyber component is integrated using a real-time simulator from OPAL-RT, facilitating the emulation of diverse devices equipped with both modern and legacy communication protocols, including IEC-61850, C37.118.c2-2011, IEC 60870-5-104, and others.

At the field level, vulnerabilities are primarily linked to factors like weak authentication methods, outdated software, lack of encryption, physical accessibility, insecure firmware, and insufficient monitoring capabilities. The presence of these issues allows attackers to exploit vulnerabilities through the service and network ports of the device, potentially leading to cyberattacks. These attacks often aim at manipulating firmware and configurations, injecting false data, and conducting reconnaissance on components at this level. Notably, these threats frequently involve zero-day exploits within closed-source firmware, commonly developed by power equipment vendors. Consequently, one of the key and distinctive tasks of the adversary setup is to specifically address firmware threats associated with power equipment at this level. The assessment of vulnerabilities and validation of findings are only feasible for modern power system equipment with the latest updates and patches employed within the CPS testbed.

E. STATION LEVEL

The station level has equipment that aggregates information from field level devices, interacts with other elements and systems within the domain, and monitors the overall performance of the processes. It serves as an intermediate tier between the field devices and the higher-level systems. Station level typically handles a larger volume of data, complex control algorithms, and have a higher degree of integration with enterprise IT systems in comparison with the field level.

On the station level, the CPS testbed explores PDCs to aggregate information from previous levels. PDCs are implemented as the workstations with installed and configured software. One of them uses commercial closed-source software SEL-5073 from the Schweitzer Engineering Laboratories (SEL) [47]. On the other, an open-source program is installed - Open PDC [48]. Additionally, according to the requirements in [49], the grandmaster clock is located at this level. The grandmaster clock uses GPS technology to synchronize time and a server with a network reference time is used as an alternate clock server.

While both field and station level cyber threats can have severe consequences, the potential impact may vary. At the field level, successful cyberattacks can disrupt localized power equipment that leads to power outages or compromise secure operations in the vicinity. Station level threats, on the other hand, can have broader implications. Breaches or disruptions at the station level can impact a larger portion of the power grid, affect multiple devices, or disrupt critical control and monitoring functions. The attack vectors employed in cyber threats can also differ. Field level threats may involve attempts to compromise or tamper with individual power system components. Despite this, station level threats can involve more sophisticated attack vectors, including targeted phishing attacks, network intrusions, supply chain attacks, or attempts to exploit vulnerabilities in higher level systems that interface with the station level infrastructure.

At this level, the location of the adversary setup provides an opportunity to exploit vulnerabilities in the network infrastructure, communication protocols, or firewalls, potentially gaining unauthorized access or manipulating control commands and data. In a typical attack strategy, the initial step involves reconnaissance, where the attacker gathers information and assesses vulnerabilities and potential entry points within the target system. Following the reconnaissance phase, the attacker possesses insights into the number and types of devices from preceding levels. The subsequent step involves the execution of threats utilizing the components of the adversary setup. These threats encompass various forms of attacks, including DoS attacks, MITM attacks, and the exploitation of protocol vulnerabilities. The purpose of these studies is to analyze the power system response to unauthorized alterations or manipulations of critical data within station level systems.

F. OPERATION LEVEL

The operation level provides the necessary tools, systems, and functions to ensure WAMPAC functions in the power system. It enables utilities to monitor and control power system operations in real-time, optimize resource utilization, respond to contingencies, and enhance overall performance considering the dynamic nature of the power system. Depending on the domain, this level could also host systems such as Distribution Management Systems (DMS), Energy Management Systems (EMS), Advanced Metering Infrastructure (AMI) headend systems, among others.

NSGL control center that represents the operation level is equipped with SEL-5702 Synchrowave Operations developed by SEL [50]. The software offers real-time monitoring and visualization of synchrophasors within the power system. It provides operators with a clear and intuitive interface to monitor the status of the devices, voltages, currents, and other important system parameters. The software records power system events for analysis, aiding in issue diagnosis and corrective actions. To conduct testing this software operates with the aggregated data from SEL-5073 PDC.

It's important to note that the boundaries between Operation and previous levels can vary depending on specific power system deployments. Threats at the station and operation level are almost similar but have some distinct differences due to the specific roles and functions of each level. Threats at this level aim to compromise or disrupt control commands and data over even a broader area as the systems and networks are responsible for managing grid-wide operations. Cyber threats at the operation level are often more complex and sophisticated due to the extensive data handling, complex control algorithms, and integration with enterprise level systems. Successful cyberattacks here can lead to widespread power system disruptions, impacting multiple substations, and critical control and monitoring functions.

During the tests at this level assume the attacker has access to information about a wide area of power systems and enterprise IT systems that interface with the operation level infrastructure. This position gives access to local and remote devices and systems from neighbor levels and the ability to manipulate a maximum volume of data and commands. The attacker's position at this level is considered a worst-case scenario and therefore requires special attention and the application of measures. Software installed in the adversary setup could conduct vulnerability scanning and identify potential entry points for attackers. Testing of these entry points could be done on both sides of the network, including the external network (internet) and remote access points (local network).

G. ENTERPRISE LEVEL

This level is where business, administrative, and operational systems converge. It includes all systems that exist in the enterprise as commercial, management, and others. Systems on enterprise and operation levels exchange power system information to deal with business decisions, asset management, billing, and forecast operations.

Exploring vulnerabilities associated with the enterprise level involves consideration of clients from the local network. Users are located in different segments of the network, use different devices, and software for connection. Properly and secure network configuration plays a crucial role in this case.

Threats at the enterprise level are more diverse and may include data breaches, regulatory compliance violations, financial fraud, phishing attacks, and supply chain vulnerabilities. Enterprise level threats can affect a broader range of stakeholders, including customers, investors, regulatory bodies, and the organization itself [51].

Connection adversary setup to the NSGL from different local network segments evaluate vulnerabilities that could be launched from enterprise systems. At this level, we consider threats from neighbor systems that could come to operation level systems. The main task for the adversary setup is to identify potential entry points for attackers, such as network connections, employee devices, third-party connections, and external interfaces.

H. INTERACTION WITH MARKET LEVEL

The market level represents processes related to energy trading, pricing, billing, and interactions between different market participants. This level involves a various array of participants, including traditional utilities, renewable energy producers, aggregators, retail energy providers, and consumers. At this level, hardware and software explore commercial and economic challenges that arise during energy generation, transmission, distribution, and consumption. By facilitating energy trading and market operations, the market level contributes to the optimization of the entire power ecosystem.

Determination of attack vectors can be challenging and varies depending on the target system. This level includes multiple scenarios for each attack vector, including different attacker motivations and potential consequences. This includes threats related to data integrity, market manipulation, unauthorized access, and regulatory non-compliance.

The control center facility and software are designed to facilitate data transfer in formats that align with the demands of market and grid operators. Additionally, data transfer can be achieved using dedicated protocols specifically designed for communication with market participants. It can also involve the creation of files in a specific format, which can be sent through programs like corporate or public email clients.

To investigate threats at this level, we consider the adversary setup location within two distinct scenarios. In the first scenario, data transmission originates from the operational or enterprise level, allowing us to assess the potential impact on market participants. In the second scenario, the adversary setup is positioned outside the local network, enabling an analysis of its effects on system components at the operational and enterprise levels. Our primary objective is to scrutinize vulnerabilities related to data exchange, with a specific focus on two critical aspects: phishing attacks and data manipulation. Phishing attacks involve the deceptive targeting of market participants or market operators through misleading emails or messages. Meanwhile, data manipulation concerns unauthorized alterations to market data, pricing, or demand response signals, which could disrupt market operations.

IV. EVALUATION OF ADVERSARY SETUP

A. INTRODUCTION TO THE SETUP

To demonstrate and evaluate the impact of the cyberattacks, three sources of data were chosen. The first source of data is an aggregated dynamic power system model simulated in the real-time digital simulator, OPAL-RT. The model is an equivalent representation of the Nordic power grid and is called Nordic44 (N44) [52]. It consists of 44 buses, 28 loads, 80 generators, and 79 branches (including 12 transformer branches and 67 overhead transmission line branches). Another data source is from the real power grid, specifically local physical PMUs installed in the NSGL and connected to the low-voltage power grid. The last data source involves the playback of previously captured data frames using the functionality of virtual PMUs. These captured data frames originate from various PMUs located in different regions of the EU, all of which are connected to the NSGL. The power grid, represented by all data sources, corresponds to the process level shown in Figure 3.

In considered cases equipment at the field level is represented by virtual and physical PMU. For data exchange between virtual and local physical PMUs, PDCs, and software in the control room protocol C37.118.2-2011 [53] was used. The PMUs, both virtual and physical, send data at a rate of 50 samples per second. This high sampling rate is used in real-world power grids that allow real-time monitoring and control of the power system.

The station level encompasses the PDCs and the grandmaster clock. The primary role of the PDCs is to collect and consolidate data from all PMUs and subsequently transmit this data to the software situated at the Operation level. The grandmaster clock, leveraging GPS technology, is responsible for maintaining precise time synchronization across the various components of the power system under investigation.

The control room is located on the Operation level and equipped with SEL Synchrowave Operations, which is a Wide Area Monitoring System (WAMS) software described in the previous section. This program receives and stores information from PDCs or individual PMUs and operates with a significantly higher amount of data compared to a traditional SCADA system.

Each level of the testbed has its own local network, which is protected by a firewall. A DMZ has been created at the operation level in the control room. This allows secure experiments to be carried out without harming the rest of the NTNU local network.

Implemented attack vectors are based on the attacker's position, communication protocol, and network. To assess the impact of cyberattacks, a case scenario was considered in which the adversary setup has access to the network traffic at the operational and station levels. This scenario mirrors the attacker's position observed in the real-life incident known as BlackEnergy 3, which occurred in Ukraine in 2015 [54]. By situating the adversary setup at this position, five distinct cyberattacks were executed using the first virtual environment and then the physical. The attack strategies and their impacts are analyzed in the following sections.

B. ATTACK 1 – PASSIVE RECONNAISSANCE

Passive reconnaissance is a critical initial step in the process of launching cyberattacks on power system components. It involves gathering information about the target system without directly interacting with it, hence the term 'passive'. This method is often used by attackers to avoid detection while gaining valuable insights about the available system components. Attackers can gain insights into the system's operations and identify potential weak points.

The communication protocol between PMU, PDC, and SEL Synchrowave software can be monitored by the attacker as well as all network traffic. Wireshark and tcpdump utilities were used to monitor network traffic in promiscuous mode from the adversary setup. The functionality of the software allows to filter the necessary data packets from all traffic in the communication channel. Additionally, python code has been specifically designed to detect traffic related to the C37.118.c2-2011 protocol. It enables the identification of data and configuration frames utilized by the target element. It allows the gathering of crucial information about the target system elements.

C. ATTACK 2 – ACTIVE RECONNAISSANCE

Active reconnaissance is a more direct approach in the process of launching cyberattacks on power systems. Unlike passive reconnaissance, it involves interacting with the target system to gather more specific information. This interaction, however, increases the risk of detection.

The developed code leverages the C37.118.c2-2011 protocol and allows specific commands to be sent to the target system as:

- IP and Port Scanning: The code uses the functionality of the Scapy library to scan a range of IP addresses. After identifying active IP addresses, the code performs a port scan to identify open ports. The selection of port numbers for this scan can be tailored to either a typical or a specific range, providing flexibility in the scanning process.
- MAC Address Retrieval: For further attacks and advanced network operations, the code retrieves the MAC addresses of devices in the target system.
- Retrieving and parsing configuration frames: The code requests various types of configuration frames from the PMUs. It then parses the received answer, which is crucial for identifying the types and numbers of the parameters.

To evaluate the received configuration frames, the PMU Connection Tester software [55], a component of OPEN-PDC, was also employed. This software offers advanced features for validating, testing, and troubleshooting connections and data streams from PMUs. It also provides real-time graphical visualization of synchophasor data. However, these capabilities could potentially be exploited by an attacker to gain information about PMU configuration.

D. ATTACK 3– TCP PACKET INJECTION

TCP packet injection, a method of cyberattack, involves an unauthorized party injecting false data into a network data stream. The manipulation of data and commands within a level can result in incorrect actions by personnel or misinterpretation of data. Furthermore, sending packets to lower levels, such as the field or process levels, can disrupt device operations or alter the functioning of the power system.

After analyzing traffic and selecting PMU for the attack based on information obtained from the previous attacks, the goal is to transmit fabricated TCP packets that mimic the actual data in parallel with the authentic PMU data. These fabricated packets should be designed in a way that the system perceives them as authentic and originating from a trusted source.

E. ATTACK 4– ARP POISONING, MITM ATTACK

In the landscape of cyberattacks on power systems, Address Resolution Protocol (ARP) poisoning stands as a formidable threat. This type of attack, also known as a MITM attack, involves an attacker intercepting and potentially altering the communication between two parties without their knowledge.

For the attack simulation, a code was developed that performs the following tasks:

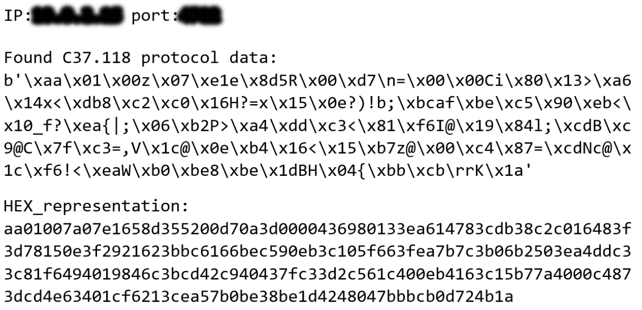
1) ARP table poisoning: To poison the ARP tables of the target devices. This allows the attacker to position themselves in the middle of the communication channel between the two devices, effectively becoming a 'man in the middle'.
2) Traffic sniffing and filtering: Once in position, developed code begins to sniff all the network traffic coming from the target PMU. The traffic is then filtered to isolate the C37.118.c2-2011 protocol.
3) Protocol parsing: The filtered C37.118.c2-2011 protocol data is then parsed with the help of saved configuration frame obtained from Attack 2 and standard documentation that describes packet structure. The parsed data provides valuable insights about the system and can be used for parameter modifications and further implementation of stealthy attacks.

Manipulation with the data can be performed 'on the fly', allowing the attacker to alter the system's operation in real-time.

F. ATTACK 5 – INTERRUPTION IN COMMUNICATION

This type of attack aims to disrupt the communication between devices. It represents one of the most potent threats as the DOS attack in the realm of cyberattacks on power systems. To analyze the consequences of this attack two strategies for interruption were used.

For the first strategy, a code was developed to poison the ARP tables of both the target device and the gateway. ARP serves as a protocol that maps an IP address to a physical address on the local network, commonly referred to as a MAC address. By leveraging information obtained from previous attacks regarding MAC addresses within the network, the ARP tables are poisoned, thereby altering the mapping. This alteration causes traffic redirection in the network specifically without forwarding it to the original destination, as seen in Attack 4. However, in this scenario, the redirection is not the end goal but rather a tool to interrupt communication between devices.



```
IP:[redacted] port:[redacted]

Found C37.118 protocol data:
b'\xaa\x01\x00z\x07\xe1e\x8d5R\x00\xd7\n=\x00\x00Ci\x80\x13>\xa6
\x14x<\xdb8\xc2\xc0\x16H?=x\x15\x0e?)!b;\xbcaf\xbe\xc5\x90\xeb<\
x10_f?\xea{|;\x06\xb2P>\xa4\xdd\xc3<\x81\xf6I@\x19\x84l;\xcdB\xc
9@C\x7f\xc3=,V\x1c@\x0e\xb4\x16<\x15\xb7z@\x00\xc4\x87=\xcdNc@\x
1c\xf6!<\xeaW\xb0\xbe8\xbe\x1dBH\x04{\xbb\xcb\rrK\x1a'

HEX_representation:
aa01007a07e1658d355200d70a3d0000436980133ea614783cdb38c2c016483f
3d78150e3f2921623bbc6166bec590eb3c105f663fea7b7c3b06b2503ea4ddc3
3c81f6494019846c3bcd42c940437fc33d2c561c400eb4163c15b77a4000c487
3dcd4e63401cf6213cea57b0be38be1d4248047bbbcb0d724b1a
```

FIGURE 4. Filtering C37.118.c2-2011 protocol in the network.

The second strategy involves leveraging the functionality of the C37.118.c2-2011 protocol, which permits the sending of command frames. In pursuit of communication interruption, we explore commands capable of disabling or enabling real-time data transmission, utilizing the capabilities of the PMU Connection Tester software for this purpose.

Evaluation of the described above attacks gives insights into their effectiveness, the potential for damage, and the resilience of the power systems. This analysis not only underscores the severity of the threats but also highlights the importance of robust security measures and the need for continual vigilance in the face of evolving cyber threats.

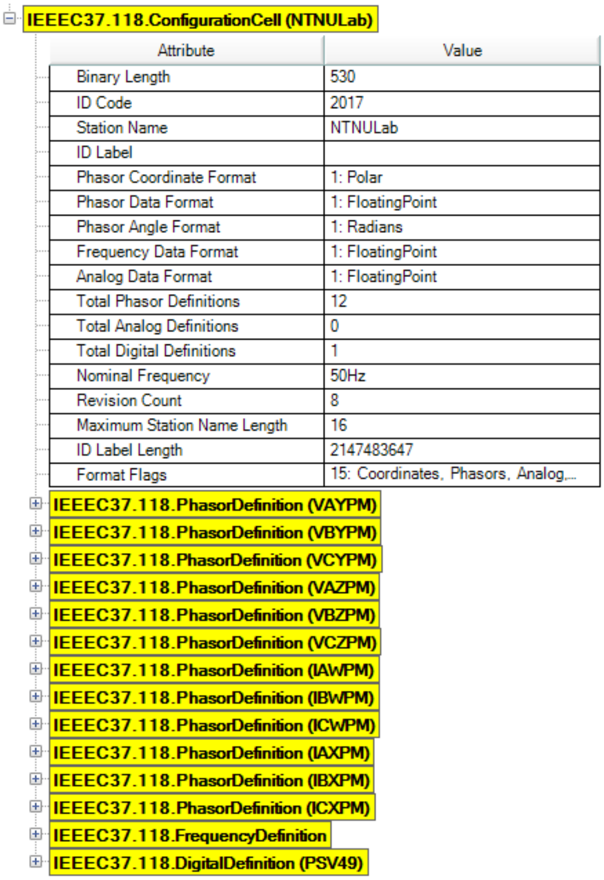
V. RESULTS

The section provides the analysis of the results of the five simulated cyberattacks which methodologies were described above. Each attack, with its unique approach and potential for disruption, leaves a distinct footprint on the power system operation. By examining these footprints, system operators and engineers can gain valuable insights into the impacts of each attack and the potential countermeasures that could mitigate these threats.

A. ATTACK 1 – PASSIVE RECONNAISSANCE

The experiment involved the analysis of IPs and ports in the network, along with C37.118.c2-2011 traffic filtering using three types of PMUs. The physical and virtual PMUs from OPAL-RT were linked to the actual network, while the virtual PMUs from OPEN-PDC were connected to the virtual network. The analysis of monitored IPs and ports identified all data exchange, along with their services. This resulted in a comprehensive map of the network infrastructure. Subsequently, the implementation of C37.118.c2-2011 traffic filtering detected the presence of synchrophasor data in each network. The result of the detection C37.118.c2-2011 protocol in the network is shown in Figure 4. Communication protocol C37.118.2-2011 is unencrypted making it possible to further data parsing that is being transmitted within the communication network.

Detecting passive reconnaissance can be challenging due to its non-intrusive nature. In our case this attack was undetected. To protect the power system network from



IEEEC37.118.ConfigurationCell (NTNULab)

Attribute	Value
Binary Length	530
ID Code	2017
Station Name	NTNULab
ID Label	
Phasor Coordinate Format	1: Polar
Phasor Data Format	1: FloatingPoint
Phasor Angle Format	1: Radians
Frequency Data Format	1: FloatingPoint
Analog Data Format	1: FloatingPoint
Total Phasor Definitions	12
Total Analog Definitions	0
Total Digital Definitions	1
Nominal Frequency	50Hz
Revision Count	8
Maximum Station Name Length	16
ID Label Length	2147483647
Format Flags	15: Coordinates, Phasors, Analog,...

IEEEC37.118.PhasorDefinition (VAYPM)
IEEEC37.118.PhasorDefinition (VBYPM)
IEEEC37.118.PhasorDefinition (VCYPM)
IEEEC37.118.PhasorDefinition (VAZPM)
IEEEC37.118.PhasorDefinition (VBZPM)
IEEEC37.118.PhasorDefinition (VCZPM)
IEEEC37.118.PhasorDefinition (IAWPM)
IEEEC37.118.PhasorDefinition (IBWPM)
IEEEC37.118.PhasorDefinition (ICWPM)
IEEEC37.118.PhasorDefinition (IAXPM)
IEEEC37.118.PhasorDefinition (IBXPM)
IEEEC37.118.PhasorDefinition (ICXPM)
IEEEC37.118.FrequencyDefinition
IEEEC37.118.DigitalDefinition (PSV49)

FIGURE 5. **Configuration frame of PMU using PMU Connection Tester software.**

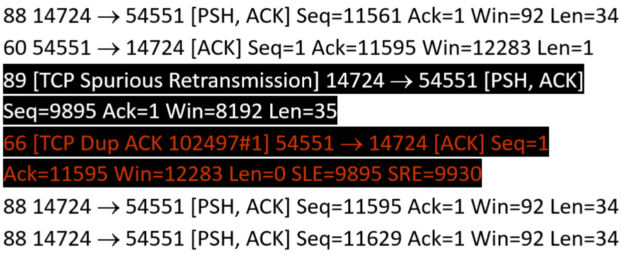
passive reconnaissance, the following measures can be implemented:

- Network segmentation. Dividing the network into smaller segments can limit the scope of reconnaissance and contain the potential impact.
- Encryption. Employing encryption protocols for data transmission to ensure the confidentiality and integrity of information, making it more challenging for attackers to monitor or manipulate data in transit.
- Regular auditing. Regularly auditing the network logs can help identify any unusual activity.

By implementing these measures, the security of the power system network can be significantly enhanced and made more resilient against passive reconnaissance.

B. ATTACK 2 – ACTIVE RECONNAISSANCE

In this experiment, the developed code interface with real and virtual PMUs from OPEN-PDC, requesting configuration frames from detected devices in the previous attack and parsing them according to the C37.118.c2-2011 protocol. Using the adversary setup we successfully received a hex string with a configuration frame and parsed it, enabling the identification of critical information essential for further data analysis. PMU Connection Tester software was also employed for this task and received a configuration frame from the local physical PMU shown in Figure 5.



```
88 14724 → 54551 [PSH, ACK] Seq=11561 Ack=1 Win=92 Len=34
60 54551 → 14724 [ACK] Seq=1 Ack=11595 Win=12283 Len=1
89 [TCP Spurious Retransmission] 14724 → 54551 [PSH, ACK]
Seq=9895 Ack=1 Win=8192 Len=35
66 [TCP Dup ACK 102497#1] 54551 → 14724 [ACK] Seq=1
Ack=11595 Win=12283 Len=0 SLE=9895 SRE=9930
88 14724 → 54551 [PSH, ACK] Seq=11595 Ack=1 Win=92 Len=34
88 14724 → 54551 [PSH, ACK] Seq=11629 Ack=1 Win=92 Len=34
```

FIGURE 6. **Captured spurious retransmission using wireshark.**

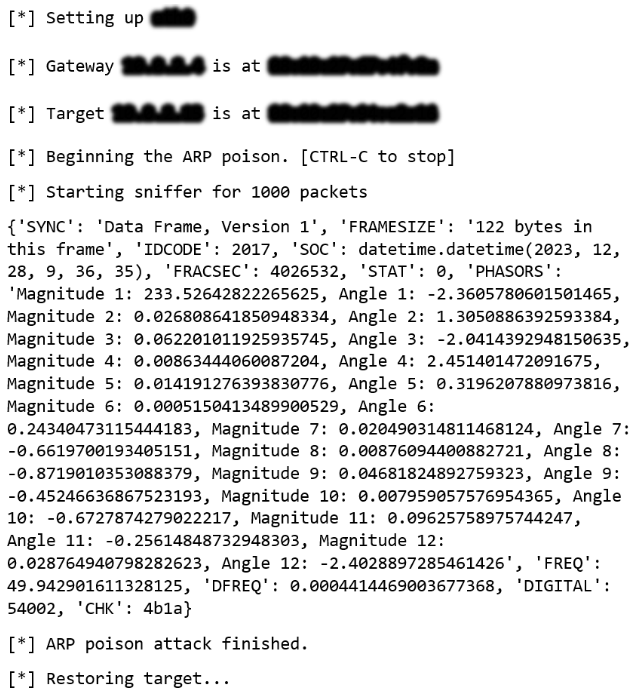
Detection of active reconnaissance in power systems is crucial for preemptive action against potential threats. In this experiment, requests for a configuration frame from the adversary setup were detected in the communication channel. Additionally, TCP handshakes and SYN packets were observed during IP and port scanning. Such anomalies or unusual querying patterns seeking sensitive data from PMUs could trigger alerts for further investigation. To prevent active reconnaissance attacks, additional several measures can be implemented in combination with the previous:

- Hide network services. Disabling Internet Control Message Protocol (ICMP) messages can indeed make a device less visible.
- Utilizing specific ports. Using unique ports can make them more challenging to determine.
- Request control. Allow requests only from verified sources and disable periodic transmission of configuration frames.
- Firewalls and Intrusion Detection Systems (IDS). These can help detect and block scanning activities.

C. ATTACK 3 – TCP PACKET INJECTION

TCP injection attack was attempted by injecting modified data using the C37.118.c2-2011 protocol into the communication channel of the power system network. The tcpdump and Wireshark were used to detect and confirm the presence of the modified packet in the communication channel. This packet was detected by Wireshark but flagged down as spurious retransmission as shown in Figure 6. This resulted in the packet not being accepted and therefore dropped. The sequence number is sensitive and must be the exact next number, any missteps will cause the packet to be flagged out and not accepted. As a result, the packet wasn't received by the PDC or visualization software and no disturbances were gathered.

Analyzing the negative result of the single TCP Packet Injection attack allows to make a few conclusions. Most likely the time necessary for the compilation of the Python code is longer than the creation of the new sequence numbers by the TCP protocol. For successful attack implementation, it is necessary to use a more advanced attack strategy. This strategy should involve additional attack steps that block data transmission from the targeted PMU or contain



```
[*] Setting up [redacted]

[*] Gateway [redacted] is at [redacted]

[*] Target [redacted] is at [redacted]

[*] Beginning the ARP poison. [CTRL-C to stop]

[*] Starting sniffer for 1000 packets

{'SYNC': 'Data Frame, Version 1', 'FRAMESIZE': '122 bytes in
this frame', 'IDCODE': 2017, 'SOC': datetime.datetime(2023, 12,
28, 9, 36, 35), 'FRACSEC': 4026532, 'STAT': 0, 'PHASORS':
'Magnitude 1: 233.52642822265625, Angle 1: -2.3605780601501465,
Magnitude 2: 0.026808641850948334, Angle 2: 1.3050886392593384,
Magnitude 3: 0.062201011925935745, Angle 3: -2.0414392948150635,
Magnitude 4: 0.00863444060087204, Angle 4: 2.451401472091675,
Magnitude 5: 0.014191276393830776, Angle 5: 0.3196207880973816,
Magnitude 6: 0.0005150413489900529, Angle 6:
0.24340473115444183, Magnitude 7: 0.020490314811468124, Angle 7:
-0.6619700193405151, Magnitude 8: 0.00876094400882721, Angle 8:
-0.8719010353088379, Magnitude 9: 0.04681824892759323, Angle 9:
-0.45246636867523193, Magnitude 10: 0.007959057576954365, Angle
10: -0.6727874279022217, Magnitude 11: 0.09625758975744247,
Angle 11: -0.25614848732948303, Magnitude 12:
0.028764940798282623, Angle 12: -2.4028897285461426', 'FREQ':
49.942901611328125, 'DFREQ': 0.0004414469003677368, 'DIGITAL':
54002, 'CHK': 4b1a}

[*] ARP poison attack finished.

[*] Restoring target...
```

FIGURE 7. ARP poisoning attack with data parsing.

more precise sequence number prediction. Advanced attack strategy overcomes spurious retransmission detection and allows observation of modified data with visualization software in the control room. In this case, countermeasures and protection strategies should be developed and evaluated to avoid inaccurate monitoring, control issues, or system instability.

In case of a successful TCP packet injection attack authors in [36], propose several protective measures that could be implemented in addition to the previous:

- Model-Based Detection. These algorithms rely on pre-defined models of expected grid behavior to detect deviations.
- Data-Driven Detection. This approach analyzes historical data to identify irregularities and detect unauthorized data injections.

D. ATTACK 4 – ARP POISONING, MITM ATTACK

In the conducted experiment, the MITM attack was executed using ARP poisoning techniques. The primary goal of this attack was to intercept and sniff the traffic between PMU and PDC. During the MITM attack, the traffic was successfully intercepted and captured by the attacker from the adversary setup. Subsequently, Figure 7 shows the data that comes from PMU to PDC through the adversary setup. These data were identified and parsed in real-time using previously acquired information, which was obtained during previous attacks. The significance of this attack lies in the adversary setup ability to read and interpret data 'on the fly'. This capability allows the attacker to gain a comprehensive understanding of the transmitted data and overcome challenges with data modifications in real-time described in Attack 3. By intercepting and parsing data during transmission, the attacker gains the ability to create stealthy attacks, posing a significant threat to the integrity and reliability of the power system operational data.

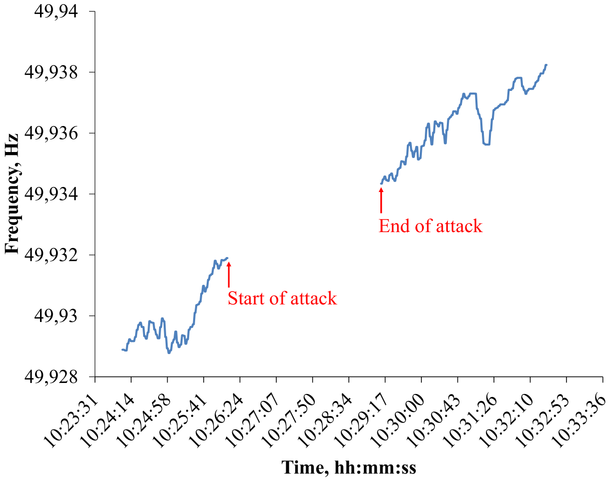


FIGURE 8. Interruption in data exchange between PDC and PMU.

Detecting a MITM attack, especially when ARP poisoning is employed, requires scrutiny of network traffic. Anomalies, such as ARP poisoning signs and a large amount of fake ARP replies in the communication channel were detected during this attack. A combination of protective measures should be implemented to mitigate the risk of MITM attacks. Measures discussed earlier in the 'TCP packet injection' attack can be utilized to defend against attacks related to false data injection. In addition, to mitigate the risk associated with ARP table poisoning authors in [37], propose several protective measures that could be implemented:

- Firewalls and Intrusion Prevention Systems (IPS). Implement robust firewalls and IPS to monitor and filter network traffic, identifying and blocking malicious packets associated with DOS attacks.
- Traffic filtering and rate limiting. Employ network traffic filtering mechanisms to block or limit excessive traffic to essential systems, preventing overload from attacks.
- Traffic diversification and honeypots. Distribute network traffic across multiple servers or pathways to reduce the impact of concentrated traffic, making it harder for attackers to overwhelm a single point in the network.

E. ATTACK 5 – INTERRUPTION IN COMMUNICATION

The case study aimed to disrupt the communication between PMU and PDC using ARP table poisoning. The attack was successful in interrupting the communication between PMU and PDC. Figure 8 depicts frequency as one of the affected parameters from the PDC side, along with the start and end times of the attack. During the attack window,

TABLE 2. Results of cyberattacks.

ID	Attack type	Aim	Result	Detection	Proposed measures
1	Passive reconnaissance	- Monitoring of all active hosts, ports, and C37.118.c2-2011 protocol	Successful	- No trace	- Network segmentation - Encryption - Regular auditing
2	Active reconnaissance	- Retrieve MAC addresses and configuration frames - Scan all available IP addresses and ports	Successful	- Logs with requests from the adversary setup - TCP handshakes and SYN packets	- Hide network services - Utilizing specific ports - Control sensitive information - Firewalls and Intrusion Detection Systems
3	TCP packet injection	- Send false data to PDC that mimic data from PMU	Unsuccessful	- Packet was flagged down as spurious retransmission, not being accepted by the TCP protocol and dropped	- Model-Based Detection - Data-Driven Detection
4	MITM attack	- Intercept, sniff, parse, and modify the traffic between PMU and PDC	Successful	- ARP poisoning signs, large amount of fake ARP replies	- Firewalls and Intrusion Prevention Systems - Traffic filtering and rate limiting - Traffic diversification and honeypots
5	Interruption in communication	- Break the communication between PMU and PDC using ARP table poisoning	Successful	- The same traces as those observed in Attack 4	- Similar measures described in Attack 4

communication between PMU and PDC was effectively disrupted, resulting in a loss of data transmission.

Detection of attacks that disrupt communication between critical components in power systems requires vigilant monitoring. Network traffic analysis tools can detect unusual patterns in ARP requests and responses, signaling potential ARP table poisoning. In this case, similar traces were observed as during Attack 4, with a significant volume of fake ARP replies in the communication channel. Consequently, comparable measures could be applied to address this case as well. By implementing these preventive measures and maintaining a proactive stance through constant monitoring, the risk of successful attacks aiming to disrupt communication between PMUs and PDCs in power systems can be significantly reduced.

The case studies highlight the five cyberattacks conducted within the context of the commonly used but vulnerable C37.118.c2-2011 protocol. The summary of the results is presented in Table 2. The considered protocol is unencrypted, like others most commonly used in power systems, making it easy to hide corrupted data or commands for attackers. To overcome these challenges in the future control centers with WAMPAC applications must leverage advanced tools and modern technologies. Prior to real-world implementation, testbeds serve as crucial platforms for assessing the efficacy of such tools and technologies. Their evaluation encompasses aspects of cybersecurity, anomaly detection, as well as the maintenance of power system processes, including data analytics, optimization, fault detection, and demand and forecast management.

VI. CONCLUSION AND FUTURE WORK

A testbed is a popular solution for conducting experiments in constrained real test environments. This paper has introduced the CPS testbed based on the SGAM and the exploration of the adversary setup within the NSGL at the NTNU. By aligning with the SGAM framework, this research delves into representing classification, assessment of threats within the structure of the CPS testbed, and analyzing varying vulnerabilities at different structural levels. Notably, the strategic placement of the adversary setup within levels permits a comprehensive examination of cyber-physical vulnerabilities within simulated systems, thus facilitating the evaluation of protective measures.

The case studies focused on the analysis of the five cyberattack simulations using the adversary setup. These attacks affected the control center infrastructure, representing operational and station levels based on the SGAM structure. The objective of these attacks was to emulate one of the typical attacker's strategies. Four attacks were successful, demonstrating the robustness of the adversary setup and allowing a potential attacker to obtain crucial information about the power system, along with the ability to manipulate it further. However, the proposed measures help to minimize risks and counteract these launched cyberattacks.

Future work involves expanding upon the foundational attack scenarios introduced here, delving into the development of more intricate and stealthy attack scenarios. Utilizing the proposed structure of the testbed will be developed and implemented a defender setup that would have the capability to detect and mitigate intricate, covert attack vectors. Then will be provided a vulnerability assessment with the position of attacker and defender according to the SGAM structure. Furthermore, additional software and modern technologies, like artificial intelligence will be implemented to manage a vast volume of information and detect abnormal conditions that play a significant role in empowering operators.

REFERENCES

[1] X. Fang, S. Misra, G. Xue, and D. Yang, "Smart grid—The new and improved power grid: A survey," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 4, pp. 944–980, 4th Quart., 2012.

[2] S. Vahidi, M. Ghafouri, M. Au, M. Kassouf, A. Mohammadi, and M. Debbabi, "Security of wide-area monitoring, protection, and control (WAMPAC) systems of the smart grid: A survey on challenges and opportunities," *IEEE Commun. Surveys Tuts.*, vol. 25, no. 2, pp. 1294–1335, 2nd Quart., 2023.

[3] Nordex. (2022). *Update on Cyber Security Incident*. [Online]. Available: https://www.nordex-online.com/en/2022/04/update-on-cyber-security-incident/

[4] P. K. R. Maddikunta, Q.-V. Pham, P. B, N. Deepa, K. Dev, T. R. Gadekallu, R. Ruby, and M. Liyanage, "Industry 5.0: A survey on enabling technologies and potential applications," *J. Ind. Inf. Integr.*, vol. 26, Mar. 2022, Art. no. 100257.

[5] R. V. Yohanandhan, R. M. Elavarasan, R. Pugazhendhi, M. Premkumar, L. Mihet-Popa, and V. Terzija, "A holistic review on cyber-physical power system (CPPS) testbeds for secure and sustainable electric power grid—Part—I: Background on CPPS and necessity of CPPS testbeds," *Int. J. Electr. Power Energy Syst.*, vol. 136, Mar. 2022, Art. no. 107718.

[6] R. V. Yohanandhan, R. M. Elavarasan, R. Pugazhendhi, M. Premkumar, L. Mihet-Popa, and V. Terzija, "A holistic review on cyber-physical power system (CPPS) testbeds for secure and sustainable electric power grid—Part—II: Classification, overview and assessment of CPPS testbeds," *Int. J. Electr. Power Energy Syst.*, vol. 137, May 2022, Art. no. 107721.

[7] M. H. Cintuglu, O. A. Mohammed, K. Akkaya, and A. S. Uluagac, "A survey on smart grid cyber-physical system testbeds," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 446–464, 1st Quart., 2017.

[8] A. A. Smadi, B. T. Ajao, B. K. Johnson, H. Lei, Y. Chakhchoukh, and Q. Abu Al-Haija, "A comprehensive survey on cyber-physical smart grid testbed architectures: Requirements and challenges," *Electronics*, vol. 10, no. 9, p. 1043, Apr. 2021.

[9] P. K. Pattnaik, R. Kumar, and S. Pal, *Internet of Things and Analytics for Agriculture*, vol. 2. Singapore: Springer, 2020.

[10] B. Vaagensmith, V. K. Singh, R. Ivans, D. L. Marino, C. S. Wickramasinghe, J. Lehmer, T. Phillips, C. Rieger, and M. Manic, "Review of design elements within power infrastructure cyber-physical test beds as threat analysis environments," *Energies*, vol. 14, no. 5, p. 1409, Mar. 2021.

[11] N. Chowdhury and V. Gkioulos, "Cyber security training for critical infrastructure protection: A literature review," *Comput. Sci. Rev.*, vol. 40, May 2021, Art. no. 100361.

[12] (2012). *National Scada Test Bed*. [Online]. Available: https://www.energy.gov/oe/national-scada-test-bed

[13] G. Elbez, H. B. Keller, and V. Hagenmeyer, "A cost-efficient software testbed for cyber-physical security in IEC 61850-based substations," in *Proc. IEEE Int. Conf. Commun., Control, Comput. Technol. Smart Grids (SmartGridComm)*, Oct. 2018, pp. 1–6.

[14] A. Hahn, A. Ashok, S. Sridhar, and M. Govindarasu, "Cyber-physical security testbeds: Architecture, application, and evaluation for smart grid," *IEEE Trans. Smart Grid*, vol. 4, no. 2, pp. 847–855, Jun. 2013.

[15] A. Ashok, P. Wang, M. Brown, and M. Govindarasu, "Experimental evaluation of cyber attacks on automatic generation control using a CPS security testbed," in *Proc. IEEE Power Energy Soc. Gen. Meeting*, Jul. 2015, pp. 1–5.

[16] G. Ravikumar, B. Hyder, J. R. Babu, K. Khanna, M. Govindarasu, and M. Parashar, "CPS testbed architectures for WAMPAC using industrial substation and control center platforms and attack-defense evaluation," in *Proc. IEEE Power Energy Soc. Gen. Meeting (PESGM)*, Jul. 2021, pp. 1–5.

[17] A. Sahu, P. Wlazlo, Z. Mao, H. Huang, A. Goulart, K. Davis, and S. Zonouz, "Design and evaluation of a cyber-physical testbed for improving attack resilience of power systems," *IET Cyber-Phys. Syst., Theory Appl.*, vol. 6, no. 4, pp. 208–227, Dec. 2021.

[18] T. Becejac, C. Eppinger, A. Ashok, U. Agrawal, and J. O'Brien, "PRIME: A real-time cyber-physical systems testbed: From wide-area monitoring, protection, and control prototyping to operator training and beyond," *IET Cyber-Phys. Syst., Theory Appl.*, vol. 5, no. 2, pp. 186–195, Jun. 2020.

[19] U. Cali, M. Kuzlu, M. Pipattanasomporn, J. Kempf, L. Bai, U. Cali, M. Kuzlu, M. Pipattanasomporn, J. Kempf, and L. Bai, "Smart grid standards and protocols," in *Digitalization of Power Markets and Systems Using Energy Informatics*. Cham, Switzerland: Springer, 2021, pp. 39–58.

[20] NTNU and SINTEF. *The National Smart Grid Laboratory*. Accessed: Mar. 7, 2024. [Online]. Available: https://www.ntnu.edu/smartgrid

[21] T. I. Strasser, E. C. de Jong, and M. Sosnina, *European Guide To Power System Testing: The ERIGrid Holistic Approach for Evaluating Complex Smart Grid Configurations*. Cham, Switzerland: Springer, 2020.

[22] M. Brand, S. Ansari, F. Castro, R. Chakra, B. H. Hassan, C. Krüger, D. Babazadeh, and S. Lehnhof, "A framework for the integration of ICT-relevant data in power system applications," in *Proc. IEEE Milan PowerTech*, Jun. 2019, pp. 1–6.

[23] C. Foglietta, D. Masucci, C. Palazzo, R. Santini, S. Panzieri, L. Rosa, T. Cruz, and L. Lev, "From detecting cyber-attacks to mitigating risk within a hybrid environment," *IEEE Syst. J.*, vol. 13, no. 1, pp. 424–435, Mar. 2019.

[24] V. Terzija, *Wide Area Monitoring Protection and Control-WAMPAC*. Edison, NJ, USA: IET, 2007.

[25] E. Ukwandu, M. A. B. Farah, H. Hindy, D. Brosset, D. Kavallieros, R. Atkinson, C. Tachtatzis, M. Bures, I. Andonovic, and X. Bellekens, "A review of cyber-ranges and test-beds: Current and future trends," *Sensors*, vol. 20, no. 24, p. 7148, Dec. 2020.

[26] *The NIS 2 Directive*. Accessed: Mar. 7, 2024. [Online]. Available: https://www.nis-2-directive.com/

[27] CERT-EU. (2023). *Threat Landscape Report 2023Q2—Main Malicious Activities*. [Online]. Available: https://cert.europa.eu/publications/threat-intelligence/2023

[28] EUA Cybersecurity. (2022). *ENISA Threat Landscape 2022*. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

[29] O. Andreeva, S. Gordeychik, G. Gritsai, O. Kochetova, E. Potseluevskaya, S. I. Sidorov, and A. A. Timorin (2016). *Industrial Control Systems Vulnerabilities Statistics*. Accessed: Mar. 11, 2024. [Online]. Available: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2016/07/07190426/KL_REPORT_ICS_Statistic_vulnerabilities.pdf

[30] R. O. Harmash. (Feb. 10, 2023). *Russian Missiles Pound Ukraine's Energy System, Force Power Outages*. [Online]. Available: https://www.reuters.com/world/europe/russian-forces-strike-ukraine-air-raid-sirens-wail-across-country-2023-02-10/

[31] A. Ashok, M. Govindarasu, and J. Wang, "Cyber-physical attack-resilient wide-area monitoring, protection, and control for the power grid," *Proc. IEEE*, vol. 105, no. 7, pp. 1389–1407, Jul. 2017.

[32] R. Leszczyna and R. Leszczyna, "Cybersecurity standards applicable to the electricity sector," in *Cybersecurity in the Electricity Sector: Managing Critical Infrastructure*. Cham, Switzerland: Springer, 2019, pp. 59–86.

[33] C.-W. Ten, C.-C. Liu, and G. Manimaran, "Vulnerability assessment of cybersecurity for SCADA systems," *IEEE Trans. Power Syst.*, vol. 23, no. 4, pp. 1836–1846, Nov. 2008.

[34] J. Searle, G. Rasche, A. Wright, and S. Dinnage. (2016). *NESCOR Guide to Penetration Testing for Electric Utilities*. Accessed: Mar. 11, 2024. [Online]. Available: https://smartgrid.epri.com/doc/NESCORGuidetoPenetrationTestingforElectricUtilities-v3-Final.pdf

[35] H. Zhang, B. Liu, and H. Wu, "Smart grid cyber-physical attack and defense: A review," *IEEE Access*, vol. 9, pp. 29641–29659, 2021.

[36] A. S. Musleh, G. Chen, and Z. Y. Dong, "A survey on the detection algorithms for false data injection attacks in smart grids," *IEEE Trans. Smart Grid*, vol. 11, no. 3, pp. 2218–2234, May 2020.

[37] A. Huseinovic, S. Mrdovic, K. Bicakci, and S. Uludag, "A survey of denial-of-service attacks and solutions in the smart grid," *IEEE Access*, vol. 8, pp. 177447–177470, 2020.

[38] A. Ashok, M. Govindarasu, and V. Ajjarapu, "Attack-resilient measurement design methodology for state estimation to increase robustness against cyber attacks," in *Proc. IEEE Power Energy Soc. Gen. Meeting (PESGM)*, Jul. 2016, pp. 1–5.

[39] S. Nabavi, J. Zhang, and A. Chakrabortty, "Distributed optimization algorithms for wide-area oscillation monitoring in power systems using interregional PMU-PDC architectures," *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2529–2538, Sep. 2015.

[40] G. Najera-Gutierrez and J. A. Ansari, *Web Penetration Testing With Kali Linux: Explore the Methods and Tools of Ethical Hacking With Kali Linux*. Birmingham, U.K.: Packt Publishing, 2018.

[41] J. Beale, A. Orebaugh, and G. Ramirez, *Wireshark & Ethereal Network Protocol Analyzer Toolkit*. Amsterdam, The Netherlands: Elsevier, 2006.

[42] *Tcpdump*. Accessed: Mar. 11, 2024. [Online]. Available: https://www.tcpdump.org/

[43] G. van Rossum and F. L. Drake, *Python Tutorial*, vol. 620. Amsterdam, The Netherlands: Centrum voor Wiskunde en Informatica, 1995.

[44] *SG-CG M490 H Smart Grid Information Security*, ESG-CC Group, CEN-CENELEC-ETSI Smart Grid Coordination Group, Brussels, Belgium, 2018.

[45] ORT. *OP5705XG Versatile Real-Time Digital Simulator*. Accessed: Mar. 7, 2024. [Online]. Available: https://www.opal-rt.com/simulator-platform-op5705xg/

[46] D. Mishchenko, I. Oleinikova, and D. Ivanko, "Cyber-security assessment of power system digital components in the conditions of hostilities," in *Proc. IEEE Belgrade PowerTech*, Jun. 2023, pp. 1–6.

[47] Schweitzer Engineering Laboratories (SEL). *SEL-5073 SynchroWAVe Phasor Data Concentrator (PDC) Software*. Accessed: Mar. 7, 2024. [Online]. Available: https://selinc.com/products/5073/

[48] *Open Source Phasor Data Concentrator*. Accessed: Mar. 7, 2024. [Online]. Available: https://github.com/GridProtectionAlliance/openPDC

[49] *Communication Networks and Systems for Power Utility Automation—Part 90-4: Network Engineering Guidelines*, P-Code, Geneva, Switzerland.

[50] Schweitzer Engineering Laboratories (SEL). (2023). *SEL-5702 Synchrowave Operations*. [Online]. Available: https://selinc.com/products/5702/

[51] W. Xiong, E. Legrand, O. Åberg, and R. Lagerström, "Cyber security threat modeling based on the MITRE enterprise ATT&CK matrix," *Softw. Syst. Model.*, vol. 21, no. 1, pp. 157–177, Feb. 2022.

[52] S. H. Jakobsen, L. Kalemba, and E. H. Solvang, "The Nordic 44 test network," Figshare, London, U.K., Tech. Rep., 2018.

[53] *IEEE Standard for Synchrophasor Data Transfer for Power Systems*, Standard C37.118.2-2011, Revision of IEEE Std C37.118-2005, 2011, pp. 1–53.

[54] R. Khan, P. Maynard, K. McLaughlin, D. Laverty, and S. Sezer, "Threat analysis of blackenergy malware for synchrophasor based real-time control and monitoring in smart grid," in *Proc. 4th Int. Electron. Workshops Comput.*, 2016, pp. 53–63.

[55] *PMU Connection Tester*. Accessed: Mar. 7, 2024. [Online]. Available: https://pmuconnectiontester.info/

DENYS MISHCHENKO (Member, IEEE) received the B.S. and M.S. degrees in electrotechnical systems of power supply from the Igor Sikorsky Kyiv Polytechnic Institute, National Technical University of Ukraine, in 2012. He is currently pursuing the Ph.D. degree with the Department of Electric Energy, Norwegian University of Science and Technology, Trondheim, Norway. His research interests include power system protection and control, data communication and protection, state estimation, and cyber-physical security, with more than 12 years of industry experience.

IRINA OLEINIKOVA received the Ph.D. degree in power engineering from Riga Technical University. She is currently a Professor with the Department of Electric Energy, the Head of the Power System Operation and Analysis Research Group, and a Smart Grid Team Leader with NTNU. She has more than ten years of management experience to carry out research projects independently with the new scientific tasks developments and application in field of smart grids. She is playing an active role in exploring research and development for industrial sector in Nordic and Baltic Countries. Her research interests include power system operation and planning, smart grids, and flexibility studies. She is the Steering Committee Member of the European Energy Research Alliance Joint Program on Smart Grids and an Expert in ISGAN WG6 Transmission and Distribution.

LÁSZLÓ ERDŐDI received the Ph.D. degree in computer security from Obuda University. He is currently an Associate Professor with the Department of Information Security and Communication Technology, NTNU. He has more than 15 years of practical and research experience in offensive security. He has an active role in capture the flag based ethical hacking education with multiple universities in Norway and Hungary. His research interests include ethical hacking, exploit development, reinforcement learning based hacking agents, and power grid security.

BASANTA RAJ POKHREL (Member, IEEE) received the Ph.D. degree in energy technology from Aalborg University. He is currently a Research Scientist with the Department of Electric Energy and associated with the National Smart Grid Laboratory, NTNU. He is active in research project formulation, execution, project management, and operation of the National Research Laboratory. His main research interests include power system operation and analysis, real time monitoring and control of the electricity grid, smart grids, WAMS/WAMPAC, and power system flexibility, with more than ten years of experience.