

Article

Living Off the Land Attacks on IEC 61850 Substations

Robin Eriksen Birkeland ¹  and Siv Hilde Houmb ^{2,*} ¹ Department of Information Security and Communication Technology, Norwegian University of Science and Technology (NTNU), 7491 Trondheim, Norway; robineb@stud.ntnu.no² Norwegian Defence Cyber Academy, Norwegian Defence University College, 2617 Lillehammer, Norway

* Correspondence: shoumb@mil.no

Abstract

Power from Shore (PfS) is becoming more widespread for offshore petroleum installations, which have introduced new dependencies and the potential for a single point of failure. In addition, the cyber threat landscape is increasing, with state-sponsored actors demonstrating the capabilities and willingness to target Operational Technology (OT) systems. Threat actors have been seen using living off the land techniques, such as with the Industroyer malware, which utilized legitimate but malicious IEC 104 commands to open circuit breakers. To evaluate these vulnerabilities, in this study, a Design Science Research approach was applied to map a generalized substation and develop a Software-in-the-Loop simulator, which was used to test a specific attack vector against substation automation systems. The results confirm that an adversary with local network access can successfully inject valid IEC 61850 Manufacturing Message Specification (MMS) commands to trigger unauthorized circuit breaker operations. Furthermore, it is also shown that a simulated substation can be used as a tool when developing OT malware.

Keywords: cybersecurity; Operation Technology; Smart Grid; IEC 61850; living off the land

1. Introduction

In 2010, Iran's uranium enrichment program was attacked from the cyber domain. This attack, Stuxnet, was one of the first to target Operational Technology (OT) systems, which is widely considered the beginning of a new era in OT security. Due to Stuxnet's complexity, it is believed that an Advanced Persistent Threat (APT) was behind it. An APT is an actor with significant expertise, extensive resources, and the willingness to operate over an extended period. APTs are therefore typically state-sponsored or -affiliated groups.

Over the last 10 to 15 years, the number of attacks targeting OT has increased significantly. This is particularly evident in Ukraine, in which Russia has attacked critical infrastructure both before and after the war broke out in 2022, as part of hybrid warfare.

To address these threats, this work investigates how the lack of security in OT protocols can be exploited to target critical power grid infrastructure. Specifically, this study focuses on living off the land (LOTL) cyberattacks against digital substations and Power from Shore (PfS) installations. Applying a Design Science Research (DSR) methodology, we develop a custom Software-in-the-Loop (SIL) testbed to evaluate these vulnerabilities. While prior research utilized physical equipment, pure software, or hybrid setups, SIL studies have been predominantly focused on time-critical Layer 2 protocols like IEC 61850 Generic Object Oriented Substation Events (GOOSE) and Sampled Values (SV). Studies simulating the IEC 61850 Manufacturing Message Specification (MMS) protocol are comparatively scarce. While previous MMS simulations often relied on isolated runtime tools,



Academic Editor: Christos Bouras

Received: 25 May 2026

Revised: 26 June 2026

Accepted: 29 June 2026

Published: 3 July 2026

Copyright: © 2026 by the authors.

Licensee MDPI, Basel, Switzerland.

This article is an open access article distributed under the terms and conditions of the [Creative Commons Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

the SIL testbed proposed in this work utilizes full network virtualization, thus making it well suited for complex Layer 3 TCP/IP routing and network segmentation research. In addition to validating the proposed SIL framework as a viable research artifact, this study demonstrates that an adversary with local network access can successfully issue malicious control commands using legitimate LOTL techniques.

The remainder of this paper is organized as follows. Section 2 outlines related work, while Section 3 describes the concept of digital substations. Section 4 introduces the basics of PfS. Subsequently, Sections 5 and 6 detail the simulation environment and its execution. Finally, Sections 7, 8, and 9 present the discussion, conclusion, and future work, respectively.

2. Related Work

2.1. Security Research on IEC 61850 Protocols

The convergence of IT and OT has expanded the attack surface of previously isolated substation automation systems [1]. Although the IEC 62351 standard [2] outlines security extensions like encryption and mutual authentication for IEC 61850 protocols, these mechanisms are rarely fully implemented in real-world environments due to strict performance requirements and multi-vendor interoperability issues [3].

Formal verification tools like Scyther have shown that Layer 2 GOOSE implementations fail to preserve data confidentiality, thus leaving user-defined parameters vulnerable to masquerade threats and falsification [4]. At the supervisory level, the protocol-aware fuzzing of MMS stacks (such as libiec61850) revealed critical vulnerabilities, in which malformed ASN.1 payloads can cause buffer overflows leading to Remote Code Execution or denial of service [5]. Further, threat actors have been observed using LOTL techniques, as seen in the 2016 Industroyer malware. As documented by Cherepanov [6], this attack targeted several OT-specific protocols, including IEC 61850 MMS, thereby manipulating legitimate services and parameters to alter system states.

2.2. Substation Cybersecurity Testbeds

To evaluate the physical and operational impacts of cyberattacks without access to physical infrastructure, the research community has used specialized testbed environments, including physical, hybrid, and simulated setups.

Physical and Hybrid Testbeds: Hardware-in-the-Loop (HIL) environments integrate real physical devices to achieve high-fidelity simulations. For instance, Reda et al. [4] utilized an industrial OPAL-RT simulator platform (OP5600 chassis) to model power system components alongside active network infrastructure, successfully validating that injected GOOSE messages can physically manipulate breaker states. Akbarzadeh et al. [7] similarly demonstrated the utility of HIL setups by evaluating cyberattacks against the Precision Time Protocol (PTP). Furthermore, distributed hybrid setups have been employed to evaluate renewable energy integrations. In one study investigating photovoltaic (PV) smart inverter installations [8], researchers used a Raspberry Pi as an intermediate programmable gateway bridging high-level IEC 61850 MMS communications from a Supervisory Control and Data Acquisition (SCADA) network directly to a physical PV inverter's internal serial Modbus interface. Using an MMS Man-in-the-Middle attack, the researchers injected forged MMS Write Requests to maliciously rewrite active power limitation variables. This successfully spoofed operating constraints, resulting in a decrease in power output from 100% to 10% and driving the physical PV inverter into a forced, non-responsive standby loop.

Simulated Testbeds: Software-based simulators are less expensive and a more flexible alternative to physical hardware. For instance, *OpenPLC* is a widely used open-source tool for simulating programmable logic controllers (PLCs). The lack of IEC 61850 protocol support was addressed by Roomi et al. [9], who expanded the platform to use the open-

source library *libiec61850*. This was combined with Mininet to create a network topology, which was used to simulate False Data Injection and False Command Injection attacks. Other researchers have also used Mininet and the *libiec61850* library for simulation [10]. By building a virtualized substation entirely within a Mininet environment, they achieved real-time Ethernet layer virtualization and deterministic GOOSE packet forwarding. Using this protocol stack, they tested replay and masquerade attacks and validated that IEC 62351 cryptographic authentication could successfully block malicious injections within strict sub-4ms time windows.

2.3. Comparison with Our Approach

To evaluate LOTL attack vectors targeting the MMS protocol, this work introduces a custom SIL testbed that simulates intelligent electronic devices (IEDs) using Docker containerization, with the network topology implemented via Graphical Network Simulator 3 (GNS3). Rather than exploiting software vulnerabilities or relying on physical hardware, our approach focuses on the abuse of legitimate protocol features within a scalable, software-defined TCP/IP network. Table 1 provides a summary of the discussed literature, highlighting how these works differ from our setup.

Table 1. An analytical comparison of related works and the proposed SIL approach.

Reference	Focus and Architecture	Strengths	Limitations	Our Improvement
Claroty Team82 [5]	Protocol Fuzzing (MMS Stack)	Discovered critical software vulnerabilities (CVEs) via deep protocol analysis.	Focuses on software crashes (e.g., buffer overflows) rather than logical protocol abuse.	Achieves physical disruption using valid MMS commands (LOTL tactics) without exploits.
Scyther and OPAL-RT [4]	Formal Verif. and HIL	High-fidelity power system co-simulation and formal protocol verification.	Relies on expensive proprietary hardware (OP5600), limiting rapid iterative testing.	Provides a lightweight, cost-effective containerized SIL alternative using open-source tools.
PV Inverter MITM [8]	Hybrid Setup (RPi to Inverter)	Demonstrates realistic physical impacts of LOTL attacks on renewable energy assets.	Requires physical hardware and protocol translation (MMS to serial Modbus).	Uses a fully virtualized environment natively running IEC 61850, eliminating hardware dependencies.
Mininet Emulation [10]	Simulated Env. (L2 GOOSE)	Enables deterministic Layer 2 Ethernet emulation for strict sub-4ms GOOSE timing.	Optimized for L2 switching; lacks robust Layer 3 routing and network segmentation.	Employs GNS3 for complex TCP/IP routing, enabling superior segmented MMS traffic simulation.
OpenPLC61850 [9]	Simulated PLC Runtime (MMS)	Adds native IEC 61850 support to OpenPLC to test software-based FDI and FCI attacks.	Operates primarily as a single-device runtime rather than a multi-node network testbed.	Uses a complete, multi-node network topology tailored for full cyber kill chains.

3. Digital Substations

Figure 1 illustrates a digital substation organized into three closely related areas: the switch yard (process level), relay room (bay level), and substation control room (station level) [11]. The physical layout maps directly to communication roles, where measurements and primary switching happen at the process level. Protection and bay control are implemented at the bay level. Finally, supervision, HMI, and remote integration are handled at the station level.

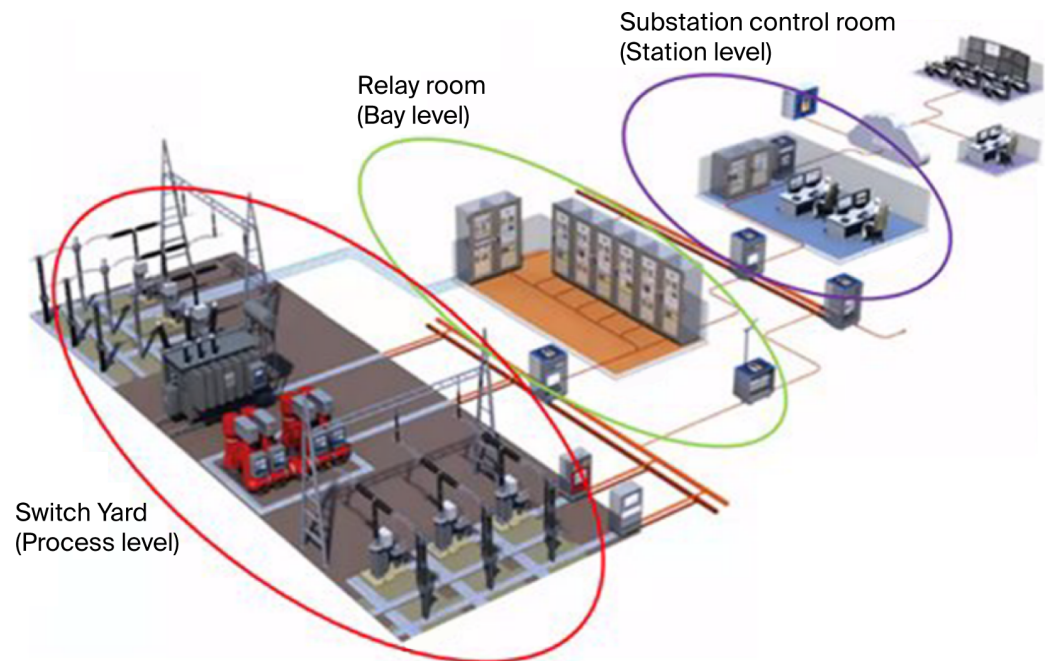


Figure 1. Digital substation, adapted from Figure 1 in [11].

3.1. Switch Yard

The switch yard contains the primary equipment, including circuit breakers, disconnectors, power transformers, and instrument transformers (CTs/VTs), as well as gas-insulated switchgear (GIS) at certain sites. For digital installations, merging units transform currents and voltages into Sampled Values frames transmitted over the process bus in accordance with IEC 61850-9-2 [12]. Furthermore, GOOSE messages enable the rapid exchange of trip and interlocking signals, though utilities might still implement parallel, hard-wired tripping mechanisms for specific critical functions [12].

3.2. Relay Room

Within each bay, a bay controller operates alongside protection and control IEDs, which manage specific tasks such as distance, differential, and breaker failure protection. These intelligent devices process measurements and issue commands over the process bus while simultaneously exchanging peer-to-peer GOOSE messages. Additionally, they interface with the station bus using the IEC 61850-8-1 mapping to MMS/Ethernet to handle configuration, reporting, and coordination with station services [13].

3.3. Substation Control Room

At the station level, HMIs and servers are responsible for supervising the entire yard. Meanwhile, engineering workstations maintain system configurations, and gateways provide the necessary connectivity to the utility control center.

3.4. IEC 61850

IEC 61850 is a comprehensive substation automation standard that replaces traditional point-based addressing with a semantic, standardized object model [14]. It defines two primary communication profiles: MMS over TCP/IP for supervisory control and Layer 2 multicast protocols (GOOSE and sampled values (SV)) for time-critical protection functions. Unless optional security extensions (IEC 62351) are fully implemented, MMS and GOOSE traffic remain unauthenticated. As demonstrated in our simulation scenarios (Section 6), this architectural gap allows a rogue device on the local network to passively sniff substation

configurations and seamlessly inject valid supervisory commands to trigger unauthorized circuit breaker operations.

4. Power from Shore (PfS)

Power from shore supplies offshore facilities with electrical power from the mainland grid through a dedicated transmission link. A power from shore implementation can be seen in Figure 2. This arrangement requires an onshore sending substation tied to the transmission grid and an offshore receiving substation that feeds the offshore installation distributed system, connected by an export cable. For High-Voltage Alternating Current (HVAC) export, this typically involves a single three-core Cross-linked Polyethylene (XLPE) subsea cable. Its capacitance introduces charging current that grows with length, so shunt reactors or other reactive power supports are often installed at one or both ends, which makes HVAC attractive for moderate distances and power levels [15]. For High-Voltage Direct Current (HVDC) export, the link uses two single-core DC cables in a bipole configuration with converter equipment at both ends. HVDC avoids cable charging current, improves efficiency over long distances or at higher power, and allows for the independent control of active and reactive power while decoupling the offshore network from the onshore grid [16,17]. In both cases, the export cable is routed from a landfall to the offshore installation with burial or external protection where needed, a dynamic section near the topsides, and fiber pairs for protection, control, and SCADA communications. Detailed design and installation follow established subsea power cable practices [18,19].

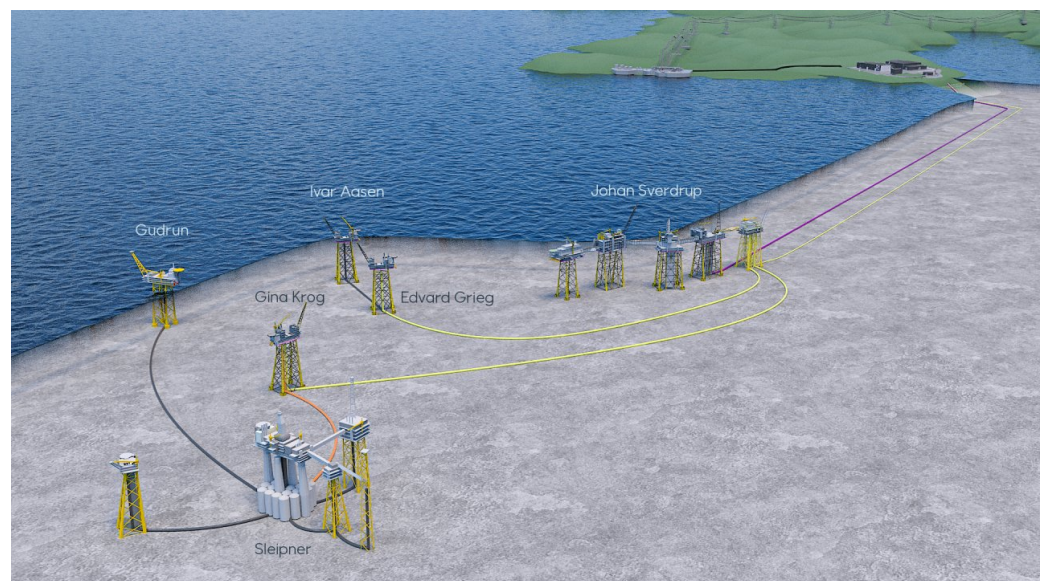


Figure 2. An overview of the subsea cable routing to the interconnected offshore facilities at Utsir-ahøyden. Adapted from [20].

5. Living of the Land (LOTL) Cyberattacks on IEC 61850

This section explores vulnerabilities within station bus communication protocols by examining attacks targeting the substation automation system. First, we define the reference network topology used as the baseline. We then detail a full attack vector on the Manufacturing Message Specification (MMS) protocol designed to achieve unauthorized control.

5.1. Reference Network Topology for a Digital Substation

The attack scenarios detailed in this section are based on the reference architecture shown in Figure 3. This topology represents a modern digital substation organized according to the hierarchical levels typical of IEC 61850 environments. It serves as the

theoretical baseline for the attack design; the specific network topology implemented in the Software-in-the-Loop (SIL) simulator is a functional adaptation of this model and detailed in Section 6.3.

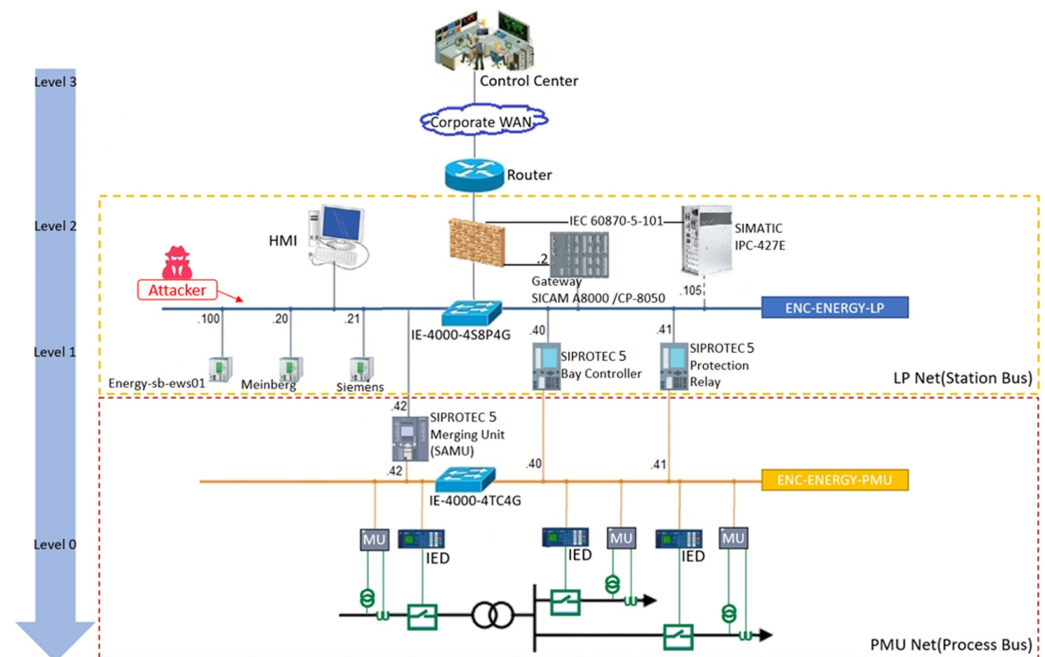


Figure 3. Example topology for a modern substation, adapted from Figure 3 in [11].

5.2. Rogue Device Sending MMS Control Messages

The rogue device cyberattack involves a malicious device on the local process network (LP Net) communicating with the bay controller via IEC 61850/MMS. The goal is to achieve the remote control of a switching device by identifying and manipulating its control objects.

5.2.1. Prerequisite

The attacker connects a rogue device to the same logical network segment as the bay controller on the LP Net. VLAN configuration and IP routing permit traffic between the attacker and target IED.

5.2.2. Attack Steps

1. Passive reconnaissance and IP mapping

The attacker uses passive listening to monitor substation bus traffic and gather intelligence.

- **GOOSE Sniffing:** The attacker captures GOOSE messages broadcast on the network. By parsing these Ethernet frames, the attacker extracts the Application ID (APPID), GoID, and dataset members. These reveal the Logical Device (LD) and logical node (LN) names, such as CSWI (switch control) and XCBR (circuit breakers).
- **MAC-to-IP Association:** The attacker identifies the source MAC address of the GOOSE messages. By cross-referencing this MAC address with ARP traffic or other captured IP packets, the attacker resolves the specific IP address of the target IED.

2. Rapid command execution (SBO-enhanced)

Using the gathered intelligence, the attacker interacts with the Intelligent Electronic Device (IED) to execute a control action. The attacker assumes an SBO-with-enhanced-security model, which is the industry standard for high-voltage switching. The entire

sequence is performed in a short timeframe to ensure that the operation stays within the required time constraints.

- **Association:** To initiate the attack, the attacker requests an MMS Associate service. This process requires establishing a TCP connection to port 102 on the target IED. If the IED lacks strong authentication, this request is accepted, thus granting the attacker an application layer session. Once established, the attacker moves to the control sequence.
- **Selection:** The attacker sends an MMS Write request to the `SelectWithValue` (or `SBOw`) attribute of the target object (e.g., `Pos`). This reserves the control point for the attacker's session.
- **Immediate Operate:** Upon receiving confirmation of the selection, the attacker's script issues the `Operate` command with the desired value (e.g., `off`). Executing these steps in rapid succession ensures the action is completed before the IED's internal `sboTimeout` or `operTimeout` windows can expire.

3. Feedback and confirmation

After issuing the control command, the attacker confirms the effect by continuing to monitor the substation bus traffic.

- **GOOSE Monitoring:** The attacker observes the same GOOSE streams identified in Step 1. A change in the status value (`stVal`) within the dataset confirms a physical state change in the breaker or switch.

6. Demonstration of IEC 61850 Cyberattack

6.1. Design Science Research Methodology

To systematically validate the theoretical attack vectors and address the research questions, this study adopts a Design Science Research (DSR) methodology [21,22]. DSR focuses on the iterative creation and evaluation of innovative IT artifacts to solve identified practical problems. To provide a structured presentation of this methodology, the research is mapped according to the following key components:

- **Research Objectives:** The primary objective is to evaluate whether an adversary with local network access can leverage standard MMS functionality to deterministically manipulate physical grid states in a digital substation. The secondary objective is to design and develop a Software-in-the-Loop (SIL) testbed capable of realistically simulating these Layer 3 network conditions and cyber threats without relying on physical hardware.
- **Artifacts:** The core artifact developed in this study is the custom SIL simulator (detailed in Section 6.2). Through an iterative design process, the artifact evolved from commercial tools into a fully virtualized TCP/IP network utilizing Docker containerization and GNS3 to accurately mirror a digital substation's routing, segmentation, and IEDs.
- **Evaluation Criteria:** The artifact is evaluated based on its functionality in executing the LOTL cyberattack (described in Section 5.2). The success criterion is the ability of the rogue device to establish an application layer session and achieve an unauthorized physical state change (e.g., opening a circuit breaker) using strictly valid MMS commands.
- **Outcomes:** The expected outcomes are twofold: first, the empirical demonstration of the attack, proving the low technical barrier to execution once internal network access is achieved, and second, the validation of the SIL environment as a scalable, cost-effective tool for future OT cybersecurity research.

6.2. Simulating an IEC 61850 Substation

To test the theoretical MMS attack, a Software-in-the-Loop (SIL) environment was used. The process of setting up a suitable SIL was not straightforward and involved several challenges.

Initially, we attempted to simulate IEDs using Omicron's IED Scout ([23]), which is a software tool designed for engineers to visualize, simulate, and test IEC 61850-compliant IEDs within power utility substations. It enables users to inspect detailed data models and communication traffic (such as GOOSE and Reports) and troubleshoot devices without requiring a functioning master station. We configured IED Scout and initialized an IED using a publicly available .SCD file. The setup successfully received and responded to IEC 61850 control messages; we were able to send MMS control commands from a Python (v3.12.3) script and observed the expected Select-Before-Operate message exchange when attempting to close a circuit breaker. However, even when IED Scout returned an "operation successful" response, the simulated breaker position did not update in the user interface. After several debugging attempts, it remained unclear whether this behavior was caused by a configuration error or a limitation of IED Scout itself. Consequently, we decided to pursue an alternative approach. We ultimately developed a custom SIL from scratch. The solution uses Docker containers running C code to emulate IEDs. Each IED operates in an isolated container, and inter-device networking is conducted via GNS3 (Graphical Network Simulator 3)(v2.2.54), which is an open-source network emulation tool. The IEC 61850 protocol stack, including MMS, GOOSE, and Sampled Values, is implemented using the open-source libiec61850 library (v1.6.1). The Human-Machine Interface (HMI) is accessible through a web-based SCADA dashboard, thus allowing operators to monitor IED states and issue control commands.

6.3. Topology

The network architecture follows the Purdue Reference Model and is segmented into three zones:

Station Bus (10.1.1.0/24)

Carries MMS traffic for supervisory control and GOOSE messaging for horizontal communication between IEDs.

Process Bus A (10.1.10.0/24, VLAN 110)

Transports Sampled Values from Merging Units associated with the first busbar section.

Process Bus B (10.1.20.0/24, VLAN 120)

Transports Sampled Values from Merging Units associated with the second busbar section.

Bay-level IEDs are dual-homed, connecting to both the station bus (via eth0) and their respective process bus (via eth1), thus enabling Level 2 control traffic to remain isolated from Level 0 process data. The simulated topology represents a 132 kV substation section with multiple circuit breakers (XCBR) and disconnectors (XSWI). The GNS3 network topology and a circuit diagram are shown in Figures 4 and 5, respectively.

6.4. Containerization Architecture

6.4.1. IED Server

Each IED container emulates a protection relay or bay controller responsible for monitoring and controlling circuit breakers and switches. The IED software acts as an MMS server (IEC 61850-8-1), exposing a data model defined in an IEC 61850 SCL/SCD configuration file. Control operations follow the Select-Before-Operate (SBO)-Enhanced model

(ctlModel=4), requiring a two-phase sequence (Select, then Operate) with a configurable timeout. Additionally, each IED supports GOOSE publishing and subscribing for real-time inter-device event notification.

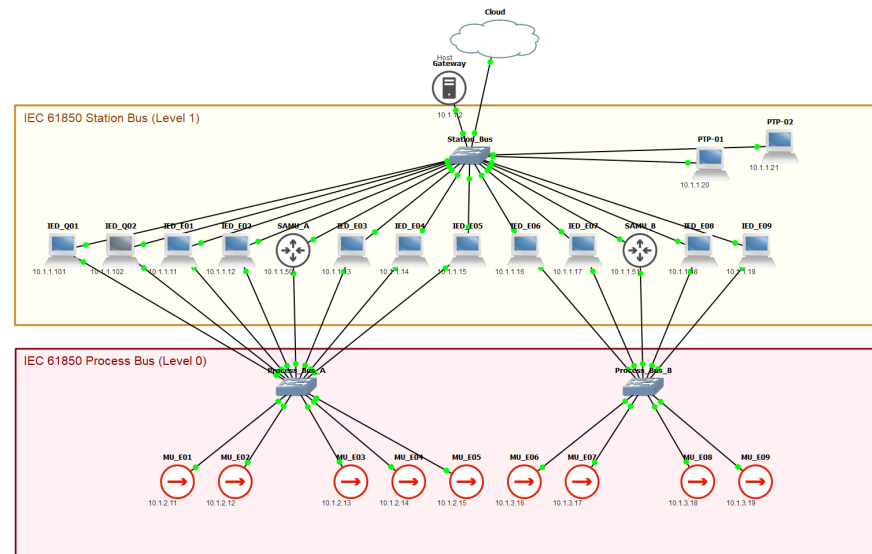


Figure 4. GNS 3 network topology.

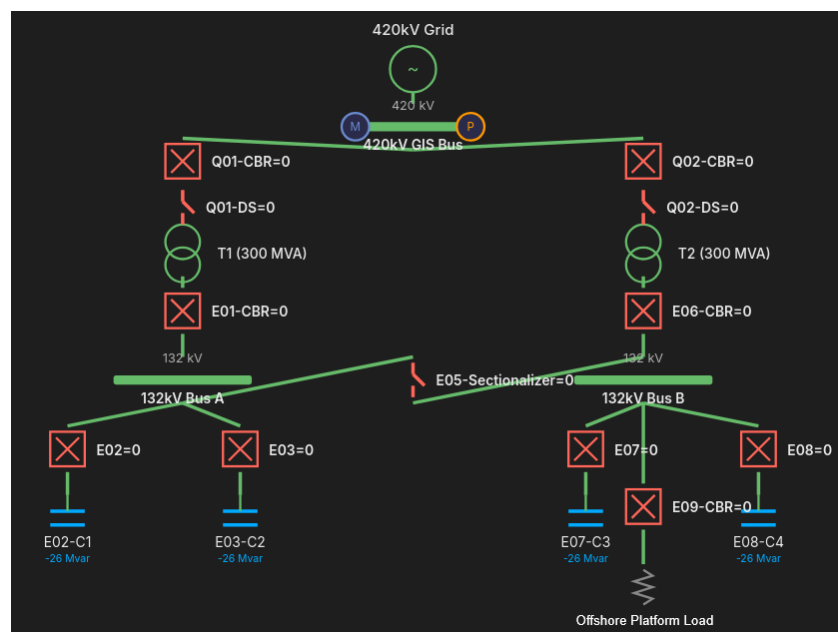


Figure 5. Circuit diagram.

6.4.2. Merging Unit (MU)

Each Merging Unit samples simulated electrical waveforms (voltage and current) and publishes them as IEC 61850-9-2LE Sampled Values (SV). The default configuration produces 80 samples per cycle at 50 Hz, yielding a sample rate of 4000 samples per second. For development environments with constrained resources, this can be reduced to 20 samples per cycle (1000 sps). Due to the PTP timing limitations described below, the published SV frames do not currently include high-precision timestamps synchronized to the PTP grandmaster.

SAMU (Stand-Alone Merging Unit/Data Concentrator)

The SAMU container operates as an SV subscriber and data aggregator. It is dual-homed, connecting to both the process (to subscribe to SV streams from Merging Units) and station buses (to publish aggregated GOOSE messages or provide data to the HMI).

6.4.3. PTP Clock

Two PTP grandmaster containers implement the IEEE 1588 Precision Time Protocol using the `linuxptp` daemon (`ptp4l`). Redundancy is achieved through the Best Master Clock Algorithm (BMCA), which autonomously elects a grandmaster based on configurable priority values. However, because the GNS3 environment runs within a VMware Workstation virtual machine (Type 2 hypervisor), timestamp accuracy is significantly limited. The virtualization layer introduces non-deterministic scheduling jitter and prevents access to hardware timestamping, thus resulting in timing accuracy on the order of milliseconds rather than the microsecond-level precision required by IEC 61850-9-2LE. This limitation could be mitigated by migrating to a bare-metal Linux host with the `PREEMPT_RT` real-time kernel and CPU core isolation, which would reduce operating system jitter to sub-10 μ s levels.

6.4.4. HMI/Gateway

The gateway container hosts a web-based SCADA dashboard built with Python (FastAPI) and JavaScript. It functions as an MMS client, enabling operators to browse IED data models, monitor real-time device states, and issue SBO control commands. The dashboard visualizes the substation topology using D3.js and displays live waveforms, GOOSE event logs, and PTP synchronization status.

6.5. Executing the Cyberattack

The first phase involves designing the attack scenario. In essence, the rogue device attack involves injecting standard control commands. Placed within the context of a kill chain, this attack begins after initial access has been established. During execution, the rogue device transmits valid control commands using the MMS protocol, which is standard in substation environments. This command actuates the circuit breaker, causing a direct transition from the execution phase to physical impact. Figure 6 illustrates a typical circuit breaker. As shown, the mechanism is encapsulated, thus making it difficult to visually verify whether the breaker is open or closed.

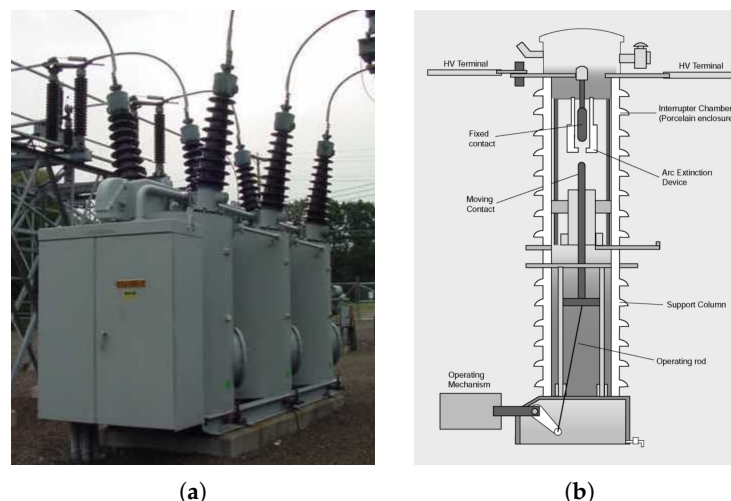


Figure 6. An overview of a high-voltage circuit breaker. (a) The physical installation of a high-voltage circuit breaker in an outdoor substation. (b) A cross-sectional view showing the internal interrupter chamber and operating mechanism. The external view (a) shows the bushings and control cabinet, while the internal schematic (b) details the fixed and moving contacts used for arc extinction. Adapted from [24].

Disconnectors operate similarly but are distinct because their open or closed status is clearly visible. This feature is critical for safety during maintenance, allowing workers to confirm that the circuit is physically broken. However, disconnectors lack arc suppression and cannot be operated under load. Opening a disconnector while current is flowing results in dangerous arcing and potential damage to the equipment (see Figure 7). To prevent this, substations use interlocking mechanisms that block the disconnector from operating if the circuit is live.



Figure 7. An open disconnector showing the visible isolation gap. Adapted from [25].

Our current simulator setup successfully executed the rogue device attack. Table 2 details how this scenario integrates into a complete kill chain.

Table 2. Kill chain.

Step	Description
1: Initial Access	The attacker begins by collecting publicly available information. Concession applications submitted to Norwegian Water Resources and Energy Directorate (NVE) and various technical public reports provide enough context about planned infrastructure and facility specifications to form a plausible hypothesis for an attack and identify critical dependencies.
2: Reconnaissance	Based on the OSINT in Step 1, the attacker narrows the scenario toward the power supply architecture. This phase uses public information from the Transmission System Operator (TSO) and offshore operators. This is combined with a review of typical substation and HVDC vendor ecosystems and the prior literature on electrical infrastructure cyberattacks to identify likely technologies and high-level architectures in scope.
3: Data Exfiltration	In this scenario, no information is taken from inside the target system. The work is based entirely on publicly available sources, and the collected OSINT is consolidated and organized in the attacker's development environment. Publicly documented attack patterns, such as prior Sandworm reporting and structured mappings like MITRE [26], are then used to shape the assessment. This leads to a focus on substations and switching functions as a plausible target area.
4: Weaponization	A substation simulator is developed and used as a controlled test environment. This allows for the development, verification, and refinement of the malware logic without requiring access to real equipment during the development phase.
5: Local Access	The scenario assumes that local access is needed to reach the operational environment. The attacker could pursue access at the offshore receiving facility or at the onshore grid connection point.
6: Delivery	Malicious capability is introduced into the relevant OT environment by connecting a compromised host to the appropriate subnet. The payload may be executed immediately or configured to be triggered at a later time.

Table 2. *Cont.*

Step	Description
7: Exploitation	Before acting, the malware performs basic validation such as checking system state and timing conditions and ensuring it targets the intended device. It then attempts the unauthorized use of legitimate substation control functionality to initiate the planned switching action.
8: Actions	The attacker's immediate objective is to open a breaker under unfavorable operating conditions. In the worst-case scenario, an incorrect switching action can create severe operational disturbance and may contribute to equipment stress or damage risk, depending on whether the system is energized.
9: Sabotage	The overall impact is intended to be the loss of power, possible equipment damage, and operational uncertainty. Persistence can be achieved through repeated triggering over time, potentially spaced out to complicate detection and response.

7. Discussion

7.1. The Evolving Threat to Critical Infrastructure

State-sponsored actors, including those affiliated with Russia, have increasingly utilized cyberattacks against OT systems in critical infrastructure as a tool for hybrid warfare, often with the intention to cause physical disruption without triggering armed escalation. A prominent example of this strategy is the 2025 attack on the Bremanger dam in Norway, in which attackers manipulated OT controls to open floodgates and cause downstream flooding [27]. A threat assessment published by the Danish Defence Intelligence Service in late 2025 states that critical infrastructure networks remain high-priority targets for these operations [28], thus aligning with the earlier report by the Norwegian Intelligence Service.

However, the targeting of substations via cyber means is not isolated to a single nation. For instance, reports indicate that cyber operations were deployed against electrical substations during the US military operation in Venezuela in early 2026 to cut power to regional grids [29]. These events suggest that cyberattacks against critical infrastructure have become a more common capability in modern conflict. Given the current geopolitical climate and the demonstrated use of cyber operations across different levels of escalation, it is reasonable to assess that state-sponsored actors will persist as a threat to Western OT infrastructure. Furthermore, as long as these OT networks lack fundamental security by design, future adversaries will likely establish OT infrastructure as a primary target.

7.2. Protocol Vulnerabilities

After analyzing different attacks against substations and proposing theoretical scenarios, it is evident that once attackers reach the correct subnet, causing physical disruption is technically possible. The common protocols used in substations were not designed with security in mind. While this gap was addressed by the security extensions defined in IEC 62351, this standard is rarely fully implemented in real-world systems. Vendors often implement the standard differently or only partially. This leads to limited interoperability between equipment and causes operators to frequently omit these security measures in active systems [3].

Since OT protocols are insecure by design, the importance of a layered defense structure with segmented networks and strict access control increases. Based on the findings, the most significant challenge in cutting power to an offshore facility is likely gaining initial access to relevant subnets. Plausible entry vectors include spear-phishing campaigns or the use of tools like Shodan [30] to identify exposed ports on misconfigured devices. However, gaining initial access is rarely sufficient; an attacker would likely need to perform lateral movement across the internal network to bridge the gap between IT and OT environments.

7.3. Potential Mitigations

The traditionally used perimeter defense makes it difficult for an adversary to gain access to the appropriate subnet to execute a rogue device attack on the MMS layer. However, to reduce the risk further for such an attack, an internal zero-trust architecture can be implemented. Since substation automation protocols fundamentally lack native security features, defenses must be applied at the IED level to constrain unauthorized associations and strictly control application layer capabilities.

7.3.1. Cryptographic and Identity-Based Access Controls

Implementing IEC 62351-3, which mandates TLS with mutual certificate-based authentication, provides a robust technical barrier against local command injection. Enforcing mutual authentication ensures that only clients with cryptographical credentials trusted by the IED can initialize an MMS association. This prevents anonymous rogue devices from establishing rogue control sessions on the LP Net. However, a full TLS deployment is rarely implemented in real systems and introduces administrative overhead, particularly regarding certificate lifecycle management, revocation tracking, and key provisioning.

If a full TLS deployment is not feasible due to hardware or operational constraints, IEDs should enforce strict association allowlists (whitelist) that restrict incoming connections to pre-approved clients based on their IP addresses. While this mechanism blocks unapproved devices from initializing an MMS association, it offers limited security against a sophisticated adversary. Because standard IP addresses lack cryptographic verification, this defense can be bypassed if an attacker on the local network segment executes an IP spoofing or man-in-the-middle attack to impersonate an allowlisted endpoint.

7.3.2. Process Interlocks and Behavioral Controls

Securing the connection channel alone is insufficient if an adversary compromises a trusted engineering workstation that already holds valid network credentials. Defensive measures can be taken by enforcing strict role-based access control. Instead of granting uniform access to all authenticated entities, users should be given authorization based on their distinct roles and operational needs.

Additionally, physical and logical process interlocks should be enforced directly at the logical node level. For example, a disconnect operation should be blocked by the device logic whenever current is measured on the process bus. Using such behavior-based constraints can neutralize malicious or harmful commands from human errors before they can actuate the physical equipment, thus mitigating the risk of dangerous arcing or structural damage.

7.3.3. Continuous Monitoring and Logging

To detect an ongoing cyberattack, monitoring and logging should be used in combination with an anomaly-based intrusion detection system (IDS). Since the cyberattacks described in this work utilize living off the land techniques and legitimate protocol services, a signature-based IDS will fail to detect them. IEDs should log all MMS association attempts, structural data model browsing, and control operations. Predefined procedures should be established and followed if the IDS detects an anomaly. These procedures should include instructions on how to both verify a true or false positive and act upon it.

8. Conclusions

A key finding from the technical analysis and Software-in-the-Loop (SIL) simulation is that the OT protocols used in digital substations and PfS lack fundamental security features by default. While security standards such as IEC 62351 exist to provide add-ons like encryp-

tion and mutual authentication, they are rarely implemented in operational environments due to complexity and interoperability constraints. Consequently, the simulation results demonstrate that it is technically possible to perform a disruptive cyberattack, such as manipulating circuit breakers, if an adversary is positioned within the appropriate subnet.

Since the technical barrier to execution is low once inside the network, the main challenge for an adversary is gaining initial access and performing the lateral movement required to reach the process bus. This shows the critical importance of a layered defense strategy, which is often referred to as defense in depth. However, reliance on perimeter defense is complicated by supply chain risks. Large-scale infrastructure projects involve numerous external contractors and vendors, particularly during the construction and commissioning of onshore converter stations. The compromise of a vendor with legitimate remote or temporary site access creates a high-risk vector, thus allowing an adversary to bypass the most resource-intensive phases of the kill chain and the perimeter and move directly to the execution phase inside the vulnerable OT subnet.

9. Future Work

To further validate the findings and improve defensive strategies, the following areas are proposed for further research:

9.1. Expanded Simulation and Hardware Validation

While the Software-in-the-Loop (SIL) environment provides a representative model of IEC 61850 network architecture, it does not implement the complete functional complexity of a physical substation. Consequently, a degree of uncertainty remains regarding whether these exact attack behaviors are perfectly reproducible in a real-world, operational substation. The current SIL simulator was effective for protocol-level testing but limited by the virtualization environment. Future work should add more features to the simulator to enable the simulation of other attacks, particularly those targeting time synchronization (PTP), which requires high-precision timing often lost in virtualization. Additionally, testing the attacks on real hardware (Hardware in the Loop) is recommended to verify the findings under realistic timing constraints and physical device behavior.

9.2. Algorithmic Target Identification via GOOSE Sniffing

In the MMS attack demonstrated, the attack script successfully extracted logical node (LN) and Logical Device (LD) names from sniffed GOOSE traffic. Currently, the attack utilizes this data to operate breakers either indiscriminately (opening all discovered breakers, which creates significant noise) or opportunistically (opening a random selection, which relies on chance). Future research should investigate the feasibility of automating the target selection process. By combining the extracted names with common utility naming schemes, an algorithm could be developed to intelligently identify the topology and pinpoint key breakers (such as bus couplers or main transformers). This would allow an attacker to disrupt the substation by operating a single critical asset, without the need to guess or operate every breaker indiscriminately, thereby increasing the stealth and speed of the attack.

9.3. Evaluation of Defensive Mechanisms

While Section 7.3 discusses theoretical mitigations such as IEC 62351 implementations, intrusion detection systems (IDSs), and zero-trust architectures, future work can use the developed Software-in-the-Loop environment to evaluate these defenses. The current containerized architecture and GNS3 network topology provide a safe, isolated testbed for implementing and measuring the efficacy of various security mechanisms without risking physical infrastructure.

Since the simulation environment uses GNS3 for the networking between components, it is highly suitable for developing and testing anomaly-based IDSs. By utilizing network tap functionalities within GNS3, station bus traffic can be mirrored to a dedicated IDS container. The simulator can be used to generate datasets comprising both normal operational baseline traffic and malicious Living off the Land (LOTL) attack traffic. This synthetic data can be used to train machine learning-based IDS models to recognize unauthorized structural data model browsing or abnormal command sequences. Furthermore, the open-source libraries used to simulate the IEDs could be extended to enforce IEC 62351-3, which mandates TLS and mutual certificate-based authentication. Implementing this in the SIL would allow researchers to verify its impact on preventing unauthorized MMS command injections and measure the performance overhead and latency introduced by cryptographic measures on time-critical substation communications.

Finally, the SIL framework serves as an ideal platform to prototype internal zero-trust architectures. Future iterations could enforce strict network micro-segmentation, dynamic access policies, and role-based access control at the logical node level. Testing these architectures will verify how effectively zero-trust principles can contain an adversary's lateral movement and neutralize unauthorized actions from an already compromised node.

Author Contributions: Conceptualization, S.H.H. and R.E.B.; methodology, R.E.B.; formal analysis, R.E.B.; investigation, R.E.B.; writing—original draft preparation, R.E.B.; writing—review and editing, S.H.H. and R.E.B.; supervision, S.H.H. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The original contributions presented in this study are included in the article. Further inquiries can be directed to the corresponding author.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

LD	Logical Device
LOTL	Living Off the Land
APT	Advanced Persistent Threat
IOA	Information Object Address
RTU	Remote Terminal Unit
SV	Sampled Values
HMI	Human–Machine Interface
SCADA	Supervisory Control and Data Acquisition
PLC	Programmable Logic Controller
MMS	Manufacturing Message Specification
TLS	Transport Layer Security
GIS	Gas-Insulated Switchgear
IT	Information Technology
OT	Operational Technology
IED	Intelligent Electronic Device
CT	Current Transformer
VT	Voltage Transformer
HVAC	High-Voltage Alternating Current
HVDC	High-Voltage Direct Current
XLPE	Cross-linked Polyethylene
DSRP	Design Science Research Process
DSR	Design Science Research
SIL	Software in the Loop
PTP	Precision Time Protocol
BMCA	Best Master Clock Algorithm
NVE	Norwegian Water Resources and Energy Directorate
TSO	Transmission System Operator
OSINT	Open-Source Intelligence
PfS	Power from Shore
GOOSE	Generic Object Oriented Substation Events
GNS3	Graphical Network Simulator 3
HIL	Hardware in the Loop
FDI	False Data Injection
FCI	False Command Injection
MITM	Man in the Middle
CVE	Common Vulnerabilities and Exposures
VLAN	Virtual Local Area Network
ARP	Address Resolution Protocol
SBO	Select Before Operate
APPID	Application Identifier
TCP/IP	Transmission Control Protocol/Internet Protocol

References

1. Line, M.B.; Tondel, I.A.; Jaatun, M.G. Cyber security challenges in Smart Grids. In *Proceedings of the 2011 2nd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies*; IEEE: Piscataway, NJ, USA, 2011; pp. 1–8. <https://doi.org/10.1109/isgteurope.2011.6162695>.
2. International Electrotechnical Commission. Power systems management and associated information exchange - Data and communications security. International Standard, IEC 62351:2026; IEC: Geneva, Switzerland, 2026.
3. Shivakumar, V.; Veena, M. Cybersecurity and IEC 62351 for SCADA Systems of Power Grid. *SSRG Int. J. Electr. Electron. Eng.* **2024**, *11*, 36–52. <https://doi.org/10.14445/23488379/IJEEE-V11I12P104>.

4. Reda, H.T.; Ray, B.; Peidaee, P.; Anwar, A.; Mahmood, A.; Kalam, A.; Islam, N. Vulnerability and Impact Analysis of the IEC 61850 GOOSE Protocol in the Smart Grid. *Sensors* **2021**, *21*, 1554. <https://doi.org/10.3390/s21041554>.
5. Claroty Team82. *Vulnerabilities in IEC 61850 MMS Protocol Stacks*; Technical Report, Security Research Report on Libiec61850 and Proprietary Protocol Stacks; Claroty Team82: New York, NY, USA, 2022.
6. Cherepanov, A. *Win32/Industroyer: A New Threat for Industrial Control Systems*; Research Whitepaper; ESET: Bratislava, Slovakia, 2017.
7. Akbarzadeh, A.; Erdodi, L.; Houmb, S.H.; Soltvedt, T.G.; Muggerud, H.K. Attacking IEC 61850 Substations by Targeting the PTP Protocol. *Electronics* **2023**, *12*, 2596. <https://doi.org/10.3390/electronics12122596>.
8. Kang, B.; Maynard, P.; McLaughlin, K.; Sezer, S.; Andr n, F.; Seitz, C.; Kupzog, F.; Strasser, T. Investigating cyber-physical attacks against IEC 61850 photovoltaic inverter installations. In *Proceedings of the 2015 IEEE 20th Conference on Emerging Technologies & Factory Automation (ETFA)*; IEEE: Piscataway, NJ, USA, 2015; pp. 1–8. <https://doi.org/10.1109/ETFA.2015.7301457>.
9. Roomi, M.M.; Ong, W.S.; Mashima, D.; Hussain, S.S. OpenPLC61850: An IEC 61850 MMS compatible open source PLC for smart grid research. *SoftwareX* **2022**, *17*, 100917. <https://doi.org/10.1016/j.softx.2021.100917>.
10. Herath, A.; Liu, C.C.; Hong, J.; Park, K. Evaluation of Real-Time Mitigation Techniques for Cyber Security in IEC 61850/IEC 62351 Substations. In *Proceedings of the CIGRE USNC 2025 Grid of the Future Symposium*, Denver, CO, USA, 10–13 November 2025.
11. Akbarzadeh, A.; Erd di, L.; Houmb, S.; Soltvedt, T. Two-stage advanced persistent threat (APT) attack on an IEC 61850 power grid substation. *Int. J. Inf. Secur.* **2024**, *23*, 2739–2758. <https://doi.org/10.1007/s10207-024-00856-6>.
12. IEC 61850-9-2:2011+A1:2020; Communication Networks and Systems for Power Utility Automation—Part 9-2: Specific Communication Service Mapping (SCSM)—Sampled Values over ISO/IEC 8802-3. International Electrotechnical Commission: Geneva, Switzerland, 2020.
13. 61850-8-1:2011+A1:2020; Communication Networks and Systems for Power Utility Automation—Part 8-1: Specific Communication Service Mapping (SCSM)—Mappings to MMS (ISO 9506) and to ISO/IEC 8802-3. International Electrotechnical Commission: Geneva, Switzerland, 2020.
14. TR 61850-1:2013; Communication Networks and Systems for Power Utility Automation—Part 1: Introduction and Overview. IEC: Geneva, Switzerland, 2013.
15. CIGR  US National Committee. Reactive Power Compensation Considerations for Offshore AC Networks. 2021. Available online: https://cigre-usnc.org/wp-content/uploads/2021/10/1B-3_Manna.pdf (accessed on 31 October 2025).
16. Brook, S.; Domijan, A.; Datta, R. *DC Collection and Transmission for Offshore Wind Farms*; Technical Report NYSERDA Report 003, Contract 109; National Offshore Wind Research and Development Consortium (NOWRDC): Albany, NY, USA, 2022.
17. SINTEF Energy Research. HVDC Transmission. 2024. Available online: <https://www.sintef.no/en/expert-list/sintef-energy-research/hvdc-transmission/> (accessed on 30 October 2025).
18. DNV-RP-0360; Subsea Power Cables in Shallow Water—Recommended Practice. DNV: Oslo, Norway, 2016.
19. DNV-ST-0359; Subsea Power Cables for Wind Power Plants. DNV: Oslo, Norway, 2021.
20. Equinor. Maksimal Utnyttelse av Kraft fra Land til Utsirah yden Bidrar til Ytterligere Utslippsreduksjon. 2019. Available online: <https://www.equinor.com/no/news/archive/2019-10-28-power-utsira-high> (accessed on 22 May 2026).
21. Hevner, A.R.; March, S.T.; Park, J.; Ram, S. Design science in information systems research. *MIS Q.* **2004**, *28*, 75–105.
22. Peffers, K.; Tuunanen, T.; Rothenberger, M.A.; Chatterjee, S. A design science research methodology for information systems research. *J. Manag. Inf. Syst.* **2007**, *24*, 45–77.
23. OMICRON electronics. IED Scout: Smart Protection and Control Testing Software. 2025. Available online: <https://www.omicronenergy.com/en/products/iedscout/> (accessed on 15 November 2025).
24. TJ|H2b Analytical Services. Understanding High Voltage Circuit Breakers. 2024. Available online: <https://tjh2b.com/blog/understanding-circuit-breakers/> (accessed on 29 January 2026).
25. saVRee. High Voltage Disconnectors Explained. Available online: <https://savree.com/en/encyclopedia/high-voltage-disconnectors> (accessed on 29 January 2026).
26. The MITRE Corporation. MITRE ATT&CK for Industrial Control Systems. 2024. Available online: <https://attack.mitre.org/matrices/ics/> (accessed on 23 May 2026).
27. Kronheim, E.H. PST Mener Prorussisk Hackergruppe Stod Bak Dam-Sabotasje p  Vestlandet og Datainnbrudd p   stlandet. 2025. Available online: <https://www.nrk.no/vestland/pst-mener-prorussisk-hackergruppe-stod-bak-dam-sabotasje-pa-vestlandet-og-datainnbrudd-pa-ostlandet-1.17587446> (accessed on 23 March 2026).
28. Forsvarets Efterretningstjeneste [Danish Defence Intelligence Service]. UDSYN 2025 [Intelligence Outlook 2025]; Technical Report; Forsvarets Efterretningstjeneste: Copenhagen, Denmark, 2025.
29. Kovacs, E. New Reports Reinforce Cyberattack’s Role in Maduro Capture Blackout. SecurityWeek. 2026. Available online: <https://www.securityweek.com/new-reports-reinforce-cyberattacks-role-in-maduro-capture-blackout/> (accessed on 29 January 2026).

30. Matherly, J. Shodan: The World's First Search Engine for Internet-Connected Devices. 2009. Available online: <https://www.shodan.io> (accessed on 15 January 2026).

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.