electronics

MDPI

Article

Attacking IEC 61850 Substations by Targeting the PTP Protocol

Aida Akbarzadeh [1,*], Laszlo Erdodi [2], Siv Hilde Houmb [1,3] and Tore Geir Soltvedt [3] and Hans Kristian Muggerud [4]

[1] Department of Information Security and Communication Technology, Norwegian University of Science and Technology, 2802 Gjøvik, Norway
[2] Department of Information Security and Communication Technology, Norwegian University of Science and Technology, 7491 Trondheim, Norway
[3] Statnett SF, 0484 Oslo, Norway
[4] Smart Infrastructure, Siemens AS, 0596 Oslo, Norway
* Correspondence: aida.akbarzadeh@ntnu.no

Abstract: Digital substations, also referred to as modern power grid substations, utilize the IEC 61850 station and process bus in conjunction with IP-based communication. This includes communication with switch yard equipment within the substation as well as the dispatch center. IEC 61850 is a global standard developed to standardize power grid communications, covering multiple communication needs related to modern power grid substations or digital substations. Unlike the legacy communication standards, IEC 60870-5-104 and DNP3, IEC 61850 is specifically designed for IP-based communication. It comprises several communication models and supports real-time communication by introducing the process bus to replace traditional peer-to-peer communication with standard network communication between substation equipment and the switch yard. The process bus, especially Sampled Measured Values (SMV) communication, in modern power grid substations relies on extremely accurate and synchronized time to prevent equipment damage, maintain power grid system balance, and ensure safety. In IEC 61850, time synchronization is provided by the Precision Time Protocol (PTP). This paper discusses the significance and challenges of time synchronization in IEC 61850 substations, particularly those associated with PTP. It presents the results of a controlled experiment that subjects time synchronization and PTP to cyber-attacks and discusses the potential consequences of such attacks. The paper also provides recommendations for potential mitigation strategies. The contribution of this paper is to provide insights and recommendations for enhancing the security of IEC 61850-based substations against cyber-attacks targeting time synchronization. The paper also explores the potential consequences of cyber-attacks and provides recommendations for potential mitigation strategies.

Keywords: smart grid; cyber security; IEC 61850; process bus; digital station; Precision Time Protocol (PTP); IEC 62351; SCADA security

check for updates

Citation: 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

Academic Editor: Ahmed Abu-Siada

Received: 4 March 2023
Revised: 12 May 2023
Accepted: 17 May 2023
Published: 8 June 2023

Copyright: © 2023 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) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

Power substations are critical links between transmission, distribution, and consumption, as shown in Figure 1. Substations play an essential role in the electricity service by converting high voltages in the generation process into lower voltages in distribution lines, so that electricity can be transmitted to consumers [1]. Over recent decades, advances in technology have led to major changes in substations and turned conventional substations with peer-to-peer serial communication into digital substations that make use of networked and IP-based communication and new standards. In this regard, the IEC 61850 standard was proposed by domain experts. This standard reduces the configuration and maintenance cost to a great extent by taking advantage of a comprehensive object-oriented data model and Ethernet technology. Indeed, replacing conventional substations with digital substations has been facilitated by the adoption of smart grid technologies and

the transition to greener power [2]. Modern substation automation systems benefit from new communication protocols, commercial off-the-shelf (COTS) computers, and various domain-specific applications that improve the operations and management of substations and increase the efficiency of the electrical grid in general.

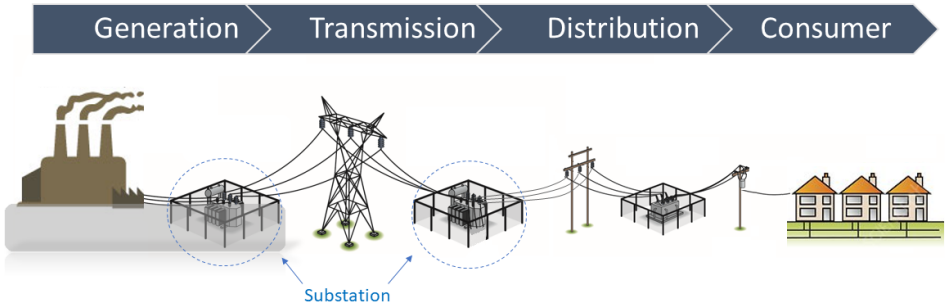

Figure 1. Location of substations in the electrical grid [1].

More specifically, the IEC 61850 standard takes advantage of a comprehensive object-oriented data model and Ethernet technology, with significant reduction in configuration and maintenance cost [3]. However, the introduction of Ethernet technology and networked communication can increase vulnerability to cyber threats, as it creates additional attack surfaces and potential entry points for attackers [4]. In the past, communication in substations used to be direct, from protection devices to primary equipment in the switch yard. However, with the introduction of IEC 61850, this communication is now provided through a network that connects various devices together. This opens up the possibility for an attacker to gain access to primary equipment by exploiting vulnerabilities in one or more devices in the substation's secondary system, such as an Intelligent Electronic Device (IED). Additionally, the communication path now extends all the way from the primary equipment to the dispatch center through networks, which could be exploited in a cyber-attack.

Power grid substations, both transmission and distribution, have over the last decade moved from using peer-to-peer communication between primary equipment (switch yard) and protection relays, and from system-specific and often proprietary protocols to Ethernet-based cross-vendor communication using the object-oriented international standard IEC 61850. The communication network within a substation is divided into three levels: process, bay, and station, as defined in IEC 61850-9-2 [3]. The process level includes the switchgear equipment, actuators, and sensors. The process bus is the communication network between the process level and bay level IEDs. IEC 61850 is a framework composed of multiple communication profiles, such as Manufacturing Message Specification (MMS), Generic Object-Oriented Substation Events (GOOSE), and Sampled Measured Values (SMV). An IEC 61850 substation uses a switched network architecture for communication and could make use of both the station bus and the process bus parts. The station bus is used to connect the IEDs and for communication with the local Human–Machine Interfaces (HMI) and the centralized dispatch center, while the process bus is design for communication between the IEDs and the primary equipment. In the context of digital substations and IEC 61850 communication, time synchronization is a critical aspect that cannot be overlooked. The process bus communication in digital substations utilizes either GOOSE or SMV messages, both of which are time-critical. In some cases, SMV messages require time source accuracy down to the microsecond, as loss of time synchronization can cause false tripping and artificial phase shift, which can be catastrophic in terms of the protection functions [5]. Therefore, devices communicating through the IEC 61850 process bus must all have the same sense of time to prevent such incidents and blocking of protection functions [5].

The synchronization of different equipment within digital substations is a crucial requirement that has been discussed in detail in [6]. This indeed turns into a more vital requirement for the operation of smart grids and for the alignment of various events across

the grid, as well as for the accurate measurement and correlation of data collected by various devices such as Phasor Measurement Units (PMUs), sensors, and IEDs. These devices play a key role in monitoring the real-time state of the grid and are primarily located at substations. Accurate time stamping of measurements is also essential for the observability, state estimation, and voltage stability of the grid [7].

Precision Time Protocol (PTP) is the preferred synchronization mechanism in IEC 61850 substations, as it is specified in IEC 61850-9-3-2016. This protocol defines how to integrate and use PTP in IEC 61850 substations, including the use of Layer 2 communication for time synchronization, the best master clock algorithm, and how to distribute time for multicast communication. Time synchronization is not just a technical issue, but a crucial service that coordinates the actions of devices dispersed across various parts of the electrical grid. The significance of time synchronization can be comprehended by recognizing the electrical grid as a complex, interconnected, and interdependent network [8]. Incidents in one part of the grid can have an impact on operations in other areas and can extend beyond the grid to other systems that depend on stable power, such as water treatment plants, transportation systems, hospitals, and so on. Therefore, it is essential to maintain the integrity of the synchronization mechanisms and ensure the stability of the power grid, especially with the increasing use of digital technologies in substations. The objective of this paper is to investigate the impact of attacks on PTP, one of the critical time synchronization protocols, and how it can influence the operation of digital substations.

1.1. Purpose and Objective

The primary aim of the research presented in this paper is to investigate potential cyber-attacks on time synchronization in IEC 61850 process bus substations, specifically through the use of Precision Time Protocol (PTP). The trustworthiness of time synchronization is paramount in enabling the efficient operation of critical use cases such as Phaser Measurement Unit (PMU), which relies on high levels of accuracy. To this end, the objective of our work has been to explore the different types of cyber-attacks on time synchronization that have the potential to cause either a loss of view, a loss of control, or both for a substation. A loss of view refers to the situation where the operator in the dispatch center loses visibility into the status and activities of the substation, while a loss of control occurs when the operator is unable to operate the substation, either remotely or locally. This paper focuses specifically on cyber-attacks which can have significant implications for the overall safety and stability of the electrical grid.

1.2. Contributions

The main contributions of this paper involve the development and testing of cyber-attacks on PTP, as well as the study of potential consequences and mitigation strategies to protect against these attacks. To conduct these experiments, cyber-attacks were run on a Hardware-in-the-loop (HIL) Digital Station testbed that utilized standard substation equipment from Siemens. These cyber-attacks were scripted in Python, and the results observed in the substation system laboratory are described in detail in this paper.

Furthermore, the paper discusses the development of mitigation strategies in collaboration with Siemens, based on recommended practices for securing IEC 61850 substations, including those outlined in IEC 62351. These strategies aim to prevent or minimize the impact of cyber-attacks on PTP and improve the overall security of digital substations. The structure of the paper is as follows. Section 2 presents a concise overview of the IEC 61850 standard and PTP. Section 3 discusses related work in the field. In Section 4, we describe the Digital Station (DS) enclave HIL testbed. Section 5 outlines the details of the implemented cyber-attacks on the testbed. Our findings, along with a potential mitigation approach to enhance the security of PTP and time synchronization, are discussed in Section 6. Finally, Section 7 summarizes our conclusions and outlines future research directions.

2. IEC 61850 and Time Synchronization

IEC 61850 defines a standard for communication and information exchange of IEDs in electrical substations [9]. The IEC 61850 standard adopts an object-oriented methodology to describe the processes in a substation and supports all functions of the substation and its engineering [10]. As shown in Figure 2, IEC 61850 supports five different communication profiles, including the SMV multicast profile, the GOOSE profile, the Generic Substation Status Event profile (GSSE), the Time Synchronization profile (TimeSync), and the Abstract Communication Service Interface profile (ACSI), which are required for different applications, as well as different communication models including client–server, publisher–subscriber, and the sample values model [3].

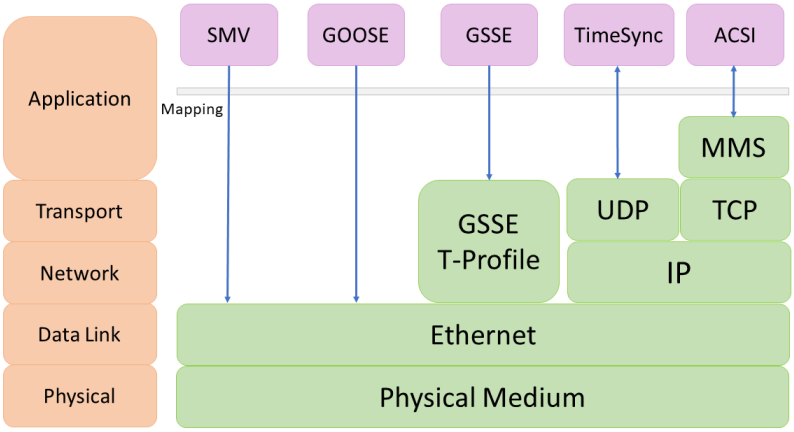

Figure 2. IEC-61850 Communication profiles [3].

In a substation, the collection of field information, such as voltage, current, and phase, through distributed communicating IEDs at different moments requires accurate time synchronization between the electronic devices [8]. Meanwhile, disturbance recording, sequential event recording, power system fault location, and sampled measured values rely on accurate timing. The importance of accurate time synchronization in power systems was highlighted by the North American blackout in August 2003 [11,12]. Additionally, based on the North American Electric Reliability Corporation (NERC) Standard PRC018-1 (https://shortest.link/eqBj (accessed on 3 March 2023)) adopted in 2006, it is a legal requirement that all recorded data provide an accuracy of 2 ms (or better) and use the Universal Coordinated Time Scale (UTC) to operate in the North American power grid [7].

Various protocols and mechanisms, including Inter-Range Instrumentation Group (IRIG) [13], Network Time Protocol (NTP) [14], Simple Network Time Protocol (SNTP) [15], and Precision Time Protocol (PTP), have been proposed for time synchronization in distributed networks [16]. Among them, PTP, which is standardized as IEEE 1588 [17], is a suitable candidate to meet these requirements, as it provides a network-based precise and accurate time distribution and allows systems with clocks of varying resolution, precision, and stability to synchronize to a single time reference with sub-microsecond accuracy [18]. PTP also meets the emerging timing accuracy needs of the station bus and process bus in IEC61850-based substations. Furthermore, IEC 61850-90-4 recommends the use of PTP for time synchronization at the substation level [19].

The use of PTP provides several benefits in networked systems, such as improved system resiliency, better monitoring of transmission and distribution networks, and the ability to meet the high-accuracy requirements of modern digital substations [20]. Furthermore, PTP is suitable for systems that include clocks of various resolution, precision, and stability and allows them to synchronize to a single time reference with sub-microsecond accuracy.

PTP is an evolution of the Network Time Protocol (NTP) and is designed to provide precise time synchronization using the waveforms of the associated clock for devices connected on a network [21]. Precision time protocol operates by synchronizing the clocks

of devices on a network to a common time reference, typically using a hardware clock or a Global Navigation Satellite System (GNSS) as the reference source. This protocol is standardized by the Institute of Electrical and Electronics Engineers (IEEE) as IEEE 1588 [17]. Precision time protocol makes use of a hierarchical network structure, where a single device known as the Grandmaster Clock (GMC) serves as the ultimate source of time for all other devices on the network utilizing PTP. Other devices, known as slave clocks, synchronize their clocks to the GMC through the exchange of PTP messages. These messages contain timestamps that are used to calculate the time offset between the slave clock and the GMC. PTP defines five different types of devices: ordinary clocks, boundary clocks, end-to-end transparent clocks, peer-to-peer transparent clocks, and management nodes [18]. Ordinary Clocks serve as either the source of time or synchronize to an existing time source and communicate over a single PTP port (Ethernet interface). A device that serves as the ultimate source of time for all other devices in the network is referred to as a Grandmaster Clock, while a device that synchronizes to another clock providing time is referred to as a Slave Clock. Boundary Clocks are multi-port network devices that synchronize to a reference time on one port and provide time on one or more other ports. These clocks are used to scale up a PTP network by servicing requests from slave clocks that would otherwise be serviced by the Grandmaster Clock.

3. Related Work

Efforts have been made over the past years by researchers to identify and implement attacks against IEC 61850, as it has been widely adopted by the power grid industry as the communication standard for digital substations. Different attacks such as *Injection attack* [22], *False data injection attack* [23–25], *Spoofing attack* [26–29], *Flooding attack* [30,31], *Replay attack* [32,33], *Man in the middle attack* [34,35] and *DoS attack* [36] are examples of attacks that have been applied against IEC 61850. Moreover, since time synchronization has a significant impact on substations and generating plants, studying the security of PTP and targeting IEC 61850 by leveraging PTP has also attracted many researchers in recent years.

Some of the known cyber-attacks that can be conducted on PTP in IEC 61850 include: Delay attacks, Spoofing attacks, Man-in-the-middle attacks, Replay attacks, Denial of service attacks, and Manipulation of transparent clocks. Table 1 describes the different types of attacks on time synchronization adapted from [37].

Table 1. Attacks on time synchronization [37].

Attack	Consequence
Denial of service (DoS)	Service Unavailable
Selective packet delay	Offset up to sync cycle
Packet manipulation	Loss of control
Byzantine master	Loss of control
Packet Removal from Control Loop	Deviation depends on clock precision
Control Loop Disruption	Deviation depends on clock precision
Packet injection	Offsets vary based on sync cycle implementation

A security analysis of PTP along with the threats associated with PTP functionality is presented in [38]. Alghamdi et al. [39] conducted two different types of attacks on PTP: a packet propagation attack and time source attack, with the aim of performing false path delay measurement and taking over the grand master clock, respectively. The experiment described in the paper was conducted on a PTP network testbed in a laboratory. However, the paper lacks clear explanations of the attack steps, and the assumption regarding the attacker's location in the system is unrealistic. Ullmann [40] has conducted a study on delay attacks on NTP and PTP time synchronization, but the authors only provide a mathematical

analysis of PTP without any experimentation or simulation. Annessi et al. [41] utilized statistical analysis to implement selective delay attacks on encrypted PTP traffic. While the authors presented an interesting and novel attack, there are potential drawbacks to consider including limited impact on many applications and lack of experimental validation.

Han and Crossley [42] discussed the impact of time synchronization attacks on PTP and performed delay attacks, packet modification attacks, spoofing attacks, and excessive traffic injection attacks on commercial PTP devices. Although the paper proposes a testbed, the authors mainly provide the attack study through mathematical analysis. The authors of the paper demonstrate the effectiveness of time delay attacks against PTP through experiments conducted on a real-time Ethernet testbed. In a recent study, Finkenzeller et al. [43] demonstrated that the introduction of delays in the transmission of PTP messages can result in significant errors in time synchronization between the master and slave clocks, thereby potentially causing disruptions in industrial control systems. The study employed an open-source testbed to evaluate the feasibility of time delay attacks against the PTP protocol. However, the limited scope of the study, which only used an open-source testbed, may not fully represent the complexity and diversity of industrial control systems in the field. Table 2 compares some of the recent works.

Reference [44] addresses security concerns related to Transparent Clocks in a Precision Time Protocol (PTP) network. The authors of [45] highlight the potential threats to PTP synchronization and demonstrate the impact of a time synchronization attack on PTP, raising concerns about the deployment of PTP in time distribution and synchronization, particularly in the smart grid. Moussa et al. [46] stated that a delay attack on PTP can highly impact smart grids. Recently, Li et al. [47] have highlighted that smart substations are the potential targets of new types of coordinated attacks, including substation trip attacks aimed directly at the substation automation systems. Such attacks can have a severe impact on the stability and reliability of smart grids and the power grid system and can also cause safety risks. Therefore, it is essential to implement security measures to protect PTP in IEC 61850 environments from cyber-attacks.

Requirements for secure clock synchronization are presented in [48] and include a definition of the necessary conditions that need to be fulfilled to secure both one-way and two-way time transfer. The detection and mitigation model proposed by Moussa et al. [46] for PTP delay attacks in substations was effective in detecting and mitigating attacks in a flat network architecture. However, it may not be as effective in different network architectures and does not address the entire PTP attack surface, highlighting the need for a more comprehensive mechanism. Alghamdi et al. [49] proposed the use of a trusted supervisor node to analyze clocks of devices for correlated drifts and identified device-specific drift rates and offset distributions to detect malicious clock de-synchronization. However, it becomes challenging to detect cases where clock manipulations occur gradually over time, and further research is needed. The proposed methods for detecting and mitigating PTP attacks have limitations, and more work is still required to study and address the evolving attack surface of PTP components. While some approaches have shown promise in detecting specific types of attacks, such as delay attacks and internal attacks, they may not be effective in all network architectures and do not cover the entire PTP attack surface.

Indeed, based on the related work discussed and as shown in Table 2, it is clear that despite the extensive research on PTP, the focus has mainly been on analyzing delay attacks. Therefore, it is imperative to explore other approaches to target PTP and manipulate time synchronization in substations beyond these limited studies. Moreover, the lack of realistic evaluation in previous works underscores the need for a comprehensive and realistic approach to testing PTP attacks. Given the complexity and diversity of industrial control systems and the differences between devices produced by different vendors, it is critical to analyze PTP using a hardware-in-the-loop (HIL) testbed. To address these gaps, this paper utilizes the Digital Station (DS) Enclave testbed as an HIL testbed to study more sophisticated attacks on PTP, rather than delay attacks, which may lead to loss of protection functions and remote control.

Table 2. Comparison of recent works on Precision Time Protocol (PTP) attacks.

Authors	Year	Focus	Types of Attack(s)	Description and Drawback
Moradi et al. [50]	2021	Mitigation	Delay attack detection	Utilizing Simulator (OMNeT++) for evaluation
Alghamdi et al. [39]	2020	Attack	Packet propagation attack and time source attack	Laboratory testbed
Ullmann et al. [40]	2009	Attack	Delay Attacks	Mathematically abstract analysis
Lisova et al. [51]	2016	Attack	Delay attack	Utilizing high level Protocol simulator
Annessi et al. [41]	2018	Attack	Delay attack	No experimental validation
Han and Crossley [42]	2019	Attack	Packet modification, spoofing, traffic injection, and delay attacks	No experimental validation

4. Digital Station Enclave Setup

In this paper, we utilize the Digital Station (DS) Enclave testbed shown in Figure 3, which covers a complete IEC 61850 substation automation system, to conduct cyber-attacks on IEC 61850 by targeting the PTP. The DS Enclave testbed has been developed as part of the CybWin Project [52] and was earlier used for analysis of different types of cyber-attacks on the SCADA protocol IEC 60870-5-104, which is used for communication between the IEC 61850 substation and the dispatch (control) center [53]. As shown in Figure 3, the digital substation consists of a station bus and a process bus, which are represented in a yellow block and a red block, respectively. The yellow block shows the station bus that interconnects all bays with the station supervisory level, while the red block depicts the process bus that interconnects the IEDs within a bay to carry real-time measurements.

The DS enclave includes digital station equipment, the control center machine, and engineering workstations used for operation and configuration. The digital station equipment used is from Siemens and desiged as a standard control system for high-voltage substations. The SICAM A8000 CP-8050 (https://cache.industry.siemens.com/dl/files/272/109757272/att_1123168/v1/Manual_CP-8031_CP-8050_ENG_DC8-026-2_18.pdf (accessed on 3 March 2023)) works as a gateway to control the interface between the local control system (i.e., substation) and the dispatch center, converts the local station protocol IEC 61850-8-1 (MMS) to the control center protocol IEC 60870-5-104, and isolates local and remote networks from each other (works as a firewall). The DS enclave utilizes an IEC 60870-5-104 test software (IECTest) to simulate the control center. As shown in Figure 3, we consider that attacks are originating from the station bus network. Section 5 explains the attack steps in more details.

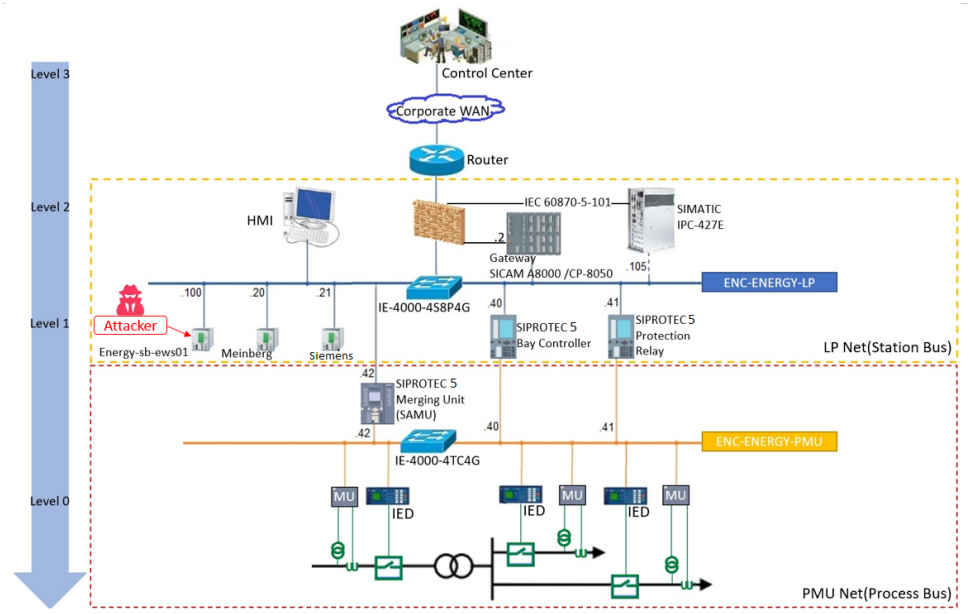

Figure 3. Digital Station (DS) enclave network architecture.

5. Implementation and Testing of Cyber-Attacks on PTP

As previously discussed, PTP is used to synchronize the time throughout the substation network. The aim of attackers is usually to break the information security triplet: confidentiality, integrity, availability. In the case of PTP, this means

- Confidentiality: Obtaining the PTP messages in the network, including the current master time, the current master clock, and the network latencies based on the delays;
- Integrity: Adding a new time source to the network, changing the master clock, and changing the time;
- Availability: Stopping a time source and preventing a device from receiving the time.

PTP operates in different modes and the PTP syncronization allows for the use of multiple clocks in the system. In the DS enclave network (see Figure 3), there are two time sources (Meinberg clock and Siemens clock). The protection relay, the merging unit, and the bay controller are also located in the same network. All of the substation equipment was connected using a Cisco industrial switch (IE-4000). To execute the attacks on PTP, we placed the attacker on the inside of the substation network (station bus), which would enable the attacker to gain access to IEC 61850 and PTP communication. There are multiple ways in which an attacker could gain access to a substation, which will be discussed later in Section 6.

The first activity that the attacker performs is reconnaissance, and Figure 4 shows the ping scan result made from the attacker's computer.

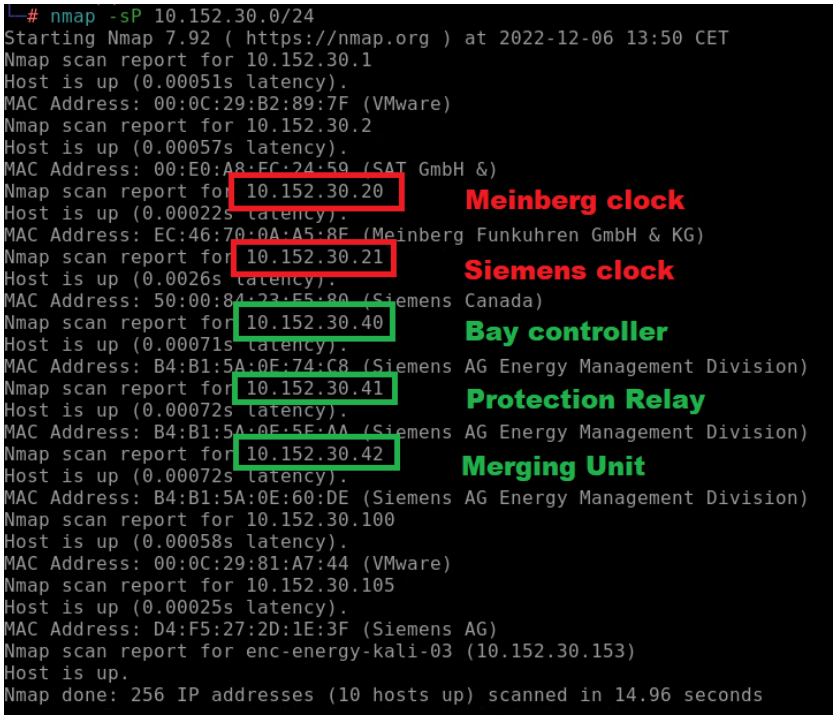

Figure 4. Discovery of the equipment communicating on the network.

In addition to the two time sources, the Cisco Industrial Ethernet Switch can work either as a transparent clock (TC) or boundary clock (BC). In our setup, it was used as a transparent clock in order to be able to forward PTP event messages with time corrections.

After the initial discovery of the network, the attacker continues with passive reconnaissance and listens to the traffic on the network. For such activity, the attacker needs to change her network adapter to be in promiscuous mode. Passive reconnaissance is carried out to avoid being detected. With a physical computer, the attacker obtains access to all broadcast messages and also the link layer messages, as can be seen in Figure 5. The attacker immediately observes that the current best master clock is the Meinberg de-

vice. To ease the next step in the attack, the attacker team developed a Python script that processed the captured traffic and matched the MAC addresses with their role, based on the previously presented ping scan. The script also highlights the main PTP parameters of the packets. The best master clock regularly sends out announce messages without a time stamp, as well as sends out sync and follow-up messages with its EPOCH time in nanosecond precision. Additionally, with access to a physical machine, the attacker also sees the link layer communication coming from the industrial switch. The figure shows that the attacker computer is connected to the leg of the switch where the MAC address ends with 84. This can be observed by the regular peer request messages, because the industrial switch as a transparent clock wants to measure the network latency between itself and the attacker's device.

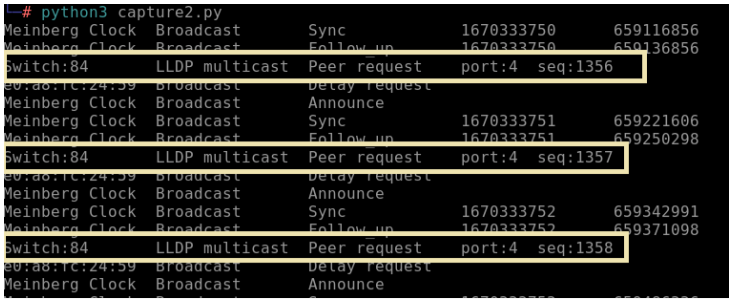

Figure 5. Passive reconnaissance.

With passive reconnaissance techniques, the attacker is able to identify

- The best master clock with its MAC address and the main characteristics (priority numbers);
- The time of the best master clock;
- The leg of the switch where the attacker's computer is connected;
- The settings of the switch (TC or BC).

By using active reconnaissance, the attacker can also send out packets and map the devices in the network, for example, with a port scan (see Figure 4). The attacker can also send out special protocol requests, for instance, to obtain the device time settings (see Figure 6). However, active techniques need to be used with care so as to not be detected. With active reconnaissance, the attacker can perform the following:

- Create an inventory of the devices in the substation;
- Obtain the MAC addresses of the devices, which might ease their identification;
- Obtain the time sources of the digital substation devices.

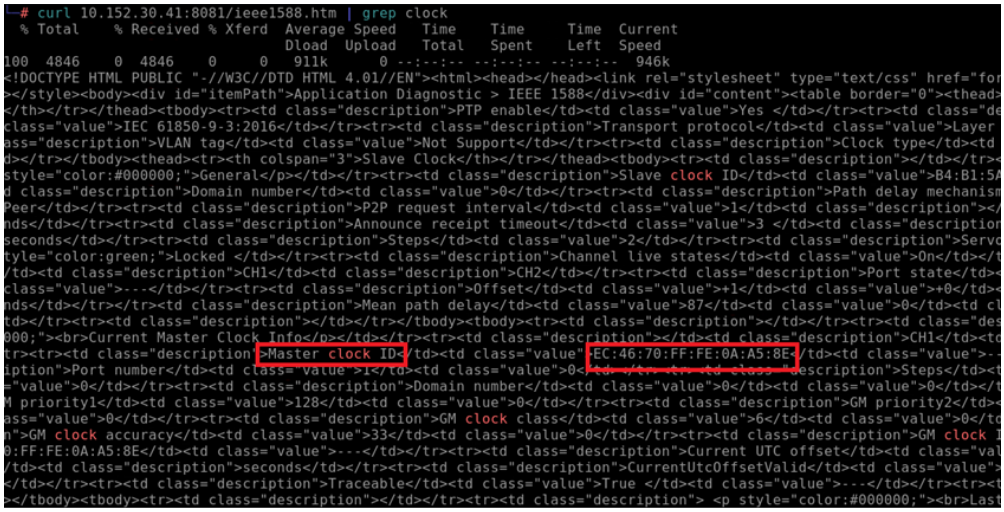

Figure 6. Obtaining the time sources of the equipment.

Based on the test carried out in our work, we concluded that the attacker most likely only needs to use passive reconnaissance to obtain the necessary information to conduct a cyber-attack on PTP. Passive reconnaissance provides information about the best master clock in the network, including its priority parameters and other settings, as well as the type of the switch used in the system and its clock settings. Using active reconnaissance, the attacker can extend this information set by directly addressing the substation equipment individually, which could be beneficial in later stages of an attack.

The next step in the attack was to manipulate the network integrity on the station bus. This attack step was made possible as the attacker had already gained access to a physical computer on the network. There are multiple ways for an attacker to achieve this, such as connecting a new device, which could alert the Intrusion Detection Systems (IDSs), if such systems are implemented, or taking over the control of a device already connected to the network. Both could be achieved by means of supply chain attacks. During our test, the aim was the following integrity changes:

- Adding a new master clock to the station bus network;
- Changing the time of the network.

Since all the clock sources send out regular announce messages, introducing a new clock requires sending out regular fake announce messages. In order to take over the best master time, the best master clock algorithm (BMCA) should be considered. The best master clock is first decided on the priority parameters, where the lower priority number represents a better clock. Our experience revealed that faking an announce message is easy; even the source MAC address of the new fake time source can be easily changed by the attacker. However, as shown in our test, merely sending out low-priority announce messages is not enough, as these are not accepted by the industrial switch, which has the role of a transparent clock, resulting in the message not being forwarded to the substation equipment. What was successful was misleading the switch with the fake announce messages, which was possible because the announce message has no timestamp that the switch can use to compare with its own time. This means that the only change that was necessary to create fake messages was to ensure increasing sequence numbers. At first, the real master clock continued sending its announcements, but after a few seconds, all time sources stopped sending broadcast messages, except for the attacker's fake time source.

Next in the attack on the integrity, the attacker started to change the time in the network. As the attacker owns the master time source and all real time sources stopped sending broadcast messages, the attacker can simply try to fake the sync and follow-up messages. This was not successful in our experiment, as these messages are not forwarded by the industrial switch, which had the role of a Transparent Clock (TC) in our setup. This could be due to the TC settings in the switch, which will be examined as part of future work. As the PTP packet forward algorithm is not made publicly available by Cisco, we cannot make conclusions based on our current experiment. However, from our experiments, the following are potential reasons why the switch did not forward the PTP packet:

- The network latency could not be calculated from the fake time source, resulting in the switch not being able to update the messages with its timestamps.
- The switch might compare the time with its own time and anomalies might have be detected, preventing the forwarding from being executed.

In order to examine the traffic going through the switch, we logged all packets arriving and leaving the switch. As presented in Figure 7, the attacker clock announce messages were forwarded on all legs, but the sync and follow-up messages appear only on one leg of the switch, which is the leg belonging to the attacker computer.

```
1669282649.883340000 Merging Unit   LLDP multicast  Peer followup   port:1  seq:5195(
1669282650.228408000 Switch:8e  LLDP multicast  Peer request    port:14 seq:58801
1669282650.228408000 Meinberg Clock LLDP multicast  Peer response   port:1  seq:58801
1669282650.238479000 Meinberg Clock LLDP multicast  Peer followup   port:1  seq:58801
1669282650.242296000 Switch:8d  LLDP multicast  Peer request    port:13 seq:19724
1669282650.277140000 Hacker Clock   Broadcast   Sync        1669282698  46025036
1669282650.305237000 Switch:83  LLDP multicast  Peer request    port:3  seq:19740
1669282650.309143000 Hacker Clock   Broadcast   Follow_up   1669282698  77347621
1669282650.348865000 Hacker Clock   Broadcast   Announce
1669282650.348865000 Hacker Clock   Broadcast   Announce
1669282650.348865000 Hacker Clock   Broadcast   Announce
1669282650.348865000 Hacker Clock   Broadcast   Announce
1669282650.348865000 Hacker Clock   Broadcast   Announce
1669282650.348865000 Hacker Clock   Broadcast   Announce
1669282650.348865000 Hacker Clock   Broadcast   Announce
1669282650.348865000 Hacker Clock   Broadcast   Announce
1669282650.349931000 Hacker Clock   Broadcast   Announce
1669282650.349931000 Hacker Clock   Broadcast   Announce
1669282650.380811000 Hacker Clock   LLDP multicast  Peer request    port:1  seq:5015
1669282650.380811000 Switch:84  LLDP multicast  Peer response   port:4  seq:5015
```

Figure 7. Switch packets on all legs during the fake time attack.

The network latency calculation between the devices and the switch is an important part of the PTP protocol when the switch is in transparent mode. To further manipulate the switch as the TC, the attacker can fake peer response and peer request messages directed to the industrial switch, which will provide network delay data and make the fake time source appear more realistic to the switch. Sending fake peer requests is relatively easy to execute since there is no timestamp inside the request. Answering the switch peer requests with peer reply and follow-up can be more tricky, since the attacker has to send a realistic time to provide realistic network delays. In our attack, the fake time source used its own EPOCH time and the switch time arriving with the switch peer responses to calculate a realistic peer response. Figure 8 shows the network data between the switch and the fake time source during the attack.

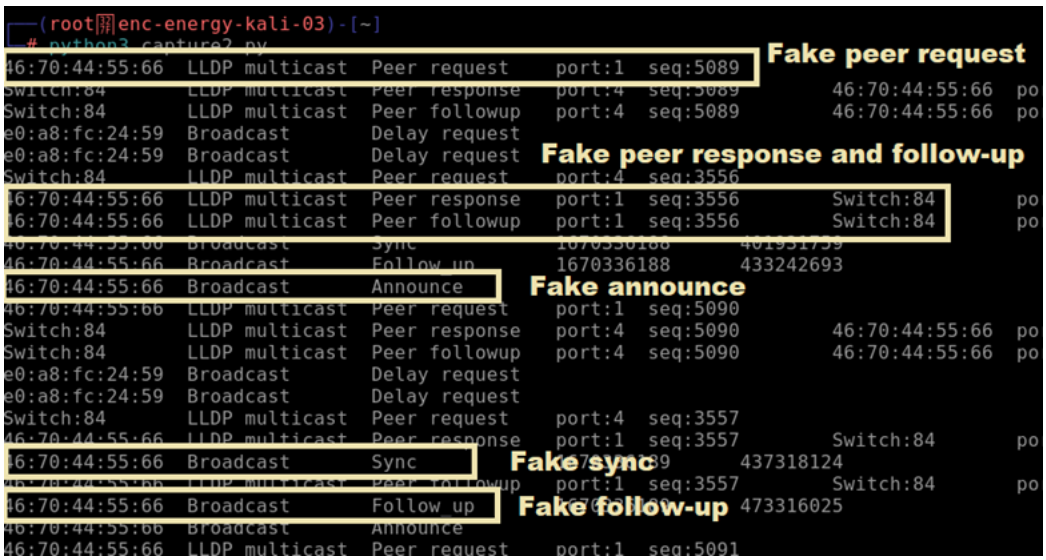

Figure 8. Faked peer request and response messages between the switch and the attacker clock.

During our testing, we implemented several fake time generation algorithms. Despite the fact that all necessary packets were emulated, the switch did not forward the attacker's fake sync and follow-up messages. From this result, we concluded that the switch as a transparent clock validates the time, even if it is coming from the best master clock, and therefore prevents sending it to the equipment on the station bus network.

Another aim of the attacker can be to create a situation similar to a Denial of Service (DoS) situation. This was the case in our experiment, as introducing a fake best master clock in the network resulted in the real time sources not longer sending time synchronization

messages, and the time synchronization on the station bus also stopped. As a result, all the equipment on the station bus will only have access to the slave time source, which is their own local time. Figure 9 shows the Merging Unit time sources during the fake master time attack.

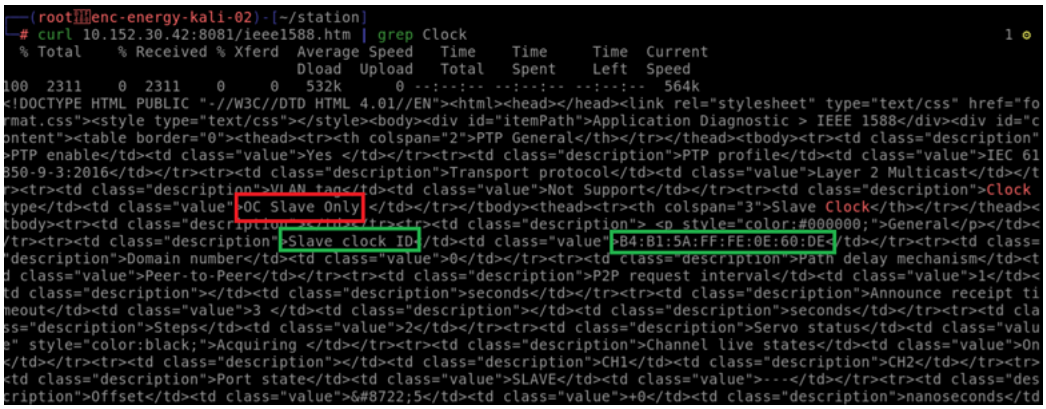

Figure 9. Merging Unit (MU) time settings after losing the best master clock PTP time.

Table 3 summarizes the attacks that were executed towards PTP on the station bus as part of our testing.

Table 3. Summary of the conducted attacks on PTP.

Attack Step	Attacker Action	Attack Technique	Outcome
Step 1 (start)	Attacker collects information regarding the clock sources (Meinberg and Siemens).	Passive reconnaissance.	Attacker obtains information that is used in later attack stages.
Step 2	Attacker takes over as the master clock	Manipulation—Rough master clock emulation.	Multiple clocks in the network (more than what is configured).
Step 3	Attacker maintains the status with the master clock emulation (repeating the message every second).	Manipulation—Rough master clock emulation with broadcast messages.	Both real clock sources stopped working. No PTP time synchronization was available in the network. IEDs start using their internal clock and flagging missing time synchronization on SVMs.
Step 4	Attacker maintains the status with the master clock emulation (repeating the message every second).	Manipulation—Rough master clock emulation with broadcast messages.	Real clocks are not operating any longer. No PTP time synchronization was available in the network. IEDs continued using their internal clock source.
Step 5	Attacker sends time synchronization messages.	Manipulation—Rough master clock emulation with broadcast messages and link layer messages.	The network switch does not forward time synchronization to IEDs. IEDs continue to use their internal clock source.
Step 6 (stop)	Attacker stops sending PTP messages.	Passive reconnaissance.	Real clock sources start to operate again after a time delay. IEDs are synchronized again after a time delay.

From step 3 of the attack, protection functions went into inactive mode, which means that the protection is blocked and no longer acting upon received sample measurement values (see Figure 10). It is important to point out that protection functions using SMVs from

multiple sources (merging units) will be blocked when PTP time synchronization is missing. This means that all recieved SMVs must be time synchronized by the same PTP time source, or from time sources synchronized by Global Navigation Satellite System (GNSS).

All described attacks were developed in Python using the Pyshark library to capture network traffic and the Scapy library to create customized network packets. The scripts were developed to accept different input parameters for the main attack characteristics. As the scripts and the controlled experiments were conducted in collaboration with a critical infrastructure owner, it was decided that the scripts themselves cannot be published.

13.02.2023 16:03:30.029	03:17:37:17.760	2000	Alarm handling	Group warning	off	good (process)	Data change	5971.301
13.02.2023 16:03:30.029	03:17:37:17.760	1999	Alarm handling	>Group Warning	off	good (process)	Data change	5971.504
13.02.2023 16:03:30.029	03:17:37:17.760	1998	General	Health	ok	good (process)	Data change	91.53
13.02.2023 16:03:30.028	03:17:37:17.759	1997	Protection:21 Distance prot. 1:General	Inactive	off	good (process)	Data change	21.901.2311.54
13.02.2023 16:03:30.028	03:17:37:17.759	1996	Protection:21 Distance prot. 1:Z 1	Inactive	off	good (process)	Data change	21.901.3571.54
13.02.2023 16:03:30.028	03:17:37:17.759	1995	Protection:21 Distance prot. 1:Z 2	Inactive	off	good (process)	Data change	21.901.3572.54
13.02.2023 16:03:30.028	03:17:37:17.759	1994	Protection:21 Distance prot. 1:Z 4	Inactive	off	good (process)	Data change	21.901.3574.54
13.02.2023 16:03:30.028	03:17:37:17.759	1993	Protection:21 Distance prot. 1:Z 3	Inactive	off	good (process)	Data change	21.901.3573.54
13.02.2023 16:03:30.028	03:17:37:17.759	1992	Protection:21 Distance prot. 1:General	Health	ok	good (process)	Data change	21.901.2311.53
13.02.2023 16:03:30.026	03:17:37:17.757	1991	Protection:21 Distance prot. 1:Z 1	Health	ok	good (process)	Data change	21.901.3571.53
13.02.2023 16:03:30.026	03:17:37:17.757	1990	Protection:21 Distance prot. 1:Z 2	Health	ok	good (process)	Data change	21.901.3572.53
13.02.2023 16:03:30.026	03:17:37:17.757	1989	Protection:21 Distance prot. 1:Z 3	Health	ok	good (process)	Data change	21.901.3573.53
13.02.2023 16:03:30.026	03:17:37:17.757	1988	Protection:21 Distance prot. 1:Z 4	Health	ok	good (process)	Data change	21.901.3574.53
13.02.2023 16:00:07.526	03:17:33:55.257	1987	Device	Cyber-security event	Login OK	good (process)	Data update	4171.322
13.02.2023 15:55:21.620	03:17:29:09.351	1986	Device	Cyber-security event	Login OK	good (process)	Data update	4171.322
13.02.2023 15:54:43.338	03:17:28:31.069	1985	Protection:21 Distance prot. 1:General	Inactive	on	good (process)	Data change	21.901.2311.54
13.02.2023 15:54:43.337	03:17:28:31.068	1984	Protection:21 Distance prot. 1:Z 1	Inactive	on	good (process)	Data change	21.901.3571.54
13.02.2023 15:54:43.337	03:17:28:31.068	1983	Protection:21 Distance prot. 1:Z 2	Inactive	on	good (process)	Data change	21.901.3572.54
13.02.2023 15:54:43.337	03:17:28:31.068	1982	Protection:21 Distance prot. 1:Z 4	Inactive	on	good (process)	Data change	21.901.3574.54
13.02.2023 15:54:43.337	03:17:28:31.068	1981	Protection:21 Distance prot. 1:Z 3	Inactive	on	good (process)	Data change	21.901.3573.54
13.02.2023 15:54:43.337	03:17:28:31.068	1980	Protection:21 Distance prot. 1:Z 1	Health	alarm	good (process)	Data change	21.901.3571.53
13.02.2023 15:54:43.337	03:17:28:31.068	1979	Protection:21 Distance prot. 1:Z 2	Health	alarm	good (process)	Data change	21.901.3572.53
13.02.2023 15:54:43.337	03:17:28:31.068	1978	Protection:21 Distance prot. 1:Z 3	Health	alarm	good (process)	Data change	21.901.3573.53
13.02.2023 15:54:43.337	03:17:28:31.068	1977	Protection:21 Distance prot. 1:Z 4	Health	alarm	good (process)	Data change	21.901.3574.53
13.02.2023 15:54:43.332	03:17:28:31.063	1976	Alarm handling	Group warning	on	good (process)	Data change	5971.301
13.02.2023 15:54:43.332	03:17:28:31.063	1975	Alarm handling	>Group Warning	on	good (process)	Data change	5971.504
13.02.2023 15:54:43.332	03:17:28:31.063	1974	General	Health	alarm	good (process)	Data change	91.53

Figure 10. Messages from the protection relay showing that it is in blocked mode (inactive).

6. Discussion

Time synchronization is a crucial service in a modern substation and critical to the substation operation, especially in IEC 61850 process bus substations. To meet the time accuracy, PTP is often applied using one or more common time sources for time synchronization. More specifically, an IEC 61850 process bus substation relies on accurate time to coordinate the actions of devices across the substation, and as devices from different vendors implement IEC 61850 and PTP differently, it was important to use physical devices rather than a simulated environment in the controlled experiments discussed in this paper. The HIL DS enclave is a setup with physical vendor hardware to enable testing of cyber-attacks on the actual implementation of the protocol rather than the theoretical implementation in a simulated environment, e.g., even though the two master clocks stopped working as a better clock was inserted into the network, the Cisco switch operating as a transparent clock (TC) did not forward the fake time to the devices on the process bus due to the implementation in the Cisco switch. This also means that switches from other vendors could respond differently, which needs to be investigated further. The same goes for substation devices from vendors other than Siemens.

As demonstrated in this paper, it is possible to put the common time source out of service by establishing a fake time source. In our testing, the common time sources (we used two in our controlled experiment) stopped working when the fake time source successfully managed to convince other devices that a more precise time source was present on the network. This means that the original and non-manipulated time sources are no longer operational. It was also observed in the experiments that the time sources often needed to be restarted to be put back into service after the fake time source attack, which extends the effect of the attack past the actual attack itself. It was further observed that it took some time from when the time sources were back online until the devices started reacting to time synchronization again. Establishing a fake time source requires the attacker to be located inside the substation network, but once located inside the network, the attack did not alert the intrusion detection systems (IDSs) in the substation (there are multiple IDSs installed in the DS enclave), as the fake clock operated with an already known MAC address and behaved in the same manner as the real master clock. The attack misused the PTP itself, which demonstrated the need for building security measures into

the protocol. Alternatively, multiple time synchronization domains can be established inside the substation, as discussed in Section 6.1.

The PTP attacks described in this paper require local access to the substation network. There are multiple ways in which this can be achieved, although all would require significant efforts and resources. In practice, this means that the attacker has the capability of an Insider or a Nation-State attacker [54]. Potential adversarial substation attack scenarios could include the following:

- An unauthorized user/device attempts to access the digital station by VPN/physically connecting to switches or to IEDs in the network.
- An infected USB drive or malware like Stuxnet can propagate in the SCADA system via removable USB drives.
- The laptop of an employee/maintenance engineer is connected to one of the smart switches in the digital station, and due to the employee/maintenance engineer's unintended or intended misuse, the attacker gains unauthorized access to the IEDs through the laptop.
- During the maintenance process of the digital station, the maintenance engineer might access the internet in order to download related updates or access the system to perform remote maintenance. An attacker may utilize this situation to penetrate the digital substation system.

Time synchronization is vital for protection functions in a digital substation environment. This was demonstrated in our experiments, as protection functions went into inactive mode, which means that the protection is blocked and no longer acting upon received sample measurement values (SMV). Protection functions using SMVs from multiple sources (merging units) will be blocked when PTP time synchronization is missing. A typical protection function for which this applies is the diffential protection, such as the transformer differential protection or the busbar differential protection. This type of protection function uses SMVs from multiple merging units and compares the incoming SMVs from one merging unit with another. During this comparison it is a prerequisite that the measured values are time-synchronized from a valid time source. This means that all recieved SMVs must be time synchronized by the same PTP time source, or from time sources synchronized by Global Navigation Satellite system.

6.1. Potential Mitigation Strategies

To improve the cyber security of PTP time synchronization and in general for process bus systems, the network topology is crucial. What characterizes a robust topology is segregation into several networks, and hence separated and independent time synchronization systems.

To protect process bus applications from being blocked due to lack of time synchronization, as was the case in the experiment described in Section 5, local PTP grand master clocks capable to time-synchronize the protection applications, even with loss of the main grandmaster clocks (i.e., Meinberg Lantime M1000 and Siemens RSG2488), can be deployed in different network segments. This capability is already available from substation automation vendors who offer implemented GMC functionality into process bus equipment, e.g., in bay controllers, protection relays, and merging units. Using this built-in capability ensures local GMC establishment in a cost-efficient manner without adding additional time synchronization equipment into the network. The same equipment also supports network features like layer 2 switching, VLAN segmentation, network redundancy protocols, e.g., High Availability Seamless Redundancy (HSR) and Parallel Redundancy Protocol (PRP). This provides the opportunity to create subnetworks within the process bus, without adding additional network equipment.

For example, to mitigate the PTP cyber-attack discussed in this paper (manipulating the grandmaster clock), the distributed busbar protection can be used, which is one of the protection functions where time synchronization is crucial. To achieve independence from the main GMCs and prevent the busbar protection from being blocked due to a

time synchronization error, the busbar relay itself can act as GMC for its underlying sampled values (SMV) publishers, e.g., the merging units. To further strengthen the time synchronization, two busbar protection relays can be used, acting as GMC 1 and GMC 2, using the best master clock (BMCA) algorithm.

For network segmentation, the distributed busbar protection can be segregated from the overlaying PRP-network by establishing a separate HSR-network, as shown in Figure 11. The internal clock in busbar protection relays 1 and 2 are date- and time-synchronized by the main GMCs (i.e., Meinberg Lantime M1000 and Siemens RSG2488). On the contrary, the merging units in the HSR network are time-synchronized by the free-running local clocks GMC 1 and GMC 2 of the busbar protection relay. If the main time sources fail or provide poor time quality, as was the case in our experiment, the local GMCs continue to operate uninterrupted, and time synchronization of the busbar protection system is provided by the local clock oscillator in busbar protection relays 1 and 2.

This mitigation strategy has not been tested as part of this work, but future work includes re-running the controlled experiments with the proposed mitigation strategy implemented to verify whether it does indeed prevent time synchronization errors on the segregated process bus devices.

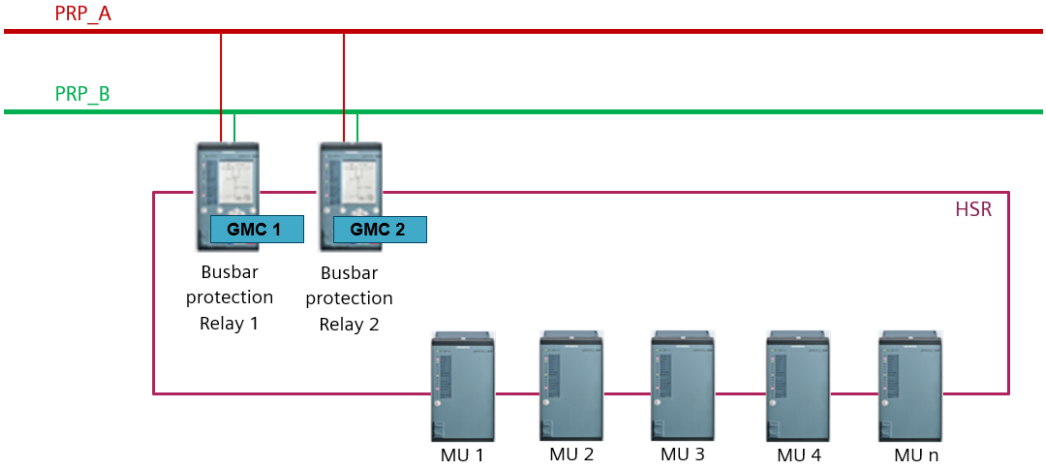

Figure 11. Segregating busbar protection from overlaying PRP-network by means of a separate HSR-network.

7. Conclusions and Future Works

Modern substations make use of the IEC 61850 station and process bus and are dependent on accurate time synchronized across all the substation devices. This paper describes an HIL testbed for an IEC 61850 process bus substation (DS Enclave) and demonstrates the consequence of manipulating the time synchronization in digital (IEC 61850 process bus) substations. This was accomplished by conducting several rounds of cyber-attacks (controlled experiments) exploiting weaknesses in the PTP protocol itself, such as by introducing a fake time source. The cyber-attacks were carried out as controlled experiments that were run several times to ensure that the results observed were not due to circumstances but due to the manner in which PTP is implemented on the specific devices. To achieve this, the controlled experiment was carried out on real substation devices, including for the clock sources. This reduced the bias associated with simulated environments, especially those related to the implementation of PTP in a device. The experiments demonstrated that it is possible to fake the time source and further affect protection functions. It is important to point out that protection functions using SMVs from multiple sources (merging units) will be blocked when PTP time synchronization is missing. Future work will include multiple merging units to further investigate which protection functions are affected and best practice how to mitigate protection blocking when PTP time synchronization is lost. Future work will also involve repeating the exact same cyber-attacks on other vendor equipment.

Future work will also focus on setting up experiments and simulations to study the impact of cyber-attacks that extend beyond a local substation. We also aim to examine the cascading effects of cyber-attacks, which were not demonstrated in this study. Such work will require the utilization of real-world simulators and will involve testing on a single substation using the Digital Station (DS) enclave, as well as a simulated environment to evaluate potential consequences across the power grid system.

Author Contributions: Writing—original draft, A.A., L.E., S.H.H., T.G.S. and H.K.M. All authors have read and agreed to the published version of the manuscript.

Funding: This work has received funding from the Research Council of Norway through the CybWin (Cybersecurity Platform for Assessment and Training for Critical Infrastructures-Legacy to digital twin) project with project no. 287808.

Data Availability Statement: Due to the sensitive and critical nature of the data involved, we are unable to provide it for public access. This decision was made to ensure the confidentiality and privacy of the entities involved in the study, as well as to comply with ethical guidelines and data protection regulations.

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

References

1. Gutierrez, S.; Botero, J.F.; Gaviria, N.; Fletscher, L.A.; Leal, E.A. *Next-Generation Power Substation Communication Networks: IEC 61850 Meets Programmable Networks*; IEEE: Piscataway, NJ, USA, 2022.
2. EPRI. *Report to NIST on the Smart Grid Interoperability Standards Roadmap*; Technical Report; EPRI: Washington, DC, USA, 2009.
3. Liang, Y.; Campbell, R.H. *Understanding and Simulating the IEC 61850 Standard*; Technical Report; University of Illinois: Champaign, IL, USA, 2008.
4. Ten, C.W.; Manimaran, G.; Liu, C.C. Cybersecurity for critical infrastructures: Attack and defense modeling. *IEEE Trans. Syst. Man Cybern.-Part A Syst. Hum.* **2010**, *40*, 853–865. [CrossRef]
5. Shrestha, A.; Silveira, M.; Yellajosula, J.; Kumar Mutha, S. Understanding the Impacts of Time Synchronization and Network Issues on Protection in Digital Secondary Systems. In Proceedings of the PAC World Global Conference 2021, Prague, Czech Republic, 31 August–1 September 2021; Schweitzer Engineering Laboratories, Inc.: Pullman, WA, USA, 2021; p. 12.
6. Ridwan, M.; Tambunan, H.; Mangunkusumo, K.; Habibie, A.; Pramana, P. Review of digital substation equipment and technical specification in Indonesia. In Proceedings of the IOP Conference Series: Materials Science and Engineering, High Tatras, Slovakia, 13–15 October 2021; IOP Publishing: Bristol, UK, 2021; Volume 1098, p. 042053.
7. Baumgartner, B.; Riesch, C.; Rudigier, M. IEEE 1588/PTP: The future of time synchronization in the electric power industry. In Proceedings of the PAC World Conference, Budapest, Hungary, 25–28 June 2012.
8. Haapoja, S. Study and Design of Inter-Range Instrumentation Group Time Code B Synchronization of IEC 61850 Sampled Values. Master's Thesis, University of Vaasa, Vaasa, Finland, 2018.
9. Mackiewicz, R.E. Overview of IEC 61850 and Benefits. In Proceedings of the 2006 IEEE Power Engineering Society General Meeting, Montreal, QC, Canada, 18–22 June 2006; IEEE: Piscataway, NJ, USA, 2006; p. 8.
10. Ozansoy, C.R.; Zayegh, A.; Kalam, A. Object modeling of data and datasets in the international standard IEC 61850. *IEEE Trans. Power Deliv.* **2009**, *24*, 1140–1147. [CrossRef]
11. Sagen, E.; Workman, K. Methods of time synchronization. In Proceedings of the 63rd Annual Georgia Tech Protective Relaying Conference, Atlanta, GA, USA, 20–21 April 2009; pp. 1–8.
12. Andersson, G.; Donalek, P.; Farmer, R.; Hatziargyriou, N.; Kamwa, I.; Kundur, P.; Martins, N.; Paserba, J.; Pourbeik, P.; Sanchez-Gasca, J.; et al. Causes of the 2003 major grid blackouts in North America and Europe, and recommended means to improve system dynamic performance. *IEEE Trans. Power Syst.* **2005**, *20*, 1922–1928. [CrossRef]
13. Matson, J. *Choosing the Correct Time Synchronization Protocol and Incorporating the 1756-Time Module into Your Application*; Rockwell Automation: Milwaukee, WI, USA, 2013.
14. Mills, D.L. Internet time synchronization: The network time protocol. *IEEE Trans. Commun.* **1991**, *39*, 1482–1493. [CrossRef]
15. Mills, D. Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI. Technical Report. 2006. Available online: https://www.rfc-editor.org/rfc/rfc4330.html (accessed on 3 March 2023).
16. Schweitzer, E.; Whitehead, D.; Achanta, S.; Skendzic, V. Implementing robust time solutions for modern power systems. In Proceedings of the 14th Annual Western Power Delivery Automation Conference, Spokane, WA, USA, 27–29 March 2012.
17. *IEEE Std 1588-2008*; IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems. IEEE: Piscataway, NJ, USA, 2008; pp. 1–269. [CrossRef]
18. Watt, S.T.; Achanta, S.; Abubakari, H.; Sagen, E.; Korkmaz, Z.; Ahmed, H. Understanding and applying precision time protocol. In Proceedings of the 2015 Saudi Arabia Smart Grid (SASG), Jeddah, Saudi Arabia, 7–9 December 2015; IEEE: Piscataway, NJ, USA, 2015; pp. 1–7.

19. *EC61850-90-4*; Network Engineering Guideline for Communication Networks and Systems in Substations. IEC: Geneva, Switzerland, 2013.
20. Jones, T.; Arnold, D.; Tuffner, F.; Cummings, R.; Lee, K. Recent advances in precision clock synchronization protocols for power grid control systems. *Energies* **2021**, *14*, 5303. [CrossRef]
21. Marrero, L.M.; Merlano-Duncan, J.C.; Querol, J.; Kumar, S.; Krivochiza, J.; Sharma, S.K.; Chatzinotas, S.; Camps, A.; Ottersten, B. Architectures and Synchronization Techniques for Distributed Satellite Systems: A Survey. *IEEE Access* **2022**, *10*, 45375–45409. [CrossRef]
22. Wright, J.G.; Wolthusen, S.D. Stealthy Injection Attacks Against IEC61850's GOOSE Messaging Service. In Proceedings of the 2018 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe), Sarajevo, Bosnia and Herzegovina, 21–25 October 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 1–6.
23. Chlela, M.; Joos, G.; Kassouf, M.; Brissette, Y. Real-time testing platform for microgrid controllers against false data injection cybersecurity attacks. In Proceedings of the 2016 IEEE Power and Energy Society General Meeting (PESGM), Boston, MA, USA, 17–21 July 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 1–5.
24. Kabir-Querrec, M.; Mocanu, S.; Thiriet, J.M.; Savary, E. A test bed dedicated to the study of vulnerabilities in IEC 61850 power utility automation networks. In Proceedings of the 2016 IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA), Berlin, Germany, 1–6 September 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 1–4.
25. Chattopadhyay, A.; Ukil, A.; Jap, D.; Bhasin, S. Toward threat of implementation attacks on substation security: Case study on fault detection and isolation. *IEEE Trans. Ind. Inform.* **2017**, *14*, 2442–2451. [CrossRef]
26. Hoyos, J.; Dehus, M.; Brown, T.X. Exploiting the GOOSE protocol: A practical attack on cyber-infrastructure. In Proceedings of the 2012 IEEE Globecom Workshops, Anaheim, CA, USA, 3–7 December 2012; IEEE: Piscataway, NJ, USA, 2012; pp. 1508–1513.
27. Kabir-Querrec, M.; Mocanu, S.; Bellemain, P.; Thiriet, J.M.; Savary, E. Corrupted goose detectors: Anomaly detection in power utility real-time ethernet communications. In Proceedings of the GreHack 2015, Grenoble, France, 20–22 November 2015.
28. Noce, J.; Lopes, Y.; Fernandes, N.C.; Albuquerque, C.V.; Muchaluat-Saade, D.C. Identifying vulnerabilities in smart gric communication networks of electrical substations using geese 2.0. In Proceedings of the 2017 IEEE 26th International Symposium on Industrial Electronics (ISIE), Edinburgh, UK, 19–21 June 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 111–116.
29. Da Silva, L.E.; Coury, D.V. A new methodology for real-time detection of attacks in IEC 61850-based systems. *Electr. Power Syst. Res.* **2017**, *143*, 825–833. [CrossRef]
30. Zhang, F.; Mahler, M.; Li, Q. Flooding attacks against secure time-critical communications in the power grid. In Proceedings of the 2017 IEEE International Conference on Smart Grid Communications (SmartGridComm), Dresden, Germany, 23–26 October 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 449–454.
31. Li, Q.; Ross, C.; Yang, J.; Di, J.; Balda, J.C.; Mantooth, H.A. The effects of flooding attacks on time-critical communications in the smart grid. In Proceedings of the 2015 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, USA, 17–20 February 2015; IEEE: Piscataway, NJ, USA, 2015; pp. 1–5.
32. Elbez, G.; Keller, H.B.; Hagenmeyer, V. A cost-efficient software testbed for cyber-physical security in iec 61850-based substations. In Proceedings of the 2018 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), Aalborg, Denmark, 29–31 October 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 1–6.
33. Strobel, M.; Wiedermann, N.; Eckert, C. Novel weaknesses in IEC 62351 protected smart grid control systems. In Proceedings of the 2016 IEEE International Conference on Smart Grid Communications (SmartGridComm), Sydney, Australia, 6–9 November 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 266–270.
34. Subramaniam Rajkumar, V.; Tealane, M.; Stefanov, A.; Palensky, P. Cyber Attacks on Protective Relays in Digital Substations and Impact Analysis. In Proceedings of the 8th Workshop on Modeling and Simulation of Cyber-Physical Energy Systems, MSCPES 2020-Proceedings, Sydney, Australia, 21 April 2020; IEEE: Piscataway, NJ, USA, 2020.
35. Kang, B.; Maynard, P.; McLaughlin, K.; Sezer, S.; Andrén, F.; Seitl, 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), Luxembourg, 8–11 September 2015; IEEE: Piscataway, NJ, USA, 2015; pp. 1–8.
36. Zhang, J.; Chen, Y.; Jin, N.; Hou, L.; Zhang, Q. OPNET based simulation modeling and analysis of DoS attack for digital substation. In Proceedings of the 2017 IEEE Power & Energy Society General Meeting, Chicago, IL, USA, 16–20 July 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 1–5.
37. Gaderer, G.; Treytl, A.; Sauter, T. Security aspects for IEEE 1588 based clock synchronization protocols. In Proceedings of the IEEE International Workshop on Factory Communication Systems (WFCS), Torino, Italy, 28–30 June 2006; pp. 247–250.
38. Tsang, J.; Beznosov, K. A security analysis of the precise time protocol (short paper). In Proceedings of the International Conference on Information and Communications Security, Raleigh, NC, USA, 4–7 December 2006; Springer: Berlin/Heidelberg, Germany, 2006; pp. 50–59.
39. Alghamdi, W.; Schukat, M. Cyber Attacks on Precision Time Protocol Networks—A Case Study. *Electronics* **2020**, *9*, 1398. [CrossRef]
40. Ullmann, M.; Vögeler, M. Delay attacks—Implication on NTP and PTP time synchronization. In Proceedings of the 2009 International Symposium on Precision Clock Synchronization for Measurement, Control and Communication, Brescia, Italy, 12–16 October 2009; IEEE: Piscataway, NJ, USA, 2009; pp. 1–6.

41. Annessi, R.; Fabini, J.; Iglesias, F.; Zseby, T. Encryption is futile: Delay attacks on high-precision clock synchronization. *arXiv* **2018**, arXiv:1811.08569.
42. Han, M.; Crossley, P. Vulnerability of IEEE 1588 under time synchronization attacks. In Proceedings of the 2019 IEEE Power & Energy Society General Meeting (PESGM), Atlanta, GA, USA, 4–8 August 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 1–5.
43. Finkenzeller, A.; Wakim, T.; Hamad, M.; Steinhorst, S. Feasible Time Delay Attacks Against the Precision Time Protocol. In Proceedings of the GLOBECOM 2022-2022 IEEE Global Communications Conference, Rio de Janeiro, Brazil, 4–8 December 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 3375–3380.
44. Treytl, A.; Hirschler, B. Security flaws and workarounds for IEEE 1588 (transparent) clocks. In Proceedings of the 2009 International Symposium on Precision Clock Synchronization for Measurement, Control and Communication, Brescia, Italy, 12–16 October 2009; IEEE: Piscataway, NJ, USA, 2009; pp. 1–6.
45. Zhang, Z.; Gong, S.; Dimitrovski, A.D.; Li, H. Time synchronization attack in smart grid: Impact and analysis. *IEEE Trans. Smart Grid* **2013**, *4*, 87–98. [CrossRef]
46. Moussa, B.; Debbabi, M.; Assi, C. A detection and mitigation model for PTP delay attack in an IEC 61850 substation. *IEEE Trans. Smart Grid* **2016**, *9*, 3954–3965. [CrossRef]
47. Li, Z.; Ma, R.; Xie, Y.; Lu, L. Overview of Intrusion Detection in Smart Substation. In Proceedings of the 2022 IEEE 10th Joint International Information Technology and Artificial Intelligence Conference (ITAIC), Chongqing, China, 8–10 December 2022; Volume 10, pp. 2377–2384. [CrossRef]
48. Narula, L.; Humphreys, T.E. Requirements for secure clock synchronization. *IEEE J. Sel. Top. Signal Process.* **2018**, *12*, 749–762. [CrossRef]
49. Alghamdi, W.; Schukat, M. Advanced methodologies to deter internal attacks in PTP time synchronization networks. In Proceedings of the 2017 28th Irish Signals and Systems Conference (ISSC), Killarney, Ireland, 20–21 June 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 1–6.
50. Moradi, M.; Jahangir, A.H. A new delay attack detection algorithm for PTP network in power substation. *Int. J. Electr. Power Energy Syst.* **2021**, *133*, 107226. [CrossRef]
51. Lisova, E.; Uhlemann, E.; Steiner, W.; Åkerberg, J.; Björkman, M. Risk evaluation of an ARP poisoning attack on clock synchronization for industrial applications. In Proceedings of the 2016 IEEE International Conference on Industrial Technology (ICIT), Taipei, Taiwan, 14–17 March 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 872–878.
52. Jørgensen, P.A.; Waltoft-Olsen, A.; Houmb, S.H.; Toppe, A.L.; Soltvedt, T.G.; Muggerud, H.K. Building a hardware-in-the-loop (HiL) digital energy station infrastructure for cyber operation resiliency testing. In Proceedings of the 3rd International Workshop on Engineering and Cybersecurity of Critical Systems, Pittsburgh, PA, USA, 16 May 2022; pp. 9–16.
53. Erdődi, L.; Kaliyar, P.; Houmb, S.H.; Akbarzadeh, A.; Waltoft-Olsen, A.J. Attacking Power Grid Substations: An Experiment Demonstrating How to Attack the SCADA Protocol IEC 60870-5-104. In Proceedings of the 17th International Conference on Availability, Reliability and Security, Vienna, Austria, 23–26 August 2022; pp. 1–10.
54. Rocchetto, M.; Tippenhauer, N.O. On attacker models and profiles for cyber-physical systems. In Proceedings of the European Symposium on Research in Computer Security, Heraklion, Greece, 26–30 September 2016; Springer: Berlin/Heidelberg, Germany, 2016; pp. 427–449.

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.