International Journal of Information Security
https://doi.org/10.1007/s10207-024-00856-6

REGULAR CONTRIBUTION

Two-stage advanced persistent threat (APT) attack on an IEC 61850 power grid substation

Aida Akbarzadeh[1] · Laszlo Erdodi[2] · Siv Hilde Houmb[1] · Tore Geir Soltvedt[3]

© The Author(s) 2024

Abstract
Advanced Persistent Threats (APTs) are stealthy, multi-step attacks tailored to a specific target. Often described as 'low and slow', APTs remain undetected until the consequences of the cyber-attack become evident, usually in the form of damage to the physical world, as seen with the Stuxnet attack, or manipulation of an industrial process, as was the case in the Ukraine Power Grid attacks. Given the increasing sophistication and targeted nature of cyber-attacks, especially APTs, this paper delves into the substantial threats APTs pose to critical infrastructures, focusing on power grid substations. Through a detailed case study, we present and explore a 2-stage APT attack on an IEC 61850 power grid substation, employing a Hardware-in-the-Loop (HIL) testbed to simulate real-world conditions. More specifically, this paper discusses two significant experiments conducted to assess vulnerabilities in the control protocols used in IEC 61850 substations: IEC 60870-5-104 and IEC 61850. The integration of findings from these experiments revealed a number of previously undiscussed potential threats to power grid infrastructure that could arise from attacking one or more substations. To better address these potential threats, the paper proposes an extension to the Industrial Control System (ICS) kill chain that explicitly accounts for the consequences of attacks on the physical aspects of Cyber-Physical Systems (CPSs).

Keywords Advanced persistent threats (APT) · Cyber-physical systems (CPS) · Digital substation · IEC 61850 · IEC 60870-5-104 · Industrial control systems (ICSs) · APT kill chain

1 Introduction

Cyber-attacks have become more sophisticated and targeted over the last decade, starting with the Stuxnet attack in 2010 [1]. Cyber-attacks are used as part of hybrid warfare, and as more nation-state attacker groups have appeared, the attacker capabilities have increased significantly. In practice, this means that cyber-attacks are part of the political climate and used both as part of defensive and offensive cyberspace operations [2]. Furthermore, when the adversary gains a foothold inside a target network, it only takes a few minutes before the network is compromised [3]. That is while it takes an average of 207 days for defenders to detect and react [4]. This means that it is necessary to develop better detection capabilities, but also that it is necessary to better understand offensive cyberspace operations, and as part of this, Advanced Persistent Threat attacks. The 'who,' 'why,' 'when,' and 'what' are essential pieces of information required to defend against cyber-attacks, particularly sophisticated APT attacks.

Reviewing recent reports on large scale security breaches and APT campaigns revealed that APT groups have expanded their focus to encompass a broad array of industries and governmental entities [5, 6]. An APT attack terminates either upon detection or upon the attackers' successful attainment of their objectives. In both instances, the targeted organization experiences substantial consequences, frequently encom-

✉ Aida Akbarzadeh
aida.akbarzadeh@ntnu.no

Laszlo Erdodi
laszlo.erdodi@ntnu.no

Siv Hilde Houmb
siv.houmb@ntnu.no

Tore Geir Soltvedt
tore.soltvedt@statnett.no

[1] Dept. of Information Security and Communication Technology, Norwegian University of Science and Technology, Gjøvik, Norway

[2] Dept. of Information Security and Communication Technology, Norwegian University of Science and Technology, Trondheim, Norway

[3] Statnett SF, Oslo, Norway

Published online: 14 May 2024

passing irreparable harm [5]. The authors in [6] mentioned that APT attacks target survivability, availability, confidentiality, and/or integrity of organizations. As a result, the severity of the consequences of an APT attack is heightened when it remains undetected until the attackers accomplish their predefined objectives.

Despite the necessity of investigating APT attacks within the industrial security community, there is a notable lack of a comprehensive and well-defined understanding of the APT research problem. Earlier work has solely focused on APT attacks as a means of data exfiltration. However, Industry 4.0 brings with it blurring of the border between Information Technology (IT) and Operational Technology (OT), and attackers have based on this found new opportunities to utilize APT attacks to cause damage to Critical Infrastructures (CIs). Consequently, this paper focuses on establishing a deeper understanding of the activities involved in APT attacks on substations, i.e., what is needed to achieve the results observed in power grid cyber-attacks thus far. The study has focused on developing APT attacks and demonstrating these on an IEC 61850 substation HIL testbed. The aim is to demonstrate potential damage to the physical equipment and the power grid process, with the goal of uncovering how to achieve longer downtime than what has been observed in previous cyber-attacks on the power grid. More precisely, this paper attempts to answer the following research questions:

- Research Question 1: Is the conventional kill chain model applicable to APT attacks targeting CPS?
- Research Question 2: What role does the physical domain play in APT attacks on CPS?

The rest of the paper is organized as follows: Sect. 2 presents background information related to APTs and digital substations. Related work is discussed in Sect. 3, including APT attacks and kill chain, while Sect. 4 describes APT kill chain on CPS and the proposed changes to the kill chain. Section 5 describes the adversary model, and Sect. 6 describes the testbed used in the case study. Section 7 describes the attack steps in the two-stage APT attack on the IEC 61850 testbed deployed in the case study. Section 8 discusses the main findings described in the paper, and Sect. 9 summarizes the main findings and contributions of the paper, as well as points to future work.

2 Background

2.1 Advanced persistent threat

Advanced Persistent Threats was established as a term in the late 2000 s as a result of an increased sophistication in cyber-attacks. According to the US National Institute of Standards and Technology (NIST) [7], an APT is characterized as an adversary possessing advanced skills and substantial resources. APTs employ various attack methods, including cyber, physical, and deception, to accomplish their objectives. These objectives often encompass gaining access to an organization's IT infrastructure, extracting information, disrupting critical missions, programs, or organizations, and positioning themselves for future actions. In summary, APTs exhibit the following characteristics: (i) pursues its objectives repeatedly over an extended period of time, (ii) adapts to defenders' efforts to resist it, and (iii) remains determined to maintain the level of interaction needed to execute its objectives.

The Titan Rain, Hydraq, Stuxnet, RSA SecureID Attack, and Carbanak are real examples of APT attacks that has been reported in recent years [5].

2.2 Digital substation

The term "digital substation" refers to a modernized substation infrastructure where data originating from process-level equipment is converted into digital format at the source. This is also often referred to as an IEC 61850 substation. In practice, this means that the substation is built up with an end-to-end communication network that facilitates the exchange of data, commands, and signals between the process level and the bay level. This communication is making use of the IEC 61850 standard which covers data format, data access, and exchange mechanisms.

In a digital substation framework, the process bus plays a pivotal role by disseminating a precise time reference to synchronize substation equipment. Additionally, it carries operational data such as current and voltage measurements, as well as control and protection signals. Meanwhile, the station bus serves as the communication backbone connecting the station and bay levels. This interconnectness enables seamless communication between these two levels and facilitates peer-to-peer communication among bay-level devices. Much like the process bus, the station bus functions as an Ethernet LAN network.

In order to transition to digital substations, the incorporation of Merging Units (MUs) becomes imperative. These units are responsible for converting traditional instrument transformers' analog data, specifically currents and voltages, into a digital form, thereby modernizing the substation infrastructure.

In the energy industry, a range of specialized standards, technologies, and protocols are used to automate substation control systems. MODBUS, IEC 60870, DNP3, and IEC 61850 (GOOSE, SV, MMS) are among the most widely used protocols.

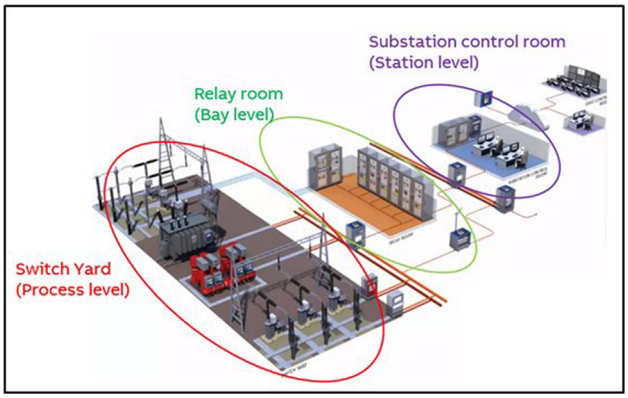

Fig. 1 Digital substation [9]

2.3 IEC 60870-5-104

IEC 60870-5-104 is a communication protocol that allows power plants or transformation stations to control their control systems remotely from a central control room [8]. The protocol can also be used for internal communication within the control system of a power plant. Using a uniform protocol allows automated systems from different suppliers to be integrated and controlled without the need for protocol converters or adaptations. IEC 104 is based on IEC 60870-5-101 (IEC 101), a telecontrol protocol for power system automation applications. IEC 104 gives IEC 101 network access, allowing control rooms and operations centers to communicate via a typical TCP/IP network. This is accomplished by deleting the serial header and replacing it with the proper headers for full duplex TCP/IP connectivity. IEC 101 requires confirmation for each message transmitted, but IEC 104 assumes the channel is stable and allows a maximum number of K-messages to be sent without waiting for confirmation from the opposing station. IEC 104 replaces the serial header with its own APCI header (Fig. 1).

2.4 IEC 61850

IEC 61850 represents a globally recognized international standard designed to govern communication networks and systems within the realm of energy supply automation. The primary objective of this standard is to establish a unified communication system that relies on optical fiber and Ethernet technologies, promoting rapid and seamless interactions. Importantly, it is designed to be compatible with other industry standards and can be implemented across various suppliers' systems.

The overarching aim of IEC 61850 is to foster more efficient operations within the energy supply sector, while also ensuring financial viability for potential future expansions or maintenance efforts. As an open standard, IEC 61850 fosters a collaborative environment, facilitating the integration of critical components such as energy system protection, control, measurement, and monitoring. This standardized approach contributes to the reliability and interoperability of energy supply systems, ultimately benefiting both providers and consumers.

2.5 Attack surface

The cyber-attack surface on a modern substation differs significantly from IT and enterprise networks and systems, and is determined by the system architecture of the substation. A modern substation, although comprised of an end-to-end network communication, does not communicate directly outside of the substation domain. The system architecture typically consist of a SCADA interface to the dispatch center (controlling station) and the substation itself with its bay and process levels. An IEC 61850 substation is comprised of a number of Intelligent Electronic Devices (IEDs) that together communication over something called the IEC 61850 station bus. The IEDs receive data from process bus devices, and although operating in a network environment, these cyber-physical devices are rarely protected and represent a potential attack surface. As was demonstrated in the 2015 Ukraine power grid attack, firmware of such devices can be replaced by malicious firmware, and as demonstrated in Stuxnet, malware can be placed inside of CPS using removable media, such as USB. Additionally, the SCADA interface represent an attack surface, not because it is connected to the Internet, but because the SCADA protocols in use does not have built-in security measures. All the attackers needs to do, is to find a way to gain access to the SCADA system, which will be demonstrated later in this paper. Table 1 lists some of the potential cyber-attacks against IEDs.

3 Related work

Advanced Persistent Threats have become increasingly critical in the cybersecurity landscape, particularly considering the increasing convergence of IT and OT in critical infrastructures. Chen et al. [11] conducted a comprehensive study on APTs and highlights the distinguishing characteristics of APTs in contrast to traditional threats as: (1) the targeting of specific entities with clear objectives, (2) the involvement of well-organized and well-funded attackers, (3) the execution of prolonged campaigns featuring repeated attempts, and (4) the utilization of stealthy and evasive attack methods. Inspired by the intrusion kill chain [12], the authors in [11] summarized that a typical APT attack encompasses six phases, namely: (1) reconnaissance and weaponization, (2) delivery, (3) initial intrusion, (4) command and control, (5) lateral movement, (6) data exfiltration. In a recent work,

Table 1 Potential cyber-attacks on IEDs in a digital substation [10]

Attack method	Description
Unauthorized access (UA)	Extracting sensitive data from the IED
Denial of service (DoS)	Disconnecting the IED from the grid
Spoofing (SP)	Physical or logical spoofing of IEDs to mislead other IEDs
Data interception (DI)	Important data on the IED are revealed
Man-in-the-middle attack (MITM)	Forwarding surveillance system and IED traffic to the attacker
Operating system attack (OSA)	Manipulating the operation database of the IED

Sharma et al. [6] extensively discussed APT attack phases and available APT attack frameworks [12–15].

The authors represented a taxonomy of APT anatomy in six phases including Reconnaissance, Weaponization, Delivery, Establish Foothold, Command & Control, Lateral Movement, and Accomplishing Goal. Similar to the previous study outlined in [11], the authors defined the primary objectives of APT attacks as Data Exfiltration and Data Destruction, emphasizing a shared focus on data-related objectives.

In another systematic review on APTs, Hussain et al. [16] classified APT threat dimensions into three distinct categories: (1) Industrial Threat Vector, (2) Military Threat Vector, and (3) Datasets. Alshamrani et al. [5] reviewed various APT attack models and discovered that existing models are either too generalized or overly specific. Through their analysis of these models, they proposed a criterion for defining APT attacks, asserting that any attack with the following five identified steps qualifies as an APT attack, regardless of its specific objectives. These steps are (1) Reconnaissance, (2) Establish foothold, (3) Lateral movement/Stay undetected, (4) Exfiltration/Impediment, and (5) Post-Exfiltration/Post-Impediment. While data exfiltration and destruction are significant motivations for attackers to conduct APT attacks, the potential of APTs to cause damage to physical equipment or the industrial process, i.e., cyber-physical attacks, particularly in critical infrastructures, has been less discussed. This work will focus on these neglected aspects.

The authors in [5] described how the nature of the goals can influence the steps involved. For instance, in step 4 (Exfiltration/Impediment), if attackers aim to acquire organizational data, they engage in actions such as retrieving and transmitting data to their command and control center. However, when their objective is to compromise critical components, their actions shift to disabling or destroying these vital elements. It is noteworthy to highlight that in step 5, a unique dimension is introduced by the authors which distinguishes this APT model from earlier works. Step 5 encompasses post-exfiltration/post-impediment activities, including ongoing data exfiltration, further compromise of critical components, such as disabling more critical components and the potential deletion of evidence to ensure a clean exit from the organization's network. Besides, although the phases of a cyber attack are often depicted as linear and sequential, in complex attacks like APTs, multiple phases can be active simultaneously. Additionally, [11] revealed that these campaigns might incorporate recursive steps. Reference [17] also showed that the progression can be non-linear, often exhibiting circular or loop-like phases. In such cases, the process may revert to earlier steps (e.g., moving from steps 1, 2, 3, and then back to step 1), thereby creating cyclical patterns in the attack strategy. Furthermore, another aspect that has not been adequately considered in the study of the lifecycle of APT attacks, particularly on cyber-physical systems, is that such attacks are not purely cyber and they often involve a number of physical actions. For instance, during the delivery stage, adversaries may use an infected laptop or removable media to inject malware into an air-gapped target network, as demonstrated in the Stuxnet attack [18]. These factors underscore the necessity of proposing a more comprehensive APT lifecycle that encompasses the characteristics of CPSs.

Lemay et al. [19] provided detailed descriptions of 40 distinct APT groups based on open-source APT reports, organizing them by country. Their analysis revealed that although the number of academic publications dedicated to analyzing and understanding APT attacks remains relatively low, the threat is growing, emphasizing the need for further research in this field. The authors in [16] evaluated eight distinct approaches to tackle APT attacks, including: (1) Honey-Pot Systems, (2) Intrusion Kill Chains (IKC), (3) Security Intelligence and Big Data Analytics, (4) Collaborative Security Mechanisms, (5) Context-Based Frameworks, (6) Attack Intelligence, and (7) Detection of Command and Control (C2) Communication in APTs. Each method's limitations were thoroughly analyzed, revealing that despite the significant efforts in developing comprehensive strategies against APTs, these approaches often fall short in terms of comprehensibility and adaptability to the evolving cyber threat landscape, with many requiring training datasets for APTs that are not publicly available. Our literature review supports these findings, showing a clear trend in recent research towards developing countermeasures for APT attacks. However, despite this growing attention, there still appears to be a lack of comprehensive understanding of the diverse aspects

and dimensions of APT attacks, in particular on cyber physical systems.

Additionally, studies of recent sophisticated attacks, such as APT attacks, reveal an increasing trend toward targeting the power domain sector, recognized as one of the most critical infrastructures [20]. In this context, we narrow the scope of our work to digital substations, known as modern power grid substations, which are vital components of modern energy infrastructures. Mai et al. [21] conducted a practical analysis of the IEC 60870-5-104 protocol, commonly used in power grid networks, and provided an in-depth summary of vulnerabilities associated with this protocol. György et al. [22] implemented a wide range of different attacks on IEC 60870-5-104 and indicated the lack of security features such as authentication, integrity protection, and encryption in IEC 60870-5-104 communication protocol. The authors in [23] presented a detailed analysis of cyberattacks on the SCADA protocol IEC 60870-5-104, which is crucial for power grid communication. Utilizing a Hardware-In-the-Loop digital station environment, the authors successfully implemented different attacks, ranging from passive reconnaissance to DoS attacks. The study underscores the need for robust cybersecurity measures in modern power grid systems.

Hong et al. [24] conducted a series of cyberattacks on substation systems based on the IEC 61850 standard. In their study using an IEC 61850 testbed, focused on GOOSE and SV message vulnerabilities, the authors showed that manipulating these packets could disrupt circuit breaker operations in substations, underlining critical security issues in IEC 61850 implementations. Kush et al. [25] explored multiple vulnerabilities in the GOOSE communication protocol. They demonstrated the feasibility of GOOSE poisoning, enabling them to interfere with legitimate GOOSE messages, hijack communications, and execute DoS attacks, highlighting serious security risks in the protocol. Biswas et al. [26] exploited injection attack in GOOSE-based communication. Kang et al. [27] investigated attacks against Manufacturing Message Specification (MMS) in the IEC 61850 protocol, implementing a Man-in-the-Middle (MITM) attack in a testbed electrical grid system and exploring a scenario with inverter-based distributed energy resources.

Hussain et al. [28], presented a work where they initially simulated the GOOSE and SV protocols packet in between IEDs and then validated them in a real-time testbed environment. The authors also implemented a False data injection attack (mainly replay and masquerade attacks) by feeding fake data to IEDs through GOOSE and SV protocol in an IEC 61850 system. Recently, Reda et al. in [29], presented an investigation into the security vulnerabilities of the GOOSE communication protocol of an IEC 61850 smart grid communication system. An in-depth experiment on real-time simulation with industry-standard HIL emulation was performed for vulnerability testing of the GOOSE publish-subscribe protocol. The findings demonstrate that the IEC 61850 based GOOSE communication protocol is vulnerable to attacks from malicious intruders. An attacker who is familiar with the substation network architecture can easily create falsified messages that can affect the operations of the smart grid communication systems.

Alghamdi et al. [30] applied a packet propagation attack and a time source attack on the Precision Time Protocol (PTP) which is the recommended time synchronization mechanism at the substation level based on IEC 61850-90-4 [31]. The authors in [32] investigate cyber-attacks on the PTP within IEC 61850 digital substations. This study highlights the crucial role of time synchronization in substation operations and demonstrates the potential consequences of PTP vulnerabilities through experiments on a HIL Digital Station testbed. The authors also discuss mitigation strategies, focusing on securing IEC 61850 substations against such cyber-attacks. Yang et al. [33] utilized a realistic testbed to investigate different types of attacks on IEC 61850 and based on the outcomes, concluded that most of the IEDs exhibit cyber vulnerabilities and different risks. Consequently, they developed and validated a fuzzy testing approach to detect and prevent cyber-attacks within IEC 61850 systems.

In summary, various cyber attacks such as Injection attack [34], False data injection attack [35–37], Spoofing attack [38–41], Flooding attack [42, 43], Replay attack [44, 45], Man in the middle attack [46, 47] and DoS attack [48] have been already applied against digital substations. Therfeore, adversaries might use these attacks individually or in combination to orchestrate complex cyber attacks on the power domain. This approach was observed in previous complex APT attacks, such as Industroyer, which targeted electricity substations in Ukraine [49], demonstrating the real-world implications of such sophisticated attacks. To address the aforementioned challenges, this paper aims to provide a comprehensive understanding of APT attacks, focusing on their lifecycle and the study of such attacks within the complex context of cyber-physical systems in power grid.

4 APT kill chain for cyber-physical system

The Cyber Kill Chain framework outlines a multi-phase strategy that adversaries use to target a system, and its study is instrumental in enhancing the system's defensive countermeasures [50, 51]. For cyber physical systems, Hahn et al. [52] introduced a cyber-physical kill-chain and illustrated the relation between the different phases of the kill-chain, which incorporate cyber, control, and physical attributes. However, this model cannot truly map out the Delivery phase of an APT on a CPS, such as occured in the Stuxnet attack [18]. In [53], Wolf et al. presented the cyber-physical kill chain which covers both the safety and security aspects of CPS. Inspired by

them, reference [54] presented a cyber-physical kill-chain for CPSs, which demonstrates how each attack step in the attack life cycle maps to the cyber and/or physical properties of a targeted CPS. Their approach comprises the following seven phases:

- **Reconnaissance**: Identification and selection of both physical and cyber targets. Potential safety vulnerabilities that might be leveraged are also considered.
- **Weaponization**: Constructing malware specific to a target user or system. The physical properties of the system could also be exploited to deliver an attack as well.
- **Delivery**: The delivery might rely on physical access to the system.
- **Exploitation**: A combination of cyber and physical approaches might be used.
- **Installation**: Installation of a remote access trojan or backdoor on the victim system. This might provide either a persistent presence or a limited duration presence.
- **Command and Control (C2)**: Manipulating and controlling the compromised system. This may enable adversaries to remotely evaluate physical damage to the system and consequently control the direction of the attack.
- **Actions**: Implementing measures for safety (i.e., detect and mitigate) and security (i.e., detect, deny, disrupt, degrade, deceive, and destroy) to achieve the initial objectives.

APT on cyber physical systems are not purely cyber since they involve a number of physical actions such as the injection of malware into an air-gapped target network reportedly through an infected laptop or removable media [18], as was the case for the Stuxnet attack. Based on our study on recent APTs targeting CPSs, most such attacks does not allow for communication in and out of the system which precludes the use of Command & Control (C2) and data exfiltration using remote access. In air-gapped systems, data and malware will need to be manually extracted and inserted, most often by an insider. This affects the steps discussed in [5], as will be discussed in the following sections.

Furthermore, APTs on a CPS might also involve physical attacks to provide attackers with complementary -and sometimes the only -means to gain privileges in the target CPS network. For example, physical access attacks may allow the attacker to penetrate protected premises hosting air-gapped cyber physical assets that could not be compromised otherwise. This also changes the manner in which APTs can be carried out on CPSs, which will be discussed in more details in the following.

Our study of APTs on cyber-physical systems, such as Stuxnet, Ukraine power grid attacks, and our work on emulating these APTs in a realistic environment [32], has shown that the steps Command & Control and Actions, as well as Installation in some cases, do not include a persistent access to the targeted CPS nor involve C2 capabilities. Our studies show that the Delivery step requires physical access, and that data exfiltration involves an insider. This also means that data exfiltration could last for months or even years, as an insider might need to transfer data out of the CPS multiple times before the attackers have sufficient details to create and test the attack malware. Once the malware is tested, the delivery of the malware will also require physical access. Figure 2 outlines the steps of our approach for a cyber physical kill chain and shows its relation with the cyber and physical aspects of a CPS. Our approach includes both the Cyber and Physical domain, as introduced in [52, 54]. The following are the steps of our approach, the APT Kill Chain for CPSs:

1. **Initial Access [Cyber and Physical]**: Initial access to the CPS can be achieved through both cyber and physical means. However, it is more common for initial access to be gained through physical means, such as involvement from an insider or supplier.
2. **Reconnaissance [Cyber and Physical]**: Data gathering and mapping out the necessary details for developing and preparing for the APT. This can be done using both the cyber and physical domain.

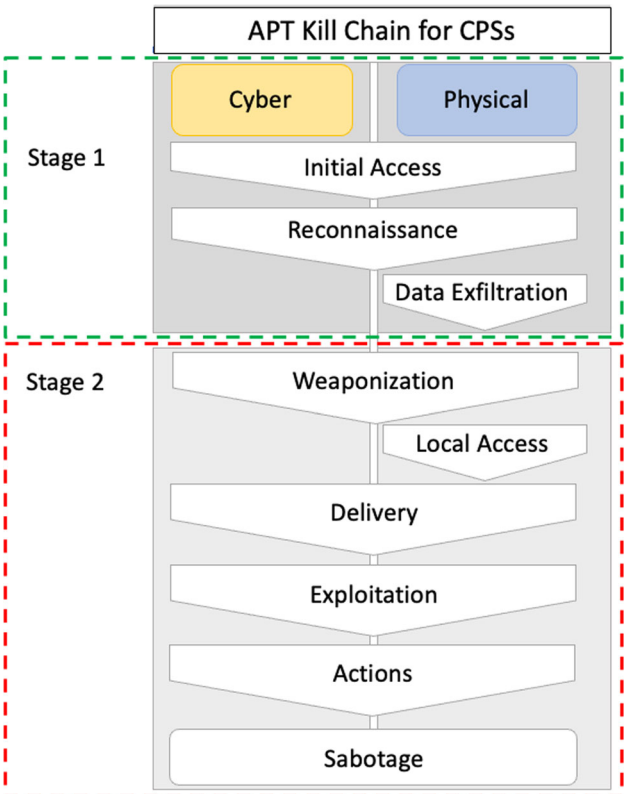

Fig. 2 Our proposed APT Kill Chain for Cyber Physical Systems

3. **Data Exfiltration [Physical]**: Data from the CPSs needs to be transported out of the system through the physical domain, for instance, by using a USB.
4. **Weaponization [Cyber]**: This step covers the development, testing and preparation that the APT threat actor performs based on the data gathered in the Reconnaissance step or by other means.
5. **Local Access [Physical]**: To transport the APT malware into the CPS, local access to the physical equipment, the CPS, is necessary. This could be done by an insider.
6. **Delivery [Cyber and Physical]**: This step covers the installation and placement of the APT malware.
7. **Exploitation [Cyber and Physical]**: This step covers the actions performed by the APT malware on the CPS.
8. **Actions [Cyber and Physical]**: This step covers the resulting actions from the exploitation on the CPS.
9. **Sabotage [Cyber and Physical]**: This step addresses the ultimate goal of the APT, which may include sabotage. However, not all APTs involve sabotage; for instance, some may focus solely on data exfiltration. In such cases, the kill chain might iterate between physical access, reconnaissance and data exfiltration.

It should be noted that our proposed kill chain outlines a comprehensive framework for understanding and studying the stages of an APT attack, but not every step may be required in every APT attack scenario. As explained by Alshamrani et al. [5], the specific aims of an APT–whether they be data exfiltration or sabotage–along with the level of access and expertise of the attackers, can lead to the inclusion or exclusion of certain steps.

5 Adversary model

A digital substation, also known as an IEC 61850 substation, can be vulnerable to various attack vectors [55]:

- Control Center Connection: There are instances of cyber threats involving unauthorized remote access, server data collection, and modification. For example, in a cyber-attack in Ukraine, attackers manipulated the software of gateway devices, ultimately gaining command and control access over the entire substation.
- Engineering PCs: Malware present on an engineering PC can execute and install itself on IEDs or SCADA servers when connected. Additionally, device settings accessible via Engineering PCs can serve as potential cyber-attack vectors.
- Testing PCs (Devices): Testing PCs, whether directly or through test sets, are connected to the station bus for testing purposes. This connection introduces the potential threat of infecting substation components, such as IEDs, Human–Machine Interfaces (HMI), and Measurement Units (MU). Test documents used during testing could also be exploited as attack vectors when the Test PC is connected to the station or process bus. Note that testing devices themselves can become entry points if attackers exploit vulnerabilities in the network infrastructure and devices. This scenario can allow unauthorized access and manipulation.
- Storage Devices: When connecting infected devices to the asset's ports, there is a risk of executing malicious software or modifying IED or SCADA system/software, potentially compromising the substation's integrity.

In our adversarial model, we consider a scenario where the attacker gains access to the substation network via a single device located within the same subnet as both the controlling station and the SCADA gateway, also known as the Remote Terminal Unit (RTU). This infiltration point serves as the launching point for the attacks on the IEC 60870-5-104 communication protocols. It is important to note that this initial access is essential to execute this attacks, and that this access is not possible from remote. It is necessary with local access. The ultimate goal in this case is to disrupt communication between the controlling station and the SCADA gateway, while masking the malicious activities as harmless technical glitches.
To execute the subsequent attacks on the Precision Time Protocol (PTP) within the IEC 61850 framework, we position the attacker on the interior of the substation network, specifically within the station bus. This strategic placement provides the attacker with access to both IEC 61850 and PTP communication channels. It is important to acknowledge that there exist multiple conceivable pathways through which an attacker could infiltrate a substation as mentioned in [23, 32, 55]. Section 7 explains the conducted APT attack in more details.

In our adversary model we consider that the attacker wants to achieve the biggest possible impact as the final aim. Causing system unavailability would mean a certain time of blackout but with synchronised attack—affecting both the station bus and the network between the control center and the SCADA gateway—the impact can be much higher and potentially damage substation equipment, also primary equipment such as circuit breakers, etc. Such an aim cannot be disregarded so we consider that the attacker tries to get access to all network segments and use the information obtained from one part of the attack on another part. IED devices such as the bay controller, the protection relay, and the merging unit are connected both to the station bus and the process bus so these devices can be targeted from both sides. One example of such a synchronised attack is to deactivate the protection relay by targeting the PTP protocol and at the same time open-

ing a circuit breaker. These activities might only be doable if the attacker has access to multiple network segments. We consider that the attacker goes deeper and deeper inside the network, first by mapping the control center network and then moving forward into the station bus.

6 Digital station (DS) enclave testbed

In this research, we leverage the Digital Station (DS) Enclave testbed depicted in Fig. 3 to conduct our APT attack research. This well-established testbed operates as a hardware-in-the-loop infrastructure, offering the essential framework for executing real-time tasks and enabling a comprehensive examination of the system's response to cyber-attacks [56].

As illustrated in Fig. 3, the digital substation comprises two key components: a station bus, denoted by the yellow block, and a process bus, represented by the red block. The station bus serves as the interconnection among all bays at the station supervisory level, while the process bus links the IEDs within a bay, facilitating real-time measurements. Within the DS enclave, several essential elements are present, including digital station equipment, the control center machine, and engineering workstations dedicated to operational and configuration tasks. The digital station equipment, provided by Siemens, is designed as a standard control system specifically tailored for high-voltage substations. At the highest level, the SICAM A8000 CP-8050 serves as a gateway with a dual role. It effectively manages the interface between the local control system (substation) and the dispatch center. This multifaceted gateway performs protocol conversion tasks, translating the local station protocol IEC 61850-8-1 (MMS) into the control center protocol IEC 60870-5-104. Simultaneously, it operates as a network isolation mechanism, essentially functioning as a firewall to delineate local and remote networks in accordance with industry standards.

In the context of precise time synchronization (PTPv2), the digital substation employs Ruggedcom RSG2488 and Meinberg M1000 time servers, which are essential for maintaining accurate time across the networks. To achieve synchronization across both networks, the station network switch and process bus network switch are interconnected. These two time servers, equipped with GPS time sources, are configured in a primary/secondary mode for Precision

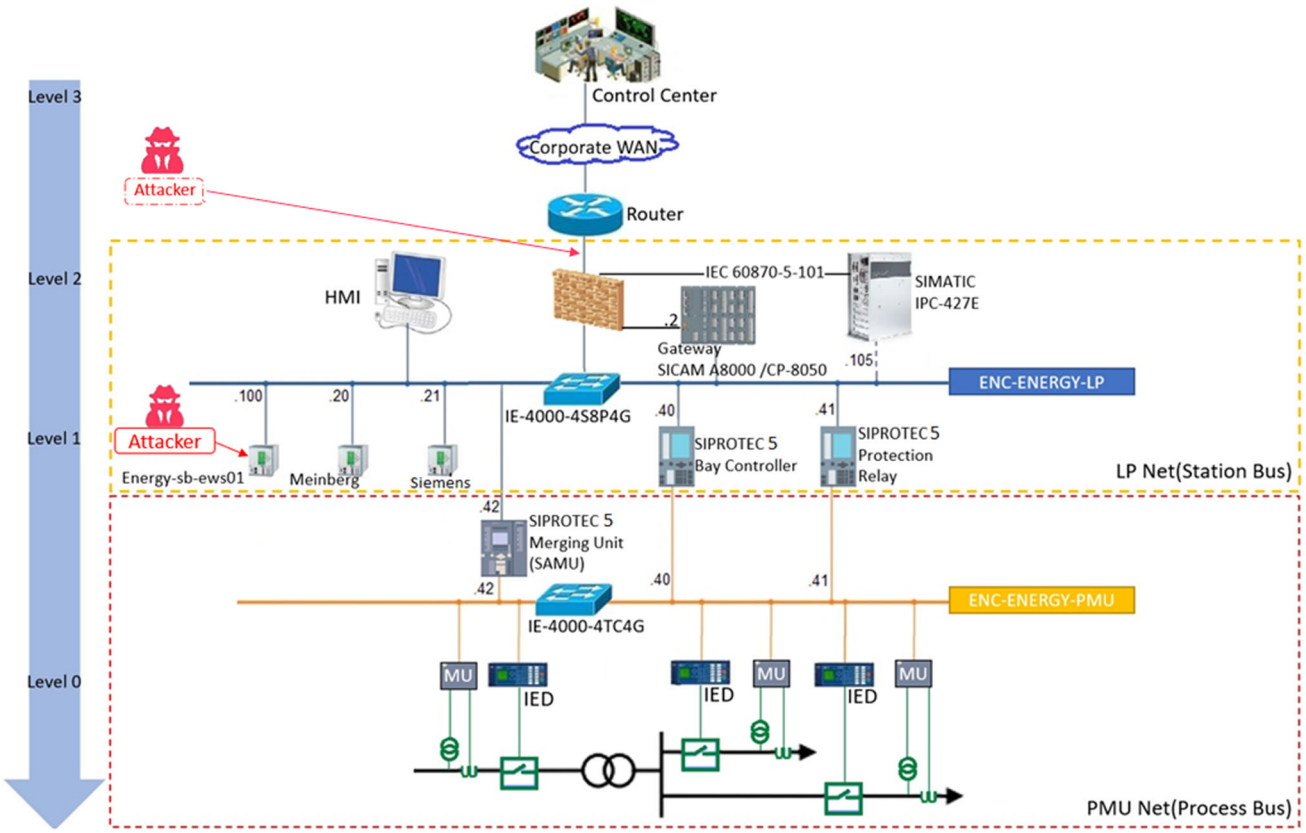

Fig. 3 Digital station enclave testbed

Time Protocol (PTP) compliance with the Power Utility Profile. To simulate the operation control room for the testbed, IECTest is employed, facilitating communication with the SICAM A8000 CP-8050 gateway. The components within the Siemens DS enclave are kept up-to-date with the latest available versions [56].

7 APT attack steps in the case study

In this section, a case study is conducted to demonstrate the practical application of the proposed APT kill chain, along with an analysis of Command and Control (C2) and Action, as previously discussed. The study employs the hardware-in-the-loop testbed detailed in Sect. 6. Table 2 outlines the sequence of steps executed during the APT attack on an IEC 61850 substation, targeting both the SCADA interface (IEC 60870-5-104) and the time synchronization within the process bus network.

The initial stage of the APT attack involves reconnaissance aimed at gathering essential information to initiate the attack (as outlined in steps 1 to 4). Upon acquiring the necessary data, the attackers move to the second stage, executing actions needed to compromise the substation (steps 5 to 8). As explained in our adversary model in Sect. 5, the attacker has local network access (Initial Access). The objective of this APT attack is to cause potential damage to the physical equipment and disrupt the power grid process (Sabotage). Therefore, in this case study, the focus is predominantly on sabotage and the technical parts executed inside the substation, namely reconnaissance in the first stage and exploitation in the second stage.

As highlighted in Sect. 4, not all steps of the APT kill chain are applicable in every scenario, hence a direct mapping of attack stages is not always feasible. Furthermore, Sect. 3 discussed that some steps of the APT kill chain might require multiple iterations. This is demonstrated in this case study, as the reconnaissance was conducted through four distinct methods by the attackers. Indeed, this approach was necessary to enable the attackers to effectively collect the required data. It should be noted that although the data exfiltration step was not incorporated into the APT kill chain in this case study, such data could potentially be transported out of the CPS if, for instance, an insider were to extract the reconnaissance findings.

7.1 APT Attack - Stage 1

The first stage of the APT attack consists of gaining access to the SCADA part of the testbed, as this enables data reconnaissance on the communication between the control center and the substation networks (station and process bus). This is an IEC 104 interface [8]. Before the attacker is able to perform reconnaissance, it is necessary to establish initial access which can only be achieved in the physical domain. In practice, this means that somebody first needs to gain physical access to a physical location where the networks are exposed, and then logical access the IEC 104 communication. The location of the attacker is the Attacker icon placed between the router and the firewall in Fig. 3. Once initial access has been established, the attacker starts with passive reconnaissance.

7.1.1 Passive reconnaissance

Passive reconnaissance in the form of listening and gathering information is relatively quiet and stealthy. It involves the attacker passively monitoring network traffic to identify visible communication between devices, establishing an understanding of the types of messages being exchanged, and to collect information like ASDU addresses, Information Object Addresses (IOAs), and measurement values. Since the attacker is essentially eavesdropping on existing communication, this step is less likely to generate noticeable network noise or trigger immediate alarms. The APT attack in the case study required two levels of passive reconnaissance.

Step 1

The first step assumes that initial access has been achieved, as discussed earlier. This means that the attacker has local access to one or multiple network parts of the substation network for a short time period. This access could be executed by an insider in collaboration with the APT attacker. The attackers' primary objective is to map the network. This involves employing passive reconnaissance, where one passively monitor network communication by listening to traffic in promiscuous mode. This method allows attackers to listen in on traffic between the controlling station and the SCADA gateway, and also on the station bus network, depending on the attacker's position. It is important to note that the communication between these devices is not encrypted, meaning that any application layer data passing through the attackers' network interface is in clear text. Attackers can intercept and collect network related information from Open Systems Intercommunication (OSI) layers 2 and 3, such as Internet Protocol (IP) addresses and Media Access Control (MAC) addresses of the network devices, even if the application layer data is encrypted. Without encryption, the attacker can also collect application layer data such as commands in use or measured values sent through the network. Even when there is no active communication on the network, the controlling station periodically sends out regular packets and the PTP master time sends out clock synchronization commands, which disclose the IP and MAC addresses of the devices (see Fig. 4).

To summarize, passive reconnaissance was performed on two levels of the substation: Level 1 (Passive Reconnaissance

Table 2 Summary of the APT attack steps in the case study

Attack step	Attack type	Attack aim	Attack technique	Outcome/detection trace
Step 1	Short term passive reconnaissance	Gathering information about the IEC 60870-5-104 network and the station bus network	Promiscuous mode listening and information gathering	Successful reconnaissance with no trace
Step 2	Long term/persistent passive reconnaissance	Gathering specific information about the IEC 60870-5-104 network (capturing non-typical data such as inordinate interrogation answers)	Promiscuous mode listening and information gathering and device fingerprinting	Partially successful reconnaissance, identifying manufacturer information, identifying inputs and outputs of devices
Step 3	Active reconnaissance with regular TCP traffic	Finding SCADA gateway (RTU) devices, controlling station, IEDs to the protected network	Port scanning (TCP full scan) the subnet for open tcp port	Successful reconnaissance, discovering key network components
Step 4	Active reconnaissance with irregular traffic	Collects additional information that is not available with regular traffic	Packet injection to force device interrogation commands, switch flooding to have more information sources	Attacker obtains additional information from the devices
Step 5	Master clock take over	Manipulates the PTP to become the master clock	Manipulation – rouge master clock emulation	Multiple clocks in the network (more than what is configured)
Step 6	Time manipulation	Attacker maintains the status with the master clock emulation and tries to block/change the time permanently	Manipulation – rouge master clock emulation with fake clock announcement and synchronization messages	Fake time syncs failed to be delivered to the devices but 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 SV messages
Step 7	Operation failure	Sending wrong measurement values and commands and attempt to propagate errors	Sending wrong data on behalf of the SCADA gateway with packet injection, sending fake breaker opening/closing commands	Successful operation failure, leading to communication disruption and diverting attention
Step 8	Denial of service	Attention diversion by disabling communication between the SCADA gateway and the control station	ASDU RESET flood with packet injection / controlling station source IP spoofing	TCP connection reset
	Denial of service	Attention Diversion by ARP poisoning	ARP poisoning without packet forward	ARP poisoning signs, large amount of fake ARP replies
	Denial of service	Attention diversion by disabling SCADA gateway accessibility	TCP level SYN flood for the RTU	Extra large amount of SYN packets towards the SCADA gateway

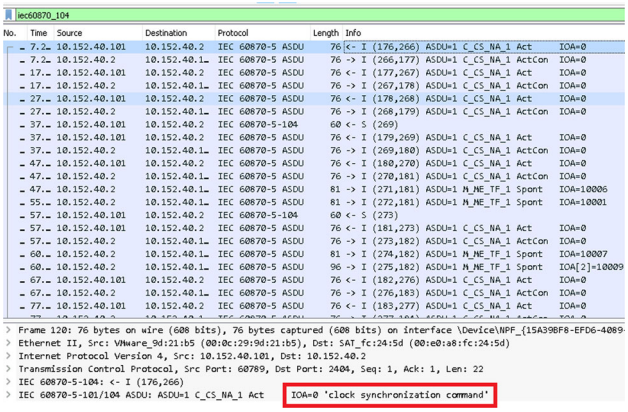

Fig. 4 Clock synchronization commands

- Identifying Device Type). Level 1 passive reconnaissance on the SCADA interface involved passive techniques like identifying device types through techniques such as MAC address grabbing. While it may reveal some information about the devices on the network, it does not involve active probing or communication that would create significant noise. However, such activities may only provide limited information about the device manufacturer.

Level 2 (Passive Reconnaissance - Collecting Information Regarding Clock Sources). Passive reconnaissance techniques were also used on the station bus network and involved collecting information about the clock sources used in the network, specifically Meinberg and Siemens. This included monitoring network traffic and examining the behavior of these clock sources. Passive reconnaissance, by nature, does not involve sending packets or generating significant network activity, so it is not noisy and should not raise immediate suspicions on the station bus network.

On the station bus level the attacker can see broadcast and link layer messages (Fig. 5). Here, the attackers immediately observe the primary master clock (Meinberg device in our case) by the regular PTP clock announcement messages.

Step 2

Following the initial data collection and network mapping, the attackers proceed with passive reconnaissance to gain deeper insights into the testbed network at the available

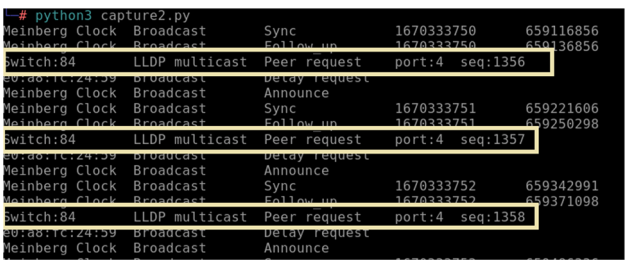

Fig. 5 Passive reconnaissance

network locations. In this step, we consider that the attacker has permanent or long term access to different network parts inside the substation. The primary objective during this step is to collect valuable information, including more MAC addresses and IP addresses, application level data such as commands, and measured values, but also to identify the device manufacturer. In the case study, it was only possible to determine e.g. the SCADA gateway manufacturer and not the specific product type.

Passive reconnaissance in this step also entails monitoring the content of Application Service Data Unit (ASDU) messages, which reveals additional details about the SCADA gateway. In specific time periods, the attacker can capture e.g. interrogation messages and the answer for these messages that encompasses information such as ASDU addresses, Object Addresses (OA), and Information Object Addresses (IOA). Because of the longer time period of listening, the attacker is able to capture network traffic at the right moment, including sensitive data such as specific commands in use and crucial real-time measurement values.

As demonstrated in Fig. 6, the captured data includes ASDU interrogation commands, providing the attackers with detailed insights into communication patterns and command usage within the testbed network. This information serves as a foundational element for subsequent attack steps, allowing the attackers to refine strategies and to execute more targeted attack actions.

On the station bus, the attacker can facilitate the next steps in passive reconnaissance by targeting PTP. The attacker team developed a Python script to process the captured traffic and match MAC addresses with their roles. This script highlights the principal PTP packet parameters, especially those from the best master clock, which transmits both timestamped and untimed messages. Additionally, with access to a physical machine, the attackers also observe link layer com-

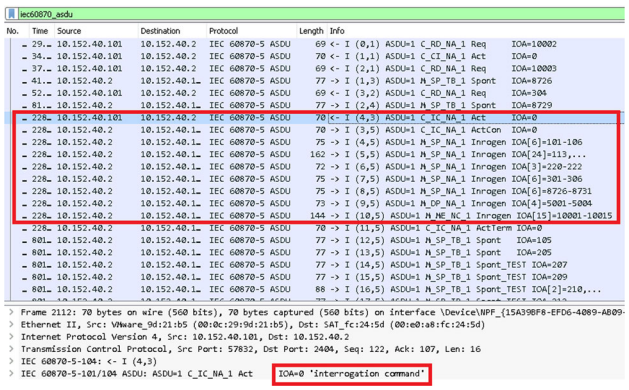

Fig. 6 Interrogation commands

munication emanating from the industrial switch. Figure 5 demonstrates the attacker's machine connected to a specific part of the switch, identified through MAC address analysis, and reveals the switch's transparent clock function used for determining network latency. Since the passive reconnaissance is long term in this step, the attacker might obtain unintended best master clock changes as well. If the best master clock runs into a technical failure, the attacker captures how the secondary clock takes over the best master clock role.

Through this process, the attacker pinpoints several key network aspects:

- The best master clock's MAC address and primary characteristics (priority numbers).
- The master clock's timing settings.
- The connection point of the attacker's machine to the switch.
- The switch's operational mode, whether a Transparent Clock or a Boundary Clock.

Step 3

After collecting preliminary information in the previous steps, attackers shift from passive network data collection to more active techniques. The primary goal in this step is to engage in proactive network probing by sending out network packets designed to elicit responses from the SCADA gateway and the controlling station. This strategy, commonly known as an active reconnaissance, aims to force these devices into revealing detailed information about themselves. As the attacker proceeds gradually to avoid early detection, the attacker sends out only regular (legitimate like) network traffic in this step. To execute this form of reconnaissance, attackers explore the following options:

- **Transfer Control Protocol (TCP) Scan**: Attackers initiate a TCP port scan for targeted ports (e.g. port 2404) within the subnet. This specific scan is employed to identify devices and services actively operating within the network.
- **Device Fingerprinting via TCP Responses**: Analyzing the network answers on protocol level, attackers enumerate devices characteristics by conducting a straightforward scan across the subnet.

Attackers delve into device fingerprinting techniques, a well-established practice for identifying operating systems (e.g., Nmap operating system fingerprinting). It is worth noting that while device fingerprinting is a well-recognized approach for conventional operating systems, its adaptation for power grid devices remains a relatively unexplored domain.

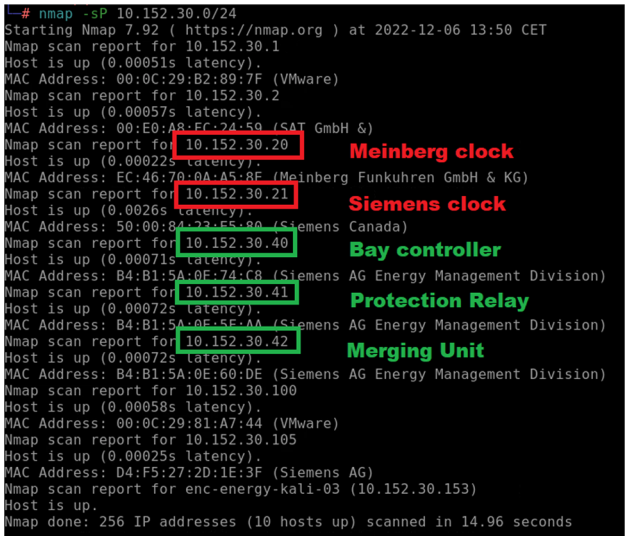

Fig. 7 Discovery of the equipment communicating on the network

These active reconnaissance techniques empower attackers with more precise insights into the network's structure, enabling them to pinpoint critical components such as SCADA gateway devices, the controlling station, and network details. On the station bus network level, active port scanning revealed Intelligent Electronic Devices (IED) devices such as the network parameters of the protection relay, the bay controller and the merging unit (Fig. 7).

This newfound knowledge serves as the foundation for subsequent attack actions, as elaborated upon in the following steps.

Step 4

The attacker can also map the network with irregular packets by accepting the fact that this is a more noisy approach, which means that the risk of being detected is higher. Given that the IEC 60870-104 protocol operates atop the TCP/IP stack, attackers consider alternative port scanning methods, such as a half-open (SYN) scan, to avoid establishing full TCP connections. In addition to this, the attacker can also carry out packet injection or ARP poisoning at this stage. Packet injection can be used e.g. to send out fake interrogation commands. The attacker first obtains the relevant TCP connection parameters such as ports, TCP sequence number, TCP acknowledgement number, and also the IEC 60870-104 level connection parameters, such as the TX and RX values. Knowing all these parameters the attacker can fake the next packet in the TCP stream on behalf of the controlling station. This operation results in forced interrogation answers so the attacker gains important data, but it did results in TCP packet duplicates and TCP communcation reset that can be detectable. TCP connection reset happens regularly without any malicious activity, so this attack detection possibility is relatively low. More noisy active reconnaissance might involve ARP poisoning. A man in the middle situation pro-

vides very rich information from the targets (the attacker could see everything between the targeted devices), but this type of attack is quite risky to execute in the reconnaissance phase.

7.2 APT attack - stage 2

The second stage of the APT attack starts after the reconnaissance has been completed, or sufficient information has been gathered to develop necessary malware and other attack tools. This is called weaponizing.

7.2.1 Weaponizing, local access, delivery, and explotation

Weaponizing covers all attack activities involved in developing the necessary malware and tools for stage 2 of the APT attack. This is done based on the data that has been gathered and exfilitrated from the CPS during stage 1.

In the case study, the attack tools were developed as a combination of Python scripts, known attack tools, and open source tools. These tools were then delivered using the same physical and logical access as previously developed. This is referred to as local access in Fig. 2.

Step 5 After weaponizing is completed and the attack tools have been developed and tested, the attacker waits for the opportunity to move forward with the APT attack. Firstly, local access is needed to deliver the tools in the CPS. The right attack time can be influenced by the data provided by the reconnaissance, working hours considerations, other external information available for the APT group, or the need to synchronize with other attacks.

Once the attack tools have been delivered, the exploitation could be performed immediately or after a specific time period. In the case study, the exfiltration started immediately as the attack required manual local activities to succeed. Exploitation started with that the attacker focused on gaining control of the master clock and disrupting the PTP by compromising network integrity on the station bus. This requires manipulating the Best Master Clock Algorithm (BMCA). As time sources in the network regularly send out Announce messages, the introduction of a new clock entails broadcasting regular fake Announce messages. The best master clock is determined based on priority parameters, where a lower priority number signifies a superior clock. Our experience revealed that generating a fake Announce message, including modifying the source MAC address of a new fake time source, is relatively simple for attackers.

Nevertheless, the case study showed that merely sending out time synchronization is ineffective, as these are not accepted by the industrial switch to be propagated to the substation equipment. Note that the industrial switch works as a transparent clock in the network. What worked in practice was to mislead the switch with fake Announce messages, as these messages do not carry a timestamp for the switch to validate against its own timing. As a result, the only necessary alteration for creating fake messages was to maintain increasing sequence numbers. After conducting this attack, the main master clock continues its announcements for a few seconds and eventually ceases, along with all other genuine time sources in the network, leaving only the attackers' fake time source active. This could have been automated in an attack tool, but it would have required a longer reconnaissance, which would need to involve more active scans and that would increase the risk of being detected.

Step 6

The fake best master clock approach effectively stops the real time sources and their synchronization messages, creating a scenario similar to a DoS attack. The next step for the attacker is to maintain this situation for a longer period to confuse the devices. In the case study, introducing a fake best master clock into the network resulted in the cessation of authentic time synchronization messages, and consequently, the station bus time synchronization was also stopped. What happened was that all equipment on the station bus needed to rely exclusively on their own local time, i.e., the slave time source. Figure 8 displays the Merging Unit time sources during the attack involving the fake master time source.

As a result, severe consequences on the operation of the substation were observed. The IEDs, including the protection relay, goes into holding mode, which means that they are blocked and are no longer acting upon received messages (see Fig. 9). This could, in worst case, mean that the operator cannot manage the power lines of the substation from the dispatch center, and that the substation needs to move to local control. Local control means that the substation will need to be operated locally at the substation. In cases where the attack is executed across multiple substations simultaneously, this could affect the balance in the power grid system, and for instance result in temporary outages.

7.2.2 Actions and sabotage

Step 7

Now that the attackers have gained control over the master clock, and thereby causing the IEDs, including the protection relay, to enter a holding state, the next step is to inflict damage to the system (sabotage). Utilizing the information collected from steps 1 to 4, the attackers are capable of inducing operational failures. This involves manipulating the system by opening or closing breakers based on their current state. It is important to note that this phase of the attack, which primarily aims at operational failure, is inherently quiet and disruptive. However, its execution during a period when the protection relay is in holding mode significantly amplifies its impact, resulting in severe damage to the system.

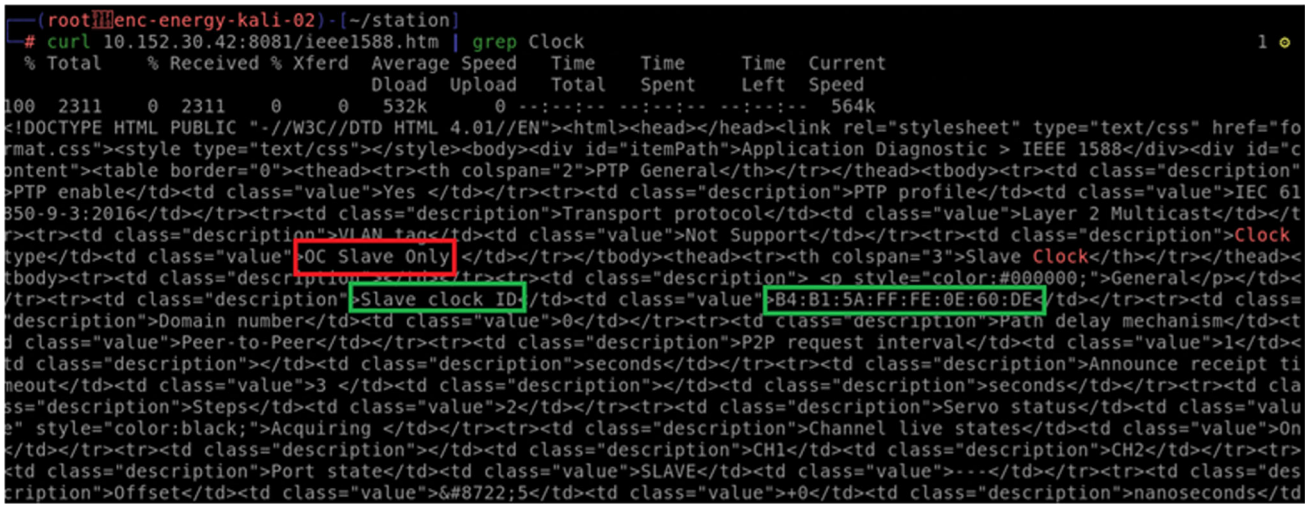

Fig. 8 Merging Unit (MU) time settings after loosing the best master clock PTP time

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

Fig. 9 Messages from the protection relay showing that it is in blocked mode (inactive)

The attackers accomplish this by sending ASDU type *0x45* commands on behalf of the control station. The goal is to send erroneous data that appears legitimate within the ongoing TCP communication. To carry out this deceptive operational failure, the attackers employ the same technique that was used for the forced interrogation, known as packet injection. This step involves capturing the last packets sent by both the controlling station and the SCADA gateway. These captured packets provide crucial information:

- The port that the controlling station uses in the TCP connection.
- The last sequence number used by the controlling station in the communication.
- The length of the last TCP packet sent by the controlling station.
- The last sequence number used by the SCADA gateway.
- The length of the last TCP packet sent by the SCADA gateway.

With this information, the attackers can send fake packets into the ongoing TCP stream that seamlessly blend with legitimate packets. These fake packets include details such as the correct source port used by the controlling station, a destination port of 2404, and precise sequence numbers. The valid sequence number is the last sequence number plus the length of the last TCP packet sent by the controlling station. Additionally, the attackers ensure the acknowledgment numbers align with the last packet sent from the SCADA gateway. Spoofing the sender's IP address as that of the controlling station, ensures the packet is accepted by the SCADA gateway at the TCP level.

The attackers specifically target ASDU type *0x45* commands to simulate breaker opening or closing actions. ASDU level sequence numbers (RX) and acknowledgment numbers (TX) have to be matched. These deceptive commands are executed, confirmed by the SCADA gateway with *ActCon* responses, and appear as authentic within the network communication.

It is important to note that this type of attack results in the reuse of sequence numbers by the controlling station, as the controlling station cannot distinguish the fake packets sent by the attackers. This sequence number reuse may trigger a time synchronization command, and subsequent sequence number reuse detection. Consequently, the SCADA gateway initiates a TCP connection reset, temporarily interrupting the communication. Figure 10 illustrates that the controlling station has rebuilt the TCP connection and started the ASDU communication with STARTDT. Note that in this attack step, the TCP connection was reset and rebuilt right after the fake packet, but the breaker closing was not prevented. Therefore, the attacker's primary objective of creating technical errors remains achieved.

Step 8

Until now, the attackers have successfully remained stealthy, causing damage to the system with minimal noise. However, to ensure the damage is prolonged and operators are further distracted, the attackers may also execute a Denial of Service attack as the final step. Therefore, in line with their strategy of maintaining stealth while inflicting damage, the attackers' next move is to implement a DoS attack, aiming to render the SCADA gateway inaccessible to the control station. This is achieved through three distinct methods:

- Continuous transmission of reset ASDU messages impersonating the control station, achieved via packet injection.
- Implementing ARP poisoning, halting packet forwarding to disrupt communication.
- Overwhelming the SCADA gateway with a flood of TCP packets.

In the case study, the first approach involved packet injection where the attackers repeatedly sent reset ASDU commands on behalf of the controlling station. The SCADA gateway executed the reset and became unavailable for a couple of seconds. When the reset was executed, the controlling station rebuilt the TCP connection and sent the initial STARTDT message. At that point, the attackers sent another reset ASDU command and continued this throughout the attack. The advantage of such Denial of Service is that this type is not extremely noisy. The attacker needs only one packet for each reset. The controlling station could only communicate with the SCADA gateway for one or two seconds, then lost the connections for a longer period as shown in Fig. 11.

The second strategy employed was ARP poisoning without packet forwarding. In this more direct approach, the attacker sends two ARP packets every second to disrupt the network. This method is slightly noisier than packet injection, but ensures continuous interruption in the communication between the control station and the SCADA gateway. By manipulating ARP messages, the attacker effectively misdirects the network traffic, preventing the SCADA gateway from communicating with the control station (illustrated in Fig. 12).

The most aggressive form of DoS implemented in our tests was flooding the SCADA gateway with TCP packets. Using tools like *Hping*, the attacker flood the gateway with traffic, completely severing control from the station. This attack not only causes immediate loss of control, but also leads to ongoing communication problems between the control station and the gateway after the system recovers, indicating the severe impact of this tactic (refer to Fig. 13).

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 case study was conducted in collaboration with a critical infrastructure owner, it was decided that the scripts themselves cannot be published.

8 Discussion

Attacking Cyber-Physical Systems presents unique challenges compared to systems operating solely in the cyber domain, such as IT systems. A CPS integrates cyber components, which control and automate physical components like robots, circuit breakers, and chemical processing units. These systems are often safeguarded by air gaps or physically segregated networks to prevent unauthorized access. Nevertheless, in recent decades, CPSs have been increasingly targeted by complex and sophisticated attacks, like APTs.

This complexity led to our first research question, which explored whether the conventional kill chain model is applicable and sufficient for studying APT attacks targeting CPS. Our investigations, including the case study presented in this paper, indicate that APT attacks cannot truly be investigated and mapped to the conventional cyber kill chain, and in some cases, several iterations of specific steps are required. Also, in some scenarios, local access is required to execute an APT attack on a CPS, with initial access typically occurring through physical means, as was the case with Stuxnet. This finding necessitated updates to the kill chain for CPS, incorporating elements that cover the necessity of physical access for steps such as reconnaissance and delivery.

In addressing our second research question regarding the role of the physical domain in APT attacks on CPS, it became evident that attacking a CPS is considerably more challenging than attacking purely cyber systems. The need for physical access, as demonstrated by the Stuxnet attack and further evidenced in our case study, is a significant barrier to entry for attackers. While physical access might not be nec-

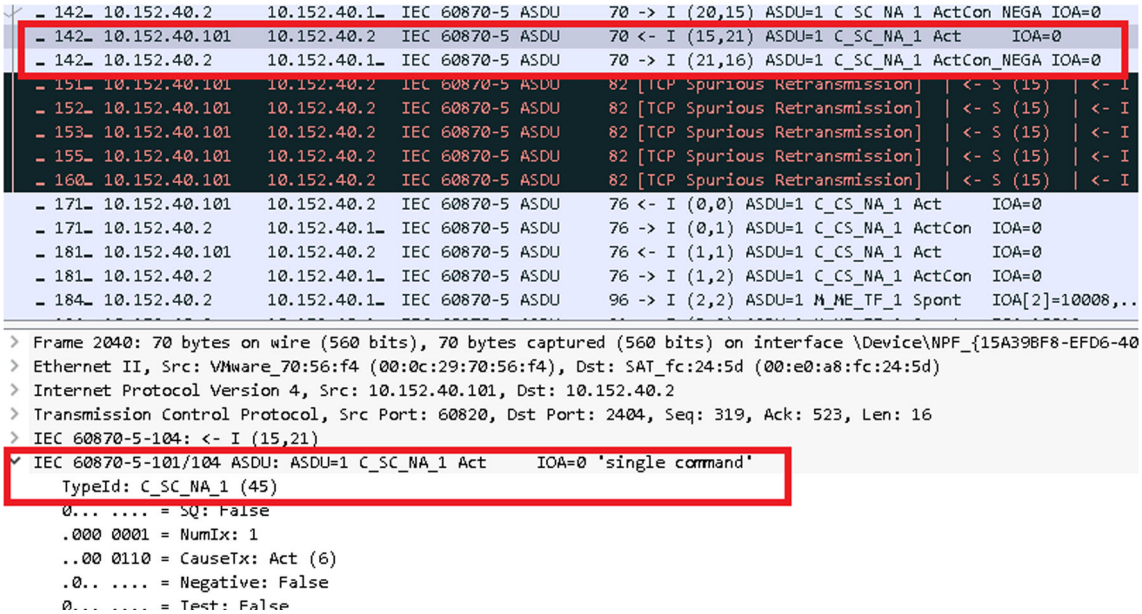

Fig. 10 Spoofed breaker close command with packet injection

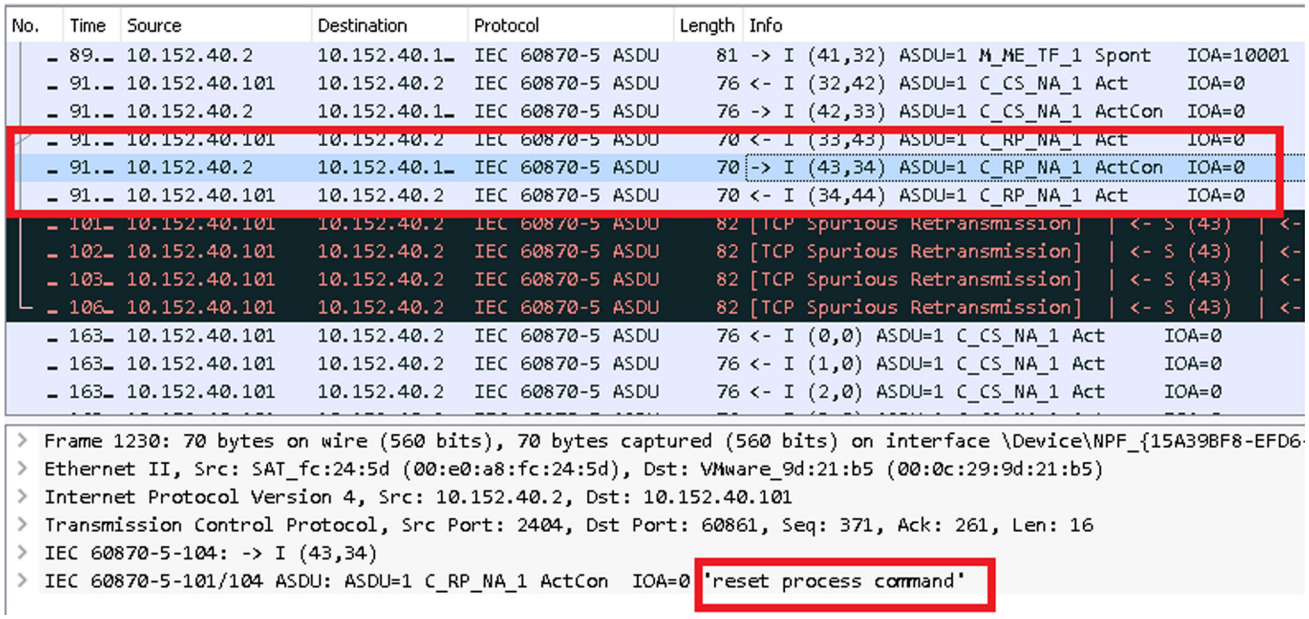

Fig. 11 DoS attack with spoofed reset commands using packet injection

No.	Time	Source	Destination	Protocol	Length	Info
84.455854	VMware_9d:21:b5	VMware_70:5…	ARP	60	10.152.40.101 is at 00:0c:29:9d:21:b5
84.471470	VMware_70:56:f4	VMware_9d:2…	ARP	60	10.152.40.2 is at 00:0c:29:70:56:f4
84.505223	VMware_70:56:f4	SAT_fc:24:5d	ARP	60	10.152.40.101 is at 00:0c:29:70:56:f4
84.535992	VMware_70:56:f4	VMware_9d:2…	ARP	60	10.152.40.2 is at 00:0c:29:70:56:f4
84.565247	VMware_70:56:f4	SAT_fc:24:5d	ARP	60	10.152.40.101 is at 00:0c:29:70:56:f4
84.605204	VMware_70:56:f4	VMware_9d:2…	ARP	60	10.152.40.2 is at 00:0c:29:70:56:f4
84.635998	VMware_70:56:f4	SAT_fc:24:5d	ARP	60	10.152.40.101 is at 00:0c:29:70:56:f4
84.669171	VMware_70:56:f4	VMware_9d:2…	ARP	60	10.152.40.2 is at 00:0c:29:70:56:f4
84.701160	VMware_70:56:f4	SAT_fc:24:5d	ARP	60	10.152.40.101 is at 00:0c:29:70:56:f4
84.732037	VMware_70:56:f4	VMware_9d:2…	ARP	60	10.152.40.2 is at 00:0c:29:70:56:f4
84.765165	VMware_70:56:f4	SAT_fc:24:5d	ARP	60	10.152.40.101 is at 00:0c:29:70:56:f4
84.797154	VMware_70:56:f4	VMware_9d:2…	ARP	60	10.152.40.2 is at 00:0c:29:70:56:f4

Fig. 12 DoS attack with ARP poisoning

tcp

No.	Time	Source	Destination	Protocol	Length	Info
17.545379	10.152.40.151	10.152.40.2	TCP	60	[TCP Port numbers reused] 33361 → 2404 [SYN] Seq=0 Win=512 Len=0
17.545379	10.152.40.151	10.152.40.2	TCP	60	[TCP Port numbers reused] 33375 → 2404 [SYN] Seq=0 Win=512 Len=0
17.545379	10.152.40.151	10.152.40.2	TCP	60	[TCP Port numbers reused] 33387 → 2404 [SYN] Seq=0 Win=512 Len=0
17.545379	10.152.40.151	10.152.40.2	TCP	60	[TCP Port numbers reused] 33388 → 2404 [SYN] Seq=0 Win=512 Len=0
17.545379	10.152.40.151	10.152.40.2	TCP	60	[TCP Port numbers reused] 33395 → 2404 [SYN] Seq=0 Win=512 Len=0
17.545379	10.152.40.151	10.152.40.2	TCP	60	[TCP Port numbers reused] 33363 → 2404 [SYN] Seq=0 Win=512 Len=0
17.545379	10.152.40.151	10.152.40.2	TCP	60	[TCP Port numbers reused] 33368 → 2404 [SYN] Seq=0 Win=512 Len=0
17.545379	10.152.40.151	10.152.40.2	TCP	60	[TCP Port numbers reused] 33381 → 2404 [SYN] Seq=0 Win=512 Len=0
17.545379	10.152.40.151	10.152.40.2	TCP	60	[TCP Port numbers reused] 33385 → 2404 [SYN] Seq=0 Win=512 Len=0
17.545379	10.152.40.151	10.152.40.2	TCP	60	[TCP Port numbers reused] 33398 → 2404 [SYN] Seq=0 Win=512 Len=0
17.545440	10.152.40.151	10.152.40.2	TCP	60	[TCP Port numbers reused] 33376 → 2404 [SYN] Seq=0 Win=512 Len=0
17.545440	10.152.40.151	10.152.40.2	TCP	60	[TCP Port numbers reused] 33396 → 2404 [SYN] Seq=0 Win=512 Len=0

> Frame 337972: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{15A39BF8-EFD6-4089-AB09-0F8DC
> Ethernet II, Src: VMware_70:56:f4 (00:0c:29:70:56:f4), Dst: SAT_fc:24:5d (00:e0:a8:fc:24:5d)
> Internet Protocol Version 4, Src: 10.152.40.151, Dst: 10.152.40.2
> Transmission Control Protocol, Src Port: 55093, Dst Port: 2404, Seq: 0, Len: 0

Fig. 13 DoS attack with SYN flood

essary in every instance, our analysis of existing APTs and our experimental work suggests it is a common requirement, underpinning the proposed modifications to the kill chain. The role of the physical aspect is not limited to initial access or delivery but extends further, as shown in our proposed APT kill chain (Fig. 2). These modifications include integrating the physical dimensions in the weaponization stage, reflecting the potential need to combine physical and cyber attack vectors. For instance, manipulating physical equipment to facilitate the execution of a cyber weapon highlights the intertwined nature of CPS vulnerabilities.

The difficulty in establishing a Command and Control channel further complicates APT attacks on CPS, restricting attackers' capabilities and necessitating meticulous planning during the reconnaissance stage. Given the potential singularity of physical access opportunities, the data collected during this initial stage is critical for developing subsequent attack steps. Successful execution of an APT attack on a CPS also requires precise development and testing of the attack in an environment that closely mirrors the target, including identical protocols, network architecture, and physical equipment configuration. This underscores the importance of further research on more realistic testbeds, using hardware in the loop, as work based solely on simulation is unable to provide the insights needed to identify vulnerabilities and propose security measures. Moreover, research that has only focused on applying one or two different types of attacks, such as man-in-the-middle attacks or DDoS, individually, could not produce realistic scenarios. Accordingly, due to the sophisticated nature of APTs, more efforts are needed to delve into studying APT attacks on CPSs in different domains in more detail.

Moreover, further research is needed to explore alternative strategies for gaining local access to the CPS, such as exploiting supply chain vulnerabilities. It is also of paramount importance to investigate approaches that may reduce the necessity of physical access. Prioritizing the development of attack strategies that result in sabotage, especially those causing long-term damage to critical components, is crucial for building better resilience into CPS in the future.

9 Conclusion and future work

This paper proposes essential changes to the APT kill chain for CPS, including the need for physical access for reconnaissance and for the delivery of the attack toolkit. It also includes the physical dimension as part of weaponizing as it might be necessary to combine physical and cyber attack vectors, such as manipulation of physical equipment by flipping run buttons to enable the cyber weapon to execute. Furthermore, the proposed approach separates the kill chain into two stages: Stage 1: Reconnaissances and Data Exfiltration, and Stage 2: Delivery, Exploitation, Actions, and Sabotage. It is worth noting that the APT attack might iterate over these two stages in practice, as well as between steps within each stage. Nevertheless, in APT attacks on CPS the opportunities for the various attack steps involved will be limited and an APT could take months to years to complete.

Future work involves exploring multiple alternatives to gaining local access to the CPS, such as supply chain attacks. It will still be challenging to exfiltrate data out of the CPS using supply chain attacks, but this is worth exploring as it would greatly simplify the attack execution and represent a communication path into the CPS. One potential strategy is to adopt an approach similar to the SolarWinds hack, which could enable the distribution of the attack toolkit across multiple software updates. Further work will also focus on automating parts of the attack to minimize the need for local access. Moreover, priority will be given to developing attack strategies that result in sabotage, particularly those causing long-term damage, such as the destruction of circuit breakers, transformers, and similar crucial for building better resilience into CPS in the future.

Acknowledgements This work has received funding from the Research Council of Norway through the CORESIM (Context-Based Real-Time OT-IT Systems Integrity Management) project with Project No. 344244.

Author Contributions All authors reviewed the manuscript.

Funding Open access funding provided by NTNU Norwegian University of Science and Technology (incl St. Olavs Hospital - Trondheim University Hospital)

Data availability Due to the sensitive nature of the topic, the codes and related data cannot be provided.

Declarations

Conflict of interest The authors declare that they have no confict of interest.

Informed consent Informed consent was obtained from all authors included in the study.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

References

1. IEEESpectrum, The real story of stuxnet, https://spectrum.ieee.org/the-real-story-of-stuxnet, 2 (2013)
2. Ajp-3.20 allied joint doctrine for cyberspace operations, January 2020, edition A Version 1. [Online]. Available: https://assets.publishing.service.gov.uk/media/5f086ec4d3bf7f2bef137675/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf
3. Ahlberg, C.: Moving toward a security intelligence program, The Threat Intelligence Handbook, 2nd ed., CyberEdge Group LLC: Annapolis, MD, USA, (2019)
4. T. Rep. (2020). Cost of a data breach report. [Online]. Available: https://www.ibm.com/security/digital-assets/cost-data-breach-report/1Cost%20of%20a%20Data%20Breach%20Report%202020.pdf
5. Alshamrani, A., Myneni, S., Chowdhary, A., Huang, D.: A survey on advanced persistent threats: techniques, solutions, challenges, and research opportunities. IEEE Commun. Surv. & Tutor. **21**(2), 1851–1877 (2019)
6. Sharma, A., Gupta, B.B., Singh, A.K., Saraswat, V.: Advanced persistent threats (apt): evolution, anatomy, attribution and countermeasures. J. Amb. Intell. Human. Comput., pp. 1–27 (2023)
7. Initiative, J.T.F.T., et al.: SP 800-39. managing information security risk: Organization, mission, and information system view. National Institute of Standards & Technology (2011)
8. Matoušek, P.: Description and analysis of iec 104 protocol, https://escholarship.mcgill.ca/concern/theses/1c18dh978, https://www.fit.vut.cz/research/publication-file/11570/TR-IEC104.pdf, p. 12, (2017)
9. Buhagiar, T., Cayuela, J.-P., Procopiou, A., Richards, S., Ramlachan, R.: "Smart substation for the french power grid," In: 2016 69th Annual Conference for Protective Relay Engineers (CPRE). minus IEEE, pp. 1–5 (2016)
10. Li, Z., Ma, R., Xie, Y., Lu, L.: Overview of intrusion detection in smart substation," In: 2022 IEEE 10th Joint International Information Technology and Artificial Intelligence Conference (ITAIC), vol. 10. IEEE, pp. 2377–2384 (2022)
11. Chen, P., Desmet, L., Huygens, C.: A study on advanced persistent threats, In: Communications and Multimedia Security: 15th IFIP TC 6/TC 11 International Conference, CMS 2014, Aveiro, Portu-

gal, September 25-26, 2014. Proceedings 15. Springer, pp. 63–72 (2014)
12. Hutchins, E.M., Cloppert, M.J., Amin, R.M., et al.: Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. Lead. Issues Inform. Warf. Secur. Res. **1**(1), 80 (2011)
13. Symantec, W.: Advanced persistent threats: a symantec perspective, Symantec World Headquarters, (2011)
14. Malone S.: Using an expanded cyber kill chain model to increase attack resiliency, Black Hat US, (2016)
15. Cho, S., Han, I., Jeong, H., Kim, J., Koo, S., Oh, H., Park, M.: Cyber kill chain based threat taxonomy and its application on cyber common operational picture, In: 2018 International conference on cyber situational awareness, data analytics and assessment (Cyber SA). IEEE, pp. 1–8 (2018)
16. Hussain, S., Ahmad, M.B., Uddin Ghouri, S.S.: Advance persistent threat—a systematic review of literature and meta-analysis of threat vectors, Advances in Computer, Communication and Computational Sciences: Proceedings of IC4S 2019, pp. 161–178, (2021)
17. Center, M.I.: Apt1: exposing one of china's cyber espionage units," Mandian. com, (2013)
18. Assante, M.J., Lee, R.M.: The industrial control system cyber kill chain, SANS Institute InfoSec Reading Room, vol. 1 (2015)
19. Lemay, A., Calvet, J., Menet, F., Fernandez, J.M.: Survey of publicly available reports on advanced persistent threat actors. Comput. Security **72**, 26–59 (2018)
20. Otuoze, A.O., Mustafa, M.W., Larik, R.M.: Smart grids security challenges: Classification by sources of threats. J. Electr. Syst. Inform. Technol. **5**(3), 468–483 (2018)
21. Mai, K., Qin, X., Ortiz Silva, N., Cardenas, A.A.: IEC 60870-5-104 network characterization of a large-scale operational power grid, In: 2019 IEEE security and privacy workshops (SPW), pp. 236–241 (2019). [Online]. Available: https://doi.org/10.1109/SPW.2019.00051
22. György, P., Holczer, T.: Attacking IEC 60870-5-104 protocol, In: 1st Conference on information technology and data science (CITDS), pp. 140–150 (2020)
23. 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, pp. 1–10 (2022)
24. Hong, J., Liu, C.-C., Govindarasu, M.: Integrated anomaly detection for cyber security of the substations. IEEE Trans. Smart Grid **5**(4), 1643–1653 (2014)
25. Kush, N., Ahmed, E., Branagan, M., Foo, E.: Poisoned goose: exploiting the goose protocol. In: Proceedings of the Twelfth Australasian Information Security Conference - Volume 149, ser. AISC '14. AUS: Australian Computer Society, Inc., p. 17–22 (2014)
26. Biswas, P.P., Tan, H.C., Zhu, Q., Li, Y., Mashima, D., Chen, B.: A synthesized dataset for cybersecurity study of IEC 61850 based substation. In: 2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), pp. 1–7 (2019)
27. 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: 2015 IEEE 20th Conference on emerging technologies factory automation (ETFA), pp. 1–8 (2015)
28. Hussain, S., Iqbal, A., Zanero, S., Suhail Hussain, S.M., Shikfa, A., Ragaini, E., Alammari, R., Khan, I.: A novel methodology to validate cyberattacks and evaluate their impact on power systems using real time digital simulation, In: 2021 IEEE texas power and energy conference (TPEC), pp. 1–6 (2021)
29. 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, **21**(4), (2021). [Online]. Available: https://www.mdpi.com/1424-8220/21/4/1554
30. Alghamdi, W., Schukat, M.: Cyber attacks on precision time protocol networks–a case study. Electronics **9**(9), 1398 (2020)
31. IEC: Iec61850-90-4: network engineering guideline for communication networks and systems in substations, (2013)
32. Akbarzadeh, A., Erdodi, L., Houmb, S.H., Soltvedt, T.G., Muggerud, H.K.: Attacking IEC 61850 substations by targeting the PTP protocol. Electronics **12**(12), 2596 (2023)
33. Yang, Y., Jiang, H.T., McLaughlin, K., Gao, L., Yuan, Y., Huang, W., Sezer, S.: Cybersecurity test-bed for IEC 61850 based smart substations. In: 2015 IEEE power energy society general meeting, pp. 1–5 (2015)
34. Wright, J.G., Wolthusen, S.D.: Stealthy injection attacks against iec61850's goose messaging service. In: 2018 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe). IEEE, pp. 1–6 (2018)
35. Chlela, M., Joos, G., Kassouf, M., Brissette, Y.: Real-time testing platform for microgrid controllers against false data injection cybersecurity attacks. In: 2016 IEEE power and energy society general meeting (PESGM). IEEE, pp. 1–5 (2016)
36. 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: 2016 IEEE 21st International conference on emerging technologies and factory automation (ETFA). IEEE, pp. 1–4 (2016)
37. 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. Industr. Inf. **14**(6), 2442–2451 (2017)
38. Hoyos, J., Dehus, M., Brown, T.X.: Exploiting the goose protocol: a practical attack on cyber-infrastructure. In: 2012 IEEE Globecom Workshops. IEEE, pp. 1508–1513 (2012)
39. 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: GreHack (2015)
40. 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: 2017 IEEE 26th international symposium on industrial electronics (ISIE). IEEE, pp. 111–116 (2017)
41. da Silva, L.E., Coury, D.V.: A new methodology for real-time detection of attacks in IEC 61850-based systems. Electric Power Systems Res. **143**, 825–833 (2017)
42. Zhang, F., Mahler, M., Li, Q.: Flooding attacks against secure time-critical communications in the power grid. In: 2017 IEEE International conference on smart grid communications (SmartGridComm). IEEE, pp. 449–454 (2017)
43. 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: 2015 IEEE Power & Energy society innovative smart grid technologies conference (ISGT). IEEE, pp. 1–5 (2015)
44. Elbez, G., Keller, H.B., Hagenmeyer, V.: A cost-efficient software testbed for cyber-physical security in iec 61850-based substations. In: 2018 IEEE International conference on communications, control, and computing technologies for smart grids (SmartGridComm). minus IEEE, pp. 1–6 (2018)
45. Strobel, M., Wiedermann, N., Eckert, C.: Novel weaknesses in iec 62351 protected smart grid control systems. In: 2016 IEEE international conference on smart grid communications (SmartGridComm). IEEE, pp. 266–270 (2016)
46. Subramaniam Rajkumar, V., Tealane, M., Stefanov, A., Palensky, P.: Cyber attacks on protective relays in digital substations and impact analysis. In: 8th Workshop on modeling and simulation of cyber-physical energy systems, MSCPES 2020-Proceedings. IEEE (2020)

47. 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 2015 IEEE 20th conference on emerging technologies & factory automation (ETFA). IEEE, pp. 1–8 (2015)
48. Zhang, J., Chen, Y., Jin, N., Hou, L., Zhang, Q.: Opnet based simulation modeling and analysis of dos attack for digital substation, In: 2017 IEEE Power & Energy society general meeting. minus IEEE, pp. 1–5 (2017)
49. Izycki, E., Vianna, E.W.: Critical infrastructure: a battlefield for cyber warfare?" In: ICCWS 2021 16th International Conference on Cyber Warfare and Security. Academic Conferences Limited, p. 454 (2021)
50. Yadav, T., Rao, A.M.: Technical aspects of cyber kill chain, In: Security in computing and communications: third international symposium, SSCC 2015, Kochi, India, August 10–13, 2015. Proceedings 3. Springer, pp. 438–452 (2015)
51. Heckman, K.E., Stech, F.J., Thomas, R.K., Schmoker, B., Tsow, A.W.: Cyber denial, deception and counter deception, Advances in Information Security, 64, (2015)
52. Hahn, A., Thomas, R.K., Lozano, I., Cardenas, A.: A multi-layered and kill-chain based security analysis framework for cyber-physical systems. Int. J. Crit. Infrastruct. Prot. **11**, 39–50 (2015)
53. Wolf, M., Serpanos, D.N.: Safe and secure cyber-physical systems and internet-of-things systems. Springer, Berlin (2020)
54. Akbarzadeh, A.: Dependency based risk analysis in cyber-physical systems, (2023)
55. Klien, A.: New approach for detecting cyber intrusions in iec 61850. [Online]. (2019). Available: https://www.omicronenergy.com/download/file/26359e4b38edaf386393dc89db4ec24e/
56. 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, pp. 9–16 (2022)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.