Cyberattacks on Power Systems

Presekal, Alfan; Rajkumar, Vetrivel Subramaniam; Ștefanov, Alexandru; Pan, Kaikai; Palensky, Peter

DOI
10.1002/9781394191529.ch15

Publication date
2025

Document Version
Accepted author manuscript

Published in
Smart Cyber-Physical Power Systems

Citation (APA)
Presekal, A., Rajkumar, V. S., Ștefanov, A., Pan, K., & Palensky, P. (2025). Cyberattacks on Power Systems. In *Smart Cyber-Physical Power Systems: Fundamental Concepts, Challenges, and Solutions* (pp. 365-403). Wiley. https://doi.org/10.1002/9781394191529.ch15

Cyber Attacks on Power Systems

Alfan Presekal, Vetrivel Subramaniam Rajkumar, Alexandru Ştefanov, Kaikai Pan*, Peter Palensky

Intelligent Electrical Power Grids, Department of Electrical Sustainable Energy, Faculty of Electrical Engineering, Mathematics and Computer Science, Delft University of Technology, The Netherlands
* College of Electrical Engineering, Zhejiang University, China

1. Introduction

Power grids are undergoing a fast-paced process of digitalization for enhanced monitoring and control capabilities and grid intelligence. Infrastructure and participants are enhanced and supported by Information and Communication Technologies (ICTs). Further integration of digital technologies is vital for the development of the future power grid, e.g., next generation Operational Technologies (OTs), Internet of Things (IoT), digital substations, artificial intelligence, and big data analytics. All this is expected to increase sustainability, affordability, and resilience of the power system. The latter, however, is also challenged by all these new elements. Opening up the energy system to everyone by means of ICTs requires careful considerations with regard to data privacy and information security in general. This combined with the trend towards distributed renewable generation, electrification of virtually all aspects of our lives, and easy market participation for all energy system participants, the cyber security and resilience requirements of the power grid become even more critical. The increased digitalization raises questions, especially with regard to vulnerabilities, threats, and cyber secure operation of the power system. It is well recognized that Information Technology (IT) – OT systems are vulnerable to cyber attacks. Furthermore, the combination of heterogeneous, co-existing smart and legacy technologies generates significant vulnerabilities and security challenges. With respect to security of supply and reliability of the future energy system provision, special attention is needed for new vulnerabilities and threats that come with digitalization. Accordingly, cyber resilience aspects are critical for a further power grid digitalization.

Examples of cyber security incidents related to power grids already exist around the world. On December 23, 2015 cyber attacks were conducted on the power grid in Ukraine that resulted in power outages, which affected 225,000 customers. More sophisticated cyber attacks on the Ukrainian power grid followed on December 17, 2016 resulting in a power outage in the distribution network where 200 MW of load was unsupplied. On March 9, 2020 it was reported that the IT network of the European Network of Transmission System Operators for Electricity (ENTSO-E) had been compromised in a cyber intrusion. Fortunately, the compromised IT network was not connected to any operational electric transmission system. However, this indicates that interconnected power grids may become targets. Such laborious cyber attacks conducted by powerful adversaries are a real threat to the security of the modern society. Cyber attacks on power systems can initiate cascading failures and result in a catastrophic blackout, ending up in a doomsday scenario especially if it is considered that the world may experience a global crisis such as a pandemic. The power outage can disrupt the entire energy chain including water supply, heating, and gas networks. Without power, hospitals and other critical services are severely affected. A disruption of service may lead to financial loss, damages, chaos, or even a loss of lives.

The complexity of cyber attacks on power systems is likely to increase. Cyber security and resilience to cyber attacks are emergent challenges for future power grids. The grid operational resilience ensures security of supply and a stable system operation following high impact, low frequency disturbances. Cyber resilience is defined as the capability of the power system to anticipate, absorb the shock, adapt and rapidly recover from cyber attacks. A cyber kill chain contains the series of stages and steps used to trace the typical phases of a cyber attack from early reconnaissance to attack execution, which can result in a physical disruption of power system operation, instability or even a blackout. The kill chain of cyber attacks on grid operators may start by exploiting vulnerabilities in the utility IT system through phishing emails and similar methods. Malware is installed to open gateways and facilitate remote access for system reconnaissance, weaponization, and OT targeting. Attackers can latterly move from the IT system into the OT system, which is used for power system operation, by stealing login credentials, escalating access privileges, and discovering networked IT-OT systems and hosts. In the OT system, they can tamper with the Supervisory Control and Data Acquisition (SCADA) system, disconnect power plants and entire substations, and cause physical damage to equipment by interfering with their control systems. To improve the cyber resilience of power grids, it is necessary to identify potential threats and IT-OT system vulnerabilities, classify and review major types of cyber attacks on power grids, analyze their impact on system operation and stability, and develop mitigation techniques to improve the four stages of system resilience.

This chapter provides state-of-the-art and essential knowledge of threats and cyber attacks on power systems. It reviews major cyber attacks on power grids and Industrial Control Systems (ICSs) and provides a detailed taxonomy of cyber attacks. In this chapter, we classify the types of attacks into six categories, i.e., phishing, malware, network-based attacks, Man-In-The-Middle (MITM), host-based attacks, and Denial of Service (DoS). The impact of cyber attacks on grid operation is analyzed in terms of loss of load, cascading effects, and equipment damage. A case study of a cyber attack scenario and simulation results are provided.

2. Cyber Kill Chain

The cyber kill chain is a framework for cyber security investigation and intelligence-driven defense. It is derived from a military model, originally established to identify, prepare to attack, engage, and destroy a target. Kill chains are used to understand, anticipate, recognize, and combat Advanced Persistent Threats (APTs), social engineering attacks, ransomware, security breaches, and advanced attacks [1]. A cyber kill chain usually consists of seven stages, which represent the typical phases of a cyber attack, i.e., reconnaissance, weaponization, delivery, exploitation, installation, Command and Control (C2), and actions and objectives. However, the order of these stages is not fixed. Based on the cyber attack scenario, they can vary and even some can run in parallel. Figure 1 depicts the cyber kill chain stages.

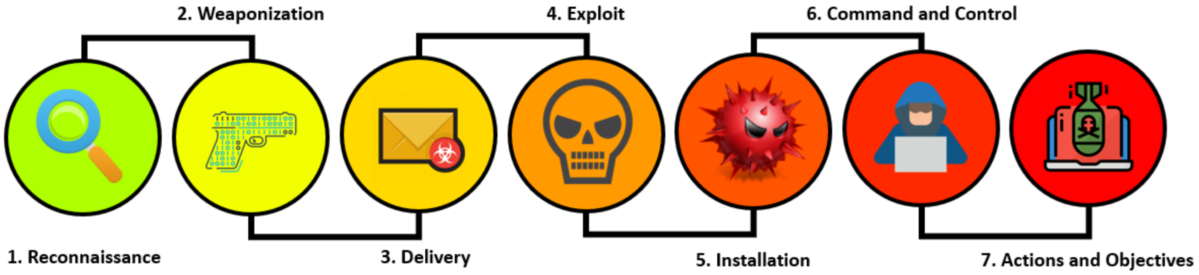


Fig. 1. Cyber kill chain

1. *Reconnaissance* is the stage where adversaries gather information about the targeted system such as network topology, communication protocols, Internet Protocol (IP) addresses, and running applications. Reconnaissance can be either active or passive. Active reconnaissance is an intrusive activity to test the target and extract more information through direct interaction. Hence, although it can uncover sensitive and critical information, it has a higher chance of detection by a defense system, e.g., Intrusion Detection System (IDS). On the other hand, passive reconnaissance does not rely on direct interaction with the targeted system, and therefore is stealthier. Passive reconnaissance is also known as passive information gathering. Passive reconnaissance was conducted in the early stages of the cyber attack in Ukraine 2015 to gather information about the Distribution System Operators (DSOs), and consequently launch a spear phishing campaign. Additionally, active reconnaissance was also conducted to extract information about network topology and active hosts in the targeted IT-OT system.
2. *Weaponization* is the process of preparing the attack vector. Weapons used in cyber attacks can be represented by malware or tools to achieve remote code execution. For an effective weaponization, adversaries first need to understand the targeted system and decide on appropriate tools to conduct the attack. Examples of weaponization include the Stuxnet malware used in the cyber attack on the Iranian nuclear reactor and BlackEnergy3 malware used in the cyber attack on the Ukrainian power grid.
3. *Delivery* is a mechanism to transfer the weaponized bundle to the victim or targeted system. Some of the most predominant delivery methods include email attachments, websites, software applications, and

Universal Serial Bus (USB) removable media. For example, in the Ukraine 2015 and 2016 cyber attacks, delivery was achieved through targeted spear phishing emails containing malicious attachments. On the other hand, in the Stuxnet attack, delivery was achieved through USB removable media.

4. *Exploitation* is a stage where attackers exploit vulnerabilities to execute code on the targeted system, e.g., vulnerabilities of operating systems, service applications, and communication protocols. For example, in the Ukraine 2015 cyber attack attackers exploited vulnerabilities present in the Windows Active Directory (AD) server to steal login credentials.
5. *Installation* is a process to deploy malware on assets, such as backdoors, Trojans, and botnets. These malicious applications allow adversaries to gain control of the targeted system and maintain their persistence. For example, in the Ukraine 2015 cyber attack, the installation process was done through a malicious macro script hidden within a Microsoft Excel file.
6. *Command and control* allow adversaries to remotely control the targeted system by exploiting system vulnerabilities using malicious applications. C2 typically can be found in botnets where the adversaries can remotely gather information and deliver commands.
7. *Actions and Objectives* represent the stage where the intruders accomplish their goals. In most cases, adversaries remain in a stealthy mode until they reach their final goal and reveal their true objective. In the Ukraine 2015 cyber attack for example, the attackers' objective was to cause a power outage. This was achieved taking over control of the SCADA system and opening multiple circuit breakers to disconnected circuits and cause a direct power outage in the distribution network.

The cyber kill chain is suitable to investigate various cyber attack strategies and APTs. Most recent trends show that there are emerging APTs targeting power grids as demonstrated repeatedly in Ukraine. These are reviewed in Section 3, based on the aforementioned cyber kill chain framework.

3. Review of Major Cyber Attacks

3.1. Cyber Attacks on Industrial Control Systems

ICS is a broad term, typically used to describe the integration of physical processes with sensors, actuators, communication networks, and controllers in order to support various industries and critical infrastructures. Large scale industrial control systems deploy SCADA for monitoring and control of the physical processes. Hence, an ICS is a cyber-physical system, integrating both cyber and physical aspects of the industrial process. Such systems are commonly found in power plants, manufacturing, and processing facilities. Due to their cyber-physical nature, industrial control systems are prone to cyber attacks. Compared to cyber attacks on IT systems, cyber attacks on ICS of critical infrastructures can have a devastating impact on the modern society with safety and financial implications. Cyber security threats targeting ICS have existed for several decades now. A historical record of cyber attacks on industrial control systems between 1982-2017 is reviewed in [2]-[4] and a summary is given in Table 1. Based on historical trends, it can be concluded that cyber attacks targeting ICS are on the rise.

Table 1. Summary of cyber attacks targeting industrial control systems

Cyber Attack	Year	Description
Siberian pipeline explosion	1982	A Trojan attack was conducted on the SCADA system of a Siberian pipeline. This attack caused an explosion equivalent to 3 kilotons of TNT.
Chevron emergency alert system hacking	1992	A former Chevron employee hacked and disabled the emergency alert system. The emergency alert system was down for more than ten hours putting at risk people from more than twenty-two states in Canada.
Salt River project	1994	Hackers gained unauthorized access and took control of the SCADA system of a 131-miles canal for five hours.

Worcester Massachusetts airport	1997	Hackers disabled for six hours the system which controlled the telephone lines in the airport.
Gazprom	1999	Hackers conducted a Trojan attack on Gazprom (a Russian gas company) and gained control of the gas flow pipelines.
Maroochy Water	2000	Hackers gained control to the water facility’s SCADA system and released 265,000 gallons of untreated sewage.
California system operator	2001	Hackers infiltrated into a process control system in California.
Davis-Besse nuclear power plant	2003	A Structured Query Language (SQL) Slammer worm infected the control system of the nuclear power plant. Safety parameters and process display computers were disabled for several hours.
CSX corporation	2003	A computer virus named Sobig infected and disabled the train signaling system in Florida, USA. The virus reportedly spread via email attachments.
Tahoma Colusa canal	2007	A former employee installed an unauthorized application to the Canal SCADA system.
Turkey pipeline explosion	2008	Attackers exploited vulnerabilities in the security camera software to gain physical access to the control center. Subsequently, they triggered a pipeline explosion.
Stuxnet	2010	A weaponized malware attack targeted the uranium enrichment processes at Iranian nuclear facilities. The malware caused centrifuges to spin abnormally, while blindsiding operators.
Night Dragon	2010	Various malware attacks targeted oil, petrochemical, and energy companies.
Duqu	2011	A malware attack targeted specific organizations including the industrial control systems of various manufacturers. It served as an ICS reconnaissance tool.
Flame	2012	A malware targeted oil companies in the Middle East and North Africa. The malware's main function is to steal data from targets.
Malware infection of the SCADA system in a power plant	2012	The SCADA system of a power plant in USA was infected with malware via an USB drive during maintenance. The infection caused a three-week restart delay of the power plant.
New York dam	2013	Iranian hackers reported the launch of a cyber attack on industrial control system of Bowman Dam in New York.
Havex	2013	A malware campaign was conducted, mainly targeting industrial control systems.
German Steel mill	2014	Cyber attacks using malware targeted the SCADA system of a German steel mill causing significant damages.
Kemuri Water company	2016	Hackers gained access to the SCADA system and manipulated the control applications.
TRITON	2017	A malware attack was conducted on a Saudi Arabian petrochemical plant targeting the industrial safety systems.

Most of the cyber attacks on ICS have not resulted in direct physical damages. However, nearly all of them have resulted in data breaches and disruptions to system operations. Nevertheless, there are some incidents that have caused a direct physical impact. One such recorded cyber attack was a Trojan software attack on the SCADA system of a Siberian pipeline in 1982. The attack triggered an explosion in the pipeline equivalent to three kilotons of TNT [5]. This cyber attack put human lives at risk and caused immense physical damage.

The most notable and well-known cyber attack targeting industrial control systems is Stuxnet, which was reported in 2010. Stuxnet was the first, widely known, cyberwarfare weapon. Reports about the Stuxnet malware have been presented in [6]-[8]. Being a weaponized malware, its creators had strong knowledge of the SCADA system operation. According to the investigation carried out in [7], it triggered a shift in rotational frequency of the motor's Programmable Logic Controller (PLC), damaging to the uranium enrichment process. In the future, industrial control systems of critical infrastructures may become obvious targets for state-sponsored cyber attacks. Hence, cyber security of ICS is an important concern for industries and governments, alike.

3.2 Cyber Attacks on Power Grids

Increased power grid digitalization, driven by the energy transition has introduced cyber attacks on power grids as a real modern-day threat. Such advanced cyber attacks come with worrying ramifications. They can be classified as high impact, low frequency events with a wide range of effects. It is worth noting however, there are only a handful of known real cases of cyber attacks specifically targeting power grids. Nevertheless, such attacks have established the means and provided a glimpse of the possible disastrous consequences. The most well-known examples of cyber attacks targeting power grids, i.e., Ukraine attacks in 2015 and 2016, are extensively dealt with in the subsequent subsections.

3.2.1. Ukraine 2015

On December 23rd, 2015, at 15:30 local time, a cyber attack was conducted on the power grid in Ukraine. This attack is the first publicly known cyber attack targeting power systems, which resulted into a power outage. The attackers compromised the SCADA systems of three DSOs and disconnected seven 110 kV and twenty-three 35 kV substations from the distribution network. The attack was conducted successfully. The power outage affected 225,000 customers [9], [10].

Figure 2 presents the typical IT-OT systems of utilities. The IT network is used for the non-operational side of the business, e.g., asset and resource management, geographic information system, legal, finance, human resources, and payroll. The IT and OT systems in the control center are interconnected. However, security controls such as firewalls are in place to keep the IT–OT networks segmented, and OT network separate from a direct connection to The Internet. Segmentation of the control center from the corporate IT network is implemented for cyber security considerations. The OT systems gather data from substation bays and station control systems, e.g., voltage and current magnitudes, active and reactive powers, circuit breaker status, and transformer tap positions, and send them to the SCADA servers in the control center. The real-time data is used by grid operators for power system operation. However, the cyber attack in Ukraine 2015 proved that the utility IT-OT systems with their current security controls are not impenetrable. The IT network segment served as the entry point for the attackers. Thereon, the attackers continued to the control center and substations with the objective to cause a blackout. Based on the results of forensic investigation, the cyber kill chain is used to divide the cyber attack into nine stages in a chronological sequence. This indicates that the attackers adopted sophisticated attack techniques at every stage.

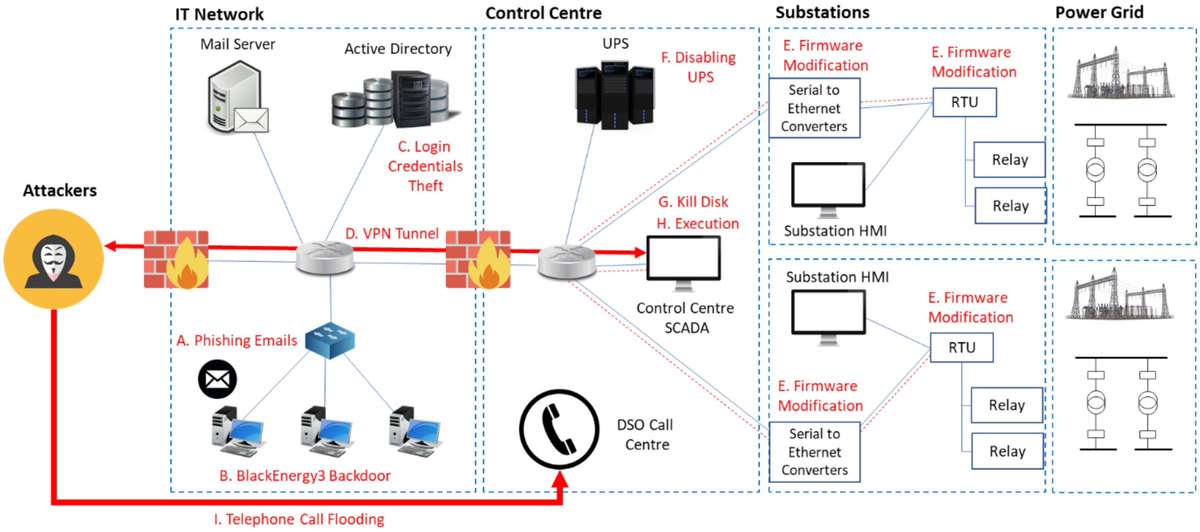


Fig. 2. Cyber attack on the power grid in Ukraine in 2015

Spear phishing served as the entry point of the attack in the corporate IT network. The attackers specifically targeted three DSOs, pretending to be officials from the Ukraine Ministry of Energy. The malicious emails, seemingly originating from trustworthy sources contained a weaponized Microsoft Excel file attachment. The attackers exploited Microsoft Excel's macro vulnerabilities to install their malware in the DSO IT network. A macro is a program created to automate tasks in Microsoft Excel using Visual Basic Application (VBA) scripts. When the recipients enabled the macro, the VBA script was launched, installing BlackEnergy3 malware on the computer. After a successful installation, the malware connected to attackers' remote C2 server using IP address 5.149.254.114 and port number 80. The remote IP address and port number were specifically coded in the malware. The connection via port 80 seemed innocuous. This is because port 80 is a common port for website traffic via Hypertext Transfer Protocol (HTTP). With the connection to the C2 server enabled, the attackers could remotely control the BlackEnergy3 malware.

BlackEnergy3 provides various functionalities such as network scanner, file stealer, password stealer, keylogger, screenshot capturer, and network discovery. BlackEnergy3 malware played a very important role during the early stages of active reconnaissance and C2. Using the network scanner and network discovery modules, the malware found information about the IT network configuration, e.g., network segments, network topology, hosts connected, etc. With BlackEnergy3, the attackers could also steal passwords using a keylogger, steal files, and capture screenshots of the targeted computers. This preliminary information was important to plan the following attack stages. The attackers transferred all the collected information directly to the remote C2 server.

From the active reconnaissance stage, the attackers found a vulnerable active directory server which became a breach point of the IT-OT system. The active directory is a Windows-based database service for IT networked system operations. An AD manages access permissions for a user by acting as a central authentication and authorization authority for managed accounts, hosts, and services. AD makes the IT system operation easier and more flexible with centralized authentication and authorization instead of using segregated services. Active directory databases also store usernames, passwords, and host and services information. Hence, the AD serves as a critical point in the entire DSO IT network. In the Ukraine 2015 cyber attack, the attackers compromised the AD server to gain access to a majority of hosts in the IT network. From the compromised AD server, attackers obtained user login credentials and gained direct access to the hosts. The attackers then traversed laterally from the IT network to the OT system in the control center and substations. They accessed the computers located in the control center with the previously stolen credentials.

After gaining access to the control center, the attackers created a Virtual Private Network (VPN) connection from a computer in the control center to a remote location on The Internet. VPN allowed the attackers to perform tunneled and encrypted connections to access the targeted computer. Instead of using a static C2 server with port 80, VPN provided more flexibility for the attackers to access the computer from any location on The Internet.

Furthermore, the VPN also aided the attackers in evading firewall detection and hide their real locations. At this point, the attackers had already gained full control to launch the final attack. However, the attackers remained stealthy, carrying out additional actions to magnify the impact of the cyber attack on the distribution network.

The attackers conducted four additional stages, i.e., E, F, G, and I summarized in Table 2, to increase the attack severity. In stage E, the attackers accessed substations to compromise Remote Terminal Units (RTUs) and the serial-to-Ethernet converters. A serial-to-Ethernet converter connects Ethernet communications in the substation, e.g., IEC 104, to serial communications with the control center, e.g., IEC 101. These devices are typically embedded without an operating system. The processes are controlled by firmware. Hence, the attackers also created malicious firmware and replaced the legitimate firmware in the RTUs and serial-to-Ethernet converters to make them dysfunctional upon reboot. The malicious firmware ensured that grid operators could not remotely control the substations to perform emergency restorative actions. In stage F, the attackers accessed the Uninterruptible Power Supply (UPS) units in the control center. Subsequently, they disabled the UPS backup power supply to cause an outage in the control center as well during power outage in the distribution network. In stage G, the attackers used KillDisk to erase hard drives and delete data in the control center servers and computers and make them unbootable. KillDisk is a module of BlackEnergy3 malware for deleting data, registry, and system configuration. In stage I, immediately after the final attack execution on December 23rd, attackers also conducted a telephone call flooding attack on the DSO call center from foreign numbers so that customers could not report the power outages. Due to these attack stages, the power outage could only be restored after 6 hours. Thus, the attackers successfully executed one of the two most significant cyber attacks targeting power systems to date. Table 2 provides a summary of the attack stages and mapping to the cyber kill chain.

Table 2. Ukraine 2015 cyber kill chain

Stage	**Process**	**Cyber Kill Chain**
A	Attackers send phishing emails containing Microsoft Excel file attachments. The file attachment is weaponized with BlackEnergy 3 malware. When the recipient opens the Excel file, a macro function is launched and BlackEnergy3 is installed onto the computer.	Weaponization, Delivery, Installation
B	The attackers use the BlackEnergy3 and compromised computers to serve as backdoors for remote C2 actions. Further investigation of BlackEnergy3 has been presented in [11], [12]. Using BlackEnergy3, attackers also performed active reconnaissance and lateral movement in the IT network.	C2 and Reconnaissance
C	The attackers successfully locate and compromise the AD server on the IT network. From the AD database, the attackers steal user login credentials. Using the stolen credentials, the attackers access devices located in the control center.	Exploitation
D	After gaining access to the OT system, attackers create a VPN tunnel from The Internet directly into the control center. This VPN tunnel allows direct access and remote execution. According to the investigation in [9], attackers compromised the IT network and control center OT system six months before the final attack execution on December 23rd, 2015. However, during this period, their malicious activities went undetected and the attack became an advanced persistent threat. The attackers could have launched their attack much earlier. However, they maintained stealth and created a more devastating impact. To increase the attack severity, stages E, F, G, and I were conducted.	Installation, Exploitation, C2
E	The attackers modify the firmware of the serial-to-Ethernet converters and RTUs in substations.	Exploitation, Installation
F	The attackers disable the UPS backup power supply in the control center.	Exploitation, Installation

G	The attackers install KillDisk in the control center and erase hard disk data, leaving no traces of activity.	Exploitation, Installation
H	On December 23rd, 2015, at 15.30 local time, attackers start the cyber attack execution on distribution network operation by remotely controlling the SCADA system and opening circuit breakers in substations. This step successfully disconnected seven 110 kV and twenty-three 35 kV substations directly causing power outages. Under normal conditions, power system restoration is done remotely from the control center or manually from substations. However, the remote control was unsuccessful as the RTU and serial-to-Ethernet converter firmware were compromised. The compromised UPS in the control center could not provide backup power to SCADA servers, exacerbating the situation. Furthermore, the SCADA system failed to operate because KillDisk execution wiped out the server's hard disks.	C2, Actions and Objectives
I	The attackers also conducted a telephone call flooding attack on the DSO call center from foreign numbers so that customers could not report the power outages. Due to this complicated situation, restoration efforts took around six hours.	Actions and Objectives

3.2.2 Ukraine 2016

On December 17, 2016, at 23:53 local time, a second cyber attack was conducted on the power grid in Ukraine. This is the first publicly acknowledged cyber attack, involving malware that targeted power systems and resulted into a power outage. It affected the SCADA system at the transmission level targeting a single 330 kV substation. The cyber attack resulted into a power outage in the distribution network where the total unsupplied load was 200 MW. Compared to the 2015 attack, the 2016 attack was more advanced in terms of the attack technique. Thankfully, this attack resulted in a much lower impact, compared to the previous one. The 2016 attack employed sophisticated malware named CRASHOVERRIDE or Industroyer. Further studies related to this attack are presented and discussed in [13]-[17]. Based on these investigations and the cyber kill chain framework, we classify the Ukraine 2016 attack into seven stages in chronological sequence as represented in Figure 3 and summarized in Table 3.

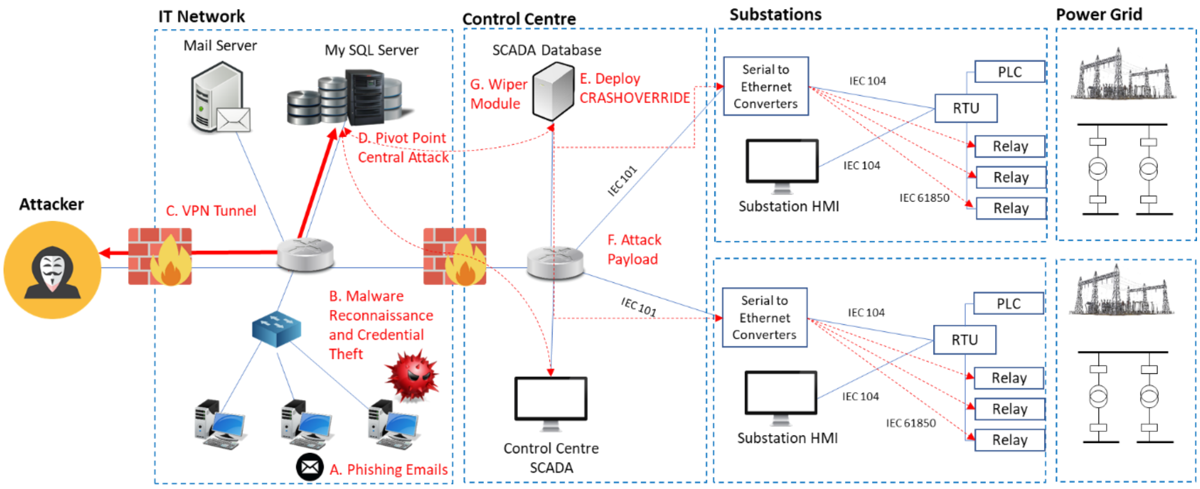


Fig. 3. Cyber attack on the power grid in Ukraine in 2016

Table 3. Ukraine 2016 cyber kill chain

Stage	Process	Cyber Kill Chain

A	In January 2016, phishing emails targeting the power grid operator in Ukraine were reported. The attackers may have used a different strategy for phishing compared to the previous year. Unfortunately, detailed information in this regard is not available. Nonetheless, phishing emails are assumed to be the entry point of the attack.	Delivery
B	Slowik et al. identified that malware was clearly involved in the early stages of the cyber attack [17]. The malware was used to conduct reconnaissance, initial lateral movement, and credential theft within the IT system. Unlike the 2015 attack, there is no substantial information on how the attackers actually stole credentials.	Weaponization, Installation, Reconnaissance
C	The attackers established a VPN tunnel to bypass the firewall and perform remote command and control via the compromised server.	Installation, C2
D	The attackers used a MySQL server as the central point of the attack, executing commands from within the IT network to the control center OT systems. At this stage, the attackers also gathered information on type of protocols being used in the control center OT network. This knowledge and information were vital for the attackers to prepare for the subsequent attack stages.	Exploitation, C2, Reconnaissance
E	Next, the attackers sent a malicious text file to the SCADA server in the OT network segment. Upon arriving at the designated host, the file changed into an executable file containing CRASHOVERRIDE malware. CRASHOVERRIDE is a unique malware, designed and created based on the knowledge of ICS protocols such as IEC 101, IEC 104, IEC 61850, and Open Platform Communication (OPC). As a result, the malware could deliver crafted traffic based on those specific protocols.	Weaponization, Delivery, Installation
F	In the final stages of the attack, the attackers took control of the compromised hosts in the control center to send malicious payloads to substations and open circuit breakers. These attacks were launched on December 17, 2016 at 23:53 local time. The attacks affected the SCADA system at the transmission level focusing on a single 330 kV / 110 kV / 10 kV substation, resulting in a distribution-level outage. Soon after, operators swiftly responded to the attack and transferred controls into manual mode.	C2, Actions and Objectives
G	After the final attack, the wiper module which was also a part of the CRASHOVERRIDE overwrote system service registry entries to null values to render the system unbootable. The wiper module removed files relating to ICS operations to prevent swift IT-OT recovery and power system restoration.	Actions and Objectives

The overall lower impact of the cyber attack in 2016 can be attributed to several causes. The primary reason was the limited success of the malicious payload injection. This was probably caused by a rigid attack technique, predefined within the code by the attackers. Most likely, they prepared the protocol payload module based on their test systems, which was later deployed on the targeted system. Hence, the attackers did not have an opportunity to fully test their attack methods on a real-world ICS. Such an attack scenario while being sophisticated, comes with the cost of easy detection by system operators. Nonetheless, the attackers successfully demonstrated advanced attack strategies with a deeper understanding and insight of the targeted power system. In the future, such types of attack may potentially become more common, leading to catastrophic damages to the power grid infrastructure. The overall comparison between Ukraine 2015 and 2016 cyber attacks is provided in Table 4.

Table 4. Comparison of Ukraine 2015 and 2016 cyber attacks

Metric	Ukraine 2015 Attack	Ukraine 2016 Attack
Malware	BlackEnergy3	CRASHOVERRIDE
Role of the malware	Remote command and control, reconnaissance, credential theft, delete system files and corrupt OT systems	Remote command and control, reconnaissance, credential theft, delete system files and corrupt OT systems, launch scheduled attack
Final attack stage	Attackers took control of SCADA via remote desktop and opened multiple circuit breakers in real-time	Automated malware was launched with malicious payload instructions to open circuit breakers
Increase attack severity	Compromise UPS, modify RTU firmware, erase system files and corrupt OT systems using KillDisk, conduct telephone call flooding	Erase system files and corrupt OT systems using wiper module
Affected substations	30	1
Power outage duration	6 hours	30 minutes
Load unsupplied	135 MW	200 MW
Affected customers	225,000 customers	Unknown

4. Taxonomy of Cyber Attacks on Power Grids

There are many attack techniques that can potentially be deployed to specifically target power grids. In this section, we classify such types of attacks into six categories, i.e., phishing, malware, network-based attacks, man-in-the-middle, host-based attacks, and denial of service. Figure 4 shows the taxonomy of cyber attacks on power systems and ICS. We delve in depth into each cyber attack category targeting industrial control systems and power grids in the following subsections.

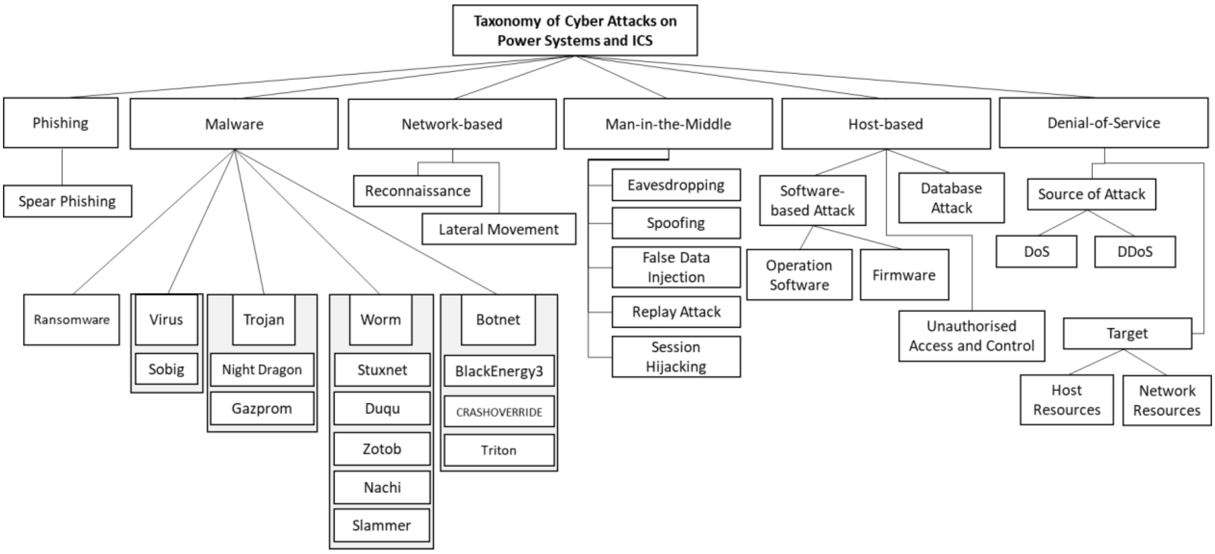


Fig. 4. Taxonomy of cyber attacks on power systems and ICS

4.1 Phishing

Phishing is a type of social engineering attack exploiting human factors. Phishing attacks aim to obtain sensitive information or data and deliver malware inside the corporate IT network, thereby often serving as entry points in the delivery mechanism of sophisticated cyber attacks. In phishing, attackers pretend to be a trustworthy source, persuading the victims to carry out certain actions. These could be opening an email, accessing Uniform Resource Locator (URL) links, downloading files, and unknowingly providing sensitive information. In this section, our discussion is focused on email phishing attacks. Emails represent an important individual identity on The Internet and also carry organizational significance as formal communication channels. Due to these reasons, emails have become the most dominant phishing media. Attackers can arbitrarily send phishing emails to any email address, aiming to persuade recipients to carry out further actions, as described above. These actions may be followed by malicious outcomes such as information breaches, malware installation, and financial losses.

Spear phishing is a variant of phishing, which targets a specific individual or organization. Before launching a spear phishing attack, an attacker gathers detailed information about the target. Information gathering can be done via The Internet or social engineering. Based on preliminary information, the attacker crafts the phishing email content to be relevant and strongly related to the target, prompting a higher success rate compared to arbitrary phishing. In general, state-sponsored attackers or cyber criminals are the ones behind spear phishing attacks. Consequently, spear phishing serves as an important entry point for advanced persistent threats. For example, in Ukraine 2015, the attackers pretended to be from the Ukrainian Ministry of Energy, which was strongly related to the targeted distribution system operators. Hence, the spear phishing campaign was successful in deceiving the DSO employees to access the malicious email attachments, resulting in the installation of malware.

Protection against phishing attacks can be achieved by strong organizational policies and corporate IT security. This can include verifying and screening email address sources, URL links, and file attachments in emails. Through such measures, malicious emails can then be flagged and filtered, serving as the initial line of defense against phishing attacks. However, the most critical defense method is raising user awareness. With proper awareness and training, users can recognize phishing emails.

4.2 Malware

Malware is a piece of malicious code that exploits software vulnerabilities in a targeted system. The occurrence of malware-related attacks has been on the rise, especially over the last decade [18]. There are various types of malware, e.g., ransomware, virus, Trojan, worm, and botnet, examples of which are presented in Figure 4. Advanced types of malware such as worms and botnets, owing to their intelligence and controllability, are gaining popularity as modern cyber attack vectors. Furthermore, given their ability to propagate and spread independently, they have become the cyber weapons of choice targeting industrial control systems. Therefore, in this section, we focus on the most well-known examples of worms and botnets involved in cyber attacks on ICS and power grids, i.e., Stuxnet, BlackEnergy, CRASHOVERRIDE, and Triton. Table 5 shows an overview of the comparison of the capabilities between most commonly found types of malware in ICS-related cyber incidents.

Table 5. Comparison of malware capabilities

No.	Capabilities	Viruses	Trojans	Worms	Botnets
1	Self-replication	✓		✓	
2	Backdoor		✓		✓
3	Remote control		✓		✓
4	Network spread			✓	✓

Table 6 shows a brief history of malware involved in ICS cyber-related incidents from 1982 to 2017. It can be seen that worms were popular in the early 2000s due to their capabilities to spread across the network. However, an attacker cannot fully control a worm, leading to an uncontrollable spread. This may result in loss of stealth and unexpected exposure and discovery. For example, the Stuxnet worm was originally created only to target Iranian nuclear reactors. Unfortunately, it ended up spreading across the world [7], leading to its discovery in 2010. As a result, botnets have become the malware of choice in recent years. A botnet can be controlled remotely and acts as a vector for advanced persistent threats [9], [16].

Table 6. History of malware involved in major ICS cyber-related incidents

No.	Target	Type of Malware (Name)	Year
1	SCADA gas pipeline, Siberia [2]	Trojan horse	1982
2	SCADA gas pipeline, Russia [2]	Trojan horse (Gazprom)	1999
3	Web service RTU, PLC [19]	Worm	2002-2003
4	SCADA database [19]	Worm (Slammer)	2003
5	SCADA petrochemical plant [19]	Worm (Nachi)	2003
6	Train signaling system, USA [2]	Virus (Sobig)	2003
7	SCADA automotive manufacturing plants [20]	Worm (Zotob)	2005
8	Energy companies [21]	Trojan horse (Night Dragon)	2009
9	SCADA nuclear centrifuge [8]	Worm (Stuxnet)	2010
10	SCADA reconnaissance [2]	Worm (Duqu)	2011
11	SCADA steel mill, Germany [22]	Botnet	2014
12	SCADA power grid, Ukraine [11]	Botnet (BlackEnergy3)	2015
13	SCADA power grid, Ukraine [17]	Botnet (CRASHOVERRIDE)	2016
14	SCADA petrochemical plant, Saudi Arabia [23]	Botnet (Triton)	2017

4.2.1 Stuxnet

Stuxnet is a worm discovered in June 2010, designed specifically to target PLCs in industrial control systems. It exploited unprecedented zero-day vulnerabilities present in the Microsoft Windows operating system, Siemens STEP7 PLC software, and Remote Procedure Call (RPC) server mechanism. Stuxnet also employed the rootkit technique to hide from commercial antivirus software. It was later identified as a state-sponsored and developed cyber weapon to target the uranium enrichment facilities in Iran. Detailed technical studies about Stuxnet are presented in [7], [24].

Stuxnet spread through three main mechanisms. The initial entry point was via USB flash drives in computers located within the SCADA system. When a USB drive is plugged into a computer, the Windows operating system will execute autorun.inf or Windows .lnk as an autorun mechanism. Exploiting this vulnerability, Stuxnet copied itself onto the computer's hard drive. The second spreading mechanism was through Windows network shares, wherein Stuxnet had the capability to duplicate itself into a shared folder on the same network. Through this mechanism, Stuxnet exploited the Server Message Block (SMB), popularly known as Samba, which is a protocol for file and folder sharing. The third spreading mechanism exploited vulnerabilities present in Siemens' software, i.e., Siemens WinCC and Siemens STEP7. Stuxnet identified and compromised access to computers that ran Siemens WinCC. Furthermore, it also replicated itself into WinCC computers via an SQL injection command. Siemens STEP7 is an application used to program Siemens PLCs. Hence, through STEP7, Stuxnet spread into PLC devices as well. If a computer was running Siemens STEP7, Stuxnet modified the Windows Dynamic Link Library (DLL) and associated executable files. With this infection, Stuxnet added malicious code into the PLC devices, allowing complete control over them. In the reported incidents, it caused centrifuges to spin abnormally, while blindsiding operators.

Taking a closer look at its structure, Stuxnet mainly consists of two modules, i.e., user-mode and kernel-mode. The user-mode module has four functions: (i) searching function for specific targets, (ii) privilege escalation, (iii) malicious code injection into PLC, and (iv) installation kernel-mode. It is interesting to note, the malware also had a time limit date set to June 24th, 2012. Hence, it was functional only until that specific date. The kernel-mode made Stuxnet work on the lower system levels, well below the application level of the user-mode. By implementing the kernel-mode, Stuxnet was maliciously launched during every Windows bootup process. This system-level execution made it more persistent and impervious to antivirus protection. The main functionality of Stuxnet was defined in its code. However, it was also designed to remotely communicate to the command and control server. This mechanism allowed adversaries to remotely update the malware. However, this remote update was never performed, in order to limit the uncontrollable spread of Stuxnet outside of its designated target.

4.2.2 BlackEnergy

BlackEnergy is a malware, initially identified in 2007 as an HTTP-based botnet for Distributed Denial of Service (DDoS) attacks. It identified and targeted multiple file extensions, including Microsoft Office, Java, and executable files. More specifically, BlackEnergy injected malicious files into the Windows System32 folder on a target Windows machine. However, its most infamous use was as a weaponized malware during the cyber attack on the power grid in Ukraine, in December 2015.

In this attack, BlackEnergy3 exploited the SMB protocol to propagate across the IT-OT networks. SMB was used as the attack vector due to its capabilities to bypass typical firewalls. Through the infected SMB, BlackEnergy3 replicated across hosts in the IT network, delivering malicious payloads. In addition, it was accompanied by an RPC to serve as a backdoor module. This was done to establish a connection between the infected hosts and the attacker's C2 server. RPC allowed the malware to receive commands from the remote C2 server, and relay critical information back. Such advanced remote capabilities allowed adversaries to perform early reconnaissance using its many plugins during the attack. These plugins were programmed with many functionalities, such as executing file operations, i.e., enumerate, execute, download, and overwrite, stealing credentials, discovering networks, and self-destructing. The self-destruction function of BlackEnergy3 was executed via KillDisk. Furthermore, BlackEnergy3 also contained information regarding the current time and location. This allowed it to run malicious activities during non-peak hours, e.g., at midnight. Overall, with all these capabilities, BlackEnergy3 has been proven to be a vicious tool for cyber attacks on power grids. Further detailed investigation of BlackEnergy3 is presented in [12].

4.2.3 CRASHOVERRIDE

CRASHOVERRIDE or Industroyer was the root cause of the cyber attack on the power grid in Ukraine in December 2016. Its many features such as backdoors, intrusion, and reconnaissance strategies are quite similar to BlackEnergy3. However, according to its code level investigations, there is no strong connection between the two malware. It is very likely that CRASHOVERRIDE was a new type of malware, specifically created for the Ukraine 2016 attack [13]. It mainly comprised of three components, i.e., backdoor, payload, and launcher.

The backdoor of CRASHOVERRIDE can be further subclassified into the main backdoor and the additional backdoor. The main backdoor served as the main controller, connecting to a remote C2 server via Hypertext Transfer Protocol Secure (HTTPS). Remote commands were encapsulated as HTTPS traffic, while source and destination addresses for establishing connectivity to C2 server were hardcoded. This clearly shows that CRASHOVERRIDE was created on purpose to specifically target the Ukrainian power grid. Using the backdoor, attackers could define a specific time to activate the malware allowing them to perform a multitude of actions. This includes remote control for process execution, switch execution into a specific user account, download file from C2 server, copy files, start and stop services, change registry values, and execute shell commands. The additional backdoor was set up as contingency, in case of a failure of the main backdoor. It was deployed in the form of a Trojan file disguised as a Notepad executable file. This additional backdoor had a different configuration and connected to a different C2 server.

The payload component described the payload for specific protocols such as IEC 101, IEC 104, IEC 61850, and OPC. Hence, in order to craft malicious packets, an adversary must possess proper knowledge about power grid communication and automation standards. These payloads are typically stored using the DLL file extension on the Windows operating system. Exploiting such mechanisms, adversaries saved critical operational data related to network configurations such as IP addresses and running protocols inside .ini extension files.

In order to carry out the attack, adversaries executed the launcher module that triggered the malicious payload execution and packet delivery into targeted substations, based on predefined protocols. These malicious packets were expected to open circuit breakers and cause a blackout. Finally, to remove all traces of the attack, the launcher module also executed the data wiper function. Data wipers changed the registry value on the Windows operating system to make it unbootable and also deleted files on the infected computers. Subsequently, the data wiper triggered process termination causing the operating system to crash. Besides these three main components, CRASHOVERRIDE possessed additional capabilities such as port scanner and DoS. The port scanner identified open ports on the target's IP address. On the other hand, the DoS tool sent malicious packets to Siemens SIPROTEC devices to make them unresponsive. Such capabilities were expected to increase the severity of the cyber attack. However, the attack did not work as expected. One of the probable reasons was the hardcoded nature of CRASHOVERRIDE that made it less flexible.

4.2.4 Triton

Triton is a botnet that targeted the Triconex Safety Instrument System (SIS) from Schneider Electric at a Saudi Arabian petrochemical processing plant in 2017 [23]. SIS is an automated mechanism in ICS to prevent operational failures and protect from hazards such as fires and explosions. Hence, Triton's objective was to disrupt SIS functioning to allow the potential occurrence of catastrophic incidents. This malware was an advanced persistent threat as almost all of its operations were carried out in a stealthy manner. Investigations shows that Triton is arguably the stealthiest malware targeting ICS to date. Hence, it is very fortunate that it was uncovered. The Triton attack was exposed because the adversaries made a mistake in triggering the safety system mechanism, thereby shutting down the entire ICS. Otherwise, it is estimated that Triton would have probably remained undetected with potentially catastrophic consequences.

Triton employed social engineering techniques to gain access to the ICS network. The plant operators received or downloaded a trilog.exe file. This file pretended to be a legitimate Schneider Triconex SIS application. The executable file served as a vector to initiate the cyber attack. The malicious file then injected the Triton payload into the memory of the Triconex SIS controller. In addition, it also injected two files inject.bin and imain.bin to the SIS devices. Inject.bin contained payload data for the attack, and imain.bin became a backdoor for allowing remote execution. To carry out such a major attack, adversaries had good knowledge of how the SIS system worked. By exploiting the payload of the SIS protocols and executing remote control, attackers conducted a coordinated attack on the SIS protection systems. There were three possible attacks performed by Triton. The first was to shutdown the SIS process itself. The second and third were to reprogram and persistently maintain the SIS in an unsafe state [25]. It is worth mentioning that there is no detailed technical information available regarding Triton's attack process. Nonetheless, Pinto et al. investigated the technical mechanism of the Triton attack process using a replicated attack environment [23] where some of the attack stages were simulated based on assumptions.

4.3 Network-based Attacks

The communication network is the backbone for data exchange between connected hosts in IT-OT systems. Thereby, a successful cyber attack can potentially target multiple aspects of the communication network, including physical connections, device information, and protocols in use. Active network reconnaissance and lateral movement are the two most common network-based attacks.

4.3.1 Network Reconnaissance

Network reconnaissance is the process of discovering information related to the computer network such as connected hosts, network topology, protocols, applications, and services running on the IT-OT network. It can also be used to discover vulnerabilities. Attackers typically employ the Internet Control Message Protocol (ICMP) to identify active hosts connected to the communication network. Based on a prediction of the range of active IP addresses in the network, an attacker launches a ping ICMP scan using tools such as tcpdump or nmap. The scan provides a list of active host IP addresses that responded to the ping message. This can be mitigated by filtering ICMP packets and discarding them. Another variant of the attack involves attackers using a Transmission Control Protocol (TCP) scan by launching TCP sync packets to the list of IP addresses. Active hosts respond with an acknowledge packet. However, for this attack one also needs to consider the number of active ports, which is time and resource intensive. Hence, TCP scanning is more challenging. In any case, as a result of network reconnaissance, attackers can obtain a list of active host IP addresses connected to the network.

From the list of active hosts, attackers can obtain further details such as the running services by scanning for active ports. For example, if port 80 is open, it may imply that the host is running an HTTP service/webserver. If port 25 is open, then the host is probably running a Simple Mail Transfer Protocol (SMTP) mail server. Taking this further, attackers can also find a detailed version of the running applications through host fingerprinting and obtain potential vulnerabilities. Therefore, in a cyber attack scenario on power grids, network reconnaissance plays an important role in discovering the target hosts and protocols on the IT-OT systems. For example, in Ukraine 2015, attackers successfully identified vulnerabilities in the Microsoft active directory server, paving the way for subsequent access to the OT systems in the control centre through login credential theft. Similarly, in Ukraine 2016, attackers successfully detected active protocols such as IEC 101, IEC 104, and IEC 61850 used for communication within substations.

4.3.2 Lateral Movement

Lateral movement is the attack process of progressively propagating throughout the targeted communication network. It starts from the most vulnerable host, serving as the entry point, moving through multiple hosts to reach the final OT target. This attack typically exploits user login credentials to access various hosts and move laterally within the IT-OT network. This technique is a common mechanism, often found in advanced persistent threats. Consequently, lateral movement was heavily employed in the cyber attacks targeting the power grid in Ukraine in 2015 and 2016. In 2015, the attackers' final objective through lateral movement was to access the SCADA system in the control centre and cause a blackout. IT-OT network segmentation is one solution to mitigate the lateral movement threat. However, as seen in Ukraine repeatedly, despite network segmentation, the attacks were still successful. This is because network segmentation alone cannot guarantee a complete protection against advanced persistent threats. Hence, power grid operators must complement network segmentation with additional security controls such as next generation firewalls and Intrusion Detection and Prevention Systems (IDPS) to minimise the threat of lateral movement.

4.4 Man-in-the-Middle Attacks

Man-in-the-middle is a type of cyber attack classified based on the location of the adversaries. In this attack, adversaries are located between two or more hosts, allowing them to maliciously observe and be involved in their communication traffic. In this section, we focus on potential MITM attacks targeting power grids, which are classified into five categories, i.e., eavesdropping, spoofing, False Data Injection (FDI), replay attacks, and session hijacking.

4.4.1 Eavesdropping

Eavesdropping, also known as sniffing or snooping, is an attack where adversaries intercept information transmitted over the network. The main objective of eavesdropping is to intercept and gather information about the contents of the transmitted data. In comparison to other attacks, adversaries seek to only observe and not change legitimate communication. To mitigate the threat of eavesdropping, encrypted protocols can be used for communication. Due to encryption, adversaries or third parties cannot easily decipher the contents of the transmitted data. However, in a real SCADA system, most of the dataflows are unencrypted. Moreover, communications between SCADA end devices such as station control systems, RTUs, protection relays, and merging units mainly work based on a broadcast communication mechanism. For example, broadcast communication through the Distributed Network Protocol (DNP3) protocol is widely adopted in SCADA communications [26]. Such broadcast mechanisms are susceptible to eavesdropping and sniffing attacks. Adversaries can easily intercept communications by gaining unauthorized access to the OT system and exploiting the vulnerabilities of the broadcast communication mechanism. Therefore, eavesdropping plays an important role in an advanced persistent threat, especially during the reconnaissance stage. Hence, it can be used as a stealthy mechanism to gather network intelligence through passive means [27]. Valli et al. present a study about eavesdropping attacks targeting smart grids in [28]. The eavesdropping is mainly focused on the Advanced Metering Infrastructure (AMI). AMI establishes communications through wireless channels between a smart grid operator and smart metering devices. Adversaries may exploit the vulnerabilities present in wireless networks to intercept communications and capture transmitted data. Research also shows that eavesdropping can lead to privacy concerns for smart grid users, as seen in [29], [30].

4.4.2 Spoofing

Spoofing is an active attack where adversaries pretend to be legitimate entities and disrupt normal communications. Such attacks can be realized through many forms of spoofing such as emails, website URLs, text messages, Global Positioning System (GPS), and IP addresses. The most widely researched spoofing attack targeting power grids is based on GPS spoofing of Phasor Measurement Unit (PMU) data. There are multiple studies in this direction, as discussed in [31]-[33]. PMUs provide magnitudes and phase angles of fundamental power system parameters such as voltages and currents, using a common time source for synchronization [34]. Hence, GPS spoofing attacks, mainly targeting the timing signals used for synchronization, may lead to distortion of observed PMU data, which includes phase angle errors [35]. There are two types of GPS signals widely in use for civilian and military applications. GPS signals for military purposes are encrypted, while civilian ones are not. Typical PMUs for power grids function based on civilian GPS signals. This may allow adversaries to spoof GPS signals by exploiting the lack of encryption and using a portable device without a direct access to the power grid communication network. Currently, there are two approaches to mitigate GPS spoofing attacks. The first is through GPS spoofing signal detection using parameter such as signal to noise ratio [36] and the second is via anomaly detection in power system measurements.

Another commonly reported type of spoofing attack on power systems is IEC 61850 spoofing. The IEC 61850 standard is a modern power system communications standard used for substation automation and protection in digital substations. It enables information exchange through different communication protocols, of which two are of utmost importance. The Generic Object-Oriented Substation Event (GOOSE) and Sampled Values (SV) protocols are used to communicate critical substation events and measurements within a substation, respectively. Although it provides increased benefits, IEC 61850 is not cyber secure. Due to strict operational constraints and timing requirements for power system protection schemes, the standard does not implement any encryption. This makes it particularly vulnerable to packet sniffing and spoofing type of attacks. Such types of spoofing attacks are well reported and have been investigated extensively in literature [37], [38]. Multiple vulnerabilities and exploits, specifically targeting GOOSE and SV protocols are widely discussed in [39]-[41].

The premise of all these discussions is similar. Due to the lack of encryption in IEC 61850, an attacker with access to the substation communication infrastructure can wreak havoc. By carefully monitoring IEC 61850 traffic via the process and station buses, it is possible to craft spoofed GOOSE packets that can maliciously open circuit breakers. When such spoofed packets are sent to a target relay, it is tricked into opening the circuit breaker. This is successful as the packet is made to appear to be originating from the station or a bay controller, within the same substation. It is also possible to inhibit protection functionality of relays due to spoofing of SV measurement data, causing protection equipment to not operate during a critical fault conditions [42]. The spoofing attack causes a relay to get blocked from further operations due to multiple concurrent input SV streams. With the target protection device blocked, other relays in the system may trip during fault conditions. Such types of spoofing attacks can have disastrous consequences for power system operation and stability. A well targeted spoofing attack can not only compromise but also disable equipment and components within a digital substation. Subsequently, this can instigate major system instabilities, and may even induce cascading failures, due to the sudden loss of multiple components. In a doomsday scenario, attackers may trigger a system-wide collapse, i.e., a blackout, by compromising critical digital substations, leading to catastrophic damages. Nonetheless, such types of spoofing attacks can be mitigated by adopting proper cyber security measures, as discussed in [43].

IEC 62351-6 is a standard that specifically addresses cyber security of IEC 61850. It recommends an additional field to the GOOSE and SV data payloads for security-related information. This field contains a Rivest-Shamir-Adleman (RSA) based digital signature to ensure payload integrity. Through this mechanism, sending and receiving Intelligent Electronic Devices (IEDs) are clearly identified and it becomes impossible to manipulate the payload. Similarly, the standard also recommends usage of Hash-based Message Authentication Codes (HMACs) using cryptographic algorithms such as SHA-256 to ensure data integrity of GOOSE and SV frames. Such techniques can prevent spoofing and sniffing attacks. However, the suggested use of the digital signatures and security based on RSA and HMAC algorithms comes with associated costs. For protection applications where a 4 ms or lower response time is strictly required, such measures are unsuitable. This is because, encryption and decryption are computationally demanding [43], [44]. Furthermore, the usage of RSA and HMAC-based authentication keys for IEDs and equipment necessitates a dedicated key management infrastructure within the digital substation. Hence, such security mechanisms have not gained widespread use, yet.

4.4.3 False Data Injection

The most extensively researched type of cyber attack on power systems is the false data injection attack. An FDI attack operates under the assumption that attackers have access to the station control systems and RTUs in substations and/or the SCADA master in the control center. Consequently, they can inject falsified SCADA measurements, maliciously introducing correlated and consistent power flow measurements into State Estimation (SE), aiming to mislead system operators. Nowadays, SE is an integral tool in the energy management system for contingency analysis, security-constrained optimal power flow, and pricing calculation algorithms. The critical nature of SE highlights the importance of making it accurate and secure for power system operation. However, as discussed above, the SCADA system is vulnerable to FDI attacks. In [45], Liu et al. introduced a class of FDI attacks that can perturb the estimated states without being detected by the safeguard scheme within the SE process. The interesting part of such attack is that the adversary is assumed to have the knowledge of the targeted power system including the power network topology and parameters, and thus can exploit such knowledge to systematically generate multiple FDIs on power flow measurements [46]. It has been illustrated that such FDI attacks can bring potential economic damages by manipulating the nodal price of market operations [47] or even physical impact such as a line overload [48]. The FDI attack may seem difficult to conduct as the adversary needs to be equipped with enough knowledge of the target power system and vast attack resources to manipulate multiple measurement data channels. However, the complexity and functionalities of malware in recent cyber incidents on industrial control systems provide credible means to realize the FDI attack [49]. Notably, in addition to FDI on state estimation, recent research also considers attack scenarios where other critical applications, e.g., automatic generation control, are targeted [50]. In addition, studies on power system vulnerability analysis have been carried out to explore how FDI attacks can achieve the desired targets with incomplete system knowledge or very few attack resources, using both static and dynamic (time-variant) FDI strategies [51], [52]. Detection and mitigation techniques at the physical layer of the power system are proposed in [53], [54] based on both model-based and data-driven detectors from control-theoretic domains or machine learning areas.

4.4.4 Replay Attack

A replay attack is a variant of the man-in-the-middle attack where attackers record communication traffic and replay it to mimic legitimate entities. Pidikiti et al. investigated replay attacks on the SCADA system exploiting IEC 101 and IEC 104 protocols in [55]. These SCADA protocols were originally created without cyber security considerations. Nevertheless, these protocols do implement a packet checksum mechanism to prevent replay attacks to a certain extent. However, the size of the checksum is small and limited by the packet frame size and bandwidth. This condition leads to unreliable checksums to ensure data integrity. Therefore, this vulnerability can be exploited to launch replay attacks on SCADA systems. On the other hand, replay attacks in IT systems are more common and usually prevented by using authentication and secure session mechanisms. For example, a countermeasure to replay attacks was proposed using Kerberos authentication protocol [56]. This protocol would force the network hosts to authenticate themselves. After a successful authentication, a secure session is established between hosts. Such a session is typically valid only for a limited period of time preventing the reuse of session information. However, adoption of such prevention mechanisms in OT systems is challenging. For example, in IEC 101 and IEC 104, the limited packet frame size makes it difficult to add more data to improve protocol security. In addition to the aforementioned authentication mechanisms at the cyber layer, research efforts have also been undertaken to study the replay attack from the perspective of the physical power system layer. Such research is focused on detection methods to secure the control process of the SCADA system in power grids [57]. However, it is to be mentioned, there could still exist sufficient conditions under which plausible replay attacks may remain stealthy irrespective of the detection mechanism used. This is applicable even to a control-theoretic approach wherein the attacker has access to all the necessary data channels and executes the replay attack at a suitable time [58].

4.4.5 Session Hijacking

Communication sessions are interactive information exchanges between two or more networked devices for a limited time duration. Typical session establishment is initiated through authentication between hosts via secure protocols. Therefore, a session hijacking attack aims to bypass these protocols, allowing adversaries to circumvent authentication mechanisms and gain unauthorized access to legitimate communications. Kleinmann et al. presented a study on session hijacking in SCADA systems by exploiting Modbus protocol [59]. Modbus was originally designed only for serial communications between field devices in substations. To improve its flexibility, it was later upgraded to implement TCP. This modification allowed Modbus to work on Ethernet connections using IP addresses providing more data faster. The session establishment in Transmission Control Protocol / Internet Protocol (TCP/IP) works based on a three-way handshake mechanism. However, TCP/IP is widely known to be susceptible to cyber attacks including session hijacking [60] and thereby compromising Modbus as well. Besides session hijacking at the protocol level, hijacking can also be conducted through web applications or Human Machine Interfaces (HMIs) of SCADA systems. A successful session hijacking attack allows adversaries to assume the identity of the compromised devices / users and provides unauthorized access and control of the OT system. Burgers et al. presented a session hijacking case study and mitigation techniques for SCADA [61]. This research focuses on session hijacking via web-based applications, which use login authentication for session establishment.

4.5 Denial-of-Service Attacks

Denial-of-Service is a cyber attack with the objective of preventing legitimate access for users / networked devices to specific system resources such as network connections, computing capabilities, and application services. The term distributed denial-of-service refers to a coordinated DoS attack originating from multiple, distributed sources to increase attack severity and prevent tracking and identification of attackers' origin. A single DoS attack can be mitigated by blocking the sole attack source. Conversely, for a DDoS attack, blocking all attack sources is challenging, making its mitigation difficult. DoS attacks can further be classified into bandwidth depletion and resource depletion attacks [62]. The bandwidth depletion DoS attack aims to overload the bandwidth capacity of a target communication network. This can be achieved by either directly flooding the communication channel with bogus traffic or via third parties, which send multiple legitimate requests at the same time in an amplification attack. As a consequence, in either instance, legitimate communication traffic is affected, which significantly reduces the overall network performance. The resource depletion attack aims to overwhelm the target's resource usage, e.g., computing resources of a targeted host, by exploiting protocols and known response mechanisms. For example, as previously mentioned, TCP/IP implements a three-way handshake mechanism, allowing two hosts to initiate communication with a preliminary request and response mechanism. Adversaries may exploit this mechanism by sending a multitude of malicious requests to the targeted host. Consequently, the targeted host is kept busy responding to all malicious requests, leading to the disruption of a proper response to legitimate ones.

DoS attacks can target SCADA systems of power grids. Studies about SCADA susceptibility to DoS attacks are reported in [63], [64]. Petrovic et al. demonstrated DoS attacks on SCADA systems using OPNET communication network simulator [63]. The attacks significantly reduced SCADA network throughput and processing capabilities, directly affecting power system monitoring and control. Similarly, Kalluri et al. demonstrated a DoS attack exploiting IEC 104 protocol used in substations, affecting the processing and communication capabilities of RTUs [64]. Carcano et al. demonstrated a resource exhaustion attack targeting IEC 62351 [65], highlighting its cyber security shortcomings. In summary, the DoS attack is a potential threat against data availability in power grids, as it prevents successful communication of measurements and controls. Attackers can either jam the SCADA communication channels or compromise field devices and prevent them from communicating data. They may also attack the routing protocols or flood the network with bogus traffic [66]. DoS attacks on power systems may be modelled to analytically study the impact of data absence on power system monitoring and control. By properly designing DoS attack sequences, attackers can corrupt the normal operation of controllers and consequently impact power system stability [67], [68]. Mitigation techniques are discussed in [69].

4.6 Host-based Attacks

A host-based attack as the name suggests is an attack targeting various hosts in IT-OT systems, such as SCADA servers and HMIs, databases, application servers, station control systems, RTUs, protection relays, and merging units. In this section, we classify host-based attacks into three categories, i.e., software-based, database, and unauthorised access and control attacks.

4.6.1 Software-based Attacks

Software-based attacks on power grids exploit vulnerabilities present in software used in IT-OT systems such as SCADA and energy management systems. Usually, the software applications and security controls in OT systems inherit the same vulnerabilities present in regular IT systems. The main issue is that software and security controls of such IT systems may be patched, and their vulnerabilities may be mitigated more often than in OT systems. It is more difficult to update the OT systems of critical infrastructures as this process can affect the normal operation of physical facilities. A disruption of service such as electricity supply to customers may result in regulatory penalties and financial loss. Furthermore, extensive commissioning is needed after each update process that prolongs the voluntary outage for maintenance.

Most SCADA system solutions provided by vendors were developed before the emergence of cyber security concerns [70]. Software vulnerabilities in SCADA systems can be classified into three categories, i.e., improper input validation, software or source code, and resources control vulnerabilities [71]. As a result of input validation vulnerabilities, SCADA software is susceptible to modification attacks such as data injection and buffer overflow. SCADA source codes have also been found to contain improper security mechanisms and vulnerabilities such as the null pointer dereference vulnerability [72]. Resources control vulnerabilities are strongly related to software updates and patches. Corporate IT security typically pushes software updates and operating system patches over the IT network. However, SCADA software updates and patching in control centers and substations are more difficult to implement. This is due to the blend of state-of-the-art and legacy end devices, in addition to continuous operational requirements of the SCADA system in production.

In August 2020, nineteen software vulnerabilities were exposed by JSOF, an Israeli cyber security company. These vulnerabilities, dubbed Ripple20, affected ICS devices using the proprietary Treck TCP/IP stack software libraries. Two of the most severe vulnerabilities are related to TCP/IP tunneled packet fragmentation [73] and DNS packet decompression mechanisms [74]. The Treck software library has widely been adopted in IoT networked devices by several vendors across a whole range of industries including manufacturing, healthcare, and power grids. It is a cause for serious concern, as shown in [74], that a specific payload injection could remotely turn off an UPS device. Therefore, we can infer that Ripple20 is a real-world example of challenges pertaining to updates and security of software in industrial control systems, further complicated by global supply chains.

4.6.2 Database Attacks

A database is an essential element of the SCADA system as it stores real-time information from substations along with user access credentials. Zhu et al. categorize a database attack as an important cyber attack vector targeting SCADA systems [75]. Most common databases work based on SQL. Thus, one of the popular attacks targeting databases is SQL injection. This attack exploits input handling of the database system. When a database cannot correctly parse and handle inputs, it may lead to database access violations and illegitimate manipulation. In the worst-case scenario, with the breached confidential database information, adversaries can gain unauthorized control of the SCADA master. Consequently, databases have proven to be an important attack element in real-world cyber attacks on power grids. For example, in Ukraine 2015 attack, adversaries gained access to the control center using stolen credentials from the Windows active directory database [74]. AD is one of the most critical applications since early 2000 as it offers flexibility and interoperability of service authentication and authorization. However, a breach in security measures of AD can lead to a breach of the entire system since AD serves as the central authentication and authorization point. There are many publicly available tools to exploit AD security. For example, Mimikatz can be used to exploit AD hashes and Kerberos ticketing mechanism. Nonetheless, there are counter measures to prevent cyber attacks targeting AD. One of the options is the application of Microsoft Credential Guard. Credential Guard is a virtualization-based isolation technology for Local Security Authority Subsystem Service (LSASS) which prevents attackers from stealing credentials and prevents hash attacks. Another option is the implementation of tiered (multi-level) administrator models. The tiered admin model can prevent attackers from gaining top level privileges in an AD. Another common practice to prevent AD breaches is to implement secure credential policies. For example, a user has to change passwords periodically and use strong combination of characters. Multi-level or two factor authentication mechanisms through mobile phone messages and emails can also be applied to increase the overall system access security.

4.6.3 Unauthorised Access and Control

Access authorization typically uses an authentication mechanism applied to secure hosts, software, and web services. Unauthorized access occurs when an adversary gains access to the system without legitimate credentials. Hence, unauthorized access and control can be achieved if attackers circumvent the authentication mechanisms. There are many techniques to achieve this objective such as credential theft using a keylogger, database breaches, brute force attacks, and buffer overflows. It is also possible to gain unauthorized access using penetration testing tools such as Metasploit. This exploits system vulnerabilities by injecting malicious payloads on the target system. The most basic form of unauthorized access is achieved through the guest (non-administrator) mode. However, in this mode attackers' options are limited. Thereby, to increase attack severity, attackers can perform privilege escalation and become administrators allowing them complete control over the compromised system. SCADA systems typically employ Windows-based operating systems. However, Windows is vulnerable to unauthorized access attacks. Thus, Windows operating systems in IT-OT systems must be regularly updated and protected with firewalls and antiviruses. Researchers have also proposed solutions to prevent unauthorized access in SCADA systems. Taylor et al. proposed a SCADA authentication technique using a custom key distribution mechanism [76] applicable to DNP3 protocol, to prevent unauthorized access and control. Similarly, Vaidya et al. proposed an authentication and authorization for substation level communications [77]. This method implements multi-level authentication and uses public key certificates to authenticate and authorize access to the substation automation system. Other approaches to prevent and reduce the risk of unauthorized access and control include measures such as securing the host operating systems and implementing security perimeters and IDPS.

5. Impact of Cyber Attacks on Power Grids

Cyber attacks on power grids are considered high impact, low frequency disturbances with a wide range of effects. These could include, but are not limited to, equipment damages, loss of load, and power system instability. In the worst case, sophisticated cyber attacks may also cause system-wide cascading failures, leading to a blackout. Hence, this section discusses the various potential impacts of cyber attacks on power grids, ranging from component to system level. Table 7 summarizes the known cyber attacks on power grids and their impact. Four of the attacks shown in Table 7 are real, except the Aurora attack. The Aurora project was an experimental cyber attack that led to the physical destruction of a 2 MW synchronous generator. This was mainly done as a demonstration to raise awareness about cyber security and associated threats. The significant cyber attack on power grids, so far, is the Ukraine 2015 attack. It has been confirmed that this attack directly led to a power outage, affecting over a quarter-million customers for a duration of over six hours. Besides the real-world examples of cyber attacks on power grids, research has also been carried out to investigate the potential impacts of cyber attacks on power system operation [78]-[80]. Such empirical studies discuss various cyber attack scenarios and associated effects. A doomsday scenario would entail a cyber induced cascading failure culminating in a complete blackout. Hence, the subsequent subsection firstly provides an overview of the cascading failure mechanism, followed by various cyber attack scenarios and their impact analysis, as reported in the literature.

Table 7. Summary of known cyber attacks on power grids and their impact

No.	Attack	Year	Category	Impact

1	Malware infection of SCADA system, Europe [3]	2003	Service disruption	Three days loss of management functions in distribution substations
2	Aurora experimental cyber attack, USA [81]	2007	Physical damage	Physical damage to 2 MW synchronous generator
3	Power plant malware infection, USA [3]	2012	Service disruption	3-weeks restart delay of power plant
4	Cyber attack on power grid, Ukraine [9]	2015	Service disruption	Power outage affecting 225,000 customers for 6 hours
5	Cyber attack on power grid, Ukraine [17]	2016	Service disruption	Power outage in distribution network, 200 MW unsupplied load

5.1 Overview of the Cascading Failure Mechanism

Any major power system blackout is preceded by the phenomenon of cascading failures. A cascading failure, as the name suggests, is a successive failure of power system elements that can lead to a complete system collapse, i.e., a blackout. Most cascading failures are initiated by one or a set of multiple related events. These can include line flashovers, protection maloperation, human error, etc. Historically, most of these events tend to be caused by a combination of equipment failures, e.g., ageing equipment, environmental conditions, and human factors. Depending on the operating state of the system and severity of the initiating events, the entire power system may enter an emergency state. Without proper control actions or remedial measures, the system is highly vulnerable to further cascading effects. In such a case, various outcomes are possible. One such outcome, commonly observed in historical blackouts such as Italy 2003 and USA 2003 [82] is as follows. Due to the initial set of events, overloading of parallel transmission lines occurs, to account for power redistribution. Eventually, these lines are also overloaded beyond their limits and start tripping, initiating a cascading process of transmission line disconnections. After a certain time, the effect of these outages is felt on system dynamics. Transient instability can occur in a matter of a few seconds due to the large disturbances. Generators may lose synchronism due to sudden loss of transmission lines. This will also affect system voltages, causing major voltage drops. Consequently, in the case of heavy system loading, voltage stability problems may also arise. An inability to meet growing reactive power demands can eventually result in a voltage collapse. If left unchecked, such dynamic phenomena can result in islanding, i.e., formation of smaller clusters in the system with a mismatch of supply and demand. Ultimately, the power system reaches a so-called point of no return [83]. From this point onwards, the entire cascading process is rapid, involving loss of multiple generator units and loads. This domino effect is uncontrollable, culminating in a blackout. It is worth mentioning here that such a sequence of events is based on historical cascading failures and blackouts, involving physical system events. In case of a well targeted and coordinated cyber attack, the effects can be severely magnified. As shown in [84], [85] cyber attacks targeting bulk power systems may initiate cascading failures. A sophisticated cyber attack can target multiple substations, disconnecting many lines and tampering with control setpoints. As a result, power system instability and associated phenomena discussed above may be induced much faster. Consequently, in comparison to previous blackouts, the point of no return may be reached much sooner in case of cyber attacks.

5.2 Impact Analysis

As previously mentioned, the physical impact of cyber attacks on power grids is wide-ranging. There are many empirical studies reported in literature, covering these impacts. The most reported consequence of a cyber attack on power grid infrastructure is equipment damage. The Aurora experiment is a good real-world example of such possible effects. The attack demonstrated how rapid opening and closing of a generator’s circuit breaker cause an out of phase reconnection and permanent equipment damage. Along similar lines, [85] extensively discusses switching attacks on generators. This work clearly highlights how sophisticated cyber attacks can not only disconnect generators and cause equipment damages, but also initiate cascading failures. By applying a fast, switching attack on a generator’s main circuit breaker, transient instability can be induced, destabilizing the entire power grid in a matter of a few seconds. Other possible impacts include damage to equipment such Flexible Alternating Current Transmission System (FACTS) devices and On-Load Tap Changers (OLTCs) through setpoint modification [86], [87]. These devices are critical in ensuring voltage stability, and such equipment damage can trickle down and affect the entire power system. Loss of load is another commonly reported result of cyber attacks on power grids. If a cyber attack affects the system frequency, automatic measures such as load shedding are undertaken to preserve system integrity. Additionally, switching or data modification attacks can directly lead to loss of load [88]. The worst possible outcome, however, is that of cyber induced cascading failures and a blackout. As discussed in [84], a cyber attack on multiple substations in any power system may lead to a blackout. Cyber attacks targeting specific grid components or equipment can impact power system stability. For example, targeting voltage control mechanisms such as Static VAR Compensators (SVCs) and Static Synchronous Compensators (STATCOMs) can severely affect voltage stability. By carrying out data modification or MITM attacks, as stated in [86], [87] reactive power compensation is severely affected. As a result, voltages throughout the system can be influenced. Sustained under voltages can lead to emergency load shedding, and in the worst case, a voltage collapse. As part of a coordinated effort, such attacks can induce system-wide cascading failures and even a blackout.

6. Study Case and Simulation Results

This section discusses a study case, involving an example of a digital substation and spoofing of the IEC 61850 communication traffic. The layout of a digital substation and its communication network based on IEC 61850 is shown in Figure 5. It comprises of the station, bay, and process levels. In this work, our focus is on the bay level where the process bus interconnects IEDs and relays, enabling power system automation and protection applications. Typical communication networks in digital substations employ a fiber ring at the bay level. Additionally, IEC 61850 implements a publisher-subscriber communication mechanism for GOOSE and SV messages. In this context, the status and trip signals are communicated as multicast GOOSE messages via the process bus between various IEDs at the bay level, as represented in Figure 5. As discussed in Section 4.4.2, since IEC 61850 traffic is not encrypted, it is susceptible to spoofing and MITM attacks. This forms the basis for the discussed study case and simulation results.

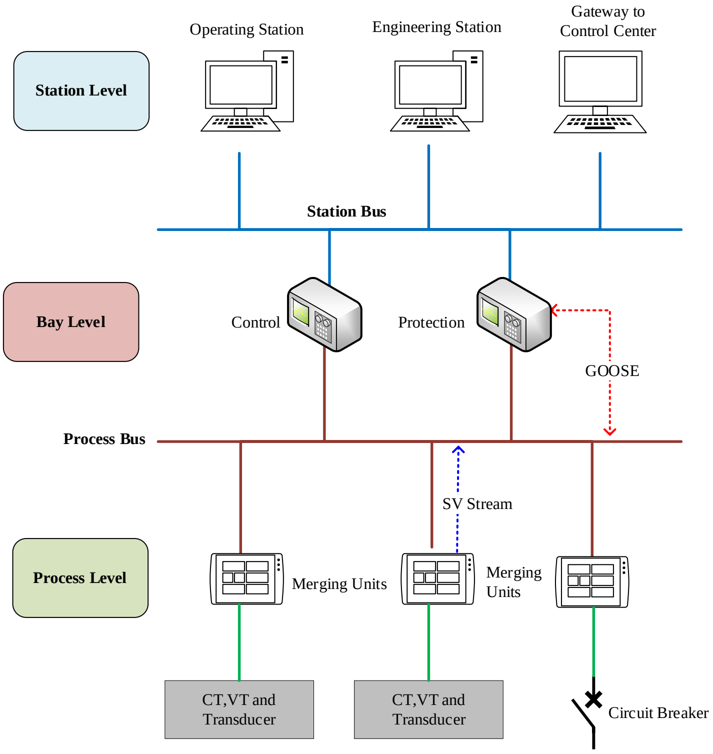


Fig. 5. Layout of communication architecture in a digital substation

6.1 Attack Scenario

The test system under study is the IEEE-39 bus transmission system. The system comprises of twenty-seven user-defined substations. The digital substation under consideration consists of three IEDs, protecting the bays for three high-voltage lines. In the attack scenario, an adversary has gained access to the substation communication network via malicious means such as phishing and malware, as outlined in Section 4. With unauthorized access to the IEC 61850 traffic within the digital substation, the adversary conducts network reconnaissance and sends crafted GOOSE packets to the target relays. Due to the correct nature of the spoofed packets, the relays open their associated circuit breakers, leading to a sudden *N-3* contingency. This occurs at simulation time *t*. Under normal circumstances, the system operator would quickly take cognizance of the situation and corrective actions would be applied, i.e., the circuit breakers will be closed. However, in this attack scenario, in addition to the GOOSE spoofing, attackers also launch a DoS attack on the utility's OT system. This hinders timely corrective actions as commands sent from the control center do not reach the substation on time. Consequently, system stability is jeopardized, initiating cascading failures and culminating with an extensive power outage. The exact sequence of events and impact of the cyber attack are discussed in the following subsection.

6.2 Simulation Results

The aforementioned cyber attack results in the malicious disconnection of lines 05-06, 04-05, and 05-08, along with a DoS attack that restricts remedial actions by the system operator. Consequently, the prolonged cyber attack affects power system stability. Multiple lines are disconnected by distance relays operating on sustained under voltages and over currents. Such a phenomenon was also observed during the North American cascading failures and blackout in 2003. A critical line tripped due to incorrect operation of zone 3 distance protection aggravating the domino effect and leading to the spread of the cascading phenomenon, ultimately ending in a large-scale blackout [82]. An example of such a trip is shown through Figures 7b and 7d for line 08-09. As a result of multiple line disconnections, generators in the system are extremely stressed and operating close to their limits. Finally, in the absence of remedial actions, generator G3 is tripped by its interface protection due to a high Rate of Change of Frequency (ROCOF) condition, well exceeding the ROCOF setting of 2 Hz/s, as seen in Figure 7a. A similar condition leads to the loss of generator G2. Now, due to the loss of generation, system frequency starts plummeting and emergency load shedding is activated to preserve system integrity. Ultimately, the cyber attack leads to a partial blackout with 10 busbars being de-energized and a loss of load amounting to 772 MW. The entire power system after the cyber attack is shown in Figure 6. The area that suffers a power outage is indicated along with the two generators lost and loads left unsupplied. The cascading failure sequence is summarized in Table 8.

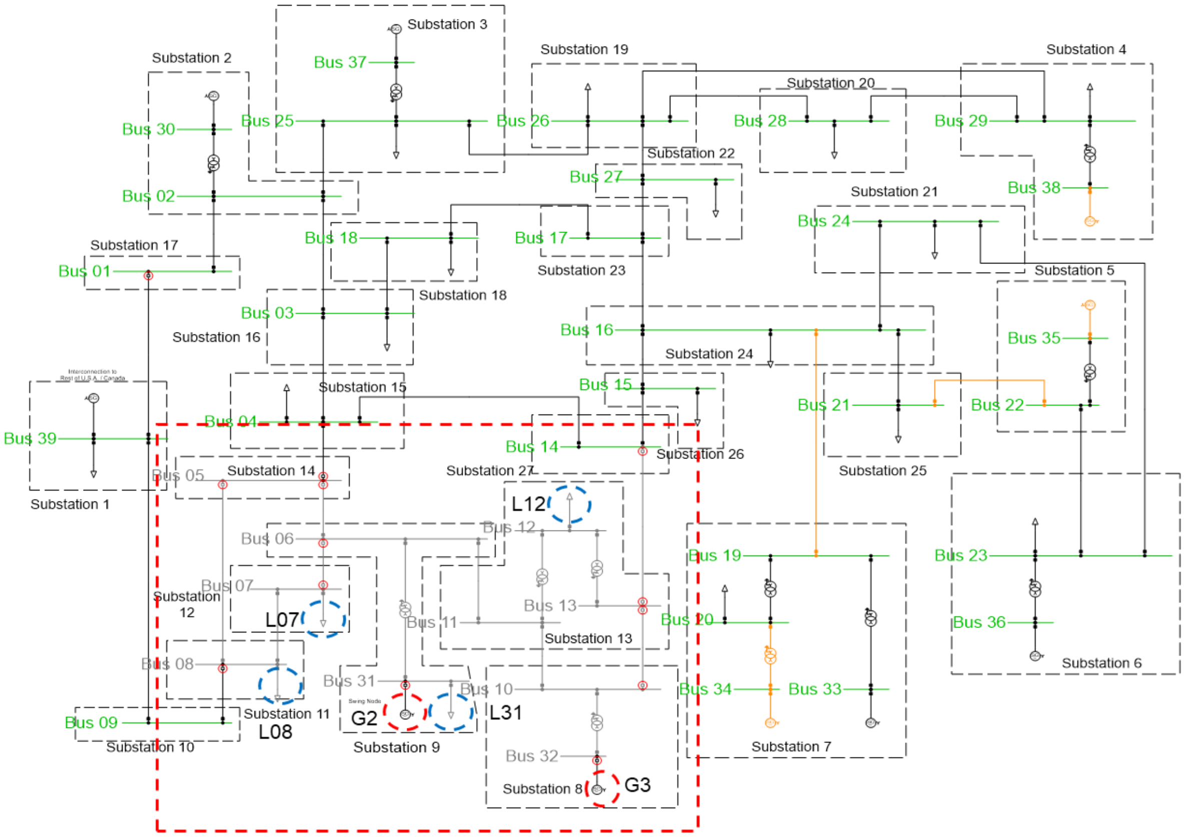
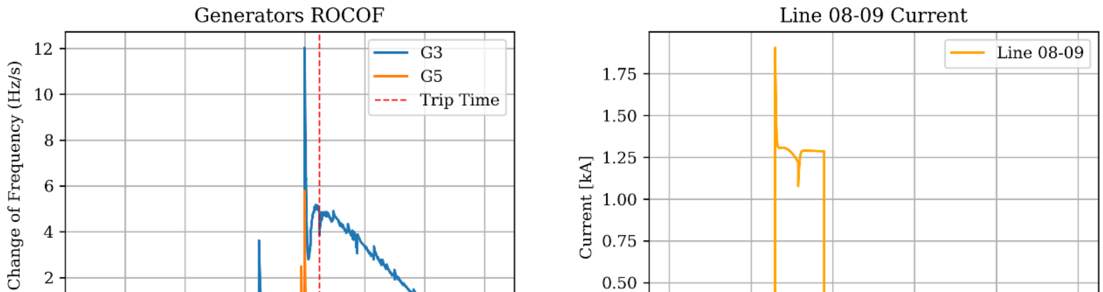


Fig. 6 Single line diagram of IEEE-39 bus system after cyber attack

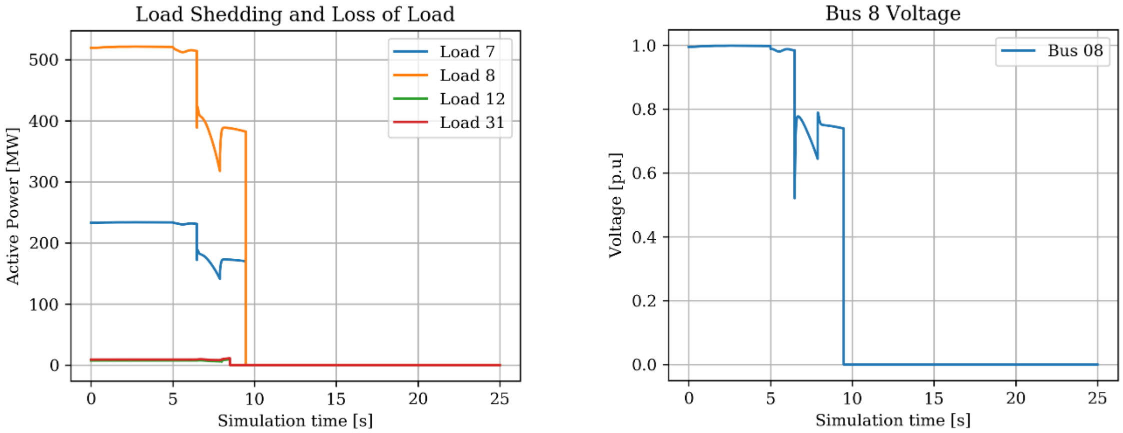
Table 8. Cascading failure sequence

No	Time [s]	Event
1	0s	Start of simulation.
2	5s	Cyber attack on substation 14. Lines 05-06, 04-05, and 05-08 maliciously disconnected.
3	6.477s	Distance relay trips line 06-07. Power grid is split into 2 isolated areas.
4	7.886 to 7.997s	Lines 10-13 and 13-14 in vicinity of attacked substation tripped by distance protection.
5	8.497s	Generators G3 and G2 tripped due to ROCOF interface protection and disconnected. System is now heavily stressed.
6	9.474s	Line 08-09 trips on distance protection. Two areas now left unsupplied.
7	12.073 to 12.548s	Underfrequency load shedding activated. All loads shed by 6.5%.
8	13.05 to 18.609s	System frequency is still below permissible limits. Underfrequency load shedding activated in steps of 5.9% and 7%.
9	25s	System suffers a partial blackout with total loss of load amounting to 772 MW. End of simulation.



(a) Generator ROCOFs

(b) Line 08-09 current



(c) Load shedding and loss of load

(d) Bus 08 voltage

Fig. 7 Simulation results showing impact of a cyber induced cascading failures and partial blackout

7. Conclusion

Power grids are undergoing a fast-paced process of digitalization, opening up the energy system to everyone by means of ICTs. However, future grid digitalization will require careful considerations with regard to data privacy and cyber security. It is now well recognized that IT – OT systems are vulnerable to cyber attacks. Hence, cyber resilience requirements of the power grid are more critical than ever before. The complexity of cyber attacks on power systems is likely to increase. To improve the cyber resilience of power grids, it is needed to identify potential threats and IT-OT system vulnerabilities, classify and review major types of cyber attacks on power grids, analyze their impact on system operation and stability, and develop mitigation techniques. Hence, this chapter provided the state-of-the-art and essential knowledge of threats and cyber attacks on power systems. It reviewed major cyber attacks on power grids and industrial control systems and provided a detailed taxonomy of cyber attacks. The most common security controls implemented in power grids include antiviruses, firewalls, network segmentation, and intrusion detection systems. Worryingly, even these security control mechanisms may be outdated or insufficient. Consequently, cyber attacks on power grids exploiting various threat vectors can have a catastrophic impact on system operation. This chapter provided indicative simulation results of such a hypothetical cyber attack scenario. Results show that sophisticated attacks may not only cause loss of load, but also induce cascading failures resulting in a blackout. Therefore, the urgent need of the hour is to develop comprehensive defense, mitigation, and incident response techniques to enhance power grid cyber resilience.

Acknowledgement

This work was supported by the Designing Systems for Informed Resilience Engineering (DeSIRE) program of the 4TU Center for Resilience Engineering (4TU.RE) and the EU H2020 project, ERIGrid 2.0 with Grant

Agreement Number 870620. DeSIRE is funded by the 4TU-program High Tech for a Sustainable Future (HTSF). 4TU is the federation of the four technical universities in the Netherlands.

List of Acronyms

AD	Active Directory
AMI	Advanced Metering Infrastructure
APT	Advanced Persistent Threat
CNN	Convolutional Neural Network
C2	Command and Control
DBN	Deep Believe Network
DDoS	Distributed Denial of Service
DLL	Dynamic Link Library
DNP	Distributed Network Protocol
DoS	Denial of Service
DPI	Deep Packet Inspection
DSO	Distribution System Operator
ENTSO-E	European Network of Transmission System Operators for Electricity
FACTS	Flexible Alternating Current Transmission System
FDI	False Data Injection
GOOSE	Generic Object-Oriented Substation Event
GPS	Global Positioning System
HMAC	Hash-based Message Authentication Code
HMI	Human Machine Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICMP	Internet Control Message Protocol
ICS	Industrial Control System
ICT	Information and Communication Technology
IDPS	Intrusion Detection and Prevention System
IDS	Intrusion Detection System
IED	Intelligent Electronic Device
IoT	Internet of Things
IP	Internet Protocol
IT	Information Technology
LSASS	Local Security Authority Subsystem Service
LSTM	Long-Short Term Memory

MAC	Message Authentication Code
MITM	Man-in-the-Middle
NGF	Next-Generation Firewall
OLTC	On-Load Tap Changer
OPC UA	Open Platform Communication Unified Architecture
OSI	Open Systems Interconnection
OT	Operational Technology
PLC	Programmable Logic Controller
PMU	Phasor Measurement Unit
ROCOF	Rate of Change of Frequency
RPC	Remote Procedure Call
RSA	Rivest-Shamir-Adleman
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SE	State Estimation
SIS	Safety Instrument System
SMB	Server Message Block
SMTP	Simple Mail Transfer Protocol
SNTP	Simple Network Time Protocol
SQL	Structured Query Language
STATCOM	Static Synchronous Compensator
SV	Sampled Values
SVC	Static VAR Compensator
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security Protocol
UPS	Uninterruptible Power Supply
URL	Uniform Resource Locator
USB	Universal Serial Bus
VBA	Visual Basic Application
VPN	Virtual Private Network

References

[1] E. Hutchins, M. Cloppert, and R. Amin, “Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains,” *Lockheed Martin Corp. Tech Report,* pp. 1-14, 2011. Accessed: Jul.

7, 2023. [Online]. Available: https://lockheedmartin.com/ content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf

[2] B. Miller and D. C. Rowe, “A Survey of SCADA and Critical Infrastructure Incidents,” in Proc Int Conf on Research in Info Tech, Calgary, Canada, Oct 2012, pp. 51–56.

[3] M. Noguchi and H. Ueda, “An Analysis of the Actual Status of Recent Cyberattacks on Critical Infrastructures,” in NEC Tech Journal Spec Issue Cybersec, vol. 12, no. 2, pp. 19–24, Jan 2018.

[4] K. E. Hemsley and R. E. Fisher, “History of Industrial Control System Cyber Incidents,” Idaho Natl Lab (INL) Tech Report, USA, Dec 2018. Accessed: Jul. 7, 2023. [Online]. Available: https://www.osti.gov/biblio/1505628

[5] T. Daniela, "Communication Security in SCADA Pipeline Monitoring Systems," in Proc Int Conf on Networking in Edu and Research, Iasi, Romania, Aug 2011, pp. 1-5.

[6] T. M. Chen and S. Abu-Nimeh, "Lessons from Stuxnet," in Computer, vol. 44, no. 4, pp. 91-93, Apr 2011.

[7] N. Falliere, L. O. Murchu, and E. Chien, “W32. Stuxnet Dossier, Symantec Security Response, Version 1.4, February 2011,” in Symantec Sec Response, vol. 4, pp. 1–69, Feb 2011.

[8] R. Langner, "Stuxnet: Dissecting a Cyberwarfare Weapon," in IEEE Security and Privacy, vol. 9, no. 3, pp. 49-51, May 2011.

[9] R. Lee, M. Assante, and T. Conway, “Analysis of Cyber Attack on the Ukrainian Power Grid,” Electricity Information Sharing Center (E-ISAC) Tech Report, pp. 1-26, Mar 2016. Accessed: Jul. 20, 2023. [Online]. Available: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2016/05/20081514/E-ISAC_SANS_Ukraine_DUC_5.pdf

[10] D. E. Whitehead, K. Owens, D. Gammel and J. Smith, "Ukraine Cyber-Induced Power Outage: Analysis and Practical Mitigation Strategies," in Proc Int Conf for Protective Relay Engineers, Texas, USA, April 2017, pp. 1-8.

[11] A. Cherepanov and R. Lipovsky, “Blackenergy-What We Really Know About the Notorious Cyber Attacks,” in Proc Virus Bulletin Conf, Denver, USA, October 2016, pp. 1-8.

[12] S. Shrivastava, “BlackEnergy - Malware for Cyber-Physical Attacks,” iTrust Cent Res Cyber Sec Analysis Report, pp. 1-15, May 2016. Accessed: Jul. 10, 2023. [Online]. Available: https://itrust.sutd.edu.sg/wp-content/uploads/2016/10/itrust-analysis-blackenergy.pdf

[13] A. Cherepanov, “Win32/Industroyer: A New Threat for Industrial Control Systems,” ESET Tech Report, pp. 1-17, June 2017. Accessed: Jul. 10, 2023. [Online]. Available: https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf

[14] J. Henry and C. I. Systems, “Sandia ICS Security Capabilities to Investigate CRASHOVERRIDE,” Tech Report, USA, Apr 2018. Accessed: Jul. 10, 2023. [Online]. Available: https://www.osti.gov/servlets/purl/1575340

[15] J. Slowik, “Anatomy of an Attack: Detecting and Defeating CRASHOVERRIDE,” in Proc Virus Bulletin Conf, Montreal, Canada, Oct 2018, pp. 53–75.

[16] Dragos Inc., “CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations,” Tech Report, pp. 1–35, March 2017. Accessed: Jul. 15, 2023. [Online]. Available: https://www.dragos.com/wp-content/uploads/CrashOverride-01.pdf

[17] J. Slowik, “Crashoverride: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack,” Dragos Inc. Tech Report, pp. 1-16, August 2019. Accessed: Jul. 15, 2023. [Online]. Available: https://www.dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf

[18] Panda Security, “PandaLabs Annual Report 2017,” Tech Report, pp. 1–42, November 2017. Accessed: Jul. 13, 2023. [Online]. Available: https://www.pandasecurity.com/en/mediacenter/src/ uploads/2017/11/PandaLabs_Annual_Report_2017.pdf

[19] R. J. Turk, “Cyber Incidents Involving Control Systems,” Idaho Natl Lab (INL) Tech Report, USA, pp. 1–58, Oct 2005. Accessed: Jul. 20, 2023. [Online]. Available: https://www.osti.gov/biblio/911775

[20] R. Derbyshire, B. Green, D. Prince, A. Mauthe and D. Hutchison, "An Analysis of Cyber Security Attack Taxonomies," in Proc IEEE European Sympo on Sec and Privacy Workshops, London, UK, Apr 2018, pp. 153-161.

[21] McAfee Labs, “Global Energy Cyberattacks: ‘Night Dragon’ Version 1.4.,” McAfee Inc. White Paper, Feb 2011. Accessed: Jul. 13, 2023. [Online]. Available: https://www.mcafee.com/blogs/wp-content/uploads/2011/02/McAfee_NightDragon_wp_draft_to_customersv1-1.pdf

[22] R. M. Lee, M. J. Assante, and T. Conway, “German Steel Mill Cyber Attack,” ICS SANS Case Study Paper, pp. 1-15, December 2014. Accessed: Jul. 15, 2023. [Online]. Available:

https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/bltc79a41dbf7d1441e/607f235775873e466bcc539c/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf

[23] A. Di Pinto, Y. Dragoni, and A. Carcano, "TRITON: The First ICS Cyber Attack on Safety Instrument Systems. Understanding the Malware, its Communications and its OT Payload," in Proc Black Hat USA, Las Vegas, USA, Aug 2018, pp. 1-26

[24] P. Mueller and B. Yadegari, "The Stuxnet Worm," University of Arizona Tech Report, pp. 1–12, June 2012. Accessed: Jul. 11, 2023. [Online]. Available: https://www2.cs.arizona.edu/ ~collberg/Teaching/466-566/2012/Resources/presentations/topic9-final/report.pdf

[25] C. G. Blake Johnson, Dan Caban, Marina Krotofil, Dan Scali, Nathan Brubaker, "Attackers Deploy New ICS Attack Framework 'TRITON' and Cause Operational Disruption to Critical Infrastructure," FireEye Threat Research Blog, Dec 2017. Accessed: Jul. 20, 2023. [Online]. Available: https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html

[26] R. Amoah, S. Camtepe and E. Foo, "Securing DNP3 Broadcast Communications in SCADA Systems," in IEEE Trans Industrial Informatics, vol. 12, no. 4, pp. 1474-1485, Aug 2016.

[27] I. A. Ibrahim Diyeb, A. Saif, and N. A. Al-Shaibany, "Ethical Network Surveillance using Packet Sniffing Tools: A Comparative Study," in Int Journal Computer Net Info Sec, vol. 10, no. 7, pp. 12–22, Jul 2018.

[28] C. Valli et al., "Eavesdropping on the Smart Grid," in Proc Australian Digital Forensics Conf, Perth, Australia, Dec 2013, pp. 54–60.

[29] H. Yuan, Y. Xia, Y. Yuan, and H. Yang, "Resilient strategy design for cyber-physical system under active eavesdropping attack," in Journal of the Franklin Institute, vol. 358, no. 10, pp. 5281–5304, Jul. 2021.

[30] P. Kumar, Y. Lin, G. Bai, A. Paverd, J. S. Dong and A. Martin, "Smart Grid Metering Networks: A Survey on Security, Privacy and Open Research Issues," in IEEE Comm Surveys & Tutorials, vol. 21, no. 3, pp. 2886-2927, Feb 2019.

[31] Y. Fan, Z. Zhang, M. Trinkle, A. D. Dimitrovski, J. B. Song and H. Li, "A Cross-Layer Defense Mechanism Against GPS Spoofing Attacks on PMUs in Smart Grids," in IEEE Trans Smart Grid, vol. 6, no. 6, pp. 2659-2668, Nov 2015.

[32] A. Xue, F. Xu, J. Xu, J. H. Chow, S. Leng and T. Bi, "Online Pattern Recognition and Data Correction of PMU Data Under GPS Spoofing Attack," in Journal of Modern Power Sys and Clean Energy, vol. 8, no. 6, pp. 1240-1249, Nov 2020.

[33] P. Risbud, N. Gatsis and A. Taha, "Vulnerability Analysis of Smart Grids to GPS Spoofing," in IEEE Trans Smart Grid, vol. 10, no. 4, pp. 3535-3548, Jul 2019.

[34] B. Sterzbach, "GPS-based Clock Synchronization in a Mobile, Distributed Real-Time System," in Real-Time Syst, vol. 12, no. 1, pp. 63–75, Jan 1997.

[35] T. Bi, J. Guo, K. Xu, L. Zhang and Q. Yang, "The Impact of Time Synchronization Deviation on the Performance of Synchrophasor Measurements and Wide Area Damping Control," in IEEE Trans Smart Grid, vol. 8, no. 4, pp. 1545-1552, Jul 2017.

[36] F. Zhu, A. Youssef and W. Hamouda, "Detection Techniques for Data-Level Spoofing in GPS-Based Phasor Measurement Units," in Proc Int Conf on Sel Topics in Mob & Wireless Net, Cairo, Egypt, Jun 2016, pp. 1-8.

[37] M. Kabir-Querrec, S. Mocanu, J. Thiriet and E. Savary, "A Test Bed Dedicated to the Study of Vulnerabilities in IEC 61850 Power Utility Automation Networks," in Proc Int Conf on Emerging Tech and Factory Automation, Berlin, Germany, Nov 2016, pp. 1-4.

[38] J. G. Wright and S. D. Wolthusen, "Stealthy Injection Attacks Against IEC61850's GOOSE Messaging Service," in Proc IEEE PES Innovative Smart Grid Tech Conf Europe, Sarajevo, Bosnia, Jul 2018, pp. 1-6.

[39] M. El Hariri, T. A. Youssef, and O. A. Mohammed, "On the Implementation of the IEC 61850 Standard: Will Different Manufacturer Devices Behave Similarly Under Identical Conditions?" in Electronics, vol. 5, no. 4, May 2016.

[40] T. A. Youssef, M. El Hariri, N. Bugay and O. A. Mohammed, "IEC 61850: Technology Standards and Cyber-Threats," in Proc IEEE Int Conf on Environment and Elect Engg, Florence, Italy, Jun 2016, pp. 1–6.

[41] N. Kush, E. Ahmed, M. Branagan, and E. Foo, "Poisoned GOOSE: Exploiting the GOOSE Protocol," in Proc Australasian Info Sec Conf, Auckland, New Zealand, Jan 2014, pp. 17–22.

[42] V. S. Rajkumar, M. Tealane, A. Ştefanov, A. Presekal and P. Palensky, "Cyber Attacks on Power System Automation and Protection and Impact Analysis," in IEEE PES Innovative Smart Grid Tech Conf Europe, The Hague, Netherlands, 2020, pp. 247-254.

[43] J. Hong, C. Liu and M. Govindarasu, "Integrated Anomaly Detection for Cyber Security of the Substations," in IEEE Trans Smart Grid, vol. 5, no. 4, pp. 1643-1653, Jul 2014.

[44] A. Elgargouri, R. Virrankoski and M. Elmusrati, "IEC 61850 Based Smart Grid Security," in Proc IEEE Int Conf on Industrial Tech, Seville, Spain, Jun 2015, pp. 2461-2465.

[45] Y. Liu, P. Ning, and M. K. Reiter, “False Data Injection Attacks Against State Estimation in Electric Power Grids,” in ACM Trans Info Syst Sec vol. 14, no. 1, pp. 1-33, Nov 2009.

[46] K. Pan, A. Teixeira, M. Cvetkovic and P. Palensky, "Cyber Risk Analysis of Combined Data Attacks Against Power System State Estimation," in IEEE Trans Smart Grid, vol. 10, no. 3, pp. 3044-3056, May 2019.

[47] L. Jia, J. Kim, R. J. Thomas and L. Tong, "Impact of Data Quality on Real-Time Locational Marginal Price," in IEEE Trans Power Systems, vol. 29, no. 2, pp. 627-636, Mar 2014.

[48] J. Liang, L. Sankar and O. Kosut, "Vulnerability Analysis and Consequences of False Data Injection Attack on Power System State Estimation," in IEEE Trans Power Systems, vol. 31, no. 5, pp. 3864-3872, Sep 2016.

[49] G. Liang, S. R. Weller, J. Zhao, F. Luo and Z. Y. Dong, "The 2015 Ukraine Blackout: Implications for False Data Injection Attacks," in IEEE Trans Power Systems, vol. 32, no. 4, pp. 3317-3318, Jul 2017.

[50] A. Ashok, Pengyuan Wang, M. Brown and M. Govindarasu, "Experimental Evaluation of Cyber Attacks on Automatic Generation Control Using a CPS Security Testbed," Proc IEEE PES GM, Denver, USA, Oct 2015, pp. 1-5.

[51] H. T. Reda, A. Anwar and A. Mahmood, “Comprehensive survey and taxonomies of false injection attacks in smart grid: attack models, targets, and impacts,” in. Renew. Sustain. Energy Rev., vol. 163, no. 112423, pp. 1-24, Jul. 2022.

[52] S. Sridhar and M. Govindarasu, "Model-Based Attack Detection and Mitigation for Automatic Generation Control," in IEEE Trans Smart Grid, vol. 5, no. 2, pp. 580-591, Mar 2014.

[53] K. Pan, P. Palensky and P. M. Esfahani, "From Static to Dynamic Anomaly Detection with Application to Power System Cyber Security," in IEEE Trans Power Systems, vol. 35, no. 2, pp. 1584-1596, Mar 2020.

[54] J. J. Q. Yu, Y. Hou and V. O. K. Li, "Online False Data Injection Attack Detection with Wavelet Transform and Deep Neural Networks," in IEEE Trans Industrial Informatics, vol. 14, no. 7, pp. 3271-3280, Jul 2018.

[55] D. S. Pidikiti, R. Kalluri, R. K. S. Kumar, and B. S. Bindhumadhava, “SCADA Communication Protocols: Vulnerabilities, Attacks and Possible Mitigations,” in CSI Trans ICT, vol. 1, no. 2, pp. 135–141, Apr 2013.

[56] G. Dua, N. Gautam, D. Sharma, and A. Arora, “Replay Attack Prevention in Kerberos Authentication Protocol using Triple Password,” in Int Journal of Computer Net & Comm (IJCNC), vol. 5, no. 2, pp. 1-12, Mar 2013.

[57] A. Hoehn and Ping Zhang, "Detection of Replay Attacks in Cyber-Physical Systems," in Proc American Control Conf, Boston, USA, Jul 2016, pp. 290-295.

[58] Y. Mo and B. Sinopoli, "Secure Control Against Replay Attacks," in Proc Int Conf on Comm, Control, and Computing, Monticello, USA, Oct 2009, pp. 911-918.

[59] A. Kleinmann, O. Amichay, A. Wool, D. Tenenbaum, O. Bar, and L. Lev, “Stealthy Deception Attacks Against SCADA Systems,” in Comp Sec, pp. 93–109, Dec 2017.

[60] M. De Vivo, G. O. De Vivo, R. Koeneke, and G. Isern, “Internet Vulnerabilities Related to TCP/IP and T/TCP,” in ACM SIGCOMM Comp. Comm. Rev., vol. 29, no. 1, pp. 81–85, Jan 1999.

[61] W. Burgers, R. Verdult, and M. Van Eekelen, “Prevent Session Hijacking by Binding the Session to the Cryptographic Network Credentials,” in Riis Nielson H., Gollmann D. (eds) Secure IT Systems. NordSec. Lecture Notes in Comp Sci, vol 8208. Springer, Berlin, Heidelberg., Oct 2013, pp. 33–50.

[62] S. M. Specht and R. B. Lee, “Distributed Denial of Service: Taxonomies of Attacks, Tools, and Countermeasures,” in Proc Int Conf Parallel and Distributed Comp Systems, San Francisco, USA, Sep 2004, pp. 543-550.

[63] J. D. Markovic-Petrovic and M. D. Stojanovic, "Analysis of SCADA System Vulnerabilities to DDoS Attacks," in Proc Int Conf on Telecom in Modern Satellite, Cable and Broadcasting Services, Nis, Serbia, Oct 2013, pp. 591-594.

[64] R. Kalluri, L. Mahendra, R. K. S. Kumar and G. L. G. Prasad, "Simulation and Impact Analysis of Denial-of-Service Attacks on Power SCADA," in Proc Nat Power Sys Conf, Bhubaneswar, India, Sep 2016, pp. 1-5.

[65] A. Carcano, A. Di Pinto, Y. Dragoni, and A. Carcano, “The Future of Securing Intelligent Electronic Devices Using the IEC 62351-7 Standard for Monitoring,” in Proc Black Hat USA, Las Vegas, USA, Aug 2019, pp. 1-21.

[66] A. Y. Lu and G. H. Yang, “Switched Projected Gradient Descent Algorithms for Secure State Estimation Under Sparse Sensor Attacks,” in Automatica, vol. 103, no. 1, pp. 503–514, Mar 2019.

[67] S. Vijayshankar, et al., "Assessing the impact of cybersecurity attacks on energy systems," in Applied Energy, vol. 345, no. 121297, pp. 1-12, Sept. 2023.

[68] K. Pan, J. Dong, E. Rakhshani, and P. Palensky, "Effects of Cyber Attacks on AC and High-Voltage DC Interconnected Power Systems with Emulated Inertia," in Energies, vol. 13, no. 21, p. 5584, Oct 2020.

[69] L. Schenato, "To Zero or to Hold Control Inputs With Lossy Links?," in IEEE Trans Auto Control, vol. 54, no. 5, pp. 1093-1099, May 2009.

[70] D. Ranathunga, M. Roughan, H. Nguyen, P. Kernick and N. Falkner, "Case Studies of SCADA Firewall Configurations and the Implications for Best Practices," in IEEE Trans Network and Service Mgmt, vol. 13, no. 4, pp. 871-884, Dec 2016.

[71] D. Upadhyay and S. Sampalli, "SCADA (Supervisory Control and Data Acquisition) Systems: Vulnerability Assessment and Security Recommendations," in Computers & Security, vol. 89, no. 101666, Feb 2020.

[72] Department of Homeland Security Office of Cybersecurity and Communication, "NCCIC/ICS-CERT FY 2015 Annual Vulnerability Coordination Report," pp. 1-14, 2015. Accessed: Jul. 15, 2023. [Online]. Available: https://us-cert.cisa.gov/sites/default/files/Annual_Reports/NCCIC_ICS-CERT_FY%202015_Annual_ Vulnerability_Coordination_Report_S508C.pdf

[73] M. Kol and S. Oberman, "CVE-2020-11896 RCE and CVE-2020-11898 Info Leak," JSOF Inc. White Paper, pp. 1-27, June 2020. Accessed: Jul. 5, 2023. [Online]. Available: https://www.jsof-tech.com/wp-content/uploads/2020/06/JSOF_Ripple20_Technical_Whitepaper_June20.pdf

[74] M. Kol, A. Schon, and S. Oberman, "CVE-2020-11901," JSOF Inc. White Paper, pp. 1-23, Aug 2020. Accessed: Jul. 5, 2023. [Online]. Available: https://www.jsof-tech.com/wp-content/uploads/2020/06/JSOF_Ripple20_Technical_Whitepaper_June20.pdf

[75] B. Zhu, A. Joseph and S. Sastry, "A Taxonomy of Cyber Attacks on SCADA Systems," in Proc Int Conf on IoT, Cyber, Phys and Social Comp, Dalian, China, Oct 2011, pp. 380-388.

[76] C. R. Taylor, C. A. Shue and N. R. Paul, "A deployable SCADA Authentication Technique for Modern Power Grids," in Proc IEEE Int Energy Conf, Cavtat, Croatia, May 2014, pp. 696-702.

[77] B. Vaidya, D. Makrakis and H. T. Mouftah, "Authentication and Authorization Mechanisms for Substation Automation in Smart Grid Network," in IEEE Network, vol. 27, no. 1, pp. 5-11, Feb 2013.

[78] R. Liu, C. Vellaithurai, S. S. Biswas, T. T. Gamage and A. K. Srivastava, "Analyzing the Cyber-Physical Impact of Cyber Events on the Power Grid," in IEEE Trans Smart Grid, vol. 6, no. 5, pp. 2444-2453, Sep 2015.

[79] G. Raman, B. AlShebli, M. Waniek, T. Rahwan, and J. C. H. Peng, "How Weaponizing Disinformation Can Bring Down A City's Power Grid," in PLoS One, vol. 15, no. 8, pp. 1–14, Aug 2020.

[80] C. C. Sun, A. Hahn, and C. C. Liu, "Cyber Security Of A Power Grid: State-of-the-Art," in Int. J. Electr. Power Energy Syst., vol. 99, pp. 45–56, Jan 2018.

[81] D. Salmon, M. Zeller, A. Guzman, V. Mynam, and M. Donolo, "Mitigating the Aurora Vulnerability with Existing Technology," in Proc Ann West Prot Relay Conf, Washington, USA, Oct 2009, pp. 1–7.

[82] G. Andersson et al., "Causes of the 2003 Major Grid Blackouts in North America and Europe, and Recommended Means to Improve System Dynamic Performance," in IEEE Trans Power Sys, vol. 20, no. 4, pp. 1922-1928, Nov 2005.

[83] P. Pourbeik, P. S. Kundur, and C. W. Taylor, "The Anatomy of a Power Grid Blackout - Root Causes and Dynamics of Recent Major Blackouts," in IEEE Power Energy Mag, vol. 4, no. 5, pp. 22–29, Sep 2006.

[84] C. W. Ten, K. Yamashita, Z. Yang, A. V. Vasilakos, and A. Ginter, "Impact Assessment of Hypothesized Cyberattacks on Interconnected Bulk Power Systems," in IEEE Trans Smart Grid, vol. 9, no. 5, pp. 4405–4425, Sep 2018.

[85] S. Liu, B. Chen, T. Zourntos, D. Kundur, and K. Butler-Purry, "A Coordinated Multi-Switch Attack for Cascading Failures in Smart Grid," in IEEE Trans Smart Grid, vol. 5, no. 3, pp. 1183–1195, Apr 2014.

[86] B. Chen, S. Mashayekh, K. L. Butler-Purry and D. Kundur, "Impact of Cyber Attacks on Transient Stability of Smart Grids with Voltage Support Devices," in Proc IEEE PES GM, Vancouver, Canada, Jul 2013, pp. 1-5.

[87] B. Chen, K. L. Butler-Purry, S. Nuthalapati and D. Kundur, "Network Delay Caused by Cyber Attacks on SVC snd Its Impact on Transient Stability of Smart Grids," in Proc IEEE PES GM, National Harbor, USA, Jul 2014, pp. 1-5.

[88] A. Castillo, B. Arguello, G. Cruz and L. Swiler, "Cyber-Physical Emulation and Optimization of Worst-Case Cyber Attacks on the Power Grid," in Proc Resilience Week (RWS), San Antonio, USA, Nov 2019, pp. 14-18.