Cyber-Physical System Security of Distribution Systems

Liu, Chen-Ching; Bedoya, Juan C.; Sahani, Nitasha; Stefanov, Alexandru; Appiah-Kubi, Jennifer; Sun, Chih Che; Lee, Jin Young; Zhu, Ruoxi

DOI
10.1561/3100000026

Publication date
2021

Document Version
Final published version

Published in
Foundations and Trends in Electric Energy Systems

Foundations and Trends® in Electric Energy Systems

Cyber–Physical System Security of Distribution Systems

Suggested Citation: Chen-Ching Liu, Juan C. Bedoya, Nitasha Sahani, Alexandru Stefanov, Jennifer Appiah-Kubi, Chih-Che Sun, Jin Young Lee and Ruoxi Zhu (2021), "Cyber–Physical System Security of Distribution Systems", Foundations and Trends® in Electric Energy Systems: Vol. 4, No. 4, pp 346–410. DOI: 10.1561/3100000026.

Chen-Ching Liu
Virginia Tech

Juan C. Bedoya
Virginia Tech

Nitasha Sahani
Virginia Tech

Alexandru Stefanov
Delft University of Technology

Jennifer Appiah-Kubi
Virginia Tech

Chih-Che Sun
Washington State University

Jin Young Lee
Washington State University

Ruoxi Zhu
Virginia Tech

now
the essence of knowledge
Boston — Delft

Contents

Cyber–Physical System Security of Distribution Systems

Chen-Ching Liu[1], Juan C. Bedoya[1], Nitasha Sahani[1], Alexandru Stefanov[2], Jennifer Appiah-Kubi[1], Chih-Che Sun[3], Jin Young Lee[3] and Ruoxi Zhu[1]

[1] *Virginia Tech, USA; ccliu@vt.edu*
[2] *Delft University of Technology, Netherlands*
[3] *Washington State University, USA*

ABSTRACT

The Information and Communications Technology (ICT) for control and monitoring of power systems is a layer on top of the physical power system infrastructure. The cyber system and physical power system components form a tightly coupled Cyber–Physical System (CPS). Sources of vulnerabilities arise from the computing and communication systems of the cyber–power grid. Cyber intrusions targeting the power grid are serious threats to the reliability of electricity supply that is critical to society and the economy. In a typical Information Technology environment, numerous attack scenarios have shown how unauthorized users can access and manipulate protected information from a network domain. The need for cyber security has led to industry standards that power grids must meet to ensure that the monitoring, operation, and control functions are not disrupted by cyber intrusions. Cyber security technologies such as encryption and authentication have been deployed on the CPS. Intrusion or anomaly detection and mitigation

Chen-Ching Liu, Juan C. Bedoya, Nitasha Sahani, Alexandru Stefanov, Jennifer Appiah-Kubi, Chih-Che Sun, Jin Young Lee and Ruoxi Zhu (2021), "Cyber–Physical System Security of Distribution Systems", Foundations and Trends® in Electric Energy Systems: Vol. 4, No. 4, pp 346–410. DOI: 10.1561/3100000026.

tools developed for power grids are emerging. This survey paper provides the basic concepts of cyber vulnerabilities of distribution systems and CPS security. The important ICT subjects for distribution systems covered in this paper include Supervisory Control And Data Acquisition, Distributed Energy Resources, including renewable energy and smart meters.

1

Introduction

Threats of cyberattacks targeting the electric power grid have been increasing in recent years (SANS, 2016; Clavel *et al.*, 2015). The consequence of cyber incidents on the power grid includes equipment damage, cascading events, large-scale power outages, and disruption of market functions (Cheng *et al.*, 2017; Sridhar *et al.*, 2012; Spolar, 2012). Government and industry have made a significant effort to strengthen the protection of the power infrastructure against cyber threats by setting standards and guidelines (e.g., Smith, 2014; Khalifa *et al.*, 2011; Sun *et al.*, 2016; Sun *et al.*, 2018; NIST, 2010; NIST, 2014).

- Critical Infrastructure Protection, Presidential Directive PDD-63, 1998.
- Cyber Security Roadmap for Energy Delivery Systems, Department of Energy (DOE), 2011.
- Guidelines for Smart Grid Cyber Security, National Institute of Standards and Technology (NIST) Report 7628.
- Critical Infrastructure Protection (CIP) Standards, Cyber Security CIP 002-014, North American Electric Reliability Corporation (NERC).

- National Electric Sector Cybersecurity Organization Resource (NESCOR), Electric Power Research Institute (EPRI).
- European Programme for Critical Infrastructure Protection (EPCIP) resulting from the European Commission's directive EU COM (2006).

As power systems become more complex and dependent on the Information and Communications Technology (ICT), the cyber system and physical system are highly connected and, therefore, the threat of cyberattacks on the power grid also increases. Intruders seeking to cause damages to the grid can compromise the communication systems to launch an attack on the power grid.

In December 2015, the power grid in Ukraine experienced a cyberattack by hackers (Ahern, 2017; Liang *et al.*, 2017). The damage caused by the sophisticated attack was a power outage affecting about 225,000 customers for about 6 h. The hacker implemented malware using a phishing email to obtain the VPN credential. From this attack, the hacker launched remote control actions through the control center computers. Denial of Service (DoS) attacks jammed phone reports of the outage to the call center. Furthermore, the data destruction software, KillDisk, was used to erase the reboot software in the workstation, causing a delay in power system restoration. Further observations can be made concerning the Ukraine attack scenario: (1) First, the hackers were knowledgeable about the operation of the targeted grid, (2) the hackers were able to manipulate the cyber–power system (CPS) from the Distribution System Operator (DSO) control center, and (3) the hackers had knowledge of critical control and operation devices. The in-depth information was obtained by penetrating the Supervisory Control And Data Acquisition (SCADA) system and staying undetected for at least 6 months. After observing for 6 months, the hackers gained sufficient knowledge about the operation and critical information of the power system. With the information garnered, the hacker(s) conducted an attack through the SCADA system to operate circuit breakers in the substations, causing a power outage.

As demonstrated by the real-world cyberattack, it is critical to fully understand the vulnerabilities of the CPS to develop the capabilities for

detecting cyber intrusions and take timely mitigation actions. Although cyber intrusions can be launched by compromising control center computers, damages could also be caused by man-in-the-middle attacks on the communication system between the control center and field devices. Therefore, the defense of the communication system is a critical issue for power systems.

Cyber security issues arise when power system components are provided with remote monitoring and control capabilities over public communication infrastructures. Remote monitoring and control for power grids have been the industry practice. This would not be a problem if the utility communication networks are private and isolated from the Internet. The problem is that the utility private communication networks, Operational Technology (OT) systems, for substation and control center communications may be connected with the general Information Technology (IT) systems used for other purposes (Nazir *et al.*, 2017) such as electricity trading, and these IT systems are in turn connected to the Internet. While there are firewalls between IT and OT systems, the firewalls may have vulnerabilities. Furthermore, some distribution system operators use public communication networks for their distribution networks (Nazir *et al.*, 2017) such as 3G/4G/5G for the pole-mounted devices. They also communicate with the control centers.

Development of the Smart Grid in recent years by large-scale deployment of ICT leads to fast-increasing connectivity of devices and systems in the power grid. Smart grid development in the United States is primarily concerned with Phasor Measurement Units (PMUs) for the transmission system as well as remote control switches and voltage/var control devices in the distribution systems. The remote monitoring and control capabilities are also created for millions of smart meters at the customer locations and DERs, including renewable energy, energy storage, and responsive load. Indeed, Advanced Metering Infrastructure (AMI) has been installed for communication and control between the utility company and numerous smart meters. As a result of the DERs, the architecture of the power grid is rapidly evolving from a centralized utility service to a distributed or decentralized structure (Liu *et al.*, 2016b). For example, Hawaii reached 23% of

renewable electricity while California has 26% renewable (Sgouras *et al.*, 2017; Finster and Baumgart, 2015) and targets a 50% level by 2030. Deployment of DERs is often conducted by nonutility parties and, therefore, the utility system may not have full control of the devices. AMI also brings new communication and control features through smart meters. As a result, additional risks emerge due to a large number of devices and noncontrollable access points (Liu *et al.*, 2016a; INL, 2007; INL, 2008; Rohde, 2005).

This survey paper is intended to serve as a module in senior-level undergraduate as well as graduate courses in power engineering. The objective of this paper, therefore, is to provide fundamental concepts of cyber security for the distribution system as a CPS. To meet the objective, vulnerabilities of cyber intrusions and mitigation strategies are discussed. The remaining sections are organized as follows. The evolution of the ICT for the power grid, sources of vulnerabilities, and cyber security measures are presented in Section 2. Sections 3 and 4 describe the ICT in the power system environment. Section 5 focuses on the cybersecurity issues of a distribution system, while Section 6 discusses smart grid communication standards and protocols. In Section 7 detection of cyber intrusions in distribution systems is considered. Mitigation strategies are provided in Section 8. Simulation cases based on the CPS model are presented in Section 9, and the paper is concluded in Section 10.

2

Power Grid Vulnerabilities and Security Measures

2.1 Age of information technology

Low-cost computer peripherals help to create an Internet-based computer communication environment. Deployment of the new ICT improves system performance, interoperability, and reliability. However, cyber security issues also arise from the fast-increasing connectivity. The CPS technology brings:

- standardized communication protocols,
- widely adopted technologies with known vulnerabilities,
- connectivity of control systems to other networks,
- use of existing security technologies and practice,
- insecure remote connections, and
- widespread availability of information about control systems.

Security flaws and malicious activities (hackers/worms) can damage cyber and physical components of the distribution system. Significant efforts are required to identify and isolate malicious actions and secure the CPC. A cyberattack taxonomy is shown in Figure 2.1.

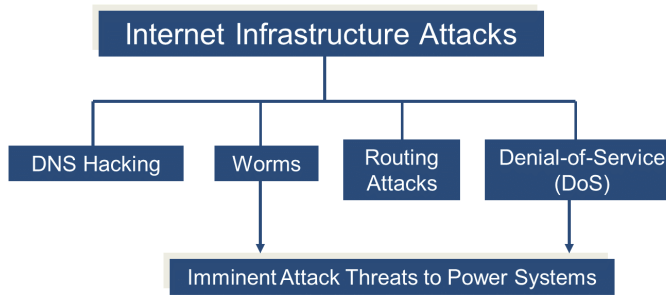

Figure 2.1: Cyber attack taxonomy.

2.2 Typical power grid vulnerabilities and mitigation actions

In DoS, an attacker aims to deny authorized users access to the target system. One way to do this is to flood the target system (for instance, SCADA communication system) with a large number of requests so as to consume server resources and make the system unresponsive to genuine instructions. Viruses/Worms are malware that install themselves in cyber components of the power system and infect critical system components to cause abnormal behaviors. Usually, these packets are injected by hackers who initiate packet sniffing using the same network as the system operator. Hackers may also maliciously modify or inject packets into the network by accessing corporate firewalls. Software bugs can be exploited to gain (unauthorized) access to control center networks and SCADA systems. Additional sources of vulnerabilities are unauthorized access points from which it is possible to send false information through the SCADA system. Disgruntled employees are also a potential source of vulnerability. Finally, there is a risk in power system control software using publicly available documentation.

The NERC Critical Infrastructure Protection (CIP) standards, CIP-002 through 014 (NERC, 2006), among others, propose the following mitigation practice to overcome CPS vulnerabilities:

- Define cyber security policies for all organizations.
- Identify critical cyber assets to safeguard.

- Demarcate an electronic security perimeter.
- Implement electronic access control mechanisms.
- Monitor electronic access periodically.
- Define electronic incident response actions.
- Develop a secure password management system and periodically modifications.
- Review authorization and access rights periodically.
- Disable unauthorized, invalidated, expired or unused computer accounts.
- Disable unused network ports and services.
- Secure dial-up connections, install, and manage firewall applications.
- Setup intrusion detection/prevention systems (IDS/IPS).
- Enable auto-updates and patch management.
- Install and keep up to date on antivirus software.
- Retain and review operator logs, application logs, and IDS logs.
- Track computer system vulnerabilities and effective responses.
- Install secure VPN connections.
- Separate corporate and control networks as much as possible.

3

ICT in Cyber-transmissions Systems

3.1 ICT model of power systems

Power generation resources are connected to numerous consumers through transmission and distribution networks. The ICT system enables real-time monitoring and control of the power system (Sun *et al.*, 2018).

Figure 3.1 shows the communication systems and devices at the transmission level of power system operation. A transmission system operator coordinates the operation of a number of power systems, each with its own control center. Substations are connected to the control center of the power system through the SCADA system, which enables data acquisition and remote control.

3.2 Substation automation system (SAS)

Monitoring and control at the substation level depends on communication and computation systems. The architecture of an IEC 61850 (Clavel *et al.*, 2015) based SAS is shown in Figure 3.2. Data and measurements are collected by CT and PT and transmitted to the

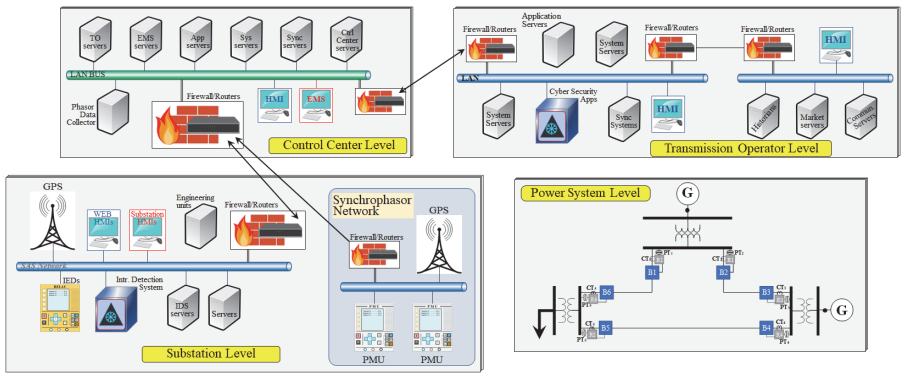

Figure 3.1: ICT model at the transmission system level.

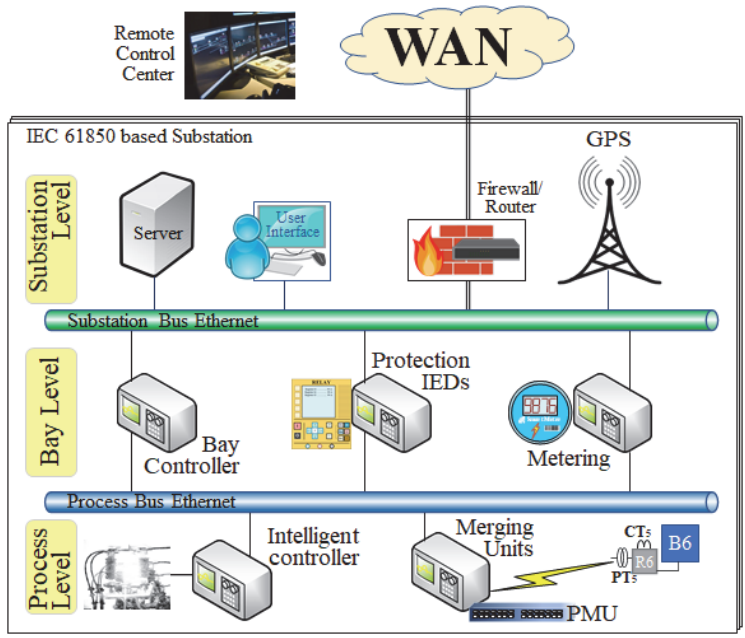

Figure 3.2: Architecture of an IEC 61850 based substation.

control center through SCADA facilities at the substation. Remote control commands from the control center are delivered to the physical devices through Intelligent Electronic Devices (IEDs). The automation system has several advantages:

(1) *Installation cost reduction*: IEDs at a substation are connected through a Local Area Network (LAN) using Ethernet-based interaction. Traditional copper-based communication networks are replaced by new technology, e.g., optical fibers, that offer reduced latency. Lower cost is achieved by the integration of massive data, measurements, and control commands in a single line for communication.

(2) *IED interoperability*: All devices based on IEC 61850, such as substation IEDs, are provided with import/export capabilities (Substation Configuration Language – SCL). SCL is represented in files that contain from/to interconnection information and are transmitted via ICT to the master server. Smart devices are designed with auto-configuration features that allow integration of IEDs from different vendors within the same substation.

(3) *Impact reduction of topology changes*: Engineers at a substation can connect IEDs into the Substation Automation System (SAS). Components of the ICT can be used to send SCL files to field IEDs and update the configuration information.

Modern substations at the transmission level are remotely controlled. System operators use different technologies to access the Substation Communication Network (SCN). Figure 3.2 presents a typical SCN architecture. The mechanism used by system operators to access the SCN can also be used by attackers to gain access to substation information and control.

Attackers explore different tactics (e.g., cracking the password) to access an SCN. Once access is granted, critical data is exposed (e.g., measurements, topology, maintenance records, historian data, and circuit breaker status). Furthermore, attackers are able to send control commands (e.g., opening circuit breakers). Once access is

granted, attackers can log on to multiple substation networks if the communication system is vulnerable. A worst-case cyberattack scenario leading to catastrophic outages may be caused by an attacker triggering a sequence of cascading events on the power grid.

4

ICT in Cyber-distribution Systems

4.1 Supervisory control and data acquisition (SCADA)

SCADA systems have been widely deployed in various industries, e.g., oil/gas, water, and power, for online monitoring and control. For power systems, SCADA is utilized for collecting measurements (e.g., voltage, current) and sending control commands from a control center to switching devices at substations. The Wide Area Network (WAN) is used as the communication system for the SCADA. In a control center or substations, the devices communicate with each other and access data through the LAN. At the remote sites, Programmable Logic Controllers (PLCs) or Remote Terminal Units (RTUs) are the functional devices for remote monitoring and control. However, PLCs are deployed for local control, whereas RTUs are used for wide area telemetry. Analytical software tools in an Energy Management System (EMS) or Distribution Management System (DMS) use the measurements to estimate the system states and the operators take appropriate actions based on the operating conditions. As shown in Figure 4.1, major components of a SCADA system are communication system (LAN/WAN), software systems (e.g., EMS/DMS), sensors (CT/PT), HMI, protective devices (relays), and control devices (circuit breakers) (Stouffer *et al.*, 2011).

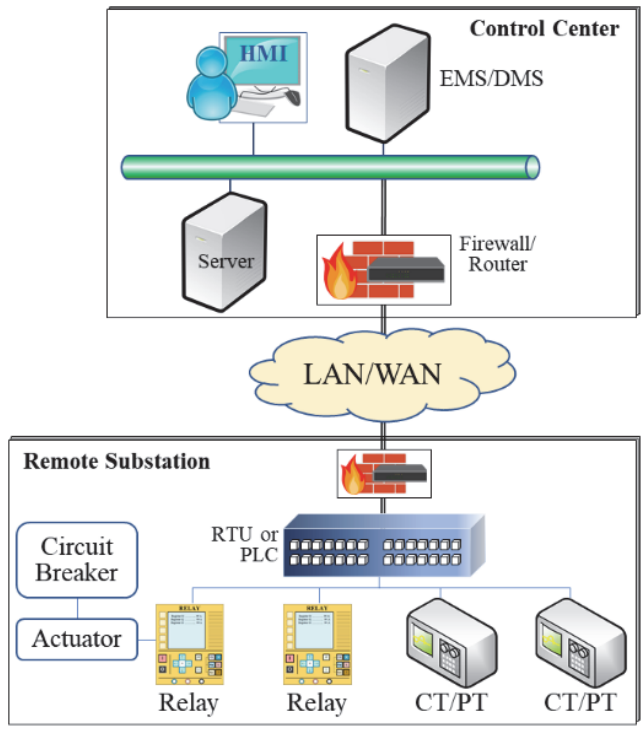

Figure 4.1: Major components of a SCADA system.

4.2 Advanced metering infrastructure (AMI)

With recent advancements in smart meter technology, AMI is used to collect power consumption data at customers' locations. Unlike the Automatic Meter Reading (AMR) system, AMI provides high rates for data exchange and is equipped with duplexed modules for communication in order to send/receive measurements and control commands (e.g., connect or disconnect service) (Fischer *et al.*, 2000).

Conventional meters were used to keep track of users' power usage and must be read on site by meter readers. Smart meters, however, provide new capabilities to record energy flow *in* and *out* (Rashed Mohassel *et al.*, 2014) (when consumers produce surplus energy from roof-top solar panels or wind). Recent applications using energy storage capabilities from plug-in hybrid electric vehicles (PHEVs), make it

possible to charge the battery when the electricity price is low and inject power back to the grid when the electricity price is high during peak hours (Liu *et al.*, 2016b). Typical components of a smart meter include current/voltage sensors, communication module, data storage, microprocessor, and RAM.

Vulnerabilities exist for smart meters and AMI. Since smart meters collect the users' electricity consumption data, cyber attackers may be able to steal electricity or gain access to users' private information (Liu *et al.*, 2012; Liu *et al.*, 2014; McLaughlin *et al.*, 2009). Also, smart meters send measurements to the control center every 5–60 min, depending upon configuration and network traffic (CENTRON, 2006). AMI communication network is characterized by users' devices, local data aggregators, and Meter Data Management Systems (MDMSs).

Figure 4.2 shows a typical communication system. IEEE 802.15.4 wireless communication protocols (IEEE, 2016) allow an extended communication distance between a local data aggregator and smart meters using point-to-multipoint configurations (CENTRON, 2006).

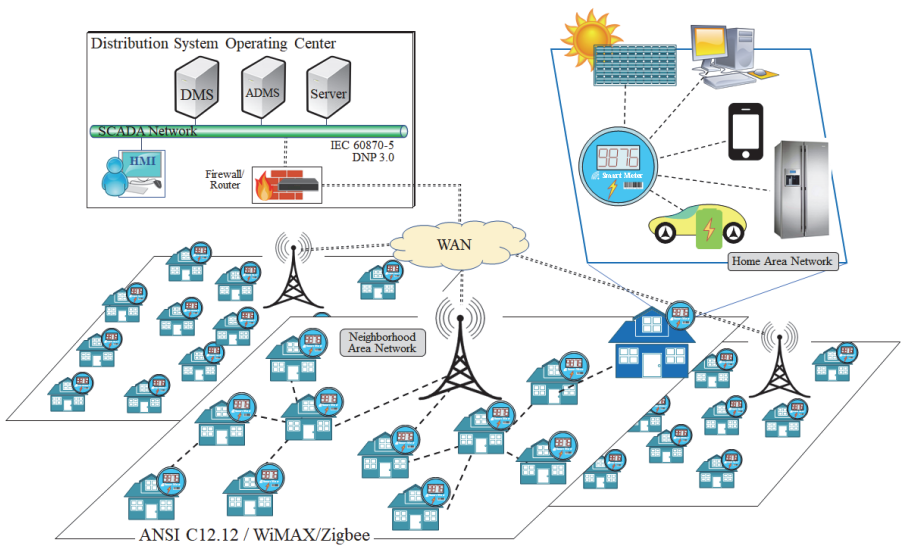

Figure 4.2: Architecture of an AMI system.

Finally, the deployment of AMI opens new opportunities for reliability improvement. Two examples are:

- Demand Response (DR): In the DR mechanism, peak load is reduced by shifting energy consumption from peak to off-peak hours. Peak shaving helps to prevent line overloading and avoid the need to invest in costly generation resources (PNNL, n.d.).
- Outage Management System (OMS): AMI automatically reports power outage events allowing the DSO to determine the outage areas if multiple devices reporting the outage condition. Compared to traditional trouble calls, AMI allows operators to respond faster and reduce the outage duration (Jiang *et al.*, 2016).

4.3 Distributed energy resources

The high penetration of solar PVs in distribution systems significantly changes the operation and control. Smart inverters with reactive power capability can support the voltage profile in distribution systems. Comparing with the traditional inverters, smart inverters with digital communication interface can provide remote-control capability in an online environment. In the electricity market (SGIP, 2014), DERs, include distributed generators, energy storage, renewable energy devices, and flexible load, are owned by utilities or third parties. In the third quarter of 2018, the installed solar energy has reached 60 GW in the United States (SEIA, 2018). To be connected through SCADA, smart inverters are equipped with a two-way communication interface. Smart inverters are critical devices for Voltage/VAR support and fault ride-through capabilities. However, these devices may not be secure because the consumers who own the devices may connect to unsecured network devices, e.g., a home Wi-Fi router. To manage a group of DERs in a utility, the facilities of DER energy management systems are deployed via WAN/LAN (Qi *et al.*, 2016).

As far as cyber security is concerned, the most critical devices in a DER network are smart inverters. Grid-tied renewable energy resources, such as wind turbines and PV panels, need a power inverter to change DC to AC and interface with a power grid. Smart inverters are monitored

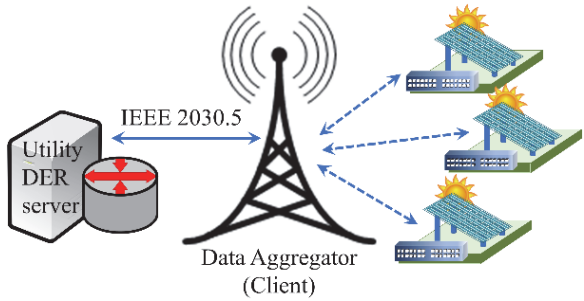

Figure 4.3: Communication structure of a DER system. System with carrier data aggregator.

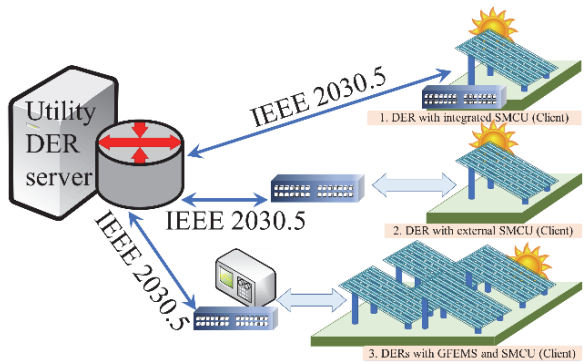

Figure 4.4: Communication structure of a DER system. Decentralized integration. DER with either GFEMS or SMCU.

and controlled via a communication system from a control center. To regulate interconnected DER devices, certain standards have been proposed. These are discussed in a later section. Among the standards, is Rule 21 (CPUC, 2015; CSIP, 2018), which was formulated by the Smart Inverter Working Group (SIWG). Communication configurations between a utility and remote devices in a DER system that are included in Rule 21 are shown in Figures 4.3 and 4.4.

5

Cyber Security of a Distribution System

Cyber intrusions are a serious threat to the reliable operation of a smart grid. From the energy section of the National Cybersecurity and Communications Integration Center (NCCIC) annual report (NCCIC, 2016), most of the reported cyberattacks target the IT system of utilities and vendors. According to the U.S. Department of Energy (DOE), the attempted cyberattack figures are higher than actually reported (USDoE, 2016). Thus, it is important to identify cyber vulnerabilities and develop the detection and mitigation strategies for potential cyber intrusions into a smart grid.

Regulatory and technical issues must be addressed to achieve a secure environment for a distribution system in transformation. The main challenges are: (1) fast evolving distribution systems; (2) vulnerabilities of communication systems and integration with new communication technologies; (3) trust from different active/passive interacting parties; (4) heterogeneous protocols/technologies; (5) proprietary systems; and (6) privacy of the participants.

Availability means that authorized parties should have privileges to access required data without compromising the system's security. *Confidentiality* refers to data disclosure to only authorized individuals

or systems. For instance, confidentiality should be maintained for metering data; privacy includes patterns of individual behaviors and can be used against customers at the meter locations, similarly for the pricing information which can be used to manipulate electricity markets. *Integrity* is the assurance that the accuracy and consistency of data are maintained without unauthorized modifications, destruction, or loss of data. *Authentication* is concerned with verifying that users' identity in the communication systems matches a valid user account.

5.1 Common cyberattacks in distribution system infrastructure

Cyber–physical threats exist in transmission systems, which depend on communication systems for monitoring and control. Similarly, distribution systems also have vulnerabilities associated with the cyber–distribution system infrastructure. Common threats and attack models at the distribution system level include:

- *Man in the Middle Attacks*: Unauthorized access to a communication channel that can be exploited to adversely alter the data from communication devices, compromising the availability and integrity of power system data (Appiah-Kubi and Liu, 2020; Choi *et al.*, 2020). They include false data injection and replay attacks:
    - *False Data Injection (FDI)*: FDI attacks result from injecting (corrupting) measurements or data, with the goal of triggering damaging control actions to the system. For example, falsified low voltage measurements from the substations may mislead system operators in a control center to take actions to raise the voltages, causing high voltages in the power system.
    - *Replay Attack*: A replay attack with a malicious intent is launched by intercepting the valid data packet and retransmitting it at a later time.
- *Rogue Devices*: Field devices that replace legitimate signals with falsified data. Vulnerability arises when an attacker gains physical access to field devices such as sensors and metering units

- *Denial of Service*: Compromising data availability by attempting to delay/block critical communication links, flooding them with falsified packets (Huseinović *et al.*, 2020). At the distribution system communication level, two main DoS attacks are described next:

- *Channel Jamming*: It is usually performed with "radio jammer" equipment that blocks wireless communication of the field physical devices.

- *Medium Access Control (MAC) DoS*: Attackers modify MAC layer parameters and pretend to be trustworthy sources. Once access is granted, data theft/modification, malware spread, parameter changes, can be performed. This cyberattack approach is also known as spoofing attack, which can be launched in different forms, such as email, website, and text messages.

5.2 Vulnerabilities in cyber infrastructures

Firewalls, as a front-line defense, are installed at the access point (router or gateway) to prevent unauthorized access. By parsing the properties of incoming traffic, i.e., time delay, IP address, and port numbers, firewalls are designed to filter unauthorized packets. However, the pre-defined rule set of commercial-grade firewalls can conflict in many cases (Chapman *et al.*, 2001; Hari *et al.*, 2000). It is challenging to develop accurate firewalls that satisfy all cyber assets for the authorized network. Furthermore, the proprietary software platform used by the power grid is usually inaccessible for the public, which complicates the rule setting for the firewalls. Identification approaches for anomalies in firewalls have been proposed (Hamed *et al.*, 2005; Al-Shaer and Hamed, 2004; Yuan *et al.*, 2006). To mitigate threats to a control system, the America National Standards Institute (ANSI)/International Society for Automation (ISA) proposes ANSI/ISA 62443-1-1 as a high-level security policy. However, firewalls cannot detect particular spoofed packets or malicious software that can bypass the rule set.

Integrity of data communication in a smart grid is critical. However, cryptographic protection mechanisms are not commonly deployed by

the power industry as cyber security was not a serious threat when these protocols were developed. Also, considering the communication latency, MODBUS, and Distributed Network Protocol 3.0 (DNP3) used in SCADA, DER, PMU, SAS systems (Modbus, 2006; Padilla *et al.*, 2014) have no cryptographic protection, which may cause security concerns. For example, DNP3 interfaces with WAN network, increasing the vulnerabilities as WAN is publicly accessible (Shahzad *et al.*, 2014). Therefore, MODBUS authentication frameworks have been proposed to secure the data communication (Phan, 2012; Hayes and El-Khatib, 2013). Also, Security Authentication (SA) in DNP3 has been proposed (Gilchrist, 2008; Amoah *et al.*, 2016; Song *et al.*, 2015).

SCADA, as a critical component of the cyber system in a distribution system, has security risks. Information exchange between LANs and WANs is vulnerable (Ericsson, 2007). In distribution systems, SCADA is a cyber system to support the DMS. It may also be integrated with smart grid subsystems, e.g., AMI, Distribution Automation (DA) and DERs. As a result, it is damaging if an adversary gains access to SCADA (Falliere *et al.*, 2011; Kushner, 2013; Ten *et al.*, 2008; Zhang *et al.*, 2016; Amanullah *et al.*, 2005; Li *et al.*, 2012).

The substation automation system plays an important role in power system operations. IEC 61850 introduces multiple multicast messages, i.e., Generic Object-Oriented Substation Event (GOOSE) and Sampled Values (SV) protocols, for various functions of substation automation. Unfortunately, cyber security mechanisms are not taken into account in the traditional design. Thus, data traffic inside a substation is vulnerable to false data injection attacks. The authentication proposed in IEC 62351 intends to protect IEC 61850 based communication protocols; however, multiple weaknesses have been exposed in the protocol's specification standard (Strobel *et al.*, 2016). One of the weaknesses is an intentional reset of the parameter "stNum," which is a counter that increases by one each time a package is sent. It is used in the GOOSE protocol to provide timestamps for packages that are received/sent. This parameter can be increased up to 2^{32} before it is reset to zero. Under normal conditions (i.e., 30 packages per second), it would take more than four years to reach the reset limit. However, the parameter can be reset when a single GOOSE package is delayed

for longer than the parameter, "timeAllowedToLive" (i.e., lifetime of the messages). This attack targeting GOOSE packets may trip circuit breakers maliciously (Hong *et al.*, 2014). If coordinated cyberattacks are launched to compromise critical substations, a cascading sequence of events may be triggered.

Other vulnerabilities are related to the network of advanced metering infrastructure. When these networks are deployed in multiple user wireless networks, they can be adversely accessed through various nodes. Meter data modification and unauthorized remote load control can be launched by intruders, causing economic losses. Cyberattacks targeting AMI include false data injection, leakage of the customer information, and energy theft (Namboodiri *et al.*, 2014; Liang *et al.*, 2013; Krebs, 2012; Rosenbaum, 2012).

5.3 Assessment of vulnerabilities

The most common assessment of distribution system vulnerabilities related with voltage, current, and other power measurements are related to Bad Data Detection Algorithms (BDDAs). Common BDDAs are based on power flow relation, state estimation, and most recently, artificial intelligence pattern recognition techniques that use historic data. BDDAs are included as part of the DMS that are used by the DSO for real-time operation purposes. The configuration of distribution

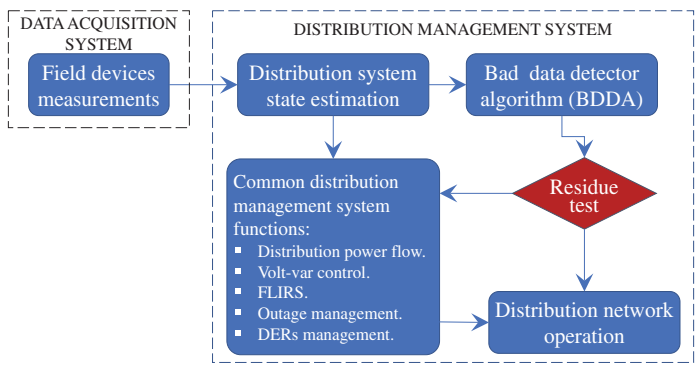

Figure 5.1: BDDA in distribution management systems.

state estimation-based (DSS-based) for bad data detection, as part of DMS modules, is shown in Figure 5.1.

Results of the power system states (voltage phasors at all nodes), estimated based on least squared errors, are evaluated in a residual test. Depending upon a pre-established threshold, bad data alarms can be triggered. System estimation results can also be used for other DMS functions such as volt-var control.

6

Smart Grid Communication and Cybersecurity Standards

Standard requirements and guidelines for data communication in power systems have been proposed (Bakken *et al.*, 2011). Several Standard Development Organizations, including International Electrotechnical Commission (IEC), Institute of Electrical and Electronics Engineers (IEEE), National Institute of Standards and Technology (NIST), and American National Standards Institute (ANSI), have developed standards to serve as guidelines for the smart grid.

Transmission system standards mainly concern SASs. Among SAS standards, IEC 61850 (Clavel *et al.*, 2015) set of standards is designed to meet the requirements of reliable communication. It includes Manufacturing Message Specification (MMS), GOOSE, and Sampled Measured Values (SMV). While the MMS standard addresses real-time data transmission, the GOOSE protocol offers a publisher–subscriber messaging system for substation devices. The SMV standard provides for the transmission of high-speed measured data points. The IEC 61850 standard, however, does not provide certain cybersecurity guarantees such as integrity, confidentiality, and authenticity. Therefore, the IEC 62351 standard is introduced to provide cybersecurity measure against

attacks (Hussain *et al.*, 2020). Other standards, recommendations, and guidelines to secure SAS network include:

- NERC: Critical Infrastructure Protection (CIP) standards, CIP-002 through 014, "provides a cyber security framework for the identification and protection of critical cyber assets to support reliable operation of the bulk electric system" (NERC, 2006).
- IEEE C37.111 (IEC 60255-24): Defines file format of measurement from IEDs.
- ESCSWG: "Roadmap to Achieve Energy Delivery System Cyber Security" is developed by Energy Sector Control Systems Working Group (ESCSWG) (USDoE, 2011).

Due to the diversity of the distribution system, distribution system standards tend to be more wide ranged. To regulate interconnected DER devices, the IEC TC Committee 57, WG 17 has released IEC 61850-90-7 providing specific object models for power converters in DER systems, while IEC 61850-7-420 provides abstract information models for general data exchange. The SIWG has updated Rule 21 to California Public Utilities Commission (CPUC) in 2014, providing a three-phase approach to regulate DER systems (CPUC, 2015). IEEE 2030.5, also known as Smart Energy Profile 2.0 (SEP 2), is suggested to be the default protocol that should be supported by three types of individual DER communication devices, including:

(1) Generating Facility Energy Management Systems (GFEMS), (2) data aggregators, and (3) Smart inverter Control Unit (SMCU). According to the latest implementation guide for smart inverters (CSIP, 2018), IEEE 2030.5 application layer protocol (IEEE, 2018) implements "A client/server model based on a Representational State Transfer architecture utilizing the core HTTP methods of GET, HEAD, PUT, POST, and DELETE". The IEEE 2030.5 profile supports smart inverter functionalities such as changing Volt-Var setpoints and regulating real power output.

The ANSI C12.18–C12.22 series provides a data object framework and an application layer protocol for smart meter communication (Barai *et al.*, 2015).

Table 6.1: Major standards for operating smart grids in distribution systems (Sun *et al.*, 2018).

Subsystem name	Standard	Applied system
SCADA	IEC 60870-6	Monitoring and control over a WAN
	IEEE 1815-2012 (DNP3)	Application layer protocol for SCADA communication
	DNP3 Secure Authentication	Address cybersecurity issues of DNP3 (authentication, integrity)
PMU	IEEE C37.118	Phasor data exchange
ICS	IEC 62443	Providing a framework to address the cybersecurity vulnerabilities of industrial control systems (ICSs)
Smart grid	NIST 7628	Guidelines for smart grid cyber security

Certain standards apply generically to SCADA systems and the smart grid in general. They are, therefore, applicable at both transmission and distribution levels. These are listed in Table 6.1.

7

Modeling and Detection of Cyber Intrusions

Firewalls serve as a first line of defense against intrusions. All traffic, both incoming and outgoing, is checked according to the set of rules. Anomalous events are subsequently flagged. This is the most prevalent type of firewalls. Other applications for cyber intrusion detection at the firewall level include Deep Packet Inspection (DPI) tools, which inspect the data being sent over a computer network and take action by blocking, re-routing, or logging it accordingly. However, DPIs are known to be slow and require complex validation rules and, therefore, they may not work for all application layer protocols.

Intrusion Detection Systems (IDSs) may be employed as an additional layer of security. IDSs detect intrusions in the network and flag them accordingly. Mitigation steps may then be implemented. An IDS may be classified according to the detection technique and style, method of decision-making, and source of the data used in intrusion detection. Table 7.1 highlights the types of classification. The following subsections discuss each type of classification.

Table 7.1: Structure of cyber protection systems (Sun *et al.*, 2018).

Detection technique	Source of intrusion data	Detection style	Method of decision making
Knowledge-based	Network-based	Passive	Centralized
Behavior-based	Host-based	Active	Decentralized

7.1 Source of data

An IDS may be installed to monitor and protect a network or host. Consequently, data for performing intrusion detection may be gathered from the network, or from the subject host. An IDS may therefore be network-based (Zhang *et al.*, 2011; Yang *et al.*, 2013; Hahn and Govindarasu, 2013), or host-based (Liu *et al.*, 2016b; Fan *et al.*, 2015; Mo *et al.*, 2014; Ten *et al.*, 2011; Wu *et al.*, 2014; Mitchell and Chen, 2013; McLaughlin *et al.*, 2013; Liu *et al.*, 2015; Berthier and Sanders, 2011). It may also be both network-based and host-based, in which case the IDS is referred to as an integrated or hybrid IDS (Hong *et al.*, 2014; Yang *et al.*, 2017; Premaratne *et al.*, 2010). An integrated IDS therefore leverages both cyber and physical properties of the system.

A Network-based IDS (NIDS) is configured to inspect network traffic. While it may look for indications such as frequency and intensity of network traffic as well as properties such as the port and IP addresses of packets, a NIDS may also perform a deep packet inspection, checking for malformed packet headers, or harmful payload, even at the application layer level.

On the other hand, a Host-based IDS (HIDS) is installed to monitor a specific device and is limited to that device. Hence, the data used in performing intrusion detection is collected from the subject device. The data may be readily available in the system logs. Information such as the frequency of system crash, usage of memory, temperature of device may be used in classifying an event as an attack.

7.2 Detection techniques

An IDS may use a whitelist approach or a blacklist approach toward intrusion detection. The knowledge-based (or signature-based) IDS makes use of a blacklist. In other words, there is a database of attack patterns, called signatures. By comparing traffic or host features to the defined signature, an event may be classified as an attack or not. A classic example is antimalware software. By virtue of this, the knowledge-based IDS is highly accurate in identifying attacks whose signatures have been uploaded in its database. However, it suffers a critical flaw of being unable to detect attacks not known in the database.

Using the whitelist approach (Barbosa *et al.*, 2013), network traffic or host parameters are compared to a preestablished normal profile and once a deviation from this is significant, an anomaly is flagged. Thus, this type of IDS is also called an Anomaly Detection System (ADS). Nevertheless, the exact definition of normal behavior for a network or host can be a difficult task. Examples of network activities that can be difficult to manage in whitelisting approaches are: (1) Software upgrading, (2) new application requirements, (3) unplanned servers' maintenance, (4) triggered even alerts, and (5) workstations and connection IPs identification. Thus, this type of IDS may be characterized by a high false positive ratio. The profile may be updated regularly to include new users or new observations about the system at normal operating conditions. Table 7.2 summarizes the types of IDS according to the detection technique.

Table 7.2: Major standards for operating smart grids in distribution systems.

Detection technique	Feature	Defects
Blacklist	Identify and block malicious traffic	Security offered is minimal Requires frequent update to rules High false negative ratio
Whitelist	Identify and pass benign traffic	Requires frequent update to rules High false positive ratio

7.3 Detection style

While some IDSs flag intrusions and delegate mitigation to the human operator, others may be configured to take mitigation actions on their own. The former is called passive IDS, while the latter is called active IDS, or Intrusion Detection and Prevention System (IDPS), or Intrusion Prevention System (IPS). IDPS reduce the impact of attacks in a shorter time.

An IDPS monitors network traffic searching for indications of potential attacks. When plausible dangerous activities are detected, actions to stop the attack that are taken, i.e., dropping malicious packets, blocking traffic, or reestablishing connections (Fawaz *et al.*, 2012). The network administrator can also receive alert signals from IDPS about potential malicious activities.

Network-based IDPS (NIPS) solutions can be installed at the firewall level. A host-based intrusion prevention system, i.e., HIPS, sits on an endpoint (user terminals), looking for malicious traffic at the host level. A wireless intrusion prevention system (WIPS) looks for unauthorized access to Wi-Fi networks. NIPS activities are similar to firewalls, but there are some differences. A firewall deals with all incoming traffic and allows it to pass through if some security criteria are met. NIPS looks at traffic that is already on the network and only blocks traffic that looks suspicious.

7.4 Method of decision-making

While an IDS may be a single system that detects and/or mitigates attacks, it may also comprise several autonomous software (called agents) which interact for the same purpose (Appiah-Kubi and Liu, 2020; Choi *et al.*, 2020; Moya and Wang, 2018). In the former, a centralized architecture is formed, whereas a decentralized technique is employed in the latter. In the centralized architecture, one detection system is installed at the point of interest to detect and/or mitigate attacks. This approach tends to suffer from single point of failures. In certain cases, there are several IDSs installed at different points within the network of interest and these report to a central system that

correlates alerts generated by the dispersed IDS to detect coordinated cyberattacks (Moya and Wang, 2018). In the case of the decentralized technique, several agents interact with one another, forming a multiagent system. In a multiagent system, a form of consensus protocol is typically employed for communication among agents. The multiagent approach may be deployed for collaborative detection (Choi *et al.*, 2020), or for collaborative correlation and mitigation (Appiah-Kubi and Liu, 2020).

7.5 Other categories of classification

Although an IDS may fit into one or several of the aforementioned broad categories, there are other categories into which it may fall. First, it may be data-driven. In data-driven techniques (Sapegin *et al.*, 2015), relevant operation data are collected from the system of interest. Data-driven techniques tend to be machine-learning-based or statistical (Sapegin *et al.*, 2015; Esmalifalak *et al.*, 2017). Machine-learning-based IDSs have become prevalent over the years, with supervised (Esmalifalak *et al.*, 2017; Khanna *et al.*, 2018), unsupervised (Karimipour *et al.*, 2019) and reinforcement learning techniques (Wei *et al.*, 2020) applied in different scenarios and for different purposes. In supervised learning, labeled data is used to train a neural network to identify features of interest. Unsupervised learning is mainly used for classification. Therefore, by nature, it is more suitable for anomaly detection (Karimipour *et al.*, 2019). In reinforcement learning, a reward scheme is used to incite the algorithm to learn optimal actions over a series of trial-and-error attempts. Reinforcement learning tends to be applied for mitigation purposes. An IDS may also be model-based; models of attack patterns (signature-based) or expected behavior (behavior-based) are created for intrusion detection. The model may be formed from data collected from the system of interest, in which case the IDS is also data-driven.

7.6 Attack modeling

Intrusion detection based on attack models is a hybrid signature- and model-based detection technique. An attack model is first formulated using attack signatures. The model may be in the form of attack trees

(Ten *et al.*, 2010), Bayesian graphs (Zhang *et al.*, 2015), Petri nets (Ten *et al.*, 2008), Markov decision processes (Chen *et al.*, 2018), among others. In the event that suspicious behavior is detected, the trajectory and next steps of the attacker may be predicted with some accuracy. Attack models provide guidance for both reactive and proactive mitigation.

8

Attack Mitigation in Distribution Systems

Mitigation is key to ensure reliability and security of the power grid, following a cyberattack. As already mentioned, an IDS alerts the operator in the event that an intrusion is detected. If the IDS is an active IDS, certain mitigation steps may be implemented. Considering that the smart grid is a CPS, mitigation steps may be taken at both the cyber and physical levels. The essence of cyber level mitigation may be to identify the attackers, disconnect them, and take back control of the power grid. At the physical level, mitigation is aimed at steering the power grid to a normal operating condition.

At the cyber level, the response taxonomy in Fawaz *et al.* (2012) is useful. Cyber mitigation strategies are grouped into learning actions and modifying actions. Learning mitigation actions could be active, such as tracing connections and starting analysis tools, or passive, such as generating alarms and reports. Modifying actions may be blocking, or recovery. Blocking includes limiting network access (Appiah-Kubi and Liu, 2020) and restarting affected system, while recovery includes renewing cryptographic keys, and distributing new attack signatures.

On the other hand, at a physical level, the preferred approach is dependent on the application. Srikantha and Kundur (2016) provided

a game theoretic model for the attacker and utility. In this model, the attacker seeks to disrupt the stability of the system. The utility (defender) mitigates this by controlling a select set of DERs in order to prevent system collapse and restore stability. Farraj *et al.* (2016) propose a mitigation framework as a response to switching attacks. When a malicious action results in tripping of smart grid switch(es), system stability may be compromised. This mitigation technique proposes a practical smart grid stabilizing controller and uses a game–theoretic approach to model DSO and attacker strategies under potential cyberattacks. Ten *et al.* (2010) present a comprehensive cybersecurity analysis for critical infrastructure. As the main mitigation strategies, it includes remedial actions such as periodic control of user role privileges, and continuous monitoring of overloaded lines and buses with voltage conditions. As a remedial action, it contemplates suspending suspicious network users and relief of overloaded lines when current/voltage problems occur in the physical system.

In the following subsections, specific cases of SCADA attack mitigation and smart meter attack mitigation are provided, respectively.

8.1 SCADA attack mitigation

The SCADA attack mitigation is explained using a two-substation system, where each of them communicates with each other using two protocols: DNP 3.0 over TCP/IP and Inter-Control Center Communications Protocol (ICCP). A testbed application has been used in this demonstration (Zhang and Parhi, 2002). In the substation, the communication among IEDs is based on IEC 61850. A Human–Machine Interface (HMI) has been implemented to enable the operator to control and monitor the substation facilities. In the testbed implementation, it uses power system simulation tools to calculate voltage, power, frequency, and current signals. The HMI acquires from the simulation tool using Object Linking and Embedding for Process Control (OPC) communication. Remote access points are implemented via dial-up, VPN, and wireless technology, which serves, for the purpose of simulation, as intrusion paths.

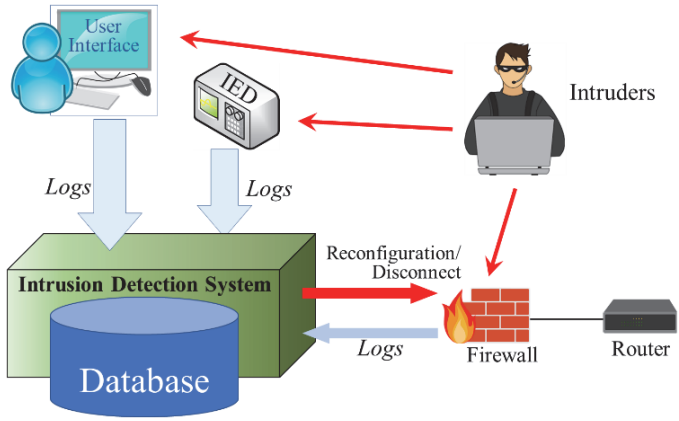

Figure 8.1: Intrusion detection system implemented in the testbed.

An attacker attempts to access a substation from remote. The attacker tries to access substation ICT network by targeting firewalls, HMI control, or IEDs. If the attacker successfully completes the access task with user extended privileges, it will be able to retrieve sensitive information, control breakers, transformer taps, causing damages to grid operation.

In Figure 8.1, the developed intrusion detection system is installed on the computer with user interface on the testbed. IDS reads the log of activities performed in the substation systems, including HMI, IEDs, and firewalls. When the logs are transmitted to the IDS database, an algorithm explores for anomalies. If an anomaly is detected, for instance, unauthorized changes made to critical parameters of the system and/or untrusted packages injected by intruders, a disconnect control signal is sent to the firewall to block the intruder's connection.

As previously discussed, the impact of a cyberattack on the physical layer of a power system is modeled by power flow and dynamic analysis simulation tools. To demonstrate the impact of the attack on system operation, a small power system model is developed, as shown in Figure 8.2. This system includes three hydro plants (150 MW each), six 110 kV transmission lines, and six loads. Simulated real-time measurements are sent to the OPC server. Using a default user ID and

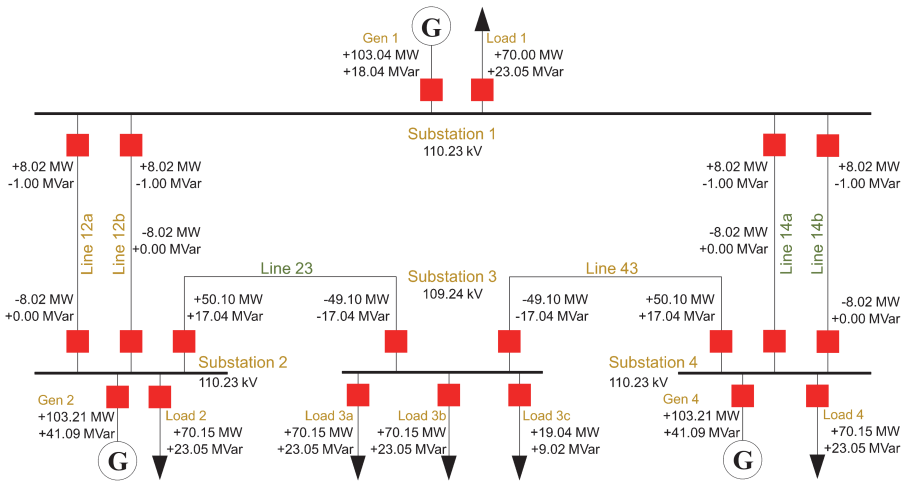

Figure 8.2: Control center SCADA display.

password, HMI is connected to the OPC client and reads data from the simulation tool and substation IEDs. DNP 3.0 protocol is used to send the information to the control center that triggers alarms in case anomalies are detected. Operator's commands are sent via SCADA to the simulation tool which performs real-time power system analysis.

An attack mitigation method to stop cyberattacks and disconnect the intruder is presented. The proposed algorithm not only intends to detect anomaly access attempts but also helps to avoid cascading events after cyberattacks. The simulated scenario is as follows.

The intruder compromises the substation computer by obtaining user IDs/passwords via VPN communication to gain access to substation HMI remote desktop connection and field devices. Since passwords have been cracked, the firewall views as legitimate the connection attempts and the attacker gains access to the network. Attacks are launched from the substation HMI. OPC client–server communication is used to acquire measurements of the power system. Cyberattacks are aimed at multiple locations (substations 2, substation 3, and hydro power plant 2). At substations 2 and 3, the attacks trigger the opening of circuit breakers and, as a result, two transmission lines and a hydro

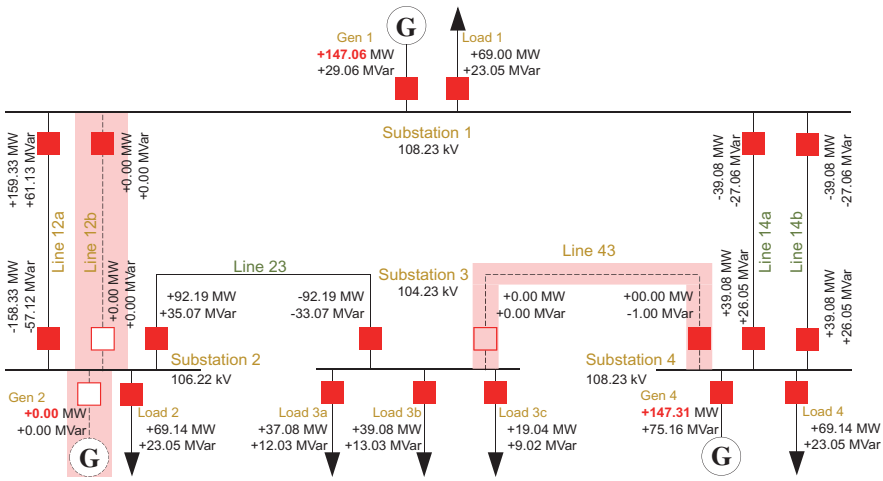

Figure 8.3: Test system after cyberattacks. Control center SCADA display.

plant are disconnected. Attack results are reported via DNP 3.0 to the control center. Alarms at the control center indicate major disturbances in the system. The cyberattack mitigation mechanism is triggered to disconnect lines 43 and 12b. The delivery paths to loads 2, 3a, 3b, and 3c rely on line 12a. See Figure 8.3.

Under these conditions, the remaining energy resources are at full capacity but still not possible to serve the total demand in the system. Hence, the system frequency falls below 48 Hz (Figure 8.4(a)). With the generator out of service, load shedding becomes necessary to maintain the system operating condition. First, intruders are disconnected by collaboration between the IDS and firewall in the substation network. Then, emergency control actions are taken to mitigate the effects of the cyberattacks as an attempt to restore a normal condition (IEEE, 2012). Next, an Optimal Power Flow (OPF) algorithm, with an objective function that minimizes load shedding, is run to determine the necessary actions to maintain system operability.

The results of the OPF show load shedding of 100% and 71% for loads 1 and 2, respectively. Figure 8.4(b) and 8.4(c) indicates that it is

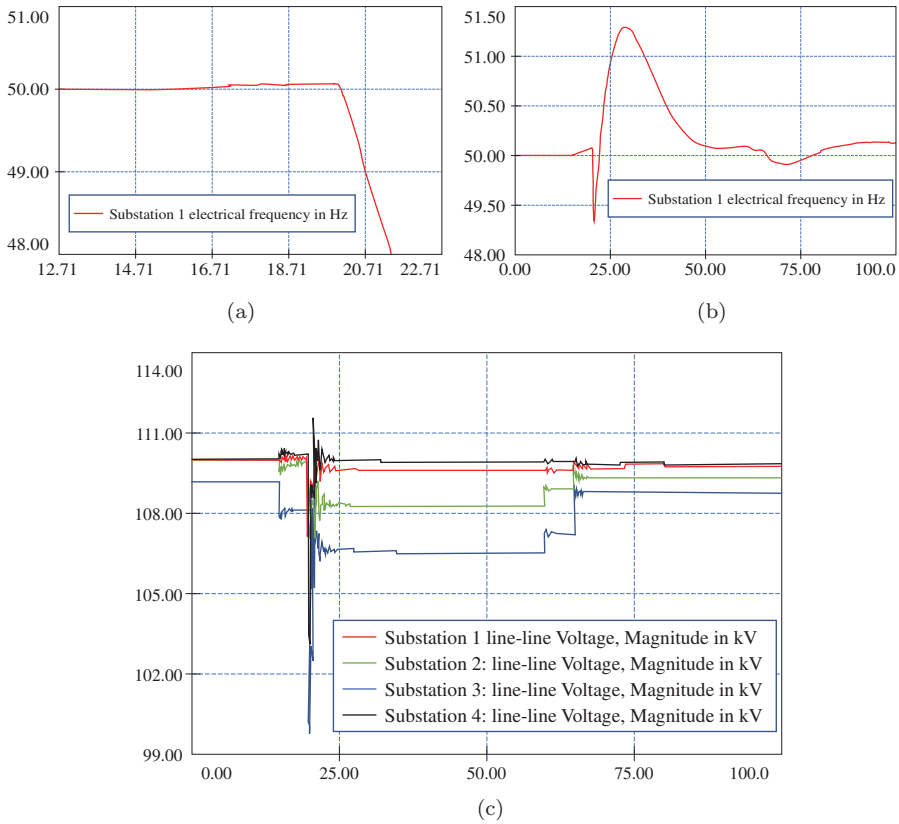

Figure 8.4: Frequency and voltages of the simulated system. (a) Electrical frequency measured at substation 1 (Hz). (b) Frequency after attack mitigation. (c) Line to line voltage at each substation in the simulated event.

possible to steer the voltage and frequency levels to within the allowable limits. Frequency oscillations are shown in Figure 8.4(b). Note that after 15 s, when the cyberattack has been launched (opening breakers), the system frequency is maintained between secure operation limits. Next, 5 s afterward, once the hydro plant is disconnected, the frequency suddenly drops to 49.4 Hz. IDS mitigation action sheds the load and reconnects lines 12b and 43 at 60 and 65 s, respectively. The system is steered back to a stable operative condition.

8.2 Attack mitigation for smart meters

AMI devices are installed at customer premises. Thus, they are exposed to attackers. They present a case study for attackers, who may tamper with either or both of the wireless channel and physical device. The primary components of a smart meter are shown in Figure 8.5. It can be observed that the components are similar to those found in mainstream ICT hardware. Hence, attackers are able to import attack strategies from mainstream devices.

As common in ICT devices, the firmware of a smart meter is responsible for critical functions that perform chip-level roles. These include data conversion and reporting. This software approach allows for easy upgrade of functionalities, either remotely over the communication channel, or manually through the onboard port. Due to its key role, firmware attacks can adversely impact a smart meter's ability to function smoothly.

A commonly used graphical model, Time Failure Propagation Graph (TFPG), is used to represent the cause–effect relations between failure modes, behavioral system discrepancies, and failure propagations. A

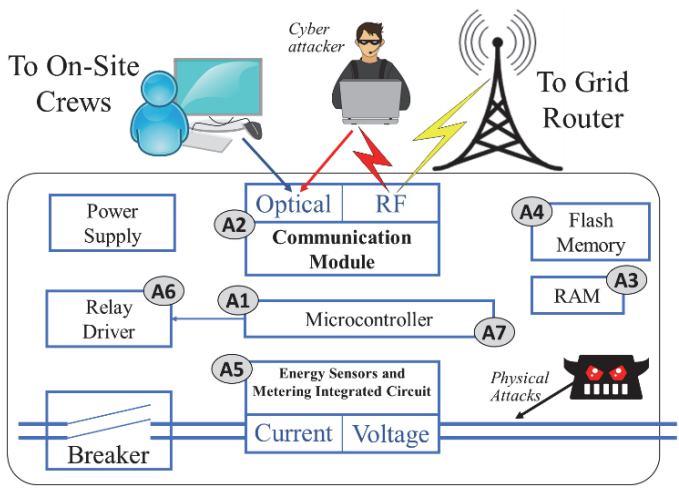

Figure 8.5: Illustrating the primary components of a smart meter and some potential targets for attack.

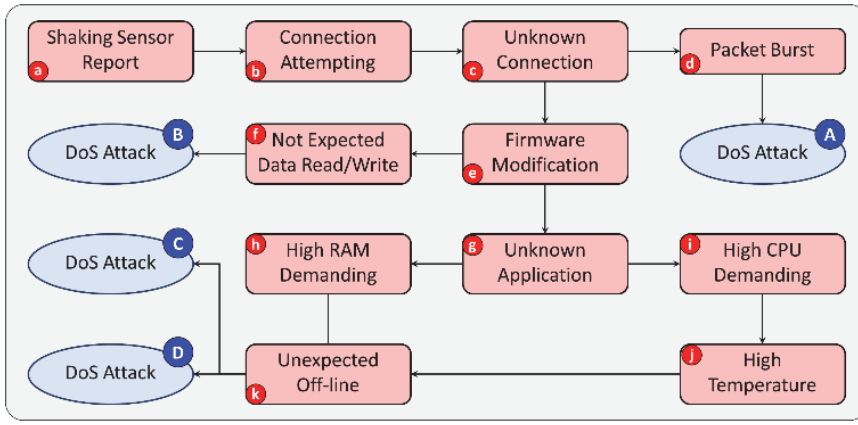

Figure 8.6: Intrusion processes based on the TFPG model for smart inverters. Anomaly event in red and attack type in blue.

TPFG along with a pattern recognition algorithm is used as an intrusion detection instrument. Considering that operational failures such as communication delay and low battery can create alarms, it is necessary that operational anomalous events are distinguished from cyberattacks. Consequently, an in-depth inspection is needed. A signature-based model is useful in such a case. A TFPG serves this purpose well as it is used to capture the causal and temporal relationships between causes and effects of events in a target system. It is therefore used to model the relationship between anomalous events and cyberattacks. Figure 8.6 shows a TFPG model that describes the cause–effect relationship of cyberattacks in a smart meter.

In the attack model, nodes indicate anomalous events while arrows are representative of attack paths. A series of anomaly events are flagged as an intrusion only if their sequence matches that in the attack model. Table 8.1 provides a description of the various anomaly types that are considered.

In this ADS, two assumptions are made: (i) the actions of the attacker are consistent with the sequence in the attack model, and (ii) ADS tend to possess a false negative ratio, so that they fail to accurately detect anomalous events. To curb the issue, the anomaly event is assigned an

Table 8.1: Anomaly types for smart meters in TFPG model.

	Anomaly type	Defects
a	Shaking sensor report	A sensor is installed onboard to detect anomalous vibrations
b	Repeated connection attempts	A series of incorrect password attempts indicate an unauthorized user
c	Unknown connection	Smart meters have fixed communication parent/children nodes. Any exceptions are regarded as an anomaly
d	Packet burst	Smart meters are configured to send beacon and measurement data every fixed time cycle. The incoming command from a control center is not a typical case
e	Modifying firmware	It is necessary that firmware is at the latest version, and updated by authorized users
f	Unxpected data R/W	The measurement data is written and sent to an MDMS every fixed time cycle
g	Unknown application	Only authorized software is allowed
h	High RAM demand	Normal operation of the smart meter should not consume all of RAM
i	Abnormally high CPU demand	As with RAM, the routine tasks of the smart meter should not consume all of CPU power
j	High temperatures	The electronic components of the smart meter can tolerate only a certain range of temperatures
k	Unexpected interruption of service	Smart meters are designed to operate without interruptions

Table 8.2: Attack route set that generated from attack model.

Attack path	Attack type	Dictionary
P_1	DoS Attack (A)	abcd
P_2	False Data Injection (B)	abcef
P_3	Filling Buffer (C)	abceghk
P_4	Overloading (D)	abcegijk

English letter from the alphabet as shown in Figure 8.6. Each path, $P \in \{P_1, P_2, P_3, P_4\}$, from the first anomaly event node (i.e., node a) to an attack-type node (i.e., nodes A, B, C, and D) is considered a correct sequence based on the dictionary shown in Table 8.2.

9

Cyber–Physical System Model

The importance of cosimulation of the physical power system and the corresponding cyber system has been recognized with the increasing penetration of smart devices, distributed generations (e.g., photovoltaics and wind generators), energy storage, and flexible loads on the distribution side. Monitoring and control of the field components are facilitated by the information and communications technology. Real-time control schemes for power system stability, sensing, and data acquisition are motivations for the integrated model. The comprehensive framework of the cyber–distribution system forms an extensive network for data transfer between the different nodes and the remote-control capabilities. In this smart grid environment, cyber threats can cause a disruption of power system monitoring and operation. The impact of a cyberattack ranges from minor service disruptions to wide-area cascading events.

This section provides simulation cases of cyberattacks and the mitigation actions to demonstrate critical concepts of cyber-physical system security of distribution systems. Three cyberattack types described in Section 5, i.e., FDI, DoS, and Replay, are used to demonstrate the impact of cyberattacks on the physical system and their mitigation actions. The

CPS model is based on the communication infrastructure in the distribution system with Feeder Remote Terminal Units (FRTUs) connected to a distribution operating center. The FRTUs are pole-mounted devices, which communicate with DMS using IEC 101 or 104 communication protocols via machine-to-machine over public broadband. The focus is on the CPS communication model and the cyber security aspects associated with the communication network. The impact of various cyberattacks on the power system is evaluated with an integrated CPS model. The ICT model for the distribution system follows the discrete event system based on the queueing model (Stefanov *et al.*, 2015). For demonstration, the CPS model has a power system layer (using static and dynamic power system models) simulated in DIgSILENT PowerFactory and a cyber layer simulated in MATLAB Simulink. These are time synchronized by the OPC server for data exchange.

Data flow of the integrated CPS model is shown in Figure 9.1. The simulated distribution ICT model (cyber layer) has two levels, i.e., a distribution system level with the field measurements (values from FRTUs) and a Control Center (CC) level which receives the measurements from FRTU level and sends control commands to be executed in the physical system. Measurements from the FRTUs go through the communication channel via the queueing system (which

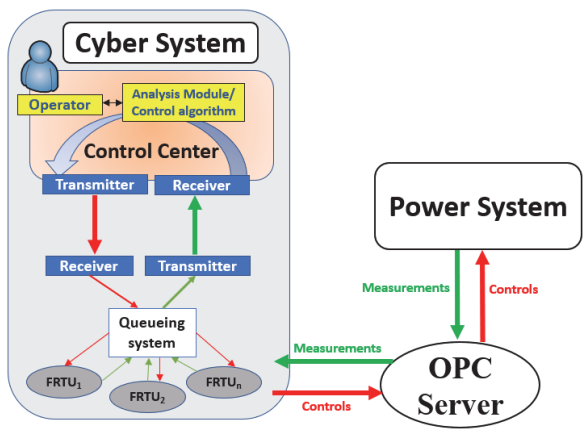

Figure 9.1: CPS simulation setup.

is a computer queue model of the cyber system). It is received by the control center. By the control decision-making process, the control command is sent back through the transmitter of the control center and is received by the receiver at FRTUs. The communication channel may be a physical fiber optical cable or wireless networks based on 4G and 5G technology or a combination of various communication technologies. The bidirectional data flow requires a reliable and secure communication system.

Figure 9.2 shows the ICT simulation arrangement for an FRTU based on the $D/D/m/K$ queuing system, where packet service time and interarrival time are deterministic (D) in nature. Also, m is the number of servers–system with a finite K queuing capacity. This model is used for the ICT devices in the system. Inputs (power, current, voltage, and switch status) from different FRTUs are combined using a round-robin algorithm and sent to the first in first out (FIFO) queue which is further sent to the control center through the processor. The SCADA system at CC receives real-time data from different FRTUs and based on the system state, the operator takes the required control action. The control

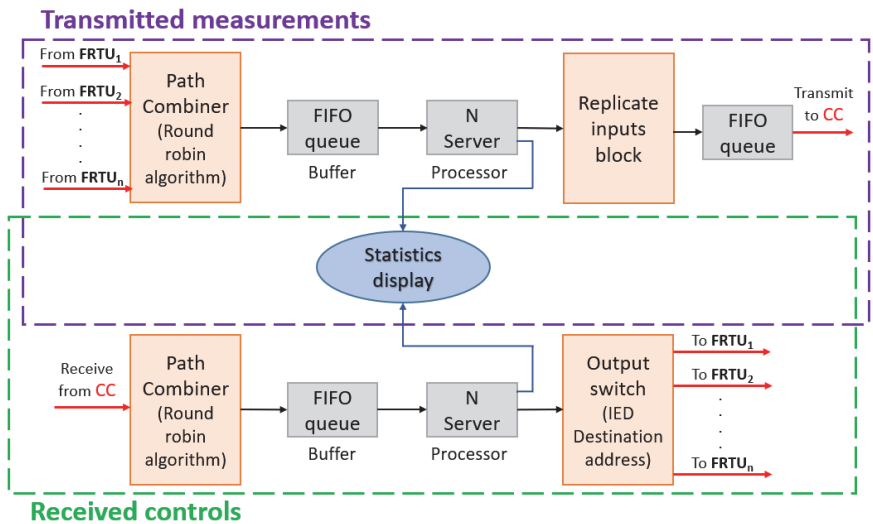

Figure 9.2: Queueing model (Stefanov *et al.*, 2015).

command data packet is sent from the CC through a queueing system to the output switch of corresponding FRTUs. The deterministic bi-directional communication system is the basic structure for continuous data exchange in the system along with security considerations for possible cyber threats.

The measurement data and control signals are sent in the form of data packets which are encrypted to ensure data confidentiality and integrity. The data packet consists of the measurement, timestamp, and an authentication code. A less computationally intensive and effective symmetric key encryption method, 256-bit Advanced Encryption Standard (AES) is implemented here (Zhang and Parhi, 2002).

9.1 Test system

The demonstration here is based on the IEEE 13-node distribution system with a diesel generator, a wind generator, a solar PV, and a battery storage. Different types of cyberattacks are simulated in the cyber layer of the distribution system. During normal operation, the distribution system is connected to the utility system. Each node represents a FRTU in the cyber system to maintain observability of the system for control and operation by the distribution operating center. It is assumed that the distribution feeder serves as a microgrid with the capability to operate in a grid-connected mode or an islanded mode when the utility system is not available. In an islanded mode, the diesel generator provides the control capabilities to maintain system stability and regulate the voltage and frequency of the microgrid.

9.1.1 False data injection (FDI) attack

The simulated scenario is as follows: The system goes from grid–connected to islanded mode at $t = 2\,\text{s}$. The attacker gains access by remote connection to the energy storage device and disconnects ($\text{Storage}_{\text{switching}} = 0$) it at $t = 3\,\text{s}$. Meanwhile, the attacker is sending false data ($\text{Storage}_{\text{switching}} = 1$) to the CC from $t = 3\,\text{s}$ showing that the storage device is connected. This attack is simulated by capturing the data packet with the switching device from the storage device at

the OPC server. It is then modified and inserted back to the OPC server from which the falsified measurement packets are encrypted at the cyber layer. The control center in the absence of a detection mechanism in the cyber layer is unable to detect or mitigate the FDI attack. As a result, the system undergoes major frequency and voltage perturbations.

The FDI attack should be detected and mitigated in the cyber layer to avoid any impact on the microgrid as shown in Figure 9.3. To detect the FDI attack, an IDS with authentication functionalities is used. The authentication code hashing algorithm (He *et al.*, 2017) returns a value generated by performing the algorithm on the measurement. This code is verified at the CC to detect data tampering. On detecting the FDI attack, CC triggers an alarm and executes a mitigation process based on the network visibility and OPF algorithm. In this simulated event, CC sends the command to connect storage at $t = 5$ sec to maintain a stable operating condition of the power system.

Figure 9.4 shows the system response to the simulated FDI attack. The system frequency returns to 60 Hz as the attack is mitigated. In

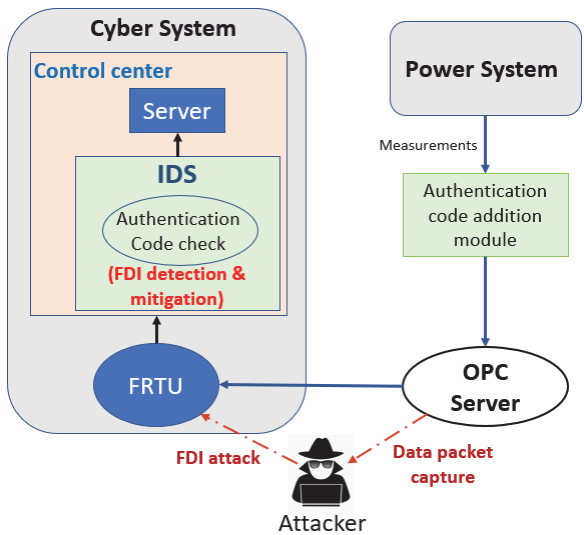

Figure 9.3: Simulated FDI attack and detection setup.

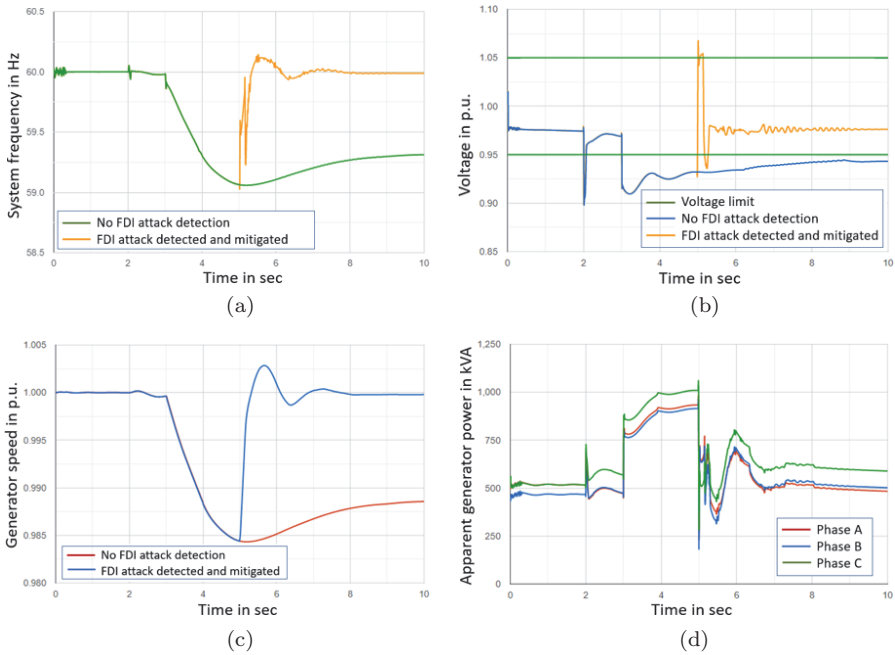

Figure 9.4: System responses to FDI attack. (a) Electrical frequency measured (Hz). (b) Voltage at the affected node in the simulated event (p.u.). (c) Speed of the diesel generator (p.u.). (d) Apparent power of the diesel generator when FDI attack is detected and mitigated (kVA).

the absence of detection, there is an undervoltage condition, but, on successful detection, the voltage is maintained within its operable limits. As the storage device is disconnected, the machine's power output goes up and after $t = 5\,\mathrm{s}$ the generator speed comes back to its normal operative condition.

9.1.2 Replay attack

In this scenario, at $t = 2\,\mathrm{s}$ the microgrid transitions from a gridconnected to an islanded mode. Initially, the capacitor present in the remote load node is in the OFF state. During normal operation, the voltage at the remote node starts decreasing due to an increase in load demand, causing an under-voltage condition. As these voltage measurements are

communicated to the CC, based on the control algorithm, CC sends the command to switch the capacitor ON to inject reactive power to restore the voltage profile.

The attacker gains access to the lower level of the cyber system i.e., the FRTU level. The replay attack is initiated with malicious intent by intercepting the valid data packet and re-transmitting it at a later instance as shown in Figure 9.5. The data packet consisting of the actual data and an authentication code is incapable of detecting a replay attack as there is no modification to the data packet. In this simulation, a timestamp-based replay attack detection method is used. The timestamp of the measurement is appended in the data packet along with the authentication code. When the attacker captures the packet and replays it at a later stage, the difference between the sent and received timestamp of the data packet will exceed a tolerance communication delay value. On detecting the replay attack, an alarm is triggered by the CC, and another secure communication channel is established after blocking the attacker's connection.

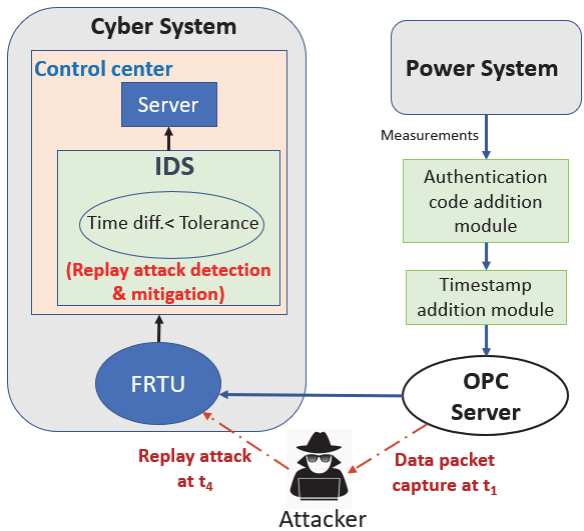

Figure 9.5: Simulated replay attack and detection setup.

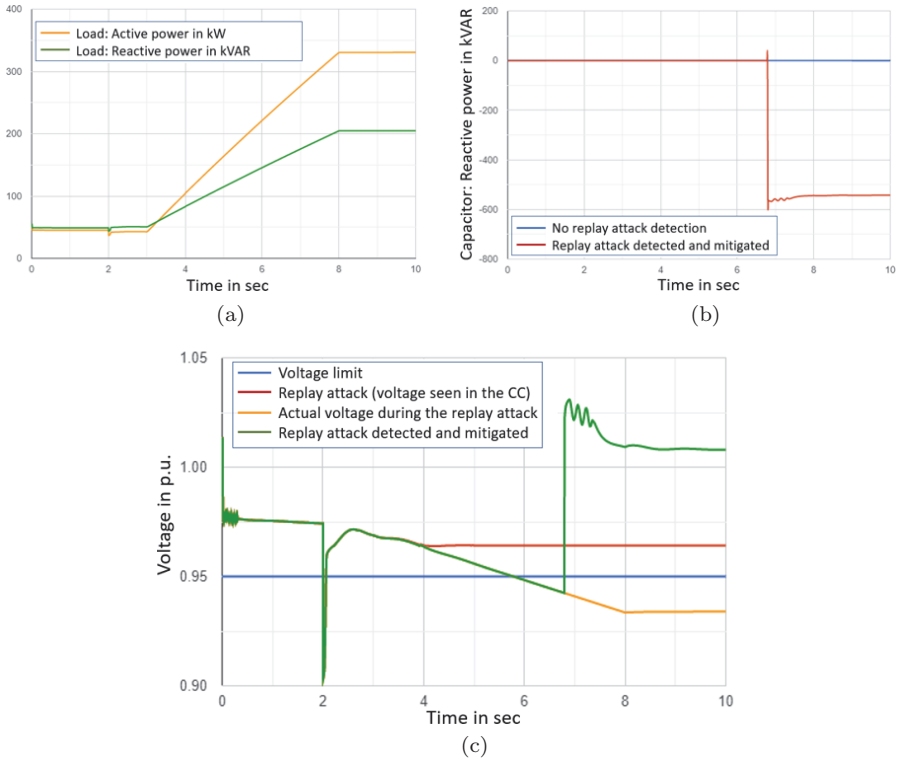

Figure 9.6: (a) Ramp increase in a remote load in the test case. (b) Capacitor reactive power injection at the remote node (kVAR). (c) Voltage at the affected node in the simulated event (p.u.).

The loading level of a remote load ramps up from 3 s to 8 s is shown in Figure 9.6(a). In the absence of a detection process for the cyberattack, the capacitor is in the OFF state and the voltage falls below the acceptable threshold of 0.95 p.u. As the replay attack is mitigated and CC sends a control action to switch the capacitor ON, illustrated in Figure 9.6(b). A replay attack is initiated at $t = 4$ s and the CC receives the re-transmitted data packet as seen in Figure 9.6(c). As a result of the mitigation, the voltage comes within its normal operating limits at $t = 6.8$ s.

9.1.3 Denial-of-Service (DoS) attack

The attacker attempts to overload the cyber system by sending connection requests or data packets (in case of established connection) to prevent legitimate packets to reach the control center. The cyber system from the FRTUs to the control center is shown in Figure 9.7(a). Figure 9.7(b) shows that the server's average utilization during normal system operation is 0.4285 but it increases to 0.8978 under the DoS attack scenario. During the attack, the utilization escalates as the server is flooded with data packets coming from both the legitimate senders and the attacker. This leads to a situation where the server is unable to process valid data traffic.

In the CPS model, it is assumed that there is complete network visibility with knowledge of the data traffic rate, so a preventive approach to DoS attack is preferred. The setup, illustrated in Figure 9.7(a), includes a firewall along with a data traffic rate-limiting router in the CC to detect and prevent DoS attacks. The firewall filters the data packets based on its sender's address, so any attempt to flood the CC by sending connection requests from an external source will be denied. However, the firewall fails to detect the case where a legitimate sender (or FRTU) initiates a DoS attack. As the data rate from each FRTU is a known parameter, the router has the rate-limiting capability to

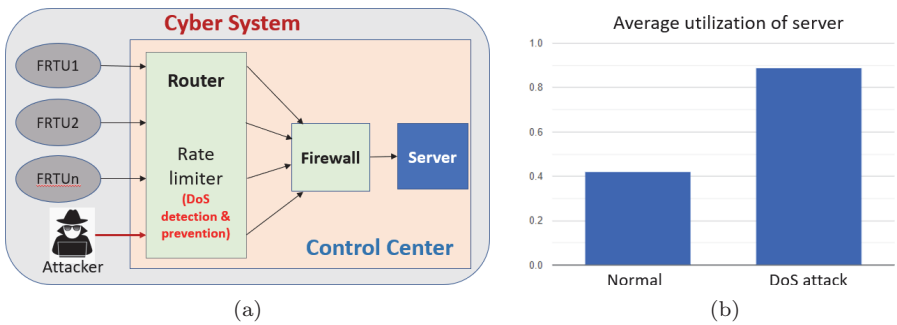

Figure 9.7: (a) Simulated DoS attack and detection setup. (b) Average utilization of the server during a normal operation and during a DoS attack in the absence of preventive measures.

check for a maximum number of data packets departed for every time instance. This approach screens for DoS attacks and prevents burdening the server in the CC. In this simulated DoS attack, the attacker or compromised FRTU tries to flood the router in the control center with data packets, but the rate-limiting capability of the router curbs the illegitimate incoming traffic.

10

Conclusion

This paper provides a survey of CPS security concepts, attack models, and defense measures for the distribution systems. To illustrate the interactions between the communication system and physical system, simulation cases are used to demonstrate the cyberattack types and mitigation actions. While transmission systems rely on the SCADA system for communication between the control center and substations, distribution systems are more fragmented in their communication and control. Indeed, as shown in this paper, distribution SCADA, renewable and storage facilities, smart remote-controlled devices, and smart meters tend to be developed as independent systems without a holistic structure. In the future, CPS security of distribution systems will require a holistic solution to prevent gaps in security measures between subsystems with diverse communications and protocols.

Acknowledgements

This work is sponsored by Department of Energy and Electric Power Research Institute through the project titled “Grid Ready Energy Analytics Training (GREAT) with Data.

References

Ahern, M. F. (2017). "Cybersecurity in power systems". *IEEE Potentials*. 36(5): 8–12.

Al-Shaer, E. S. and H. H. Hamed (2004). "Discovery of policy anomalies in distributed firewalls". *IEEE INFOCOM*. 4: 2605–2616.

Amanullah, M. T. O., A. Kalam, and A. Zayegh (2005). "Network security vulnerabilities in SCADA and EMS". In: *IEEE/PES Transmission & Distribution Conference & Exposition: Asia and Pacific*. Dalian. 1–6.

Amoah, A., S. Camtepe, and E. Foo (2016). "Securing DNP3 broadcast communications in SCADA systems". *IEEE Transactions on Industrial Informatics*. 12(4): 1474–1485.

Appiah-Kubi, J. and C. C. Liu (2020). "Decentralized intrusion prevention (DIP) against Co-ordinated cyberattacks on distribution automation systems". *IEEE Open Access Journal of Power and Energy*. 7: 389–402.

Bakken, D. E., A. Bose, C. H. Hauser, D. E. Whitehead, and G. C. Zweigle (2011). "Smart generation and transmission with coherent, real-time data". *Proceedings of the IEEE*. 99(6): 928–951.

Barai, G. R., S. Krishnan, and B. Venkatesh (2015). "Smart metering and functionalities of smart meters in smart grid — A review". *IEEE Electrical Power and Energy Conference (sEPEC)*: 138–145.

Barbosa, R. R. R., R. Sadre, and A. Pras (2013). "Flow whitelisting in SCADA Networks". *International Journal of Critical Infrastructure Protection*. 6: 150–158.

Berthier, R. and W. Sanders (2011). "Specification-based intrusion detection for advanced metering infrastructures". In: *Proc. IEEE 17th Pacific Rim Int. Symp. Dependable Computing*. 184–193.

CENTRON (2006). *CENTRON Meter Technical Reference Guide*. Available online at: http://www.smartmetereducationnetwork.com/uploads/how-to-tell-if-I-have-a-ami-dte-smart-advanced-meter/Itron%20Centron%20Meter%20Technical%20Guide1482163-201106090057150.pdf. Liberty Lake, WA: Itron Inc.

Chapman, D., A. Fox, and R. Stiffler (2001). *Cisco Secure PIX Firewalls*. Cisco Press.

Chen, Y., J. Hong, and C. C. Liu (2018). "Modeling of intrusion and defense for assessment of cyber security at power substations". *IEEE Transactions on Smart Grid*. 9(4): 2541–2552.

Cheng, X., W. J. Lee, and X. Pan (2017). "Modernizing substation automation systems: Adopting IEC standard 61850 for modeling and communication". *IEEE Industry Applications Magazine*. 23(1): 42–49.

Choi, I.-S., J. Hong, and T.-W. Kim (2020). "Multi-agent based cyber attack detection and mitigation for distribution automation system". *IEEE Access*. 8: 183495–183504.

Clavel, F., E. Savary, P. Angays, and A. Vieux-Melchior (2015). "Integration of a new standard: A network simulator of IEC 61850 architectures for electrical substations". *IEEE Industry Applications Magazine*. 21(1): 41–48.

CPUC (2015). "Recommendations for Utility Communications with Distributed Energy Resources (DER) Systems with Smart Inverters". Sacramento, CA: California Energy Commission and California Public Utilities Commission (SIWG Phase 2). Available online at: https://www.energy.ca.gov/electricity_analysis/rule21/documents/SIWG_Phase_2_Communications_Recommendations_for_CPUC.pdf.

CSIP (2018). "IEEE 2030.5 Implementation Guide for Smart Inverters". San Jose, CA: Common Smart Inverter Profile Working Group., SunSpec 2018. Available online at: https://sunspec.org/wp-content/uploads/2018/03/CSIPImplementationGuidev2.003-022018-1.pdf.

Ericsson, G. (2007). "Toward a framework for managing information security for an electric power utility—CIGRÉ experiences". *IEEE Transactions on Power Delivery*. 22(3): 1461–1469.

Esmalifalak, M., L. Liu, N. Nguyen, R. Zheng, and Z. Han (2017). "Detecting stealthy false data injection using machine learning in smart grid". *IEEE Systems Journal*. 11(3): 1644–1652.

Falliere, N., L. O. Murchu, and E. Chien (2011). "W32.Stuxnet dossier". *Symantec Security Response, Version 1.4*. Available online at: https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

Fan, Y., Z. Zhang, M. Trinkle, A. D. Dimitrovski, J. B. Song, and H. Li (2015). "A cross-layer defense mechanism against GPS spoofing attacks on PMUs in smart grids". *IEEE Transactions on Smart Grid*. 6(6): 2659–2668.

Farraj, A., E. Hammad, A. A. Daoud, and D. Kundur (2016). "A game-theoretic analysis of cyber switching attacks and mitigation in smart grid systems". *IEEE Transactions on Smart Grid*. 7(4): 1846–1855.

Fawaz, A., R. Berthier, and W. H. Sanders (2012). "Cost modeling of response actions for automated response and recovery in AMI". *2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm)*: 348–353.

Finster, S. and I. Baumgart (2015). "Privacy-aware smart metering: A survey". *IEEE Communications Surveys & Tutorials*. 17(2): 1088–1101.

Fischer, R., N. Schulz, and G. H. Anderson (2000). "Information management for an automated meter reading system". In: *Proceedings of the 62nd American Power Conference*.

Gilchrist, G. (2008). "Secure authentication for DNP3". In: *Proc. IEEE Power Energy Soc. Gen. Meeting-Convers. Del. Elect. Energy 21st Century*. Pittsburgh, PA, USA. 1–3.

Hahn, A. and M. Govindarasu (2013). "Model-based intrusion detection for the smart grid (MINDS)". In: *ACM Proc. of the Eighth Annual CSIIRW*. New York, NY, USA.

Hamed, H., E. Al-Shaer, and W. Marrero (2005). "Modeling and verification of IPSec and VPN security policies". In: *13th IEEE International Conference on Network Protocols (ICNP'05)*. 10.

Hari, A., S. Suri, and G. Parulkar (2000). "Detecting and resolving packet filter conflicts". In: *Proceedings of the IEEE INFOCOM 2000. Conference on Computer Communications*. 1203–1212.

Hayes, G. and K. El-Khatib (2013). "Securing modbus transactions using hash-based message authentication codes and stream transmission control protocol". In: *2013 Third Intl. Conf. Commun. and Inf. Technol. (ICCIT)*. Beirut. 179–184.

He, D., S. Chan, and M. Guizani (2017). "Cyber security analysis and protection of wireless sensor networks for smart grid monitoring". *IEEE Wireless Communications*. 24(6): 98–103.

Hong, J., C. C. Liu, and M. Govindarasu (2014). "Integrated anomaly detection for cyber security of the substations". *IEEE Transactions on Smart Grid*. 5(4): 1643–1653.

Huseinović, A., S. Mrdović, K. Bicakci, and S. Uludag (2020). "A Survey Of Denial-Of-service attacks and solutions in the smart grid". *IEEE Access*. 8: 177447–177470.

Hussain, S. M. S., T. S. Ustun, and A. Kalam (2020). "A review of IEC 62351 security mechanisms for IEC 61850 message exchanges". *IEEE Transactions on Industrial Informatics*. 16(9): 5643–5654.

IEEE (2012). "Intruders in the grid". *IEEE Power & Energy Magazine*. Available online at: https://magazine.ieee-pes.org/january-february-2012/intruders-in-the-grid/.

IEEE (2016). *IEEE Standard for Low-Rate Wireless Networks, IEEE Standard 802.15.4-2015*. (Revision of IEEE Standard 802.15.4-2011).

IEEE 2030.5-2018 (2018). "IEEE standard for smart energy profile application protocol".

INL (2007). *National SCADA Test Bed: Fact Sheet*. Idaho National Laboratory (INL).

INL (2008). *Common Cyber Security Vulnerabilities Observed in Control System Assessments by the INL NSTB Program*. Idaho National Laboratory (INL).

Jiang, Y., C. C. Liu, M. Diedesch, E. Lee, and A. K. Srivastava (2016). "Outage management of distribution systems incorporating information from smart meters". *IEEE Transactions on Power Systems*. 31(5): 4144–4154.

Karimipour, H., A. Dehghantanha, R. M. Parizi, K. R. Choo, and H. Leung (2019). "A deep and scalable unsupervised machine learning system for cyber-attack detection in large-scale smart grids". *IEEE Access*. 7: 80778–80788.

Khalifa, T., K. Naik, and A. Nayak (2011). "A survey of communication protocols for automatic meter reading applications". *IEEE Communication on Surveys & Tutorials*. 13(2): 168–182.

Khanna, K., B. K. Panigrahi, and A. Joshi (2018). "AI-based approach to identify compromised meters in data integrity attacks on smart grid". *IET Generation, Transmission, and Distribution*. 12(5): 1052–1066.

Krebs, B. (2012). *FBI: Smart Meter Hacks Likely to Spread*. Available online at: http : / / krebsonsecurity . com / 2012 / 04 / fbi - smart - meterhacks-likely-to-spread/.

Kushner, D. (2013). "The real story of Stuxnet". *IEEE Spectrum*. 50(3): 48–53.

Li, G. W., W. Y. Ju, and D. Y. Shi (2012). "Functional vulnerability assessment of SCADA network". In: *2012 Asia-Pacific Power and Energy Engineering Conference*. Shanghai. 1–4.

Liang, G., S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong (2017). "The 2015 Ukraine blackout: Implications for false data injection attacks". *IEEE Transactions on Power Systems*. 32(4): 3317–3318.

Liang, X., X. Li, R. Lu, X. Lin, and X. Shen (2013). "UDP: Usage-based dynamic pricing with privacy preservation for smart grid". *IEEE Transactions on Smart Grid*. 4(1): 141–150.

Liu, J., Y. Xiao, S. Li, W. Liang, and C. L. P. Chen (2012). "Cyber security and privacy issues in smart grids". *IEEE Communications Surveys & Tutorials*. 14(4): 981–997. Fourth Quarter 2012.

Liu, X., P. Zhu, Y. Zhang, and K. Chen (2015). "A collaborative intrusion detection mechanism against false data injection attack in advanced metering infrastructure". *IEEE Transactions on Smart Grid*. 6(5): 2435–2443.

Liu, Y., S. Hu, and T. Ho (2014). "Vulnerability assessment and defense technology for smart home cybersecurity considering pricing cyberattacks". In: *2014 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*. San Jose, CA. 183–190.

Liu, Y., S. Hu, and T. Ho (2016a). "Leveraging strategic detection techniques for smart home pricing cyberattacks". *IEEE Transactions on Dependable and Secure Computing*. 13(2): 220–235.

Liu, Y., S. Hu, and A. Y. Zomaya (2016b). "The hierarchical smart home cyberattack detection considering power overloading and frequency disturbance". *IEEE Transactions on Industrial Informatics*. 12(5): 1973–1983.

McLaughlin, S., B. Holbert, A. Fawaz, R. Berthier, and S. Zonouz (2013). "A multi-sensor energy theft detection framework for advanced metering infrastructures". *IEEE Journal on Selected Areas in Communications*. 31(7): 1319–1330.

McLaughlin, S., D. Podkuiko, and P. McDaniel (2009). "Energy Theft in the Advanced Metering Infrastructure". In: *4th Workshop on Critical Information Infrastructures Security*. 176–187.

Mitchell, R. and I. R. Chen (2013). "Behavior-rule based intrusion detection systems for safety critical smart grid applications". *IEEE Transactions on Smart Grid*. 4(3): 1254–1263.

Mo, Y., R. Chabukswar, and B. Sinopoli (2014). "Detecting integrity attacks on SCADA systems". *IEEE Transactions on Control Systems and Technology*. 22(4): 1396–1407.

Modbus (2006). *Modbus Application Protocol Specification, V1.1B*. Modbus Organization. Available online at: http://www.modbus-IDA.org.

Moya, C. and J. Wang (2018). "Developing correlation indices to identify coordinated cyber-attacks on power grids". *IET Cyber-Physical Systems: Theory & Applications*. 3(4): 178–186.

Namboodiri, V., V. Aravinthan, S. N. Mohapatra, B. Karimi, and W. Jewell (2014). "Toward a secure wireless-based home area network for metering in smart grids". *IEEE Systems Journal*. 8(2): 509–520.

Nazir, S., S. Patel, and D. Patel (2017). "Assessing and augmenting SCADA cyber security — A survey of techniques". *Computers & Security*. 70: 436–454.

NCCIC and ICS-CERT (2016). "NCCIC/ICS-CERT 2015 Year in Review". 2016. Available online at: https://ics-cert.uscert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2015_Final_S508C.pdf.

NERC (2006). "North American Electric Reliability Corporation". CIP Standard. Available online at: http://www.nerc.com/fileUploads/File/Standards/Revised_Implementation_Plan_CIP-002-009.pdf (accessed on 2 May 2006).

NIST (2010). *Guidelines for Smart Grid Cyber Security, NISTIR 7628*. National Institute for Standards and Technology. Available online at: http://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf (accessed on 30 September 2010).

NIST (2014). *The Cyber Security Coordination Task Group: Smart Grid Cyber Security Strategy and Requirements*. [Online]. National Institute for Standards and Technology. Available online at: http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol2.pdf (accessed on 2 October 2014).

Padilla, E., K. Agbossou, and A. Cardenas (2014). "Towards smart integration of distributed energy resources using distributed network protocol over ethernet". *IEEE Transactions on Smart Grid*. 5(4): 1686–1695.

Phan, R. C. W. (2012). "Authenticated modbus protocol for critical infrastructure protection". *IEEE Transactions on Power Delivery*. 27(3): 1687–1689.

PNNL (n.d.). "The U.S. Pacific Northwest National Laboratory (PNNL)". AMI communication requirements to implement demand-response: Applicability of hybrid spread spectrum wireless". Available online at: http://www.pnnl.gov/main/publications/external/technical_reports/PNNL-20806.pdf.

Premaratne, U. K., J. Samarabandu, T. S. Sidhu, R. Beresh, and J. C. Tan (2010). "An intrusion detection system for IEC61850 automated substations". *IEEE Transactions on Power Delivery*. 25(4): 2376–2383.

Qi, J., A. Hahn, X. Lu, J. Wang, and C. C. Liu (2016). "Cybersecurity for distributed energy resources and smart inverters". *IET Cyber-Physical Systems: Theory & Applications*. 1(1): 28–39.

Rashed Mohassel, R., A. Fung, F. Mohammadi, and K. Raahemifar (2014). "A survey on advanced metering infrastructure". *International Journal of Electrical Power & Energy Systems*: 63.

Rohde, M.-R.-P. (2005). *Cyber Assessment Methods for SCADA Security*. Instrumentation, Syst. Autom. Soc. (ISA), Tech.

Rosenbaum, H. (2012). *Danville Utilities Sees Increase in Meter Tampering*. Available online at: http://www.wset.com/story/20442252/danville-utilities-sees-increase-inmeter-tampering.

SANS and Electricity Information Sharing and Analysis Center (E-ISAC) (2016). "Analysis of the cyber attack on the ukrainian power grid". March 18. Available online at: http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf.

Sapegin, A., A. Amirkhanyan, M. Gawron, F. F. Cheng, and C. Meinel (2015). "Poisson-based anomaly detection for identifying malicious user behaviour". In: Mobile, Secure, and Programmable Networking, MSPN 2015, *Lecture Notes in Computer Science*. Vol 9395. Springer.

SEIA (2018). "Solar Energy Industries Association". "Solar State by State," SEIA: Washington, DC. Available online at: https://www.seia.org/states-map.

SGIP (2014). "Smart Grid Interoperability Panel (SGIP)". Distributed Energy Resources (DER): Hierarchical Classification of Use Cases and the Process for Developing Information Exchange Requirements and Object Models," White Paper, 2014. Available online at: http://www.sgip.org/wp-content/uploads/Distributed-Energy-Resources_DER-Hierarchical-Classification-of-Use-Cases-and-the-Process-for-Developing-Information-Exchange-Requirements-and-Object-Models-2014-07-18.pdf.

Sgouras, K. I., A. N. Kyriakidis, and D. P. Labridis (2017). "Short-term risk assessment of Botnet attacks on advanced metering infrastructure". *IET Cyber-Physical Systems: Theory & Applications*. 2(3): 143–151.

Shahzad, A., S. Musa, A. Aborujilah, and M. Irfan (2014). "Industrial control systems (ICSs) vulnerabilities analysis and SCADA security enhancement using testbed encryption". In: *Proceedings of the 8th International Conference on Ubiquitous Information Management and Communication. (ICUIMC'14)*. New York, NY. 7.

Smith, R. (2014). "Assault on California power station raises alarm on potential for terrorism". *The Wall Street Journal*. Available online at: http : / / online . wsj . com / news / articles / SB10001424052702304851104579359141941621778.

Song, K. Y., K. S. Yu, and D. Lim (2015). "Secure frame format for avoiding replay Attack in distributed network protocol (DNP3)". In: *International Conference on Information and Communication Technology Convergence (ICTC)*. Jeju. 344–349.

Spolar, S. (2012). *Cyber Attack Task Force*. Atlanta, GA: North American Electric Reliability Corporation. Final Rep.

Sridhar, S., M. Govindarasu, and C. C. Liu (2012). *Control and Optimization Methods for Electric Smart Grids*. vol. 3. Springer, 275–294.

Srikantha, P. and D. Kundur (2016). "A DER attack-mitigation differential game for smart grid security analysis". *IEEE Transactions on Smart Grid*. 7(3): 1476–1485.

Stefanov, A., C. C. Liu, and K. Liyanage (2015). "ICT modeling for cosimulation of integrated cyber–power systems". *Securing Cyber-Physical Systems*. CRC Press, pp. 46–81.

Stouffer, K., J. Falco, and K. Scarfone (2011). *Guide to Industrial Control Systems (ICS) Security*. Washington, DC: Nat. Inst. Standards Technol. (NIST), U.S. Dept. Commerce (Special Pub. 800-82).

Strobel, M., N. Wiedermann, and C. Eckert (2016). "Novel weaknesses in IEC 62351 protected smart grid control systems". In: *IEEE International Conference on Smart Grid Commun. (SmartGridComm)*. Sydney, NSW. 266–270.

Sun, C. C., A. Hahn, and C. C. Liu (2018). "Cyber security of a power grid: State-of-the-art". *International Journal of Electrical Power & Energy Systems*. 99: 45–56.

Sun, Q., H. Li, Z. Ma, C. Wang, J. Campillo, Q. Zhang, F. Wallin, and J. Guo (2016). "A comprehensive review of smart energy meters in intelligent energy networks". *IEEE Internet of Things Journal*. 3(4): 464–479.

Ten, C. W., J. Hong, and C. C. Liu (2011). "Anomaly detection for cybersecurity of the substations". *IEEE Transactions on Smart Grid*. 2(4): 865–873.

Ten, C. W., C. C. Liu, and G. Manimaran (2008). "Vulnerability assessment of cybersecurity for SCADA systems". *IEEE Transactions on Power Systems*. 23(4): 1836–1846.

Ten, C.-W., G. Manimaran, and C. C. Liu (2010). "Cybersecurity for critical infrastructures: Attack and defense modeling". *IEEE Transactions on Systems, Man, and Cybernetics Part A: Systems and Humans*. 40(4): 853–865.

USDoE (2011). "The U.S. Department of Energy, Energy Sector Control Systems Working Group (ESCSWG)". Roadmap to achieve energy delivery system cyber security". Available online at: http://energy.gov/oe/downloads/roadmap-achieve-energy-delivery-systems-cybersecurity-2011.

USDoE (2016). "Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector". The U.S. Department of Energy. Available online at: https://energy.gov/sites/prod/files/2017/01/f34/Cyber%20Threat%20and%20Vulnerability%20Analysis%20of%20the%20U.S.%20Electric%20Sector.pdf.

Wei, F., Z. Wan, and H. He (2020). "Cyber-attack recovery strategy for smart grid based on deep reinforcement learning". *IEEE Transactions on Smart Grid*. 11(3): 2476–2486.

Wu, J., J. Xiong, P. Shil, and Y. Shi (2014). "Real time anomaly detection in wide area monitoring of smart grids". In: *IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*. San Jose, CA. 197–204.

Yang, Y., K. McLaughlin, T. Littler, S. Sezer, B. Pranggono, and H. F. Wang (2013). "Intrusion detection system for IEC 60870-5-104 based SCADA networks". In: *2013 IEEE Power & Energy Society General Meeting*. Vancouver, BC. 1–5.

Yang, Y., H. Q. Xu, L. Gao, Y. B. Yuan, K. McLaughlin, and S. Sezer (2017). "Multidimensional intrusion detection system for IEC 61850-based SCADA networks". *IEEE Transactions on Power Delivery*. 32(2): 1068–1078.

Yuan, L., H. Chen, J. Mai, C. N. Chuah, Z. Su, and P. Mohapatra (2006). "FIREMAN: A toolkit for firewall modeling and analysis". In: *2006 IEEE Symposium on Security and Privacy (S&P'06)*. Berkeley/Oakland, CA.

Zhang, X. and K. K. Parhi (2002). "Implementation approaches for the advanced encryption standard algorithm". *IEEE Circuits and Systems Magazine*. 2(4): 24–46.

Zhang, Y., L. Wang, W. Sun, R. C. Green II, and M. Alam (2011). "Distributed intrusion detection system in a multi-layer network architecture of smart grids". *IEEE Transactions Smart Grid*. 2(4): 796–808.

Zhang, Y., L. Wang, Y. Xiang, and C. W. Ten (2016). "Inclusion of SCADA cyber vulnerability in power system reliability assessment considering optimal resources allocation". *IEEE Transactions on Power Systems*. 31(6): 4379–4394.

Zhang, Y., L. Wang, Y. Xiang, and C.-W. Ten (2015). "Power system reliability evaluation with SCADA cybersecurity considerations". *IEEE Transactions on Smart Grid*. 6(4): 1707–1721.