15. Security Analysis of Smart Grid

Charalambos Konstantinou[1*] and Michail Maniatakos[2]

[1]Electrical and Computer Engineering, New York University Polytechnic School of Engineering, Brooklyn, New York, U.S.A.
[2]Electrical and Computer Engineering, New York University Abu Dhabi, Abu Dhabi, U.A.E.
[*]ckonstantinou@nyu.edu

Legacy power grids were typically designed with reliability as the main goal. With the transition to the smart grid, security concerns have begun to arise; due to the computational and communication capabilities of the integrated elements, smart grid technologies are becoming vulnerable to cyber attacks. This chapter aims to enumerate existing threat vectors in the various layers of smart grid architecture and provide insights of how security techniques should be implemented in order to ensure smart grid resiliency.

15.1. Introduction

The electric power grid is increasingly integrating advanced digital technologies into its existing infrastructure. These Information and Communication Technologies (ICT) operate as the control layer on top of the physical energy grid aiming to manage and automate stable operation of power system processes. As a result, the grid is evolving towards a smart grid in order to ensure more reliable and efficient delivery of electricity. While the ICT integration is of paramount importance for the smart grid transformation, it comes at the cost of exposing the entire power system network to new security challenges. Specifically, since the ICT-based systems expand the threat landscape, the smart grid is effectively becoming more prone to cyber intrusions and attacks.

The attack incident against the Ukrainian power system in late 2015 shows the grid vulnerability and how real the threat is. Specifically, on December 23, 2015, media reported a cyber attack on the Ukrainian grid that left thousands of people in the Ivano-Frankivsk region without electricity [1]. The attackers compromised control systems and infected software with malicious code. As a result, they were able to trip breakers, cause a power outage, and prevent the utility from detecting the attack. This real-world example demonstrates the potential implications and damage that a sophisticated cyber attack can cause on the critical infrastructure.

The main smart grid components (generation, transmission, distribution, and consumption) are equipped with cyber systems, as seen in Figure 15.1, including communication networks, control automation systems, and Intelligent Electronic Devices (IED). Bulk generation and Distributed Energy Resources (DER) are equipped with Programmable Logic Controllers (PLC) and other

Distributed Control Systems (DCS) enabling automation and adjustment of the power generation level. At the transmission level, substations, power lines, and towers support Supervisory Control and Data Acquisition (SCADA) and Energy Management Systems (EMS), Wide Area Monitoring Systems (WAMS) with Phasor Management Units (PMU), Dynamic Line Rating (DLR) sensors, etc. Distribution systems deal with the increasing occurrence of Decentralized Generation (DG) and focus on the control, monitoring, and automation of power distribution through the utilization of Remote Terminal Units (RTU). The introduction of smart meters at the consumption level has driven Advanced Metering Infrastructure (AMI) to be an imperative component of smart grid by providing a two-way communication scheme between utilities and customers. Modernizing the grid through the integration of ICT technologies at every level of the system increases both the complexity of the grid and the exposure to potential attacks.

Figure 15.1. *The smart grid structure equipped with cyber systems (dashed line boxes).*

The threat landscape of smart grid is in a constant state of evolution due the inadequate level of security measures. In order to assess the security of physical processes it is necessary to identify the vulnerability sources. Embedded elements such as PLCs, RTUs, data concentrators, etc. are hardware designs that control a cyber physical process. Attacks on the hardware level of these systems aim to gain access to critical information, cause denial of important services, and generally lead to various kinds of security failures. ICT and control systems employ a variety of software platforms. Vulnerabilities in these interfaces may range from simple software errors to poor management of authentication credentials. Every smart grid implementation contains a proliferation of hardware equipment and software, interacting on a network communication layer. Regardless of network topology, vulnerabilities within the network can be introduced from the different composing elements (e.g., insecure communication protocols). Furthermore, security issues may emerge on the operational and process layer of smart grid. For instance, attackers could inject falsified data to operational critical routines in order to hamper the state of the system.

Since smart grid security threats are constantly evolving, proper defenses require advanced cyber security mechanisms. Achieving a secure smart grid is a difficult and complex task. It is essential to understand potential vulnerabilities and weaknesses as well as identify the challenges arising from the incorporation of ICT systems in every level of smart grid. Mitigation and defense mechanisms can be further designed to detect and ultimately prevent malicious attempts to attack the smart grid. Also, initiatives, guidelines, and reference models are valuable, and it is highly recommended that these standards are studied in detail. The security of the grid can be further improved through initiatives that raise awareness and provide training among grid operators, utilities, services providers, manufacturers, and end consumers.

This chapter analyzes the challenges that smart grids and their supporting infrastructure pose to the security of power system components. To that end, the analysis begins by describing the nature of threats due to the various motives of adversaries. The main part of the chapter deals with the attack strategies and the protection mechanisms that can be implemented in all the layers of smart

grid. In order to give a complete picture, efforts and guidelines aiming to mitigate vulnerabilities are described. The chapter also includes a case study with experimental results demonstrating attack and defense techniques. Finally, the future of the smart grid security is discussed by examining the trends in cyber security considerations and industry directions.

15.2. Nature of Threats

Understanding the nature of threat actors in a smart grid environment helps to determine the appropriate assessment and mitigation strategies that will take into consideration the sensitive grid dependencies and connectivity. Threats are typically defined as the "possible actions that can be taken against a system" [2]. These actions, depending on the impact they may cause, can create significant safety issues to people, energy market participants, operations and maintenance routines, damage equipment, and even trigger a power outage. The merge of ICT with Industrial Control Systems (ICS) expands the threat landscape and increases the exposure to potential risks and vulnerabilities. Therefore, as the number of threat agents increases, the nature of threat actors must be examined in detail in order to determine their characteristics.

Smart grid threats can be classified into two broad categories: inadvertent or deliberate. Inadvertent threats may be further categorized based on the origin of failure such as natural disasters, equipment and safety failures. Due to the diversity and complexity of smart grid, the intent of deliberate malicious threats again smart grid components is also important for determining proper risk assessment techniques. Deliberate threats may be further divided to active or passive threats. Figure 15.2 summarizes the existing threat types and their subcategories in smart grid environments.

Figure 15.2. *Security threats classification.*

Threats resulting from inadvertent actions could be attributed to failures, natural disasters, and carelessness in establishing security policies. Failures can result from equipment breakdowns, poorly designed protocols, and non-compliance with safety codes. For instance, MODBUS, a common SCADA protocol, was originally designed for use only within simple process control networks to enable low speed serial communications between clients and servers. Hence, threats could lead to vulnerability exploitations since MODBUS cannot address security concerns [3]. Natural threats such as severe weather conditions, earthquakes, hurricanes, and other phenomena (e.g. vegetation, animals) are also an ongoing threat to grid infrastructure. Smart grid planning should encounter the behavior of the system subjected to such natural hazardous events. Events related with careless actions can result in incorrect operation and control of the grid. Unintentional errors from inadequately trained employees can allow unauthorized personnel to acquire authentication credentials. In addition, unfamiliarity and non-compliance with security procedures, standards, and policies can cause accidental risks to the smart grid implementations. Finally, individuals and companies often become complacent when it comes to security. Managers can be satisfied with

mediocre security performance and do not work to improve the environment by raising security awareness and eliminating the potential threats.

In addition to inadvertent threats, deliberate security threats can cause physical damage to the power system operation with huge financial, social, legal, and political impact. Deliberate threats can be classified as passive and active. Passive threats arise from attempts which aim to learn or make use of information that can affect the performance of the system. Although such threats can cause harm to the smart grid, their target is not to alter the operational state of the system but to gain insight to its inner workings and operational details (e.g. insecure communication links may allow adversaries to eavesdrop the traffic and deduce practical/useful information between communication parties). On the other hand, active threats could affect the operation or resources of the power system. The exploitation of active threats has the potential to impact more victims and have more far-ranging effects than any other type of threat. The growing number of network interconnections in smart grid implementations results in the creation of new active threats and greatly increases the number of entry points for attacks. The outcome of orchestrating the exploitation of these exposed threats results in damaging grid components causing operation disruptions and performance degradation.

Deliberate threats vectors may arise from actions taken by security hunters who view the security mechanisms deployed in smart grid infrastructure as a puzzle to be cracked for amusement. Customers driven by financial motives pose also a type of threat in smart grid. Fraudulent activities in AMI systems include hacking into smart meters targeting to falsify billing information and eventually manipulating energy usage data. The race to modernize power grid systems and, at the same time, keep the cost low increased industrial espionage. Spies, malicious insiders, and even disgruntled employees operating on behalf of utility competitors can gather critical information of power system services. In addition, independent groups and nation-wide terrorists often view grid infrastructure as an attractive target, which if attacked, can result in extensive financial and political implications besides the direct physical damage. The scale of incidents resulting from both passive and active threat actors indicates that adversaries target valuable information on their way to attack a critical system. In 2013, almost one-third of utilities reported losing valuable internal information with 46% citing cyber criminals and competitors as the probable culprit [4].

In order to implement defense strategies against malicious adversaries, it is important to examine all smart grid elements from an attacker's perspective. Adversaries may follow different attack methodologies depending on their motives, capabilities, and resources. The awareness regarding vulnerabilities exploitation approaches will lead to the development of detection and protection schemes able to capture the various threats across all smart grid layers.

15.3. Attacking the smart grid

Identifying the potential threats and vulnerabilities at all levels, ranging from operation management procedures to hardware specific aspects, is the first step towards protecting the smart grid. The various paths an attacker could utilize in order to exploit grid vulnerabilities and circumvent

security features should be taken into consideration when configuring networks and devices.

For adversaries to successfully achieve their malicious objectives, the attack target must be identified first, as presented in Figure 15.3. Possible targets and attack vectors include service provider systems and their customer information interfaces, wide area measurement routines in EMS, smart meters in AMI, etc. The dependencies between the smart grid interconnections often allow attack exploits to propagate within the system and reach additional targets. For instance, a SCADA server may be connected to an industrial Ethernet *switch*[1] which is further connected with *routers* that are accessible from the utility's corporate network. In the scenario which the SCADA server allows write access to the system settings through the slave controllers, a breached device could modify the information sent from other units to the server.

Figure 15.3. *Steps of attack methodologies.*

The identification and enumeration of possible attack targets follows the planning of the attack methodology. This methodology aims to enumerate the steps needed to exploit vulnerabilities specific to a device or related to the network design. For example, software vulnerabilities such as non-inclusion of device memory checks can provide an adversary with the ability to disrupt the operation of grid units like PLCs and PMUs. Attackers capable of violating these boundaries can alter the way the software program operates or trigger execution of malicious code. In addition, widely adopted serial or IP-based protocols have vulnerabilities that may result in *Denial-of-Services (DoS)* attacks [3].

The inclusion of legacy systems into grid technologies provides opportunities to an attacker to seamlessly exploit existing vulnerabilities. To achieve this, vulnerability databases such as the National Vulnerability Database (NVD), the Open Source Vulnerability Database (OSVDB), etc. can be utilized. For industrial systems in particular, the ICS Cyber Emergency Response Team (ICS-CERT) provides alert notifications related to critical infrastructure threats. The security warnings provide information about threats, activity, exploits, and the potential impact.

A vulnerability is exploited by attackers to compromise the target system. Nowadays, most of the adversaries employ readily available intrusion tools and exploit scripts. For example, operation Night Dragon in 2010 utilized common hacking tools aiming to extract financial information and specific project details about oil, gas, and energy companies [5]. Depending upon the vulnerabilities of the system, the methodology could follow different approaches in order to remain undetected and effective as long as possible. A cyber security firm discovered that it takes, on average, 205 days before target companies identify security breaches [6]. Due to the complexity and interconnections within smart grid environments, many attack methodologies use a multilayer threat model, i.e. the attack strategy could target one or multiple layers of smart grid presented in Figure 15.4. Such attacks leverage vulnerabilities in different layers in order to affect as many infrastructure domains as possible (markets, consumers, distribution, transmission, generation, etc.), increase the severity of the damage and the speed of contagion on the infected equipment. For in-

[1] A glossary of terms used in this chapter (presented in *italic* throughout the text) appears in Appendix A.

stance, databases can be connected to computers or other databases with web-enabled applications located at the business network. An attacker able to gain access to the database on the business network could thereafter exploit the communication channel between the two networks and thus bypass the security mechanisms protecting the control systems environment.

Figure 15.4. *Layered smart grid architecture.*

15.3.1. Operation layer

The delivery of electricity to end users in a reliable and secure manner relies on the interaction and interoperability across all the layers that form the smart grid. Power systems operational behavior determines the balance between supply and demand and relies on the dynamic process characteristics of the designed smart grid model. Attacks on the operation layer of the grid aim to hamper the efficiency of the controlled process and therefore degrade the performance of operational routines. Such operation-centric attacks may inject spurious data through specially crafted commands and modify run-time process variables or control logic in order to disturb the operation state and ultimately cause denial of critical services. Besides crashing or halting an industrial process, attack strategies in the operation layer of smart grid aim to conceal their digital footprints and action. Consequently, it is often infeasible for the system operator to determine whether or not the variations in the system process are nominal effects of an expected operation or an attack indicator.

A prominent example of an operation-aware attack is Stuxnet. The malware is believed to be a state-developed cyber weapon and it is considered the most sophisticated malware targeting industrial operations [7]. Stuxnet, presented in Figure 15.5, could spread stealthily between Windows computers running a Siemens specific programming software for PLCs (Step7). It has been estimated that the malware infected around $100k$ systems worldwide. Capable of reconfiguring the operation of PLCs, Stuxnet infiltrated a uranium-enriching plant and accessed the control mechanisms of the centrifuges spin speed. The manipulation of the spin speed of centrifuges allowed the attackers to cease the operation of nuclear plants several times. Since the malware has been identified in mid-June 2010, ICS-targetting malware like Flame, Duqu and Gauss have appeared, sharing many code similarities to Stuxnet [8]. Operation-centric cyber attacks have been also uncovered before the appearance of Stuxnet. For instance, in 2001, hackers installed a *rootkit*, a special category of malicious computer software, to the network of California Independent System Operator (Cal-ISO) [9]. The rootkil caused rolling blackouts throughout the state, affecting over $400k$ utility customers.

Figure 15.5. *Attack strategy of Stuxnet.*

In the context of smart grid, *False Data Injection (FDI)* attacks can manipulate the system state estimation and have a significant impact on the power distribution. An adversary able to obtain access to SCADA could alter the measurement data send from the RTUs to the master station.

Bad Data Detection (BDD) system as part of the state estimation module identifies and eliminates data attributed to topology errors and measurement abnormalities. The goal of an adversary is to corrupt the measurement data from a subset of RTUs D_S. As a result, the measured data $\boldsymbol{z} \in \mathbb{R}_{mx1}$ will become $\boldsymbol{z_a} = \boldsymbol{z} + \boldsymbol{a}$, where $\boldsymbol{a} \in \mathcal{A}$ is the attack vector and $\mathcal{A}$ is the set of feasible attack vectors:

$$\mathcal{A} \triangleq \{\boldsymbol{a} \in \mathbb{R}_m : a_i = 0, \forall i \notin D_S\} \tag{15.1}$$

where $\boldsymbol{H} \in \mathbb{R}_{mxn}$ is the non-linear function vector determined according to the physical structure of the power system and it provides the relationship between state variables and measured values. The malicious vector $\boldsymbol{a}$ is called the FDI attack that can pass the BDD scheme if and only if $\boldsymbol{a}$ can be expressed as a linear combination of the columns of $\boldsymbol{H}$, that is $\boldsymbol{a} = \boldsymbol{Hc}$. It has been shown that data can be falsified in order to introduce errors in certain state variables without being detected by the BDD system [10]. This class of attacks could compromise signals in the electricity market or even mask the outage of lines. Also, the impact from FDI attacks could be the same as removing the attacked RTUs from the network [11].

As in every layer of smart grid architecture, an authorized employee or in general a legitimate user can access privileged system's resources to perform malicious actions. Particularly in the operation layer, insider's knowledge of operational intrusion detection and protection mechanisms allows an attack methodology to effortlessly bypass protection settings to achieve its malicious intents. The Maroochy attack in 2000, although not targeting directly smart grid equipment, demonstrated the impact of a malicious insider attack on ICS. Specifically, a disgruntled employee used inside knowledge to attack a sewage treatment plant and pump $800k$ liters of sewage in a river in Queensland, Australia [12].

15.3.2. Network layer

The communication and interaction of smart grid systems is achieved via the network layer. Due to the various entry points in the network layer, there is a large number of ICS-related vulnerabilities connected with the operation of smart grid at this level. Such entry points include control networks and protocols that link the SCADA systems to lower-level control equipment. Firewalls and modems can also be listed as entry point candidates. Firewalls aim to protect certain network levels by applying filtering policies on the monitored communication packets. Modems enable devices to communicate by converting data in order to be transmitted over a modulated carrier wave. Similarly, communications systems and routers transfer messages between two networks. In addition, entry points include industrial network protocols that link field sensors and other devices to control units (fieldbus protocols). By eavesdropping on the exchanged protocol data, adversaries can manipulate the integrity of communication packets. Remote access points are also ideal candidates for attack entry points to the system since they can remotely query network data and configure smart grid technologies. The poor configuration and the lack of patch management procedures remains, however, the main security risk to emerging threats [13]. Finally, even though most of the smart grid systems are not directly connected to untrusted networks, portable media can be transferred inside the trusted perimeter by personnel. As a result, malware can infect system components and

propagate to the critical field equipment (e.g. Stuxnet).

Implementation and design flaws in industrial communication protocols are frequently the source of smart grid related vulnerabilities. In 2013, 22% of ICS/SCADA vulnerabilities appeared in communication protocols [14]. The most widely used protocols in the electric sector are IEC 60870-5, DNP3, Modbus, FOUNDATION Fieldbus and ICCP [15]. Moreover, smart grid equipment vendors often include support of proprietary communication protocols in their products. In both cases, a number of these protocols offer security through obscurity[2] measures while others have known vulnerabilities or they are insecure by design. Modbus and DNP3, two widely used protocols in SCADA systems, have several identified vulnerabilities [16]. Figure 15.6 illustrates the percentage of vulnerabilities identified in industrial communication protocols in 2013 [14]. The absence of integrity, confidentiality, anti-replay and authentication check features in these protocols is the main source of their inherit vulnerabilities. The lack of these mechanisms allows a variety of network attacks such as *Man-in-the-Middle (MitM)* attacks, *replay attacks*, denial of control and monitor services, identity *spoofing* attacks, etc.

Figure 15.6. *ICS/SCADA protocol vulnerabilities (2013).*

In MitM attacks, an adversary intercepts the communication between two systems, A and B, as shown in Figure 15.7. The attacker "splits" the original communication link into two connections, one between system A (e.g. SCADA server) and the attacker, and the other between the attacker and system B (e.g. slave RTU). While the two systems believe that they directly communicate with each other, the adversary acts a proxy who eavesdrops on the connection. The execution of a MitM attack by the unauthorized party requires to modify the exchanged data or inject new traffic into the communication channel. In the scenario which the communication protocol transfers encrypted data or supports authentication mechanisms, MitM attacks are still feasible by eavesdropping for key exchanges. The MitM party may establish two distinct key exchanges with the two systems, masquerading as A to B, and vice versa, allowing the MitM to decrypt and then re-encrypt the messages passed between A and B. However, industrial protocol connections often do not support authentication and encryption mechanisms, therefore MitM attacks could allow access to entire smart grid networks with minimal effort.

Figure 15.7. *An illustration of the Man-in-the-Middle attack.*

Since industrial control traffic is often exchanged unencrypted, the communication packets via a valid data transmission link can be maliciously repeated or delayed. Replay attacks intercept the data and retransmit a desired process command into a protocol stream received by an ICS component. For instance, if an attacker captures the network traffic between the commands from master SCADA stations requesting tripping of relay controllers, then these packets can be replayed

[2]Security through obscurity is the use of secrecy in the design or implementation of particular protocol modules (e.g. how the authentication password gets encrypted) to provide security.

to perform the same trip task. In cases which the transmitted traffic is in plain text, custom packets can be crafted to perform other tasks ultimately altering the behavior of the entire system. If the receiver in the communication path is a PMU, setpoint registers can be overwritten to falsify the phasor measurements transferred to the transmission system operation center.

Identity spoofing attacks allow attackers to impersonate authorized users. Consequently, spoofed messages are transmitted through the smart grid network and appear to be originated from a trusted system. For example, if the attacker can manipulate a network address or routing mechanisms, identify spoofing attacks can further trigger MitM and replay attacks to the grid network [17].

Firewalls and *Virtual Private Networks (VPNs)* are essential for the network perimeter. If these devices and networks are poorly configured the risk of cyber intrusions could significantly increase. Improper firewall setup can allow attackers to inject large number of packets into the network that may cause congestion and limit the network's availability. VPNs create encrypted connections to ensure secure and confidential data transmission between a client device and a server device. These VPN links, however, secure only the connection tunnel and not the client or the server unit. VPN connection hijacking can be avoided by integrating VPN communications into suitable firewalls. Additionally, when designing a network architecture for a smart grid system, special attention should be paid towards separating the industrial from the corporate network. In cases where the networks must be connected, only minimal connections should be allowed and the connection must be through a firewall and a *Demilitarized Zone (DMZ)*, i.e. "a network area (a subnetwork) that sits between an internal network and an external network" [18].

Although power utilities are taking steps to establish better protection against attacks on the smart grid infrastructure, many of the products currently being deployed in power systems have not been designed with security in mind. Commercial-Off-The-Shelf (COTS) designs typically use common technologies that have both known and unknown security vulnerabilities. The extensive use of such devices led to the porting of serial protocols over TCP/IP for interoperability reasons. However, this tactic has expanded the attack surface by including *TCP/IP attacks*. Several industrial processes are connected directly to the Internet via TCP/IP as evident by the Shodan search engine [19]. In early 2016, ICS Radar, built on top of the Shodan engine, registers more than $14k$ Internet-facing systems that use DNP3 and Modbus protocol over TCP/IP. This facilitates reconnaissance and ICS targeting. For example, a study utilized Shodan to first identify Internet-connected PLCs and then acquire their code via specially crafted network requests [20].

15.3.3. Software layer

The variety of applications and platforms within the software layer increase the smart grid's attack surface. Terminal systems and Human-Machine Interface (HMI) suites interacting with the industrial processes may include sections of code that contain errors or implement poor *access control* mechanisms. For example, *memory corruption* errors between 1988 and 2012 demonstrate the prevalent impact of such vulnerabilities: about 35% of "critical" CVEs were memory corruptions [21]. In addition, software interfaces and terminals are frequently based on commodity Operating Systems (OSs). These vulnerabilities could be exploited by adversaries to gain administrative ac-

cess to key system components. Attackers can then modify the legitimate *control flow* and alter the behavior of software platforms responsible for controlling the system.

The highest percentage of vulnerabilities identified in industrial control products include improper input validation by ICS software, poor management of credentials, and authentication-related vulnerabilities [22]. The analysis of ICS-related software flaws from 2010 until 2013 shows that improper input validation, at 61% of reported vulnerabilities, is by far the most commonly identified vulnerability [23]. Improper input validations arise in scenarios where the data or control flow of a software platform is affected by the incorrect or non-existent validations of input packets. Hence, an attacker able to craft the software input in a form that is not properly handled by the designed platform, can cause modifications to the software control flow or even achieve arbitrary code execution.

Besides attacks applicable to the smart grid software itself, additional attacks are feasible, particularly in cases which web browsers are used on the same system as part of multipurpose workstations or as part of the HMI platform. For instance, *cross-site scripting (XSS)* attacks could enable malicious adversaries to inject client-side script into web pages viewed by other users. Thus, attackers could disclose host files, steal session cookies, install further malware, and alter the browser exchanged data. The prevalence of XSS attacks is highlighted from an analysis report that indicates that from 1988 to 2012, 13% of all CVE security advisories were related with XSS code injection vulnerabilities [21].

Sophisticated malware often target both firmware and software. Firmware includes instructions and data that reside between the hardware and software of devices. It is programmed into the read-only memory of a system. The functionality of firmware ranges from booting the hardware and providing run-time services to loading an OS. In order to meet the real-time constraints related to the behavior of smart grid operations, firmware-driven systems typically employ real time OSes. Similarly to software vulnerabilities, firmware flaws pose a severe threat to the security of smart grid. For instance, malicious firmware images can be distributed from a central system in AMI to smart meters [24]. Firmware vulnerabilities in wireless access points and recloser controllers could even cause serious erosion of the power system's stability margin [25]. In addition to the research studies, real-world examples clearly indicate that power systems are vulnerable to firmware-related threats. In late 2015, attackers were able to cause a blackout in the Ivano-Frankivsk region of Ukraine by overwriting the legitimate firmware on critical devices at the substations, leaving them unresponsive to any remote commands from operators [26]. Specifically, the adversaries wrote malicious firmware to replace the legitimate firmware on serial-to-Ethernet converters at more than a dozen substations, rendering the converters thereafter inoperable and unrecoverable, unable to receive commands. A case study presenting the impact of modifying the firmware of such critical controllers is examined in Section 15.5.

Data acquisition in smart grid begins at the RTU or PLC level. The meter readings and device status reports from such equipment is transferred to the SCADA master as required by the network model. These special purpose field devices may include vulnerabilities in the software layer allowing attackers to exploit them either remotely or locally. As a consequence, malicious activity

could compromise the device integrity and availability. PLCs deployed in many complex control processes run ladder-logic[3] program code containing numerous intentional or unintentional errors. Furthermore, IEDs as "smart" sensors/actuators are often identified with vulnerabilities contributing to MitM and DoS attacks [28].

In the past, several real-world examples have shown that the grid as an ICS is exposed to various software threats that can lead to severe consequences. In March 2008, the Hatch nuclear power generation plant in Georgia, USA, was forced into an emergency shutdown for 48 hours [29]. The shutdown is attributed to a software update on a single computer, charge of the chemical process monitoring and diagnosis data of one of the plant's primary control systems. After applying the update, the computer rebooted and the synchronization software routine reset the data on the control network. Safety control systems misinterpreted the reset action causing a sudden drop in the reactor's water reservoirs and initiated an automatic shutdown. The 48-hour disruption of the nuclear plant operation is a striking indication of the impact of malicious software patches and their resultant financial costs. Considering power transmission and distribution, in 2009 cyber spies accomplished to penetrate part of the US electricity grid, installing malicious software capable of disrupting power supplies [30]. According to US public administration officials, the malicous software had the ability to interfere with critical control systems and leave thousands of people without electricity at any given point during its existence.

Regardless of the attacker's incentive, the exploitation of the underlying vulnerabilities at the software layer is simplified and accelerated by leveraging attack frameworks. Malicious adversaries typically use common tools and tactics in order to attack computer programs and identify the vulnerabilities of grid components, such as Metasploit [31] and Nessus [32]. Additionally, attackers seek opportunities in underground markets for *zero-day* exploit sales [33]. The "purchase" of zero-day exploits anonymously minimizes the effort invested by adversaries. Since these exploits are unknown to software and security developers, they are expected to remain unpatched for extended periods of time, increasing the attack surface of the smart grid software layer.

15.3.4. Hardware layer

All the electronic equipment and physical elements such as microcontrollers, data storage disks and microprocessors constitute the hardware layer of a computer system. Attack vectors in this layer rely on routes or methods used to get into hardware and physically corrupt or manipulate a combination of hardware objects. This requires detailed knowledge of the specifics of the system and its architecture. In the cyber security context of smart grid, the role of hardware layer is essential, as all the other layers rely and build upon it to perform all operations. Hardware-based components in smart grid include embedded systems such as PLCs, RTUs, IEDs, SCADA servers, workstations, relays, and communication routers. These hardware modules are susceptible to both invasive and non-invasive hardware attacks. For example, hardware backdoors can be exploited by adversaries to enable remote control of the target device. The activation of hardware attacks can

[3]Ladder logic is widely used to program PLCs and it represents a software program by a graphical diagram based on the circuit diagrams of relay logic hardware. PLCs can be also programmed with both graphical and textual programming languages. IEC 61131 standard for instance, defines two graphical (ladder diagram, function block diagram) and two textual (structured text, instruction list) PLC programming language formats [27].

rely on a specific timing or functional condition which when activated will degrade the performance of the system or even disable the circuit logic [34].

Due to supply chain globalization, security in the hardware development cycle is a major concern. Attackers can inject malicious hardware logic at any stage of the supply chain including the fabrication phase. Attack vectors that rely on hardware *trojans* can introduce potential risks in the implementation of vital security functions resulting in hardware reliability problems [35]. Besides vulnerabilities arising from supply chain, smart grid systems are prone to attacks targeting specific hardware modules initially designed to accelerate certain procedures such as testing, verification, memory expansion, etc. For instance, unauthorized users can use the *Joint Test Action Group (JTAG)* interface, an industry standard employed for testing Integrated Circuits (ICs), for reverse engineering and intellectual property [36]. Peripherals also introduce hardware vulnerabilities. Malicious USB drives, for example, can redirect communications by changing network settings or destroy the circuit board [37]. Memory units, expansion cards, and communication ports, pose as well a security threat [38]. Real incidents reveal that hardware backdoors exist in critical equipment. Specifically, a backdoor discovered in widely used routers allows information to be transmitted to unauthorized users [39].

Fault injection attacks deliberately inject hardware faults during the normal operation of a device in order to manipulate the computation results. One method of injecting faults into a hardware unit is clock glitching, i.e. the attacker gradually decreases the clock period via glitch injection in order to make the hardware circuit fail. A number of existing false injection attacks are destructive to the circuit and require physical proximity to the hardware device. However, they are effective in disrupting the integrity of smart grid devices and leaking confidential information [40]. Depending on the fault injection method, faults can be transient or permanent. Also the accuracy of false injection attacks varies. Low accuracy fault injection attacks can be realized using electromagnetic (EM) pulses, by falsifying the environment temperature of the device, manipulating the system power supply and clock, etc. On the other hand, high accuracy fault injection attacks require costly and more sophisticated tools (e.g. focused ion beams) which are able to achieve a granularity of single bit-flips.

Information can be extracted from the hardware of smart grid devices through side-channels [41]. Side Channel Attacks (SCAs) are known to be quite effective on hardware and they are related to adversary actions that take advantage of the physical module information leakages. The leaked information (mostly unintentionally) from a particular module to its environment can be derived from data such as power consumption, EM radiation, timing information, acoustic vibrations, etc. In general, there are various information sources leaking information from hardware modules that can consequently be exploited by malicious attackers. These characteristics are directly visible from measurement traces and could simply compromise the confidentiality of the data computation. SCAs based on reverse engineering techniques are easy to implement and ultimately entail powerful attacks, mainly against cryptographic primitives. Most of the times, it is assumed that cryptographic implementations are ideal "black-boxes" and thus their internals cannot be observed or interfered by malicious activities. It is unrealistic, however, to consider that these blocks pro-

vide perfectly secure solutions. Cryptographic primitives rely on both software and hardware and hence this interaction can instigated and monitored by adversaries. For instance, a malicious user could monitor the power traces of cryptographic computations to gather information regarding the algorithm rounds and thereafter use this valuable information to deduce the number of internal secret keys.

Figure 15.8. *Side-channel attack methodology: it compares observations of the side-channel measurements (e.g. timing information, power dissipation, etc.) with model estimations of the leakage.*

15.4. Smart grid security enhancement

The outcomes of cyber attacks against the smart grid range from electricity theft to widespread blackouts. Towards protecting the grid against such threats, security standards, guidelines, and regulatory documents play a key role in smart grid cyber security. These publications provide guidance in understanding smart grid interoperability, interconnections, architectural designs and layers in order to achieve seamless, secure, and reliable operation of the electric power system.

In general, availability, integrity, and confidentiality are the core information objectives that provide assurance of security requirements for smart grids. The comprehensive security requirements of a smart grid, however, are different from traditional IT security due to the constraints imposed by the scale, complexity, and distributed nature of the grid. Therefore, when designing protection solutions against smart grid threats, first it is essential to be aware of the fundamental differences between the security requirements in those two domains. The following list provides a basic understanding as to why smart grid security is different than any other traditional security:

- Lifetime cycle: The average life of the equipment and systems deployed within the grid exceeds 10 years. In comparison with traditional IT systems, the development of secure power systems is inherently difficult. Many grid technologies due to their long life cycle and improper patch management operational procedures, are running systems with published vulnerabilities.

- Performance and availability: Availability in smart grid systems is critical since power outages are not acceptable. Furthermore, grid interactions and processes are continuous in nature making smart grid applications time-critical. For example, cryptography as a security control mechanism used in smart grid may cause unacceptable communication overhead and computational cost. Also, patching often requires downtime which for power systems may result in both operational and economic consequences.

- Proprietary control and communication protocols: In smart grid systems there is a high amount of proprietary information due to the unique standards and protocols. Moreover, many designs use specialized software and hardware. These proprietary or customized system implementations and interfaces are often designed to support specific processes and may

not have build-in any security capabilities. Additionally, proprietary systems are not exposed to the scrutiny of public auditing.

- Risk management goals: Human safety is foremost, followed by protection of process. Other major risks include regulatory compliance, loss of equipment or production, environmental impacts, etc.
- Component location: Power systems consist of geographically disperse and isolated resources, for which gaining physical access may require extensive effort. For the same reason, many of these components may be exposed to physical attacks.
- Security mechanisms: The protection of central servers and field components is significant. In addition, "fail-closed" security mechanisms are restricted to avoid prevention of accessing a system in critical situations.
- Legacy systems: Every domain of electric grid includes implementations with legacy communication, control and monitoring systems. These legacy technologies were not necessarily developed with resilience against cyber attacks as a primal concern.

15.4.1. Policies and Standards

Federal, state, and local agencies and organizations involved in the electric industry should cooperate for the creation of smart grid security plan templates. The templates can be adapted to each particular situation, accelerating the response of both personnel and infrastructure components in attack incidents. The plan guidelines can include details regarding crisis management, operational, cyber and physical security recommendations, technical information, roles and responsibilities, etc. In addition, smart grid stakeholders should establish channels for information sharing. Such initiatives can assist both the government and the private sector to develop situational awareness in support of smart grid security. For example, the S. 754 "Cybersecurity Information Sharing Act of 2015" aims to enhance information sharing between government and private entities [42]. Furthermore, vulnerability databases can help in effectively dealing with cyber attacks. Regulators, customers, and especially utilities can have a reference for publicly disclosed vulnerabilities and the required actions for mitigating the threat. Training, education, and awareness programmes and events are also necessary. Such programs must link availability and safety with good cyber security practices. Every person involved in any smart grid related activity should be trained for security awareness as a way to mitigate the threats arising from the increased use of ICT.

The different needs of smart grid technologies in terms of security have been recognized by governments, agencies, and institutes. Several published security guidelines provide guidance and recommendations for a resilient smart grid. Table 15.1 presents some of the most frequently used security roadmaps. Several other reports exist in literature which provide the appropriate measurements to be taken in order to meet industrial systems security challenges [43, 44, 45, 46].

Due to the large complexity of the smart grid, different models are used for different studies. Each model represents a particular view of the system aiming to solve a specific issue. For example, power systems commonly adopt a graph-theoretic model in which each link (e.g. distribution

Table 15.1. *Mission-critical systems security: roadmaps and security guidelines.*

Policies/Documents	Issues Addressed
ENISA: Smart Grid Security, Recommendations for Europe and Member States [47]	Makes 10 recommendations to the public and private sector regarding the implementation of smart grids
NIST SP 800-82: Guide to Industrial Control Systems (ICS) Security [48]	Identifies cyber security concerns within ICS systems, including SCADA and DCS systems
ISA99 (ANSI/ISA-62443): Industrial Automation and Control Systems Security [49]	Includes standards, recommended practices, technical reports, and related information for implementing manufacturing and control systems securely
NIST-IR 7628 Rev. 1: Guidelines for Smart Grid Cybersecurity [50]	Provides a comprehensive overview for cyber security strategy practices, taking into account privacy and vulnerability classes
NERC/DOE: High-Impact, Low-Frequency Event Risk to the North American Bulk Power System [51]	Determines the appropriate balance of prevention, resilience, and restoration in the American power system
NERC: Critical Infrastructure Protection (CIP) [52]	Requires the identification and protection of all cyber assets supporting the power grid
MIT: The Future of the Electric Grid [43]	Provide a detailed portrait of the U.S. electric grid including the challenges and opportunities it is likely to face over the next years
GAO-11-117: Electric Grid Modernization [44]	Identifies challenges for securing smart grid systems
EOP: A Policy Framework for the 21st Century Grid: Enabling Our Secure Energy Future [45]	Outlines fundamental concerns related to the security of electric grid
DHS (ICS-CERT): Cross-Sector Roadmap for Cybersecurity of Control Systems [46]	Contains a set of priorities that address specific control systems needs over the next decade

line) is the connection between two nodes (e.g. smart meters). The data and measurements of the system are then used in an estimation model (e.g. power flow model) to solve the formulated problem. The smart grid also endorses the use of Common Information Models (CIMs) as a key to achieve interoperability objectives, i.e. to supply a common format for information exchange to support power system management. For example, CIMs such as the IEC-61970 and IEC-61968 focus on transmission and distribution systems respectively, defining the required structures, information and relationships that facilitate grid support and harmonization development [53]. In order to address current and future security threats, the electric power industry should also foster and leverage research on smart grid information modelling as a way to forge ahead with grid modernization.

15.4.2. Multilayer protection for smart grid

Since threats are constantly evolving, protection demands advanced cyber security mechanisms. The development of a secure smart grid should adopt fundamental security techniques for defending against cyber attack methodologies at all layers of the smart grid. In the **operation layer**, integration of energy and information technologies are necessary to ensure resiliency and permit two-way flow for communication and control. The first step to achieve these goals, is to perform vulnerability assessments in order to identify security weaknesses and potential risks with the industrial operation. Due to the real-world consequences of smart grid operations, vulnerability assessment must be performed regularly to ensure that the grid elements, composing the grid infrastructure and interface with the system perimeter, are secure. In addition, the assessment should take into consideration the sensitive smart grid dependencies and connectivity and also account for all possible operating conditions of each smart grid component. The steps of vulnerability assessment methodologies include: document analysis, mission and asset prioritization, vulnerability extrapolation, design of an assessment environment, testing and impact assessment, vulnerability remediation, validation testing, and continuous monitoring [54].

Operation-centric access points in the smart grid should be hardened to limit access only to authorized processes and personnel (role-based access control). One of the basic concepts in system hardening is applying the principle of "least privilege": only points necessary for reliable operation should be enabled. Unnecessary applications should be removed and access should be limited to the minimal level. Furthermore, practices such as separation of services are recommended to prevent cross-contamination when a smart grid system becomes compromised.

Similarly, in the **network layer**, the identity between communication parties should be verified with proper authentication procedures. It is also important to secure the communication link between grid elements (e.g. smart meters and gateways) without compromising the communication performance. In the past, smart grid systems used to be isolated or "air-gapped", i.e. having a physical air gap with no common system crossing that gap. The Stuxnet case demonstrated that an ultimate air gap does not work in real environments, thus VPNs, point-to-point firewall rules, etc. must be applied for proper network segmentation. In addition, industrial protocols are required to protect communication networks in smart grids. For instance, IEC-61850 communication standard defines data formats and interoperability technologies for layered substation communication architectures [55]. Due to the concerns related with the security of the protocol, IEC-62351 is a support standard defining how to secure IEC-61850 communications [56].

Network Intrusion Detection System (IDS) technologies should be included in smart grid network designs to augment host or network-based defenses and monitor system activities for malicious attempts. IDS modules installed distributively along the network hierarchy can profile network communications in order to flag any suspicious traffic and identify deviations from correct behaviors [57]. The role of an IDS is typically passive, i.e. it gathers network information with the purpose only to identify and alert anomalous/suspicious activity. Thus, IDS technologies have limitations in protecting network systems. Intrusion Prevention Systems (IPS) on the other hand, are considered active security solutions since they can protect the system from outside and

inside network attacks. IPS designs have all the capabilities of an IDS and can also use attack signatures and deep packet inspection to prevent specific types of attacks. Figure 15.9 illustrates the utilization of IPS technology for networks in smart grid environment to keep intruders off the network devices.

Figure 15.9. *The use of Intrusion Prevention System (IPS) technology in different levels of smart grid networks.*

The main causes of incidents in industrial networks are attributed to errors and malware attacks in the **software layer** [58]. The negative effects of software-related problems could have several implications in the control operation of smart grid systems. Therefore, implementing software security controls such as code integrity checking and anti-virus software can minimize or even eliminate the exposure and propagation of malicious software activities. Smart grid software-based systems must be also updated and patched frequently to avoid running code that is known to have software vulnerabilities. Furthermore, embedded systems in smart grid typically run software supplied merely by the manufacturer. Thus, manufacturers should incorporate software validation procedures in their products. For example, validation keys can be located in a secure memory storage of the device to protect users from installing rogue copies of the software. In addition, application *whitelisting* solutions can prevent unauthorized software program execution without impacting the performance of the system. On one hand, in contrast with anti-virus and other software packages, whitelisting does not require to be updated regularly. On the other hand, every time software applications are patched their signature changes; it is therefore require that administrators update the whitelist database.

Providing security countermeasures to firmware malicious actions should be one of the initial steps for protecting not only embedded systems, but any kind of computing system within the smart grid. If the underlying firmware is not trusted then any other mechanisms implemented at the OS or application level cannot be trusted. Considering the limited resources of an embedded system (e.g. computation resources, memory usage, communication bandwidth, etc.) as well as the requirement to defend legacy systems within the grid, malicious firmware detection techniques must remain low-cost and overcome the challenges and constraints imposed by the security model. For example, low-level hardware events such as *Hardware Performance Counters (HPCs)* can be utilized to monitor and model the behavior of firmware images [59].

At the **hardware layer** and therefore at the device level, hardware-assisted functionality can make systems more resilient and able to reduce recovery time in case of a malicious attack. Hardware support of cryptographic capabilities can empower devices like RTUs and IEDs. Due to the limited storage space within the hardware of field devices, lightweight authentication protocols can assist in securing the communication amongst various components at different points of the smart grid. A Trusted Platform Module (TPM) can also be used to provide hardware-based trust for the smart grid equipment [60]. A TPM is a cryptographic chip designed to provide greater levels of security (than was previously possible) within the hardware layer of a device. Currently,

TPM technology is part of most the computer designs and is manufactured by nearly all chip producers, including Intel, Atmel, STMicroelectronics, Broadcom, Toshiba, etc. The main functions of a TPM are: *a)* to verify the integrity of the software running on the platform, i.e. it provides to the challenger that the attester executes legitimate software packages with the assistance of a remote trusted third party (remote attestation), *b)* data sealing, i.e. encrypted data is sealed to a specific TPM platform and a particular system configuration, and *c)* data binding, i.e. user data is encrypted using a capable of migrating secret key.

Besides TPM authentication of general purpose computing platforms, security extensions to already deployed processors can enable protection of both peripherals and memory. For instance, TrustZone technology, a security extension in ARM processors [61], employs two virtual processors (called normal and secure) backed by hardware-based access control to provide isolation and enforce tighter *Digital Rights Management (DRM)*. In addition, hardware enforced virtualization can reduce hardware dependencies, separate memory access, isolate execution environments, reduce the costs of maintaining hardware computing platforms, and most importantly, limit the damage from a successful attack within the virtual machine. Virtualization can also assist in restoring the system to a previous snapshot. The ability to return back to a previous point in time is useful during forensic investigations after a successful breach into the system.

15.4.3. Security assessment environment

It is important to understand that realistic impact assessment of cyber attacks on electricity service requires appropriate representation of the studied system. The impact analysis should identify dependencies between various complex systems (both cyber and physical) showcasing the characteristics of interdependent networks. Hence, for proper vulnerability evaluation assessment, testbeds provide an ideal development environment. A testbed typically includes interdependent software, physical/hardware equipment, and network components for studying, understanding, and improving smart grid security without causing real-world failures. A large number of testbeds exist for a variety of purposes and industries. In 2014, over 35 smart grid applicable testbeds had been developed in the United States [62]. In order to expand the vulnerability impact analysis to nation-scale, the hardware testbed needs to be combined with an adequate simulation model. For that purpose, Hardware-In-the-Loop (HIL) testbeds are attractive as assessment environments [63]. HIL methodologies connect hardware equipment to a host computer that runs the simulation model.

A HIL testbed must model the operation and evaluate the security of electronic equipment employed in smart grid domains. The configuration setup outline of a sample testbed is presented in Figure 15.10. It includes a data acquisition that processes the information regarding the testbed network structure (sectionalized areas through relay controllers). The acquired data are used in a power flow simulation environment to calculate the optimal electricity flow through the network. The testbed also contains a Real-Time Automation Controller (RTAC) that collects data from smart meters and relay controllers. The information collected via the RTAC is transmitted to a LTE router which shares it with a 4G/3G/2G connection to the SCADA control center. This sample testbed can

address vulnerabilities for each smart grid layer and across layers. Besides the security objectives, it can also be used to ensure the interoperability of components and capture the information flow throughout the layers of the grid architecture. Moreover, since the structure of the environment can be reconfigurable, the testbed offers flexibility to examine several scenarios and emulate different conditions of the real smart grid environment.

Figure 15.10. *Diagram of a sample smart grid testbed.*

15.5. Case Study

In this section, a case study is presented focusing on both attack and defense mechanisms applicable to the firmware layer of smart grid systems. Particularly, the study illustrates the capabilities of cyber attacks in the smart grid context and examines the security and reliability of the network. Preparing for the future smart grids, studies are essential to evaluate security requirements and practises in the power industry. In addition, by mapping attacks onto proposed protection models, the following study can demonstrate the effectiveness of security countermeasures.

The challenge: The digitization of smart grid technologies leads to the formation of power systems substantially dependent on embedded devices. Firmware in embedded systems, such as microprocessor-based relays, controls the hardware of the device. Therefore, firmware attacks can bypass access control and security modules. An attacker capable of maliciously modifying the firmware can introduce backdoors, control the operation of a device, and have unrestricted access to the system components. In the smart grid scenario, one of the attack challenges is to alter the relay firmware in order to open and close circuit breakers at undesirable time, inducing catastrophic damage to machines or even leading to cascading systems failure [25]. Given the critical role of firmware in these embedded systems, implementation of effective security controls against malicious actions is essential [59]. The design of such countermeasures needs to take into consideration the resources constrains in embedded devices (e.g. computation resources, power consumption, memory usage, etc.).

The impact: Firmware reverse engineering can reveal information of the system features and unlock hidden functionalities. In this study, the firmware analysis findings of a commercial relay controller are applied to corrupt the circuit breaker status signal in a developed testbed. Two firmware attack vectors are developed based on the aurora-type vulnerability and the relay inability to sense a fault and initiate a trip to the breaker.

Every relay has a deliberate operational delay to avoid any protection activity during transients. These delays leave an open window of opportunity for defective operation [64]. The out-of-sync closing of breakers via the connected relays results in the aurora vulnerability by changing the operating frequency of the generator and causing frequency difference between the machine and the grid. To meet the requirement of repeatedly sending trip and reclose commands to the generator relay, the first firmware modification disables the communication port of the relay controller so that there is no transmission of digital data to the master SCADA system (DoS attack). While the relay

is offline, the relay reboot address is injected into specific firmware locations in order to cause the relay to restart resulting in an aurora-type event.

Protective relays are designed to handle power network faults (e.g. short-circuits). This involves detecting the presence of faults, isolating them by tripping the breaker connected to the relay and reclosing circuits automatically. Failure to sense and clear the fault may start a chain reaction to the system. The second attack vector modifies the relay protection profiles specifying the operation of the relay control. This is accomplished by altering the calibration control mechanisms encompassed in the firmware initialization process. In order to keep the modifications minimal, changes are only performed for the overcurrent protection parameters. For example, even if the phase and ground minimum trip currents set in the relay software are 400A and 280A respectively, the calibration registers are modified to be always programmed to the relay maximum trip settings i.e. 3200A for phase and 1600A for ground minimum trip currents.

The proposed attack scenarios are applied on a HIL testbed. The breaker control signal is transmitted to the simulation environment modelling the IEEE 14 benchmark. The contingency ranking of the system specifies that the most critical generators are G5 and G3 [65]. The developed bus system however, is able to handle both $N-1$ and $N-2$ contingencies, i.e. the generator rotor angles are transiently stable after causing G5 and G3 breakers to trip.

In the first scenario, the modification of aurora-type event is simulated by intentionally opening the CBs at $t = 1s$ and reclose/trip every 15 cycles ($0.25s$). When the breaker opens and closes once (scenario $1a$), the out-of-phase generators are imposed to torque pulsation to remain in synchronism with the grid. When the attack is repeated two times, there is a voltage collapse due to the limited power transfer capability (scenario $1b$). The graphs for this case are shown in Figure 15.11. In the fault-clearing failure scenario, the firmware modifications are simulated by applying a short-circuit three phase fault to the system. When the fault current flows above the preset overcurrent value, the corresponding relay instead of initiating the status signal to open the corresponding breakers, the breakers remain close and the system fails to clear the fault. Figure 15.12 shows the inability of the breaker to clear faults, which leads to voltage instability responsible for network collapse.

(a)(b)

Figure 15.11. *Generators bus voltage due to (a) N-1 (G5) and (b) N-2 (G5, G3) generator aurora-type contingencies [scenario* $1a$ *(solid line), scenario* $1b$ *(dotted line)].*

(a)(b)

Figure 15.12. *Generators bus voltage due to (a) N-1 (G5) and (b) N-2 (G5, G3) generator fault-clearing failure contingencies.*

The solution: Since a firmware program is composed of a sequence of various types of instructions

and data, the program behavior can be uniquely characterized by the total occurrences of hardware events during its execution as well as the relationship between the counts of different monitored events. The low-level hardware events can be efficiently measured using HPCs. Although HPCs are typically used for performance tuning, HPCs can be utilized for security purposes with no extra hardware cost [59]. HPCs events include retired instructions, branches, returns, etc. When firmware is maliciously modified, the counts of the executed HPCs events will be different from those during legitimate firmware runs.

The high-level structure of the HPC-based security module is shown in Figure 15.13. A legacy *bootloader* is extended to include three components: *a)* an insertion module that places checkpoints to the monitored firmware, *b)* an HPC handler that drives the HPCs, and *c)* a database that stores valid HPC-based signatures. All these components are stored in write-protected non-volatile memory. This prevents attacks from compromising the security module while still allowing authorized updates. Once the execution reaches a checkpoint, the control flow is intercepted and redirected to the core module. The core then communicates with the HPC handler and the HPC-based signature database. Specifically, the event counts for the previous check window are read and compared with the corresponding signatures in the database. Then the HPCs are reset for the next check window and the execution of the monitored firmware continues. The HPCs keep counting the occurrences of the hardware events until the next checkpoint is reached.

Figure 15.13. *High-level structure of the security module. The core consists of three components: an insertion module that inserts checkpoints to the monitored firmware, an HPC handler that drives the HPCs and a database that stores valid HPC-based signatures.*

The benefits: The effectiveness of the designed security mechanism is tested with two real-world firmwares of embedded systems on two different platforms[4]. The first embedded system is an ARM-based wireless access point and access gateway. In this device, a DoS attack is performed which targets the task scheduling module of the firmware. When a task with a specific ID is running it will occupy the processor without being switched out, thus will impact the availability of other tasks. Owing to their repeatability, 4 events are selected to be monitor: INSTRUCTION executed, BRANCH instruction executed, LOAD instruction executed and STORE instruction executed. There are seven valid paths in the original scheduling subroutine. At runtime the HPC-based signature are compared with a subset of the valid signatures to check if a match occurs. The results are shown in Table 15.2 (a) for 3 randomly selected check windows. The minimum deviation for a malicious path to be detected is 8.7% in check window 3 (among the events whose occurrences have changed). In this case, the monitored LOAD event defines the minimum noise detection threshold N. For example, a detection threshold of 5% is adequate to identify the malicious modifications in every chosen check window.

The second embedded system in this study is a commercial relay controller. The PowerPC-based controller firmware is modified to implement a MitM attack that sniffs Ethernet packets.

[4]Samsung Exynos Arndale (ARM Cortex-A15, 6 HPCs, 70 events) and Freescale MPC8308RDB (PowerPC e300c3, 4 HPCs, 40 events)

The attack targets the Ethernet packet receiving subroutine in order to capture the packets of data flowing across the network. The modification intercepts the control flow and copies the received packets to a specific memory location. As a result, an attacker can retrieve the critical information in the received Ethernet packets. Due to the hardware events occurrences, the selected events are similar to the ARM-based platform. The HPC-based signature of the malicious path exhibits large deviations when compared with the signatures of the five valid paths in the Ethernet packet receiving task. The generated signature is compared with the valid ones included in the checking window. The results are presented in Table 15.2 (b) for 3 randomly chosen check windows. The smallest deviation in this scenario is 4.2% due to the LOAD event counts of check window 1. Selecting the appropriate threshold N, for instance 4%, the implemented security mechanism differentiates between valid and malicious paths in order to detect the packet sniffing.

Table 15.2 Detection capability using HPCs. The numbers are the event count deviations (%) of the malicious path from all the valid paths in monitored subroutines for **(a)** the wireless access gateway and **(b)** the recloser controller. For each path, the bold number indicates the largest deviation among all events. The tested path (malicious) is not matched to any valid path indicating a successful detection.

Table 2 (a)

Path	Hardware event			
	INSTRUCTION	BRANCH	LOAD	STORE
Check window 1				
1	27.3	33.3	37.5	**50.0**
2	77.1	71.4	**81.5**	50.0
3	73.3	71.4	**76.2**	60.0
4	51.5	**60.0**	58.3	0.0
5	65.9	50.0	**75.0**	60.0
6	69.8	71.4	**76.2**	33.3
7	62.8	**71.4**	66.7	33.3
Check window 2				
1	77.8	33.3	**150.0**	0.0
2	44.8	60.0	16.7	**66.7**
Check window 3				
1	33.8	**175.0**	31.6	40.0
2	**16.5**	15.8	8.7	12.0

Table 2 (b)

Path	Hardware event			
	INSTRUCTION	BRANCH	LOAD	STORE
Check window 1				
1	65.0	**266.7**	78.6	250.0
2	10.0	10.0	0.0	**55.6**
3	41.4	**83.3**	16.7	33.3
4	6.5	22.2	4.2	**47.4**
5	5.7	10.0	7.4	**33.3**
Check window 2				
1	**95.8**	76.8	62.1	30.0
2	19.5	51.1	**70.6**	30.0
3	**65.0**	46.7	37.5	44.0
Check window 3				
1	30.3	12.0	16.7	**47.4**

Figure 15.14 shows the execution time overhead on the monitored firmwares when different check window sizes are applied. For instance, a check window size of 500 instructions leads to an average execution time overhead of 8.48% on the ARM Cortex-A15 platform and 5.62% on the PowerPC e300c3 platform. For the test cases, the performance overhead for the scenario that includes all the subroutine paths is 14.2% and 7.3% for the ARM and PowerPC case respectively. The storage overhead of the security module is mainly for storing the components instructions (less than 10 KB) and the known valid HPC-based signatures. For example, an HPC vector in a check window that counts 5 hardware events requires 10 $byte$ storage for the signature of a valid path. If 10 check windows are applied and there are 10 valid paths in each window, then the required storage is 1 KB. In the scenario where the firmware image size is 1 MB then the storage overhead (10 KB + 1 KB) is translated to approximately 1% of the firmware code size.

Figure 15.14. *The execution time overhead with different sizes of check windows in terms of number of total instructions.*

15.6. Future cyber security considerations

Successfully implementation of secure smart grid systems requires careful attention to the future cyber security landscape. Smart grid technologies will need to take into consideration trends in malware activity, cyber espionage, protocol vulnerabilities, network dependencies, etc. In addition, the multitude of new research studies and innovative technological developments can enhance observability in system operation and control.

One step towards improving cyber security is to create quantitative metrics for attack incidents. The metrics can be used to assess the dependency among information and communication objects, help to evaluate the impact of incidents, and prioritize the adoption of appropriate security countermeasures. Future cyber security considerations of the smart grid should also consider the introduction of security breach notification frameworks. Early notification warnings about disclosed vulnerabilities along with improved information sharing mechanisms can assist utilities to coordinate and implement strong security controls to mitigate the identified risks.

Smart grid investments must allow the integration of new products and services that can provide comprehensive and coherent protection against cyber threats. In addition, "smart" equipment can enable demand participation and therefore improve both observability and controllability of the grid networks. Moreover, the optimal placement and sizing of distributed energy resources have the potential to strengthen energy security and provide greater stability and efficiency to the smart grid. Transmission and distribution automation deployments are expected to receive more attention in the future. Such systems can assist in maintaining a reliable and secure electricity infrastructure by optimizing the utilization of assets and efficiently leverage smart grid instruments in the field. Additionally, big data analytics will play a vital role in future implementations. The aggregation and analysis of smart grid operational information (e.g. logs/databases, alarms/events, etc.) can assist in identifying threats and breaches as well as predict and prevent equipment failure.

Due to the rapid smart grid modernization, the nature of human interaction with electric systems is expected to result in dramatic changes (as demonstrated in the past with cell phone communications and Internet). This social transformation will define new levels of security and privacy for data. Hence, to successfully maintain the security of both customers and the system, current and future smart grid technologies need to be supervised and controlled by appropriate policies and regulations that will address the upcoming cultural change. In addition, it is necessary as we advance toward a smart grid to adopt a cross-disciplinary approach that instills greater coordination and interaction among government, electric utilities and customers.

15.7. Conclusions

Over the last decade, the grid infrastructure has faced a transition from legacy systems to new technologies. The increased dependency of these components on cyber resources has an immediate impact to the exposure of the grid to potential vulnerabilities. During this transition multilayer security approaches can help all involved stakeholders to defend against malicious actions and assess the security designs deployed in the smart grid. The attack methodologies and countermeasures discussed in this chapter aim to reflect the needs for current and future frameworks towards reducing the risks to an acceptable secure level and providing fine-grained security solutions.

A. Appendix - Glossary

- **Access Control Mechanism**: is a set of controls enforcing security policies that restrict access to particular resources. A security policy is a statement of what is, and is not, allowed.
- **Bootloader**: is responsible for locating and loading the OS or firmware. If the device is a non-OS based system then the firmware execution tasks are run in an infinite loop.
- **Control flow**: is the order in which instructions, functions, or statements of a program are executed or evaluated.
- **Cross-site scripting (XSS)**: attack is a type of attack based on web application vulnerabilities. It involves client-side code injection where malicious scripts are injected into web pages executed on the user's web browser (client-side).
- **Demilitarized Zone (DMZ)**: is a *network area (a subnetwork) that sits between an internal network and an external network* [18]. DMZs allow connections from the internal and the external network to the DMZ network. However, connections from the DMZ are only permitted to the external network.
- **Denial-of-Service (DoS)**: attack is a type of attack against the availability of a service, machine or network, i.e. DoS prevent legitimate users from accessing information or services.
- **Digital Rights Management (DRM)**: technologies impose access control mechanisms and restrictions that control the usage of proprietary hardware and copyrighted works.
- **Gateway**: is a hardware-based device that serves as a network point allowing entrance to another communication network.
- **Hardware Performance Counters (HPCs)**: are special-purpose registers built into the performance monitoring unit of a modern microprocessor. The number of available HPCs as well as the number of hardware events vary from one processor model to another.
- **Joint Test Action Group (JTAG)**: interface is an IEEE 1149.1 industry standard used for testing ICs using boundary scanning [66]. JTAG is widely used to communicate with microcontrollers and perform operations such as single step execution and breakpoint insertion.

- **Memory corruption**: errors which occur from violations of memory contents due to non-inclusion of memory boundaries checks (e.g., buffer overflow).
- **Rootkit**: is a special category of malicious computer software which can enable privilege access to a computing system or areas of its software while at the same time hides its existence (or the existence of other software modules or both) in user-level objects.
- **Router**: is a "traffic directing" hardware device that determines the next point within a network to which a data packet should be forwarded until it reaches its destination.
- **Switch**: is a device that utilizes packet switching to process the incoming data from multiple ports and forwards that data to the intended destination (bridge between network points).
- **TCP/IP attacks**: refer to any type of attack that exploits vulnerabilities in the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite.
- **Trojan**: In the context of software, a trojan is a malicious program which hides within other seemingly harmless programs that misrepresent themselves to appear interesting or useful in order to persuade and eventually trick a victim user to install it. Similarly, hardware trojans can be described as malicious and deliberately stealthy modifications to the circuitry of an integrated circuit.
- **Virtual Private Network (VPN)**: is a technology that expands a private network over a less secure public network. It creates virtual network connections using virtual tunnelling protocols, dedicated links, or traffic encryption.
- **Zero-day vulnerability**: is a vulnerability that is unknown to the vendor. Such undisclosed security hole is known as a "zero-day" because once the vulnerability becomes known, the developer has zero days to patch and thus fix the flaw.

B. References

[1] D. Trivellato, D. Murphy. *Lights out! Who's next? How to anticipate the next "cyber-blackout"*, (2016).

[2] American National Standard (ANSI). *ANSI/ISA99.00.012007 Security for Industrial Automation and Control Systems, Part 1: Terminology, Concepts, and Models. International Society of Automation (ISA)*, (2007).

[3] Y. Mo, T. H.-J. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, B. Sinopoli. "Cyber–physical security of a smart grid infrastructure", *Proceedings of the IEEE*, **100(1)**, pp. 195–209, (2012).

[4] PricewaterhouseCoopers (PWC). *Power & Utilities: Key Findings from the Global State of Information Security Survey*, (2013).

[5] McAfee. *Global Energy Cyberattacks: Night Dragon*, (2011).

[6] FireEye. *M-Trends 2015: A View from the Front Lines*, (2015).

[7] N. Falliere, L. O. Murchu, E. Chien. "W32. stuxnet dossier", *White paper, Symantec Corp.*, (2011).

[8] B. Bencsáth, G. Pék, L. Buttyán, M. Felegyhazi. "The cousins of stuxnet: Duqu, flame, and gauss", *Future Internet*, (2012).

[9] SANS Institute. *Can Hackers Turn Your Lights Off? The Vulnerability of the US Power Grid to Electronic Attack*, (2001).

[10] Y. Liu, P. Ning, M. Reiter. "False data injection attacks against state estimation in electric power grids", *ACM Transactions on Information and System Security*, **14(1)**, (2011).

[11] O. Kosut, L. Jia, R. Thomas, L. Tong. "Limiting false data attacks on power system state estimation", *Information Sciences and Systems (CISS), 2010 44th Annual Conference on*, pp. 1–6, (2010).

[12] J. Slay, M. Miller. *Lessons learned from the Maroochy water breach*, (Springer, 2008).

[13] C. Nan, I. Eusgeld, W. Kröger. "Hidden vulnerabilities due to interdependencies between two systems", *Critical Information Infrastructures Security*, pp. 252–263, (Springer, 2013).

[14] A. Sarwate. *Vulnerability analysis of 2013 SCADA issues*, (Qualys Inc., 2007).

[15] Sandia. *Control system devices: Architecture and supply channels overview*, (2010).

[16] S. East, J. Butts, M. Papa, S. Shenoi. "A taxonomy of attacks on the dnp3 protocol", *Critical Infrastructure Protection III*, volume 311, pp. 67–81, (Springer Berlin Heidelberg, 2009).

[17] U. Premaratne, J. Samarabandu, T. Sidhu, R. Beresh, J.-C. Tan. "An intrusion detection system for iec61850 automated substations", *Power Delivery, IEEE Transactions on*, **25(4)**, pp. 2376–2383, (2010).

[18] ICS-CERT. *Control System Security DMZ*, (2016).

[19] *SHODAN search engine for Internet-connected devices*, (2016).

[20] P. M. Williams. "Distinguishing internet-facing ics devices using plc programming information", Technical report, DTIC Document, (2014).

[21] Y. Younan. "25 years of vulnerabilities: 1988-2012", Technical report, Sourcefire Vulnerability Research, (2013).

[22] DHS. *Common Cybersecurity Vulnerabilities in Industrial Control Systems*, (2011).

[23] ICS-CERT. *Year in Review*, (2014).

[24] CRitical Infrastructure Security AnaLysIS. *Crisalis Project EU, Deliverable D2.2 Final Requirement Definition*.

[25] C. Konstantinou, M. Maniatakos. "Impact of firmware modification attacks on power systems field devices", *6th IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pp. 283–288, (IEEE, 2015).

[26] K. Zetter. *Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid*, (Wired, 2016).

[27] K. H. John, M. Tiegelkamp. *IEC 61131-3: Programming Industrial Automation Systems Concepts and Programming Languages, Requirements for Programming Systems, Decision-Making Aids*, 2nd edition, (Springer Publishing Company, Incorporated, 2010).

[28] J. Weiss. *Protecting Industrial Control Systems from Electronic Threats*, (Momentum Press, 2010).

[29] F. Skopik, P. Smith. *Smart Grid Security: Innovative Solutions for a Modernized Grid*, (Elsevier Science, 2015).

[30] The Wall Street Journal. *Electricity Grid in U.S. Penetrated By Spies*, (2009).

[31] D. Maynor. *Metasploit toolkit for penetration testing, exploit development, and vulnerability research*, (Elsevier, 2011).

[32] N. I. Daud, A. Bakar, K. Azmi, M. Hasan, M. Shafeq. "A case study on web application vulnerability scanning tools", *Science and Information Conference (SAI), 2014*, pp. 595–600, (IEEE, 2014).

[33] A. Greenberg. *New Dark-Web Market Is Selling Zero-Day Exploits to Hackers*, (Wired, 2015).

[34] R. Karri, J. Rajendran, K. Rosenfeld, M. Tehranipoor. "Trustworthy hardware: Identifying and classifying hardware trojans", *Computer*, **(10)**, pp. 39–46, (2010).

[35] N. G. Tsoutsos, C. Konstantinou, M. Maniatakos. "Advanced techniques for designing stealthy hardware trojans", *Proceedings of the 51st Design Automation Conference*, pp. 1–4, (2014).

[36] M. Breeuwsma. "Forensic imaging of embedded systems using jtag (boundary-scan)", *digital investigation*, **3(1)**, pp. 32–42, (2006).

[37] D. Schneider. *USB Flash Drives Are More Dangerous Than You Think*, (IEEE Spectrum, 2014).

[38] S. Skorobogatov. "Flash memory 'bumping' attacks", *Proceedings of Cryptographic Hardware and Embedded Systems*, pp. 158–172, (Springer, 2010).

[39] J. Duffy. *ISP Routers Have Backdoors That Expose User Data*, (Network World, 2010).

[40] H. Bar-El, H. Choukri, D. Naccache, M. Tunstall, C. Whelan. "The sorcerer's apprentice guide to fault attacks", *Proceedings of the IEEE*, **94(2)**, pp. 370–382, (2006).

[41] D. Agrawal, B. Archambeault, J. R. Rao, P. Rohatgi. "The EM sidechannel (s)", *Cryptographic Hardware and Embedded Systems–CHES 2002*, pp. 29–45, (Springer, 2003).

[42] *S.754 - Cybersecurity Information Sharing Act of 2015*.

[43] Massachusetts Institute of Technology (MIT). *The Future of the Electric Grid*, (2011).

[44] United States Government Accountability Office. *GAO-11-117, Electric Grid Modernization*, (2011).

[45] Executive Offcie of the President of the U.S. *A Policy Framework for the 21st Century Grid: Enabling Our Secure Energy Future*, (2011).

[46] ICS-CERT. *Cross-Sector Roadmap for Cybersecurity of Control Systems*, (2011).

[47] European Network and Information Security Agency (ENISA). *Smart Grid Security - Recommendations for Europe and Member States*, (2012).

[48] National Institute of Standards and Technology (NIST). *Nist special publication 800-82, guide to industrial control systems (ics) security*, (2011).

[49] International Society of Automation (ISA). *ISA99 Security Guidelines and User Resources for Industrial Automation and Control Systems*, (2015).

[50] National Institute of Standards and Technology (NIST). *Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security*, (2010).

[51] North American Electric Reliability Corporation (NERC). *High-Impact, Low-Frequency Event Risk to the North American Bulk Power System*, (2010).

[52] North American Electric Reliability Corporation (NERC). *Critical Infrastructure Protection (CIP) standards*, (2007).

[53] J. Hughes. "Harmonization of iec 61970, 61968, and 61850 models", *Electric Power Research Initiative (EPRI) Rep.*, (2006).

[54] S. McLaughlin, C. Konstantinou, X. Wang, L. Davi, A. R. Sadeghi, M. Maniatakos, R. Karri. "The cybersecurity landscape in industrial control systems", *Proceedings of the IEEE*, **PP(99)**, pp. 1–19, (2016).

[55] D. Baigent, M. Adamiak, R. Mackiewicz, G. M. G. M. SISCO. "Iec 61850 communication networks and systems in substations: an overview for users", *SISCO Systems*, (2004).

[56] S. Fries, H. J. Hof, M. Seewald. "Enhancing iec 62351 to improve security for energy automation in smart grid environments", *Internet and Web Applications and Services (ICIW), 2010 Fifth International Conference on*, pp. 135–142, (IEEE, 2010).

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

[58] K. Lab. *Cybethreats to ICS systems: You don't have to be a target to become a victim*, (2014).

[59] X. Wang, C. Konstantinou, M. Maniatakos, R. Karri. "Confirm: Detecting firmware modifications in embedded systems using hardware performance counters", *Proceedings of the 34th IEEE/ACM International Conference on Computer-Aided Design*, pp. 544–551, (2015).

[60] J. D. Osborn, D. C. Challener. "Trusted platform module evolution", *Johns Hopkins APL technical digest*, **32(2)**, p. 536, (2013).

[61] T. Alves, D. Felton. "Trustzone: Integrated hardware and software security", *ARM white paper*, **3(4)**, pp. 18–24, (2004).

[62] NIST. *Measurement challenges and opportunities for developing Smart Grid testbeds*, (2014).

[63] A. Keliris, C. Konstantinou, N. G. Tsoutsos, R. Baiad, M. Maniatakos. "Enabling multi-layer cyber-security assessment of industrial control systems through hardware-in-the-loop testbeds", *2016 21st Asia and South Pacific Design Automation Conference (ASP-DAC)*, pp. 511–518, (IEEE, 2016).

[64] M. Zeller. "Myth or realitydoes the aurora vulnerability pose a risk to my generator?", *Protective Relay Engineers, 2011 64th Annual Conference for*, pp. 130–136, (IEEE, 2011).

[65] A. Srivastava, T. Morris, T. Ernster, C. Vellaithurai, S. Pan, U. Adhikari. "Modeling cyber-physical vulnerability of the smart grid with incomplete information", *Smart Grid, IEEE Transactions on*, **4(1)**, pp. 235–244, (2013).

[66] "IEEE standard test access port and boundary scan architecture", *IEEE Std 1149.1-2001*, pp. 1–212, (2001).

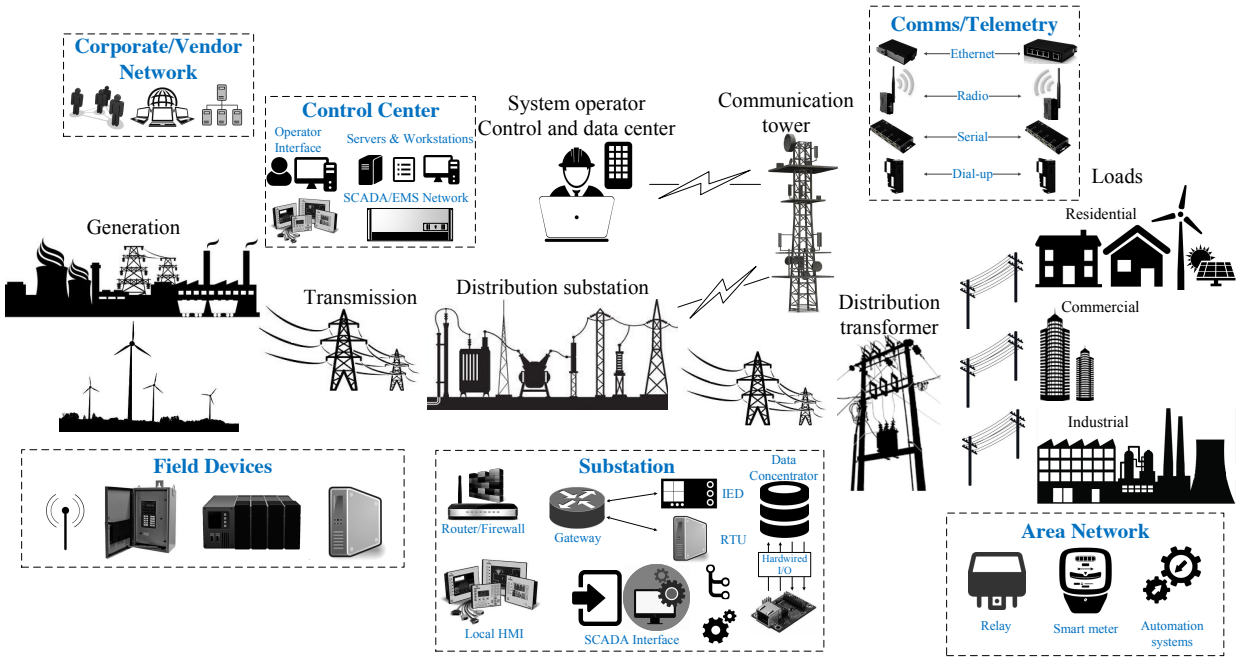

Figure 15.1. *The smart grid structure equipped with cyber systems (dashed line boxes).*

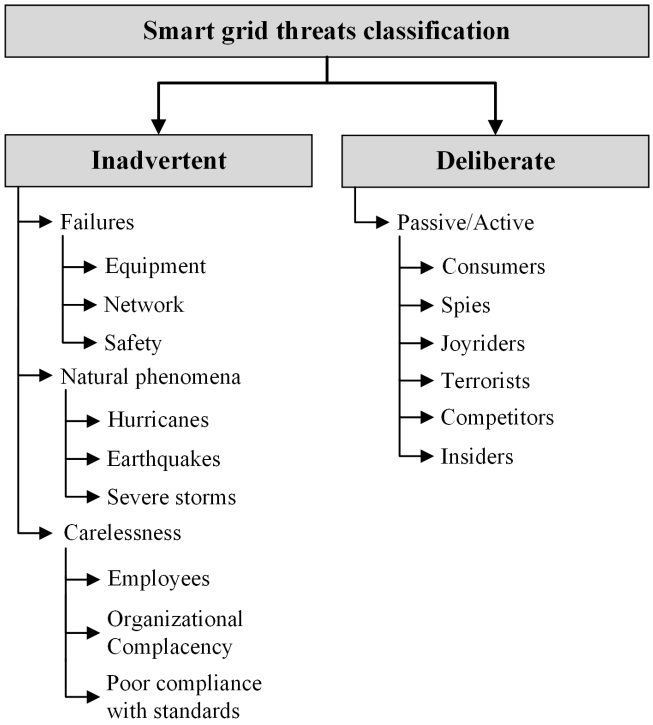

Figure 15.2. *Security threats classification.*

Figure 15.3. *Steps of attack methodologies.*

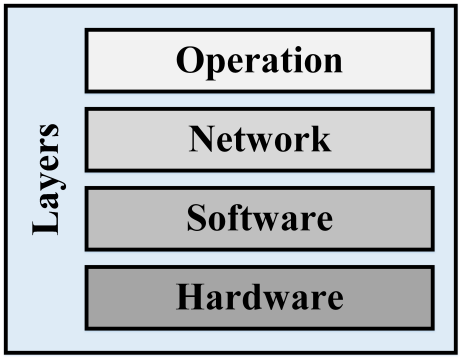

Figure 15.4. *Layered smart grid architecture.*

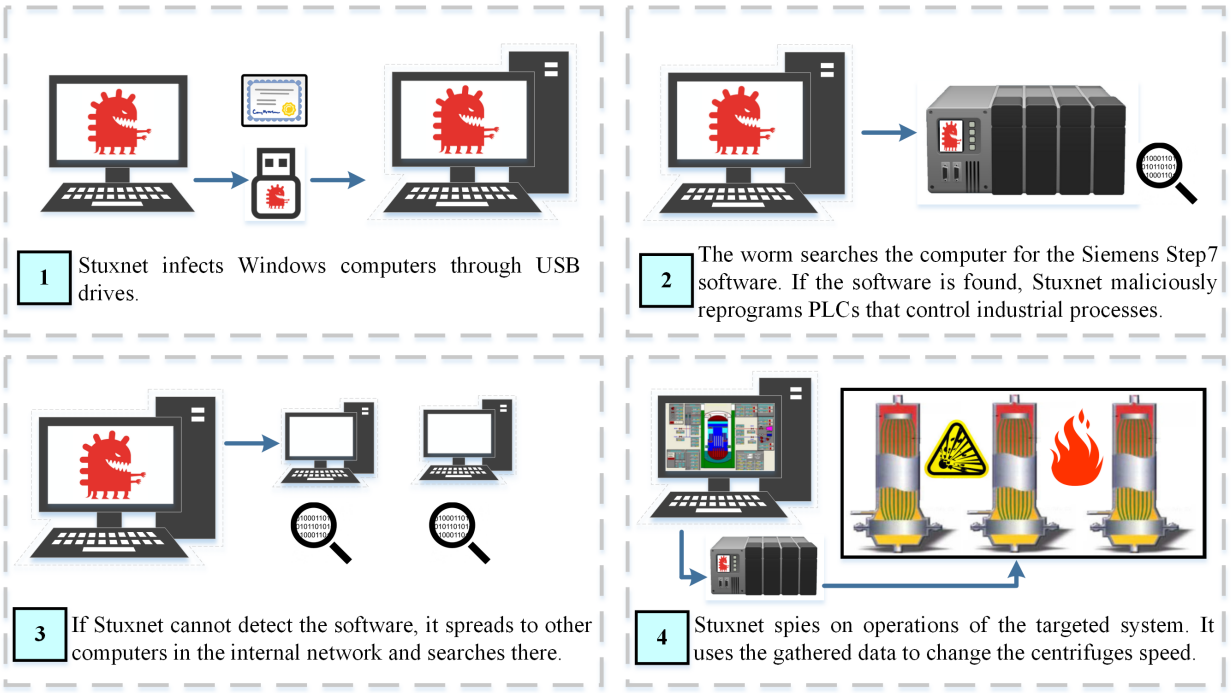

Figure 15.5. *Attack strategy of Stuxnet.*

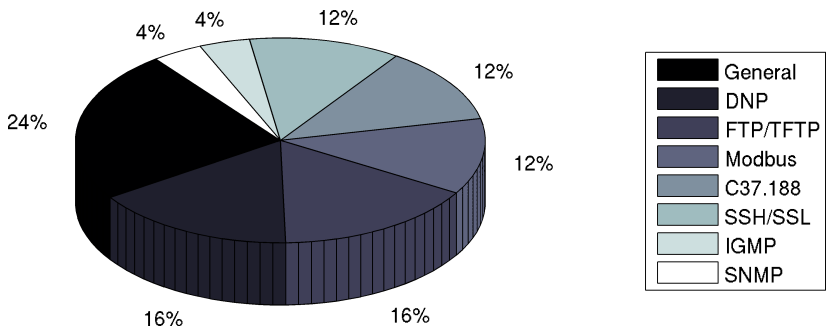

Figure 15.6. *ICS/SCADA protocol vulnerabilities (2013).*

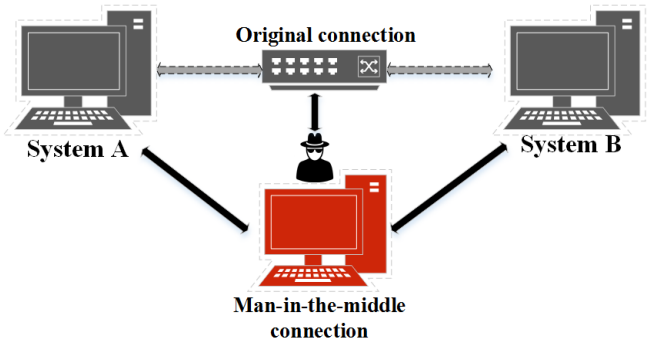

Figure 15.7. *An illustration of the Man-in-the-Middle attack.*

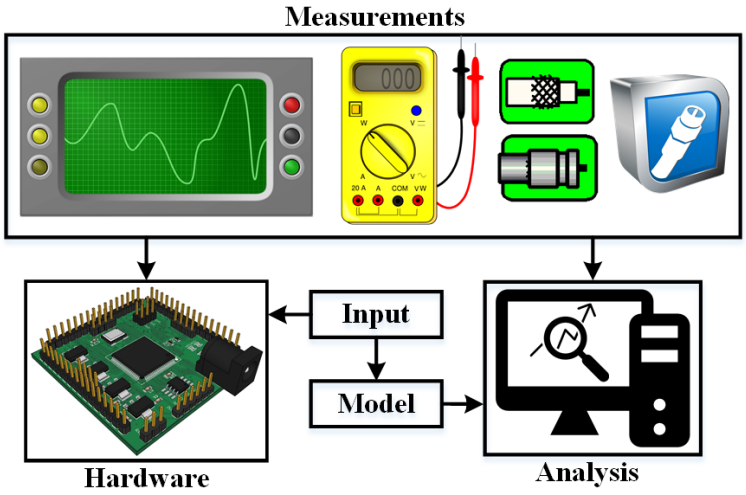

Figure 15.8. *Side-channel attack methodology: it compares observations of the side-channel measurements (e.g. timing information, power dissipation, etc.) with model estimations of the leakage.*

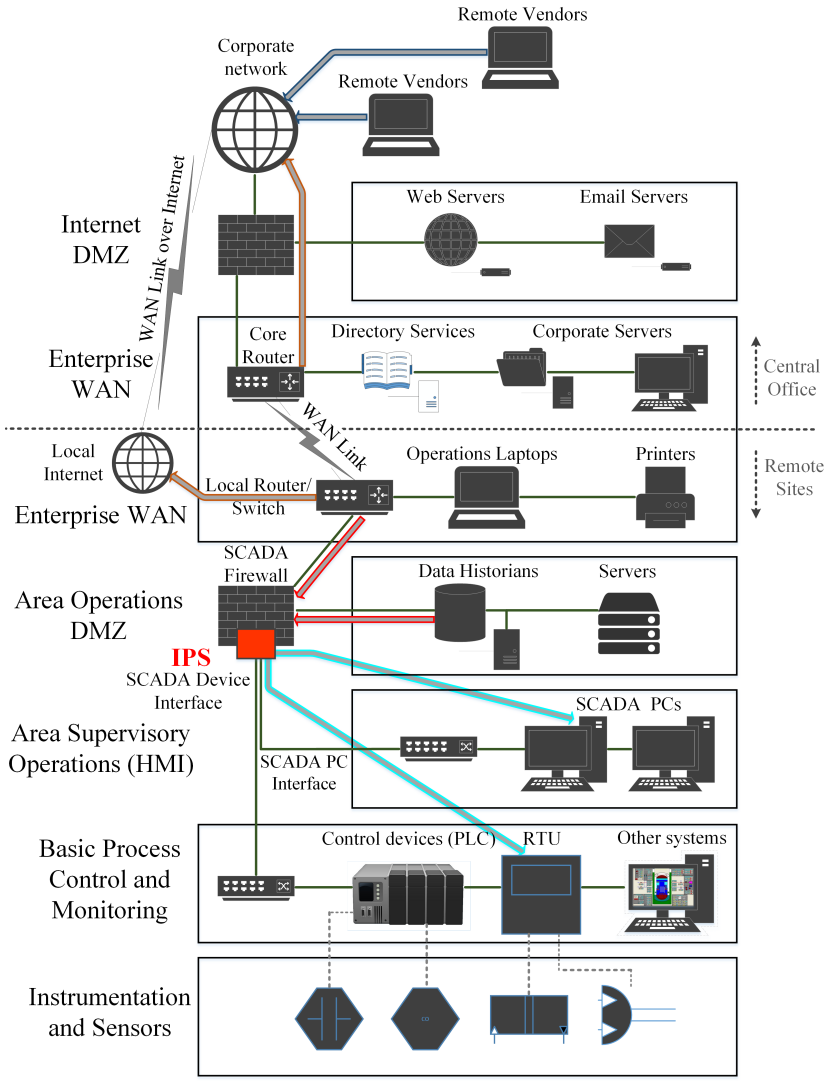

Figure 15.9. *The use of Intrusion Prevention System (IPS) technology in different levels of smart grid networks.*

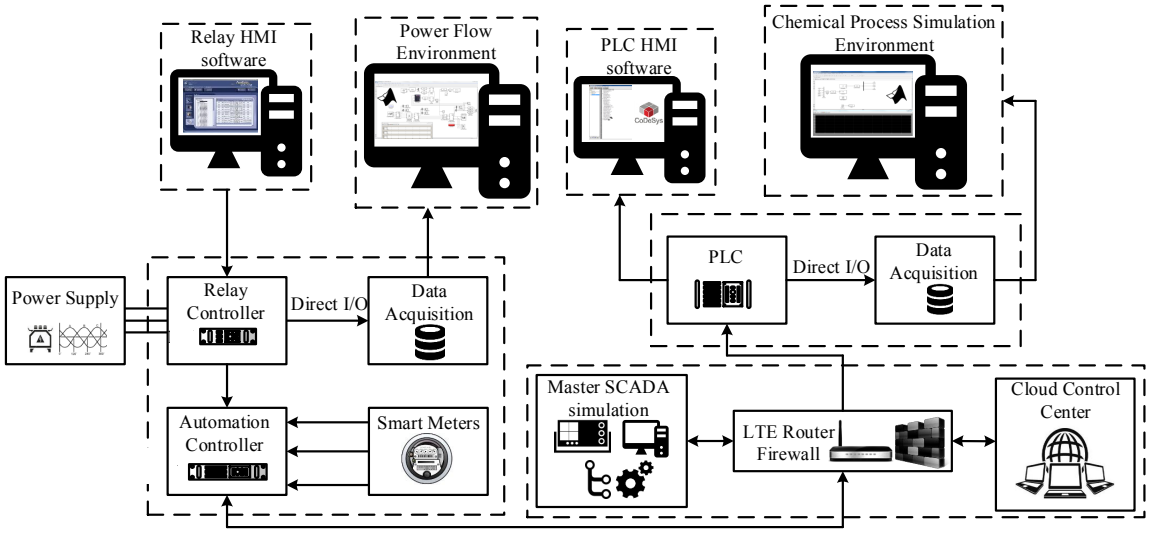

Figure 15.10. *Diagram of a sample smart grid testbed.*

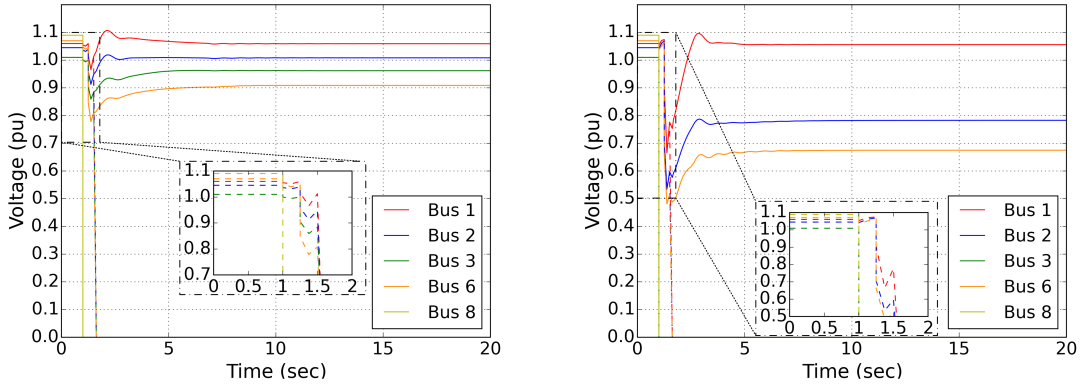

Figure 15.11. *Generators bus voltage due to (a) N-1 (G5) and (b) N-2 (G5, G3) generator aurora-type contingencies [scenario* 1*a (solid line), scenario* 1*b (dotted line)].*

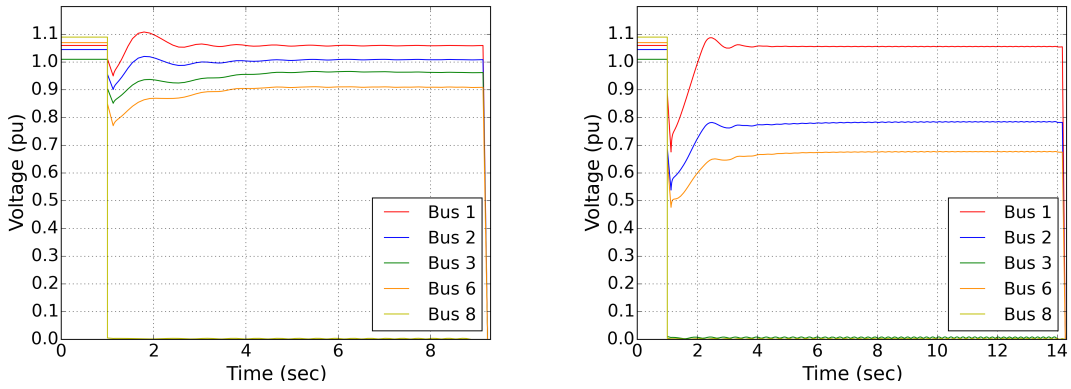

Figure 15.12. *Generators bus voltage due to (a) N-1 (G5) and (b) N-2 (G5, G3) generator fault-clearing failure contingencies.*

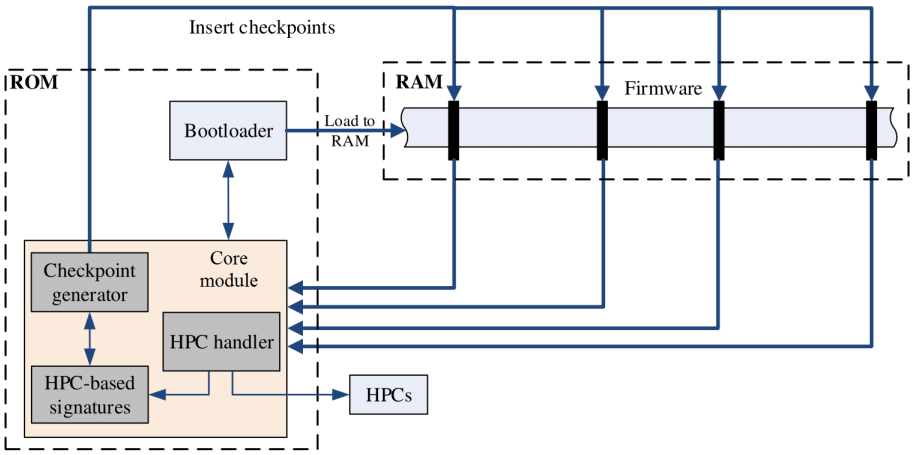

Figure 15.13. *High-level structure of the security module. The core consists of three components: an insertion module that inserts checkpoints to the monitored firmware, an HPC handler that drives the HPCs and a database that stores valid HPC-based signatures.*

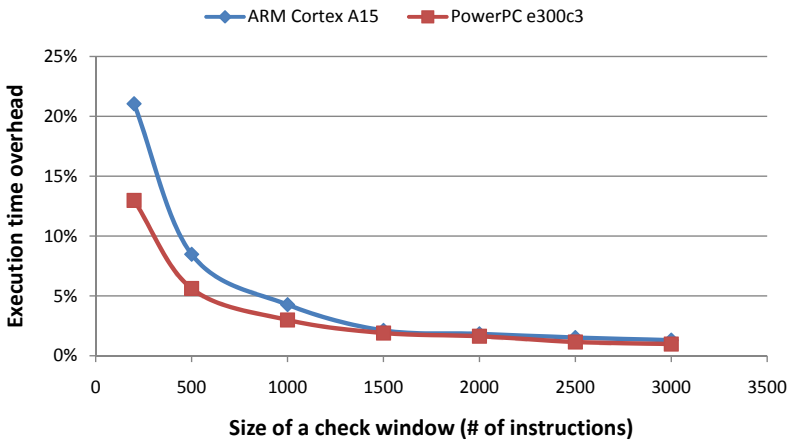

Figure 15.14. *The execution time overhead with different sizes of check windows in terms of number of total instructions.*