Cyber-Attacks Related to Intelligent Electronic Devices and Their Countermeasures: A Review

Jingyu Wang [1], Dongyuan Shi [2]
State Key Laboratory of Advanced Electromagnetic Engineering and Technology
Hubei Electric Power Security and High Efficiency Key Laboratory
School of Electrical and Electronic Enginnering, Huazhong University of Science and Technology
Wuhan 430074, China
[1] jywang@hust.edu.cn, [2] dongyuanshi@hust.edu.cn

***Abstract*—Intelligent electronic devices (IEDs) are deployed in power systems to facilitate advanced automation for controlling critical equipment. Once an IED is compromised, attackers can seize the control of the physical entities in substations. They may interrupt the normal functioning of switch devices, sabotage primary equipment and manipulate measurements to impact the stability of power supply. If multiple correlative attacks are launched simultaneously, attackers may even cause cascading failures, whose consequences are often catastrophic. In this paper, a systematic review of cyber-attacks related to IEDs and their countermeasures is provided. By retrieving relevant research, the information including potential threat vectors, attack types, and defense countermeasures are analyzed. The primary purpose of this paper is to remind the researchers and engineers of up-to-date attacks and to inspire studies on countermeasures to protect IEDs and ensure power system cybersecurity.**

Keywords—intelligent electronic device, cybersecurity, threat vector, cyber-attack, defense countermeasure

I. Introduction

Intelligent electronic devices (IEDs) have been widely deployed in smart substations to improve the automation level of the power transmission process. Typical IEDs include digital relays, fault recorders, and controllers for circuit breakers, capacitor banks, tap changers, and other equipment. Phasor measurement functions are also embedded in some IED products [1]. These microprocessor-based devices receive measurement data from sensors and operate under the regulation of setting files. It is common that several IEDs work collaboratively to finish some tasks. For example, once a digital relay senses the current is surpassing the setting values, its protection function will be activated to trigger the circuit breaker controller to cut off the faulted line to maintain the stability of the power system. To promote interoperability, IEDs produced by different manufacturers often support some nonproprietary protocols, such as Modbus, DNP3, IEC 61850, IEC 60870-5, etc. These protocols allow data to be encapsulated as TCP/IP packets. High speed switched Ethernet is applied to provide routes for data frames to flow over a substation. Control centers and other users like manufacturers need remote access to monitor and manage these devices. Routers and firewalls are thus used to enable the communications from substations to remote users and to isolate private communications from outer traffics.

Using Ethernet and TCP/IP based communications makes IEDs smoother to collect data and issue control. However, at the same time, it will force IEDs open to the Internet or the vast private wide-area networks (WAN). It is no wonder that potential vulnerabilities which can be exploited to launch cyber-attacks exist in power systems, given the vast spatial scale and complex management hierarchy. In fact, the likelihood for cyber-attacks against power utilities is growing in both sophistication and frequency [2]. Multiple successful attacks have occurred in Ukraine, including the attacks in Kiev and the Ivano-Frankivsk region in 2015 and the attack against Ukrenergo in 2016 [3] [4]. Besides, 236 cyber incursions into American and Canadian energy sectors were reported from 2013 to 2015, despite that they all finally fail to disrupt the normal operations [5]. The increasing trend of cyber-attacks has inspired the industry and academia to research in this field.

Although numbers of related papers have been published in recent years, they mostly focus on some specific issues in certain aspects of IED cybersecurity. In this paper, a systematic review which summarizes the latest research is provided. In Section II, the threat vectors related to IED hardware, firmware, software, and communications are discussed. Based on these threat vectors, what types of cyber-attacks can be launched to disrupt the normal operations of power systems are given in Section III. Section IV presents the latest development of the defense countermeasures. Section V finally concludes the paper. The primary purpose of this paper is to remind the researchers and engineers of the up-to-date attacks and to inspire future studies of countermeasures to protect IEDs.

II. Potential Threat Vectors

A. Hardware-Related Threat Vectors

Physical tampering is the most direct and deadly threat to IED hardware. Although IEDs are mainly installed in strictly protected substations, authorized insiders are still able to get access to them [6]. Meanwhile, the deployment of unmanned smart substations makes it easier for outsiders to break in. With the aid of some social-engineering techniques or specialized hacking tools such as keystroke emulators, attackers can probably steal the passwords of IEDs and then seize control of these devices [7]. They can grab configuration files or data history logs to gain a better understanding of the controlled grid. They can also reconfigure or even inject false data into IEDs to make them operate abnormally [8]. Since this kind of attacks requires no penetration into the communication networks, it can hardly be detected by conventional intrusion detection systems.

Electromagnetic interference (EI) is regarded as another threat to IEDs. In fact, IEDs are exposed to electromagnetic fields of natural or humanmade sources. It is inevitable for any

This work was supported by the National Natural Science Foundation of China (Grant No. 51777081).

978-1-5386-2910-9/18/$31.00 ©2018 IEEE

electronic device to be impacted by EI, either directly from these radiation sources or via the coupled connections of power, signal, and ground [9]. Attackers can launch some types of attacks like Intentional Electromagnetic Interference (IEMI) to disturb the normal functioning of IEDs [10] [11]. Electromagnetic fault injection can also be used to manipulate the values stored in IED registers [12] [13]. Besides, wireless communication such as Wi-Fi and ZigBee is currently regarded as a cost-effective way to bridge IEDs and substation computers [14] [15]. Since wireless networks operate based on radio transmission, it is more prone to electromagnetic interference issues than wired networks [16].

GPS spoofing and jamming are also two types of threat targeting at IEDs. In a smart substation, GPS is often applied to provide a unique time reference for different IEDs. For digital relays, this reference is used to provide time stamping of waveform data and internal logic events. For fault recorders, time synchronized data can be matched with other information sources to analyze incidents. Besides, as phasor measurement functions are often embedded in IEDs, an accurate grid-wide time reference is crucial for the normal operation of wide-area monitoring, protection, and control. GPS spoofing attempts to deceive a GPS receiver by broadcasting fake GPS signals or by replaying real signals captured elsewhere or at a different time [17]. GPS jamming transmits high-power signals to impede the reception of legitimate GPS signals. Spoofed or jammed GPS clock will mess up the time-synchronization of IEDs [18] [19].

Theft of cryptographic keys used in public/private encryptions is feasible if the keys are stored in non-volatile memories in IEDs. This hardware-based key storage had long been treated as a secure means. However, newly developed methods can reveal these valuable assets by dumping the chips [20]. This theft of keys is even easier if attackers can get scrapped devices since people usually neglect to remove the information storing in the chips before discarding IEDs.

B. Firmware-Related Threat Vectors

Firmware update modification is a common threat related to IED firmware. Vendors often distribute firmware updates from their websites. However, the downloaded updates are not always immune to deliberate modification [21]. Attackers may be able to inject malicious codes after conducting reverse engineering [22] [23]. By installing these manipulated updates, attackers can change the normal input/output (IO) of IEDs or let them halt and repeatedly try to download new versions of updates (reloading death spiral) or even irreversibly damage them through data corruption or misconfiguration [24].

Pin control attack is another type of threat related to IED firmware. The I/O interfaces of an IED are usually controlled by a System on Chip (SoC). SoCs typically employ hundreds of pins connected to the electrical circuit. Some of these pins have a single defined purpose, while others have multiple mutually exclusive functionalities. The pins of SoC are managed by a pin controller, through which one can configure pin multiplexing or the I/O mode of pins by changing the values of a set of registers. However, the alteration of the pin configuration does not trigger any interruption, preventing the IEDs to react to it. This feature can be exploited by attackers to launch pin control attacks to stealthily modifying the physical meaning of the I/O data flows of IEDs [25].

Boot process hijacking becomes a potential cybersecurity threat to IEDs because many high-level protection mechanisms are unable to be executed during the boot process [26]. After a device is turned on, it generally first loads some trusted boot programs stored in its hardware. Subsequent boot processes will then be validated and called one by one until the device is fully started up. Boot process hijacking tries to break the normal boot sequence and install unvalidated firmware or payload to the devices [27] [28].

C. Software-Related Threat Vectors

Payload attack is a kind of threat targeting at the payload control logic in the IEDs. An IED is a high-end programmable logic controller (PLC) designed to execute its control logic in loops. Control logic can be edited with a software application running on a computer. In the case of Stuxnet, the software application Siemens Step 7 on the computer was compromised to inject unexpected logics to the exported PLC payload while returning regular feedbacks to the users [29]. Payload attacks can lurk in IEDs for a long time before they are triggered either by external inputs or outputs of some control logic [30]. They can block control outputs to induce system failures or steal data for further attacks. Some payload attacks can even replicate themselves to other PLCs in the same SCADA network [31].

Ransomware has evolved significantly over the years. It infects computers or other devices, encrypts their contents with robust encryption algorithms, and then demands a ransom to decrypt that data. It has been reported that similar threat can be posed to cause harm to the cybersecurity of PLCs [32] [33]. Once the ransomware is executed on the victim machine, it will grab the ladder logic diagram from the PLC and try to upload it to a remote server. It will also start a countdown that will finally trigger a process to wipe the logic diagram unless the victim pays to cancel the timer and to stop the attack.

Vulnerabilities in human-machine interfaces (HMI) are also common sources of threat. Human-machine interfaces of IEDs usually include operation panels on the devices and web-based or client-based remote control entrances. Vulnerabilities may exist in the HMI-related software, including intentionally left backdoors for debugging ease and unintentional vulnerabilities produced by bad design and coding practices [34]. These vulnerabilities can be exploited to interrupt communications or take the device down completely. Common vulnerabilities in HMI are listed in Table I.

D. Communication-Related Threat Vectors

Sabotage of communication media will interrupt normal transmission of information. Most IEDs support remote access via private wide-area networks. The communication media is susceptible to sabotage due to its large spatial distribution. In some remote areas, it is effortless to cut off a cable or other communication lines to install bypass tapping devices because of the lack of sufficient protection. Besides, for IEDs performing pilot differential protection, it is critical to ensure the reliability and timeliness of the communications between the line-end devices. Nowadays, optical fiber composite overhead ground wires (OPGWs) are widely used for high-voltage power transmission. In addition to human vandalism, tower collapse or wire breakage accidents will result in the loss of efficacy of pilot differential protection [38].

TABLE I. COMMON VULNERABILITIES IN HUMAN MACHINE INTERFACES

Vulnerability	Description
Unchanged default passwords or weak password policies	If **default passwords are left unchanged**, attackers can use login information available in user guides. **Weak passwords** can be cracked by guessing, dictionary attacks or brute-force attacks [35].
Debug features left in the production	**Displaying debug information** will reveal device functionality, allowing attackers to understand the internal behaviors of the devices. **Backdoors** open for the ease of debugging allow attackers to escalate user's rights and access sensitive information.
Weak encryption and exposition of sensitive information	The weak computational capability of smart devices makes them hard to perform computation-intensive tasks. Many devices use **low-complexity encryption** algorithms or **lack encryption** entirely [36]. Network traffic will be exposed to sniffing, spoofing, and manipulation if no encryption is deployed. **Printing plain passwords** directly on the operation panel of IEDs should also be prohibited [37].
Code injection	For web-based remote access pages, attackers may extend the original function by injecting malicious codes, such as **SQL injection** or **XSS execution**.
Bad design and coding practices	**Missing input validation** may lead to a crash if attackers enter out-of-range values that may not be tolerated by the internal design. **Memory leaks or buffer overflow** may be exploited to consume all memory or use unallocated memory to crash the devices. **No limits in utilization rates** may be exploited to exhaust the computational resources. **Integration of untrusted third-party components** may prompt the broadcast of exposed vulnerabilities.

Black or gray holes stand for compromised network nodes. Consider a SCADA network running the DNP3 protocol, where unsolicited messages are reported to notify the occurring exceptions. If a black or gray hole exists in the network, it will drop all or some parts of network packets flowing through them. Since the master cannot anticipate the appearance time of these unsolicited messages, it would be difficult to detect the black or gray hole that stealthily drops data [39]. Moreover, coordinated holes can even be employed to isolate a particular subnet [40].

Rogue nodes are compatible equipment introduced by attackers to pretend as legitimate nodes. A rogue node can read all communications on the network and generate messages, including commands to actuators. Setting up a rogue node is a preliminary step for launching other attacks. In [41], a rogue wireless device is managed to connect to a SCADA network. This device then continuously transmits junk packets to occupy the channel resources, which prevents other devices from sending responses correctly.

Communication protocol vulnerabilities are also threat vectors of IED-involved SCADA network. The vulnerabilities in some nonproprietary protocols used in smart grids, including DNP3, Modbus, IEC 61850, IEC 60807-5, IEC 61400-25, and IEEE C37.118, are listed in Table II. These vulnerabilities can be attributed to the lack of authentication, authorization, integrity, availability, encryption, and confidentiality [42].

TABLE II. VULNERABILITIES IN COMMUNICATION PROTOCOLS

Vulnerability	Description	Existence
Lack of authentication	No authentication mechanisms to judge whether an identity is real or not.	
Lack of authorization	No authorization mechanisms to rule what tasks an identity is allowed to do.	
Lack of integrity	No guarantee of correctness of the data transmission process, which may cause malfunctioning of the control system.	
Lack of availability	No guarantee of the availability of the communications, which may lead to loss of control of power systems.	
Lack of encryption	Transmitted data are transparent that can be captured by attackers.	
Lack of confidentiality	Unauthorized users can achieve secret information of the ICS.	

DNP3 Modbus IEC 60870-5 IEC 61850 IEC 61400-25 IEEE C37.118

III. TYPES OF CYBER-ATTACKS

A. Direct Control of Actuators

If attackers can access to the specifications of a substation, the most straightforward idea for them to launch a cyber-attack may be to disguise themselves as authorized operators and send commands to the actuator IEDs such as circuit breakers. Based on the potential threats discussed in Section II, there are many possible ways to launch this kind of attack. By hacking an actuator, attackers can cause power outages at once. It may even lead to cascading failures if post-fault control strategies do not work as expected. In 2007, Aurora vulnerability was demonstrated by intentionally open and close a breaker to cause out-of-phase contingency of the connected rotating equipment [43]. In the 2015 Ukrainian blackouts, coordinated cyber-attacks are launched by malicious remote operation of the breakers, which was conducted by multiple external humans using either existing remote administration tools at the operating system level or remote industrial control system (ICS) client software via virtual private network (VPN) connections. It is believed that the attackers acquired legitimate credentials before remote access [3]. It is usually disastrous if outages happen concurrently in numerous critical substations [44].

B. Measurement Manipulation Attacks

Many applications in energy management systems, such as automatic generation control, automatic voltage regulation, optimal power flow, and transient stability assessment, rely heavily on accurate measurements to be aware of the situation of power systems to make control decisions. Once the measurements from IEDs are manipulated, unwanted control actions may be taken, which will threaten the stable power supply [45]-[48]. Manual operations may aggravate the impacts if human operators are misled. Two types of typical measurement manipulation attacks, i.e., **false data injection attack** (FDIA) and **replay attack,** are discussed as follows.

Initially aimed at weighted-least-square-based (WLS-based) state estimation, FDIA proposed in [49] rapidly became one of the most popular topics on power system cybersecurity. It first stresses that by compromising some strategically selected measurements, attackers can bypass the bad data detection to inject false data to the state estimates. Many pieces of research focus on the attack model and detection methods under some state estimation variants based on either WLS or other principles such as Kalman filter or low-rank decomposition [50]-[52]. FDIAs may even be drawn into the field of electricity markets to help attackers maximize their profits [53].

Replay attack assumes that attackers can hijack the sensors and record their readings for a certain amount of time, and replay them afterward. Displayed normal measurements may make human operators relax their vigilance of contingencies. In

contrast, if human operators see on the screen that a "fault" is happening somewhere and isn't automatically removed, they may think the relay protection system is malfunctioning and may hurry to remove it manually. By misleading automatic control process or human operators, this kind of attack can cause severe consequences to power systems [54]-[56].

C. Resource Depletion and Response Delaying

Cyber-attacks can also target the communication and computation resources of IEDs. By sending surges of junk packets to IEDs, attackers can not only congest the transmission routes but disable the devices by exhausting their computational capabilities as well [57]-[59]. Thus, legal packets cannot be timely transferred and processed by these devices, which is known as Denial of Service (DoS). Many power system applications are sensitive to latency. For example, remedial action schemes (RASs) detect predetermined system conditions and respond with automatic corrective actions to mitigate the propagation of a small disturbance into a large-scale event. Such actions typically include load or generation shedding and changes in system configurations. RASs are extremely sensitive to time delays and have strict timing requirements, typically in the order of 50ms [60]. Thus, the delay in data transmission will impact the associated physical systems [61].

D. Time Synchronization Attack

Many operations in power grids, such as fault detection, event location, voltage stability monitoring, and traveling wave protection, depend on precise timing information. By applying GPS time as the grid-wide time reference, all IEDs in the smart grid can work synchronously. If attackers can modify the sampling timestamp by interfering with the reception of real GPS signals and introducing forged GPS signals, the mentioned power system applications can no longer work properly [18]. GPS receivers need to compute the clock offset to calibrate the onboard satellite time because the transmission distances of GPS signals are very long. If attackers simulate a rogue GPS signal and cause the GPS receiver of an IED to latch onto the new signal by gradually overpowering the authentic GPS signal, the calculated receiver clock offset may be incorrect [19]. For those IEDs not based on GPS, the loss of time synchronization may also exist due to problematic A/D and D/A conversion [62].

E. Attacks Against Relay Protection Schemes

In addition to just controlling independent relay IEDs, latest research has also paid attention to the carefully planned attacks against relay protection schemes. Bus differential protection is an important relay protection scheme since nodal fault will disconnect large numbers of generators, loads, and lines, and thus cause system instability. By strategically determining the attack area, attackers can maximize their attack expectation [63]. In the newly proposed agent-based relay protection schemes, peer relays exchange information to determine which action should be taken when local relay sensors detect an issue [64]. The communications between these relay IEDs may be aimed at to launch cyber-attacks to trip normal lines [65] [66].

IV. Defense Countermeasures

A. Device-Level Defense

Towards the cyber-attacks directly conducted to IEDs, some research pays attention to the device-level defense mechanisms. Vendors are required to provide products meeting the security regulatory compliance requirements, such as NERC CIP, IEEE 1686, and ISA-99/IEC-62443 [67]. Countermeasures should be added to prevent physical tampering if needed [68]. Control program obfuscation, which introduces extra control variables to prevent reverse engineering, can be applied [69]. Trusted firmware and software can be stored as benchmarks right after updating, which can be used to compare with current version to discover malicious codes [30]. Moreover, side channel analysis of some external factors as power consumption, timing, temperature, and electromagnetic fields may facilitate the discovery of behavior deviations, which can be used to detect firmware or software modifications [70].

B. Network-Level Defense

Cyber-attacks taking advantage of the vulnerabilities similar to those in computer networks can be mitigated by adopting some general countermeasures, e.g., firewalls, antivirus software, regular patching, etc. Novel techniques in computer science, such as new encryption algorithm for preventing manipulation and IP hopping technique for defending against DoS attacks can be employed to strengthen cybersecurity in SCADA network with IEDs. However, these techniques are not entirely adequate for dealing with the attacks leveraging vulnerabilities in IED-specific protocols. Studies are carried out on intrusion detection systems (IDSs) that can not only understand IED-related protocols but also take power system background knowledge of into consideration [71]-[73]. Many works further focus on using machine-learning-based methods to extract signatures from communication traffics to detect illegal behaviors [74]-[75]. Except for IDSs, putting honeypots in the networks to lure the attackers into aiming at these artificial vulnerabilities to expose themselves is another creative method to detect attacks [76].

C. Application-Level Defense

Power system will always be the eventual victim of cyber-attacks related to IEDs. Different from device-level and network-level defense mechanisms, application-level defense countermeasures are proposed based on the enhancement of power system advanced applications. A series of research has been conducted to enable the bad data detection module in state estimation process to detect FDIAs. The proposed methods include protecting a set of basic measurements, placing extra PMUs to increase the observability, etc. [50]. Differences between some power system characteristics under normal and attacked conditions can also be used to develop some application-specific defense countermeasures [45] [55][56][77]. For example, Kullback-Leibler distance is used as a metric to show the deviation degree of the probability distributions of both historical measurements and attacked measurements [78]; the variations in equivalent impedances of transmission lines can also be used to detect PMU data manipulations [79]. Some promising new techniques also deserve more attention. By dynamically changing some of the power system parameters, the so-called moving target defense can increase the knowledge uncertainty and reduce the opportunity window for attackers to conduct FDIAs [80][81]. Blockchain technique can also be used to enhance the self-defensive capability of power systems against measurement manipulation attacks [82]. By introducing

consensus among peer nodes, the efforts to launching successful cyber-attacks are increased.

V. Conclusion

Zero-day vulnerabilities and new types of cyber-attacks are emerging endlessly. Enumerating all existing research in such a short paper is impossible. In this paper, some of the most representative threat vectors are first chosen to be categorized according to their target, i.e., hardware, firmware, and software of IEDs, and the communications between IEDs. In our opinion, these threat vectors are possible technical means to harm the normal operations of certain aspects of power systems. Based on the introduced threat vectors, what types of cyber-attacks can be launched are then discussed. The study of these abstracted attack models bridges the gap between cyber-attacks and physics of power systems. Preventing, detecting, and defending against cyber-attacks will never be a trivial task. Countermeasures should be taken not only on IED device level but also on network and power system application levels. Besides, for power utilities, power system cybersecurity is a comprehensive matter of regulations, management, trustworthiness, and ongoing maintenance. Researchers and engineers should be encouraged to pay more attention to cybersecurity issues related to IEDs to build more secure and stable future power systems.

References

[1] M. Patel, et al., "Real-time application of synchrophasors for improving reliability," North American Electric Reliability Corp., Oct. 2010.

[2] C. Glenn, D. Sterbentz, A. Wright, "Cyber threat and vulnerability analysis of the US electric sector," Idaho National Lab., Aug. 2016.

[3] ICS-CERT, "Alert (IR-ALERT-H-16-056-01): Cyber-attack against Ukrainian critical infrastructure." [Online]. Available: https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01

[4] J. Lamp, C. E. Rubio-Medrano, Z. Zhao and G. J. Ahn, "OntoEDS: Protecting energy delivery systems by collaboratively analyzing security requirements," *3rd IEEE CIC*, San Jose, CA, 2017.

[5] U.S. Department of Energy, "Transforming the nation's electricity system: the second installment of the QER," Jan. 2017.

[6] ICF International, "Electric grid security and resilience: establishing a baseline for adversarial threats, " Jun. 2016.

[7] S. D. Swartz, M. Assante, "Industrial control system (ICS) cybersecurity response to physical breaches of unmanned critical infrastructure sites," SANS Institute, Orlando, FL, Jan. 2014.

[8] D. Formby, S. S. Jung, S. Walters and R. Beyah, "A physical overlay framework for insider threat mitigation of power system devices," *SmartGridComm*, Venice, Italy, 2014, pp. 970-975.

[9] A. I. Tarmizi, M. D. Rotaru and J. K. Sykulski, "Electromagnetic compatibility studies within smart grid automated substations," *49th UPEC*, Cluj-Napoca, Romania, 2014.

[10] W. A. Radasky and R. Hoad, "An overview of the impacts of three high power electromagnetic (HPEM) threats on Smart Grids," *EMC EUROPE*, Rome, Italy, 2012.

[11] A. A. Glazunov, M. Bäckström and B. D. Oakes, "Probability distribution function of the electric field strength from a CW IEMI source," *IEEE Trans. Electromagn. Compat.*, vol. 56, no. 6, pp. 1550-1558, Dec. 2014.

[12] N. Moro, A. Dehbaoui, K. Heydemann, B. Robisson and E. Encrenaz, "Electromagnetic fault injection: towards a fault model on a 32-bit microcontroller," *2013 FTDC*, Santa Barbara, CA, 2013, pp. 77-88.

[13] A. Chattopadhyay, A. Ukil, D. Jap and S. Bhasin, "Towards Threat of Implementation Attacks on Substation Security: Case Study on Fault Detection and Isolation," *IEEE Trans. Ind. Informat.*, Early Access.

[14] S. T. Watt, H. Loehner, S. V. Achanta, A. Kivi, and B. Rowland, "Extending SCADA networks using wireless communication," *PACW Americas Conf.*, Raleigh, NC, 2015.

[15] P. P. Parikh, T. S. Sidhu and A. Shami, "A comprehensive investigation of wireless LAN for IEC 61850-based smart distribution substation applications," *IEEE Trans. Ind. Informat.*, vol. 9, no. 3, pp. 1466-1476, Aug. 2013.

[16] A. Abdrabou and A. M. Gaouda, "Uninterrupted wireless data transfer for smart grids in the presence of high power transients," *IEEE Syst. J.*, vol. 9, no. 2, pp. 567-577, June 2015.

[17] N. O. Tippenhauer, C. Ppper, K. B. Rasmussen, and S. Capkun, "On the requirements for successful GPS spoofing attacks", *CCS'11*, Chicago, IL, 2011, pp. 75-86.

[18] Z. Zhang, S. Gong, A. D. Dimitrovski and H. Li, "Time synchronization attack in smart grid: impact and analysis," *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 87-98, Mar. 2013.

[19] X. Jiang, J. Zhang, B. J. Harding, J. J. Makela and A. D. Domínguez-García, "Spoofing GPS receiver clock offset of phasor measurement units," *IEEE Trans. Power Syst.*, vol. 28, no. 3, pp. 3253-3262, Aug. 2013.

[20] S. Skorobogatov, "Fault attacks on secure chips: From glitch to flash," presented at *Design Security Cryptographic Algorithms Devices*, Albena, Bulgaria, May 2011.

[21] L. Garcia, F. Brasser, M. H. Cintuglu, A. R. Sadeghi, O. Mohammed, and S. A. Zonouz, "Hey, my malware knows physics! Attacking PLCs with physical model aware rootkit," *NDSS*, San Diego, CA, 2017.

[22] A. Cui, M. Costello and S. J. Stolfo, "When firmware modifications attack: a case study of embedded exploitation," *NDSS*, San Diego, CA, 2013.

[23] C. Schuett, J. Butts, and S. Dunlap. "An evaluation of modification attacks on programmable logic controllers," *International Journal of Critical Infrastructure Protection*, vol. 7, no. 1, pp. 61-68, Mar. 2014.

[24] C. W. J DPhil, M. H. Saleem, M. Evanglopoulou, M. Cook, R. Harkness, and T. Barker, "Defending against firmware cyber attacks on safety-critical systems, " *ISSC*, Albuquerque, NM, 2017.

[25] A. Abbasi and M. Hashemi, "Ghost in the PLC: designing an undetectable programmable logic controller rootkit via pin control attack, " *Black Hat EU*, London, UK, 2016.

[26] J. Wurm *et al*., "Introduction to cyber-physical system security: a cross-layer perspective," *IEEE Trans. Multi-Scale Comput. Syst.*, vol. 3, no. 3, pp. 215-227, Jul.-Sept. 1 2017.

[27] O. Arias, J. Wurm, K. Hoang, and Y. Jin, "Privacy and security in internet of things and wearable devices," *IEEE Trans. Multi-Scale Comput. Syst.*, vol. 1, no. 2, pp. 99–109, Apr.-Jun. 2015.

[28] N. Lawson, "Apple iphone bootloader attack," Mar. 2008. [Online]. Available: http://rdist.root.org/2008/03/17/apple-iphone-bootloader-attack

[29] D. Kushner, "The real story of stuxnet," *IEEE Spectrum*, vol. 50, no. 3, pp. 48-53, March 2013.

[30] N. Govil, A. Agrawal, N. O. Tippenhauer, "On ladder logic bombs in industrial control systems, " *CyberICPS & SECPRE*, Oslo, Norway, 2017, pp. 110-126.

[31] R. Spenneberg, M. Brüggemann, and H. Schwartke, "PLC-Blaster: a worm living solely in the PLC, " *Black Hat Asia*, Marina Bay Sands, Singapore, 2016.

[32] P. Paganini, "Schneider Electric, Allen-Bradley, General Electric (GE) and more vendors are vulnerable to ClearEnergy ransomware, " Security Affair, Apr. 2017. [Online]. Available: https://securityaffairs.co/wordpress/57731/malware/clearenergy-ransomware-scada.html

[33] D. Formby, S. Durbha, and R. Beyah, "Out of control: randomware for industrial control systems," *RSA Conf.*, San Francisco, CA, 2017.

[34] P. E. Weerathunga and A. Cioraca, "The importance of testing smart grid IEDs against security vulnerabilities," *CPRE*, College Station, TX, 2016.

[35] A. Keliris, C. Konstantinou, and M. Maniatakos, "GE multilin SR protective relays passcode vulnerability," *BlackHat US*, Las Vegas, NV, 2017.

[36] J. Wurm, O. Arias, K. Hoang, A.-R. Sadeght, and Y. Jin, "Security analysis on consumer and industrial IOT devices," *ASPDAC*, Macau, China, 2016, pp. 519–524.

[37] S. Ward *et al*., "Cyber Security Issues for Protective Relays; C1 Working Group Members of Power System Relaying Committee," *IEEE PESGM*, Tampa, FL, 2007.

[38] IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities, IEEE Standard 1686-2013, 2013.

[39] D. H. Shin, J. Koo, L. Yang, X. Lin, S. Bagchi and J. Zhang, "Low-complexity secure protocols to defend cyber-physical systems against network isolation attacks," *CNS*, National Harbor, MD, 2013, pp. 91-99.

[40] N. M. Torrisi, O. Vuković, G. Dán and S. Hagdahl, "Peekaboo: a gray hole attack on encrypted SCADA communication using traffic analysis," *SmartGridComm*, Venice, Italy, 2014, pp. 902-907.

[41] B. Reaves and T. Morris, "Discovery, infiltration, and denial of service in a process control system wireless network," *2009 eCrime Researchers Summit*, Tacoma, WA, 2009.

[42] Y. Xu, Y. Yang, T. Li, J. Ju and Q. Wang, "Review on cyber vulnerabilities of communication protocols in industrial control systems," *IEEE EI2*, Beijing, China, 2017.

[43] D. Salmon, M. Zeller, A. Guzmán, V. Mynam, and M. Donolo, "Mitigating the Aurora vulnerability with existing technology," *64th GATech PRC*, Atlanta, GA, 2010.

[44] R. Bulbul, C. W. Ten and A. Ginter, "Cyber-contingency evaluation for multiple hypothesized substation outages," *ISGT*, Washington, DC, 2014.

[45] S. Sridhar and M. Govindarasu, "Model-based attack detection and mitigation for automatic generation control," *IEEE Trans. Smart Grid*, vol. 5, no. 2, pp. 580–591, Mar. 2015.

[46] B. Chen, K. L. Butler-Purry, and D. Kundur, "Impact analysis of transient stability due to cyber attack on facts devices," *NAPS*, Manhattan, KS, 2013.

[47] Q. Yang et al., "Toward data integrity attacks against optimal power flow in smart grid," *IEEE IoT J.*, vol. 4, no. 5, pp. 1726-1738, Oct. 2017.

[48] A. Anwar, A. N. Mahmood, M. Ahmed, "False data injection attack targeting the LTC transformers to disrupt smart grid operation," *ICST & SecureComm*, Beijing, China, Sep. 2014, pp. 252-266.

[49] Y. Liu, P. Ning and, M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *CCS'09*, Chicago, IL, 2009, pp. 21-32.

[50] G. Liang, J. Zhao, F. Luo, S. R. Weller and Z. Y. Dong, "A Review of False Data Injection Attacks Against Modern Power Systems," *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1630-1638, July 2017.

[51] Q. Yang, L. Chang, W. Yu, "On false data injection attacks against Kalman filtering in power system dynamic state estimation," *Security Comm. Networks*, vol. 9, no. 9, pp. 833-849, Jun. 2016.

[52] J. Zhang, Z. Chu, L. Sankar, O. Kosut, "False data injection attacks on phasor measurements that bypass low-rank decomposition, " *IEEE SmartGridComm*, Dresden, Germany, 2017.

[53] R. Moslemi, A. Mesbahi and J. Mohammadpour Velni, "Design of robust profitable false data injection attacks in multi-settlement electricity markets," *IET Generation, Transmission & Distribution*, vol. 12, no. 6, pp. 1263-1270, Mar. 2018.

[54] Y. Mo and B. Sinopoli, "Secure control against replay attacks," *47th Annual Allerton Conf. Comm., Control, and Comp.*, Monticello, IL, 2009, pp. 911-918.

[55] M. Ma, P. Zhou, D. Du, C. Peng, M. Fei, H. M. AlBuflasa, "Detecting replay attacks in power systems: a data-driven approach, ". *LSMS & ICSEE*, Nanjing, China, 2017.

[56] T. Irita and T. Namerikawa, "Detection of replay attack on smart grid with code signal and bargaining game," *ACC*, Seattle, WA, 2017, pp. 2112-2117.

[57] R. Kalluri, L. Mahendra, R. K. S. Kumar and G. L. G. Prasad, "Simulation and impact analysis of denial-of-service attacks on power SCADA," *NPSC*, Bhubaneswar, India, 2016.

[58] J. D. Markovic-Petrovic and M. D. Stojanovic, "Analysis of SCADA system vulnerabilities to DDoS attacks," *11th TELSIKS*, Nis, Serbia, 2013, pp. 591-594.

[59] S. Liu, X. P. Liu and A. E. Saddik, "Denial-of-Service (DoS) attacks on load frequency control in smart grids," *ISGT*, Washington, DC, 2013.

[60] A. Ashok, M. Govindarasu and J. Wang, "Cyber-physical attack-resilient wide-area monitoring, protection, and control for the power grid," *Proc. IEEE*, vol. 105, no. 7, pp. 1389-1407, July 2017.

[61] Z. Lu, X. Lu, W. Wang and C. Wang, "Review and evaluation of security threats on the communication networks in the smart grid," *MILCOM*, San Jose, CA, 2010, pp. 1830-1835.

[62] P. M. Corcoran, H. Melvin, "Synchronization issues for smart grids," *ENERGY 2011*, Venice, Italy, 2011, pp. 108-113.

[63] R. Bulbul, Y. Gong, C. W. Ten, A. Ginter and S. Mei, "Impact quantification of hypothesized attack scenarios on bus differential relays," *2014 PSCC*, Wroclaw, Poland, 2014.

[64] K. J. Ross, K. M. Hopkinson and M. Pachter, "Using a Distributed Agent-Based Communication Enabled Special Protection System to Enhance Smart Grid Security," *IEEE Trans. Smart Grid*, vol. 4, no. 2, pp. 1216-1224, June 2013.

[65] M. S. Rahman, H. R. Pota and M. J. Hossain, "Cyber vulnerabilities on agent-based smart grid protection system," *IEEE PESGM*, National Harbor, MD, 2014.

[66] J. Zhang and Y. Dong, "Cyber attacks on remote relays in smart grid," *CNS*, Las Vegas, NV, 2017.

[67] P. E. Weerathunga, "Securing IEDs against cyber threats in critical substation automation and industrial control systems," *CPRE*, College Station, TX, 2017.

[68] S. Skorobogatov, "Physical attacks and tamper resistance," in *Introduction to Hardware Security and Trust*, M.Tehranipoor, C. Wang, Ed., New York, NY: Springer, 2012, pp. 143-173.

[69] S. McLaughlin and P. McDaniel, "SABOT: Specification-based payload generation for programmable logic controllers," *CCS'12*, Raleigh, NC, 2012.

[70] Z. H. Basnight, "Firmware counterfeiting and modification attacks on programmable logic controllers", M.S. thesis, Dept. Elec. and Comp. Eng., Air Force Ins. Tech., Wright-Patterson Air Force Base, Ohio, 2013.

[71] Y. Yang, H. Q. Xu, L. Gao, Y. B. Yuan, K. McLaughlin and S. Sezer, "Multidimensional intrusion detection system for IEC 61850-based SCADA networks," *IEEE Trans. Power Del.*, vol. 32, no. 2, pp. 1068-1078, April 2017.

[72] J. Hong and C. C. Liu, "Intelligent electronic devices with collaborative intrusion detection systems," *IEEE Trans. Smart Grid*, Early Access.

[73] G. Koutsandria, V. Muthukumar, M. Parvania, S. Peisert, C. McParland and A. Scaglione, "A hybrid network IDS for protective digital relays in the power transmission grid," *SmartGridComm*, Venice, Italy, 2014, pp. 908-913.

[74] A. Almalawi, X. Yu, Z. Tari, A. Fahad, I. Khalil, "An unsupervised anomaly-based detection approach for integrity attacks on SCADA systems," *Computers & Security*, vol. 46, Oct. 2014, pp. 94-110.

[75] S. Pan, T. Morris and U. Adhikari, "Developing a hybrid intrusion detection system using data mining for power systems," *IEEE Trans. Smart Grid*, vol. 6, no. 6, pp. 3104-3113, Nov. 2015.

[76] K. Wang, M. Du, S. Maharjan and Y. Sun, "Strategic Honeypot Game Model for Distributed Denial of Service Attacks in the Smart Grid," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2474-2482, Sept. 2017.

[77] Y. He, G. J. Mendis and J. Wei, "Real-time detection of false data injection attacks in smart grid: a deep learning-based intelligent mechanism," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2505-2516, Sept. 2017.

[78] G. Chaojun, P. Jirutitijaroen and M. Motani, "Detecting false data injection attacks in ac state estimation," *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2476-2483, Sept. 2015.

[79] S. Pal, B. Sikdar and J. Chow, "Classification and Detection of PMU Data Manipulation Attacks Using Transmission Line Parameters," *IEEE Trans. Smart Grid*, Early Access.

[80] M. A. Rahman, E. Al-Shaer, and R. B. Bobba, "Moving target defense for hardening the security of the power system state estimation," *MTD'14*, New York, NY, Nov. 2014, pp. 59-68.

[81] J. Tian, R. Tan, X. Guan, and T. Liu, "Hidden moving target defense in smart grids," *CPSR-SG*, New York, NY, 2017, pp. 21-26.

[82] G. Liang, S. R. Weller, F. Luo, J. Zhao and Z. Y. Dong, "Distributed Blockchain-based data protection framework for modern power systems against cyber attacks," *IEEE Trans. Smart Grid*, Early Access.