A New Classification of Attacks against the Cyber-Physical Security of Smart Grids

Ghada Elbez, Hubert B. Keller, Veit Hagenmeyer
Institute for Automation and Applied Informatics (IAI)
Karlsruhe Institute of Technology (KIT)
Eggenstein-Leopoldshafen, Baden Württemberg, Germany
{ghada.elbez,hubert.keller,veit.hagenmeyer}@kit.edu

ABSTRACT

Modern critical infrastructures such as Smart Grids (SGs) rely heavily on Information and Communication Technology (ICT) systems to monitor and control operations and states within large-scale facilities. The potential offered by SGs includes an effective integration of renewables, a demand-response action and a dynamic pricing system. The increasing use of ICT for the communication infrastructure of modern power systems offers advantages but can give rise to cyber attacks that compromise the security of the SG. To deal efficiently with the security concerns of SGs, a survey of the different attacks that consider the physical as well as the cyber characteristics of modern power grids is required. In the present paper, first the specific differences between SGs with respect to both Information Technology (IT) systems and conventional energy grids are discussed. Thereafter, the specific security requirements of SGs are presented in order to raise awareness of the new security challenges. Finally, a new classification of cyber attacks, based on the architecture of the SG, is proposed and details for each category are provided. The new classification is distinguished by its focus on the cyber-physical security of the SG in particular, which gives a comprehensive overview of the different threats. Thus, this new classification forms the necessary knowledge-basis for the design of respective countermeasures.

KEYWORDS

Cyber-physical security; attacks; smart grids; classification.

ACM Reference Format:
Ghada Elbez, Hubert B. Keller, Veit Hagenmeyer. 2018. A New Classification of Attacks against the Cyber-Physical Security of Smart Grids. In *ARES 2018: International Conference on Availability, Reliability and Security, August 27–30, 2018, Hamburg, Germany.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3230833.3234689

ABBREVIATIONS

AMI	Advanced Metering Infrastructure
BDD	Bad Data Detection
DDOS	Distributed Denial of Service
DNP	Distributed Network Protocol
DOS	Denial Of Service
FDIA	False Data Injection Attack
ICCP	Inter-Control Center Protocol
ICS	Industrial Control System
ICT	Information and Communication Technology
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IPS	Intrusion Prevention System
IT	Information Technology
MITM	Man-In-The-Middle
PCS	Process Control System
PLC	Programmable Logic Controller
RT	Real-Time
SCADA	Supervisory Control and Data Acquisition
SE	State Estimation
SG	Smart Grid

ARES 2018, August 27–30, 2018, Hamburg, Germany

ACM ISBN 978-1-4503-6448-5/18/08…$15.00
https://doi.org/10.1145/3230833.3234689

1 INTRODUCTION

Smart Grids (SGs) refer to the modern generation of power grids. The upgrade of conventional power grids is mainly based on the integration of ICTs to meet the ever-growing demand on electricity and the dynamic supply [1]. To achieve that goal, SGs integrate renewable energy sources such as wind power, solar power, etc. in the generation phase [13]. Use of Information and Communication Technology (ICT) in the SG will allow a demand-response action that consists in ensuring a balance between energy consumption and demand. Consumers will be able to shift their electricity consumption from peak periods. Electricity providers will as well be able to avoid overloads through the use of smart sensors that detect peak loads and automated switches that reduce power strategically.

Besides bringing considerable advantages, demand-response systems may introduce significant threats related to the security and the privacy of the SG [1]. In fact, the authenticity and integrity of all demand-response events must be verified [30]. A dynamic pricing system provided by utilities to their customers can also be offered by modern SGs. This may help potential electricity and money savings. However, it can also rise concerns regarding the privacy of the consumers [1]. Even though SGs are considered as a promising power delivery infrastructure [23], increased interconnection and communication may lead to new risks and vulnerabilities. To have an overview of the different risks threatening the cyber-physical security of critical infrastructures, different works have been carried out in the past few years. However, most of them have focused on the classification of attacks against Supervisory Control and Data Acquisition (SCADA) systems in general which are used in different processes and not specifically in SGs. Zhu et al. [37] proposed a

classification of cyber-attacks against SCADA systems into attacks on hardware, on software and on the communication stack. Zhu et al. also presented a set of security property goals for SCADA systems. Miller and Rowe [25] proposed a survey of incidents in SCADA systems and critical infrastructures. A description as well as a taxonomy of the different cyber-security incidents was provided. A comprehensive survey of the different tools and testbeds used to simulate attacks on SCADA systems was proposed by Nazir [28]. Simulators of cyber-attacks against SCADA systems were classified into: malware attacks, network attacks, communication protocol attacks, Denial Of Service (DOS) attacks, Man-In-The-Middle (MITM) attacks, False Data Injection Attacks (FDIAs), etc. Nazir et al. presented also different tools used for pentesting as well as Intrusion Detection Systems (IDSs), Intrusion Prevention Systems (IPSs) and honeypots. These taxonomies and surveys were limited to SCADA systems and do not cover the whole attack surface of SGs.

A different taxonomy was proposed by Fleury et al. [10] focusing on attacks against energy control systems. The suggested taxonomy is based on the AVD (Attack-Vulnerability-Damage) model which describes possible ways to exploit vulnerabilities in order to perpetrate an attack resulting in different kinds of damage. Even though the suggested model covers different aspects of attacks in energy control systems, some relevant categories are lacking such as details about the used protocols and/ or operating systems to give a better overview of the cyber-security in energy systems.

In the present paper, a novel classification of cyber-attacks against SGs, based on the SG architecture model, is proposed. The remainder of this paper is organized as follows: the motivation is presented in Section 2 with a survey of the recent incidents in SGs and SCADA systems. Specific features differentiating modern SGs from conventional ones and from IT systems are listed in Section 3. An overview of security requirements to protect SGs against similar incidents is described in Section 4. Section 5 introduces the new classification of attacks against the cyber-physical security of the SG with a detailed description of each category. Finally, conclusions and future research are presented in Section 6.

2 MOTIVATION

As cyber security and privacy issues in the SG are new areas in the field of power industry [23]; there is a need to have an overview of the specificities and the security requirements of the SG. A good understanding of the different threats and risks is essential to deal with the security challenges induced by the highly-interconnected structure of this critical infrastructure. A survey of the various attacks against the cyber-physical security of the SG helps choose suitable techniques to prevent, detect and recover from attacks.

The damage caused by an attack on a critical infrastructure depends on one hand on the vulnerabilities inherent in the components and the communication within the facility, and on the other hand on the motivation, capabilities and interest of the attacker. Recent incidents have shown that adversaries have the required means and the motivation (financial gain, political interests, fame and glory, etc.) to perpetrate attacks against critical infrastructures.

Some of the major cyber attacks against critical infrastructures, in particular SGs, in the recent years are presented in the following:

- In June 2010, a spread of the Stuxnet worm affected SCADA systems mainly in uranium centrifuges in Iran. It targets Siemens applications (PCS7, WinCC and STEP7) and hardware (Siemens S7 Programmable Logic Controller (PLC)). After gaining access to the control system, attackers downloaded malicious code remotely. USB devices and zero-day vulnerability exploits were used to infect the plant. Damage to the plant was caused by the change of the rotational speed of the motors as Stuxnet periodically modifies the variable-frequency drives [35]. More details about attacks against equipment are described in Section 5.1.2.
- On December 23, 2015, the attack perpetrated on an Ukrainian power grid is considered to be the first known successful cyber attack on a power grid. The attackers gained access to three energy distribution companies compromising their information system causing an outage of 7 hours affecting 700.000 residents.
- In December 2016, another attack hit the electrical Ukrainian infrastructure. Hackers took control of a Remote Transmission Unit (RTU) at the substation Pivnichna whose shutdown resulted in an outage of one hour. The two previous attacks were both benign even though it was reported that the consequences on the SG could have been more tragic [14]. It is believed that a modular malware, Industroyer, targeting Industrial Control Systems (ICSs), was used to perpetrate the attack. It enabled attacker to collect valuable information about the system process and even to take direct control of switches and circuit breakers [3].

The reader can find more details about incidents in SCADA systems and critical infrastructures in the survey of Miller and Rowe [25]. Considering the threats targeting SGs, a first step towards ensuring their cyber-physical security is to discern their specific features.

3 SPECIFIC FEATURES OF MODERN SMART GRIDS

The interconnection among the SG and the integration of ICT to improve the power system through two-way communication and power flows results in SGs specific features that differentiate them from IT systems and conventional power grids. Awareness of the particular characteristics of the SG is fundamental to take up the major challenge of securing it.

3.1 Differences from IT Systems

The Smart Grid (SG) security is fundamentally different from regular IT security [20] as the latter targets information whereas the former is focused on the industrial process connected to ICT. Differences between IT and ICSs arise mainly from the connection of control systems with the physical world [4]. The following list covers some of the characteristics of ICSs in comparison with IT systems:

- In contrast to IT security, no frequent patching and updating are possible in existing ICS.
- Long-term and well-tested security mechanisms in legacy systems are not always easy [4].
- SGs may suffer a huge damage subsequent to an attack whereas the damage is mainly local when it comes to general IT systems [1].
- An advantage of industrial networks over conventional ones is that the formers have simpler dynamics [4]. In fact, industrial

networks have a fixed topology, a stable user population, a regular communication patterns and a limited number of protocols.
- In IT networks, IP-based Ethernet protocols are used to connect all devices. In automation networks, different communication protocols such as Distributed Network Protocol (DNP)3, IEC61850, Inter-Control Center Protocol (ICCP), etc. are used which toughen the development of a common host-based or network-based security solutions for the SG [34].

3.2 Differences from Conventional Grids

The increasing need for electricity helped develop SGs as a successor to conventional power grids. Some of the discernible characteristics of the modern SG are listed below:
- Integration of small-scale distributed energy resources for electricity generation in SGs. The fusion of renewable resources with the traditional bulk power generation requires a flexibility in demand that compensates the volatility of supply
- Deployment of smart devices to access timely information
- Use of IT for the control and Real-Time (RT) monitoring of SGs
- Modeling the cyber and the physical systems in Advanced Metering Infrastructure (AMI) and SCADA is challenging [1]
- Coexistence of legacy systems with smart devices may result in incompatibilities and challenges in interdependency modeling

Security requisites may raise confusions when it comes to choose adequate defense techniques. In fact, solutions adopted from IT systems or conventional SG cannot be applied directly in the context of modern SGs to ensure the rising security challenges [4].

4 SECURITY REQUIREMENTS OF SMART GRIDS

Requirements for the cyber-physical security of the SG have been evolving [18] in order to address the challenges raised by the new operational structure of the SG integrating cyber and physical components. The security requirements in conventional power grids were summarized by Aloul et al. [2] as following: human safety, equipment and power lines protection and system protection. However, different security goals emerged to tackle the new threats:

(1) **RT Availability** refers to the accessibility of data or services to authorized parties when required which guarantees an uninterrupted functioning without any unexpected downtime. Contrarily to availability in IT systems, RT availability is tightly related to the dynamics of the physical system [4] in the SG.
(2) **Integrity** deals with protecting the consistency, dependability and authenticity of the information by securing data from unauthorized changes. Integrity in SCADA systems according to [37] includes the trustworthiness of the generated, transmitted, stored and displayed data syntactically and semantically as well as the legitimacy of the sender and the receiver.
(3) **Confidentiality** encompasses all aspects related to the disclosing data to unauthorized parties. Confidentiality is considered less critical than integrity and availability in SG [12].
(4) **Reliability** is the ability of a system to operate without downtimes during a period of time under certain circumstances: redundancy is commonly used to enhance reliability [19].
(5) **Resiliency** refers to the resistance of the SG to disturbances (failures, cyber attacks, natural disasters, etc) and its ability to recover from them while maintaining an acceptable level of service. Resiliency of the SG enhances its reliability.
(6) **Scalability** covers one of the main features of modern critical infrastructures. The SG consists of a large number of devices which is challenging to model for resiliency architecture [1].
(7) **Privacy** refers to considerations related to the protection of transmitted data across the different utilities of the SG. Concerns may arise from AMIs that include information of consumers.
(8) **Safety** includes all policies and protections deployed in the SG to guarantee that humans or facilities of the plant are not affected by harms and/or hazards that cause injury or loss.

5 NEW CLASSIFICATION OF ATTACKS

In this section, we introduce the new classification of cyber attacks against SGs in Figure 1. The Smart Grid Architecture Model (SGAM) - which is a reference model defined by EU Mandate M/490 forthe SG architecture [5] - was used as a classification criterion.

The three chosen categories describe the main layers in the architecture of the SG (see Figure 1) namely: attacks against power and energy systems layer (see Section 5.1), attacks against computer/IT layer (see Section 5.2) and attacks against communication layer (see Section 5.3) were depicted in Figure 1. Each class of cyber attacks is divided in two subcategories. As illustrated in Figure 1, the upper subclass of each category represents mainly vulnerabilities such as buffer overflows in software attacks. Thus, they describe security flaws that an attacker may exploit to launch attacks against one or several layers of the SG. The lower subclass represents cyber attacks that are standalone or may be based on vulnerabilities in the energy system, in the network or in the communication. In the following, details about each category are presented.

5.1 Attacks against Power and Energy Layer in SGs

5.1.1 Attacks against Control Stations. State Estimation (SE) is one of the central functions in Energy Management Systems (EMS). It provides RT data for analysis, control and optimization functions [27] by deducing state variables from measurements collected from the power network of the SG. FDIAs are attacks against SE.

Contrarily to DOS attacks that compromise the availability of resources, FDIAs are a specific case of deception attacks [29] compromising the integrity of control packets or measurements. They were first introduced by Liu et al. [24] who describe them as a malicious measurement introduced by an adversary to dupe the SE process. Despite the existence of mechanisms in power systems against measurement errors, FDIAs were proven to be able to bypass Bad Data Detection (BDD). A well-crafted nonzero vector designed so as not to trigger alarms, is injected into the measurement data to cause a deviation in the vector of the estimated state variables.

Since the pioneer paper of Liu et al. [24], considerable work has been done in creating new injected vectors based on full or partial knowledge of the topology and parameter information of the SG. FDIAs can be classified based on the relation of the line measurements and the states of the power systems as following:
- **DC SE based FDIA** Liu et al. [24] describe how DC SE based FDIA, assuming full knowledge of the grid topology, can be perfectly stealthy to DC SE and bypass BDD mechanisms. When

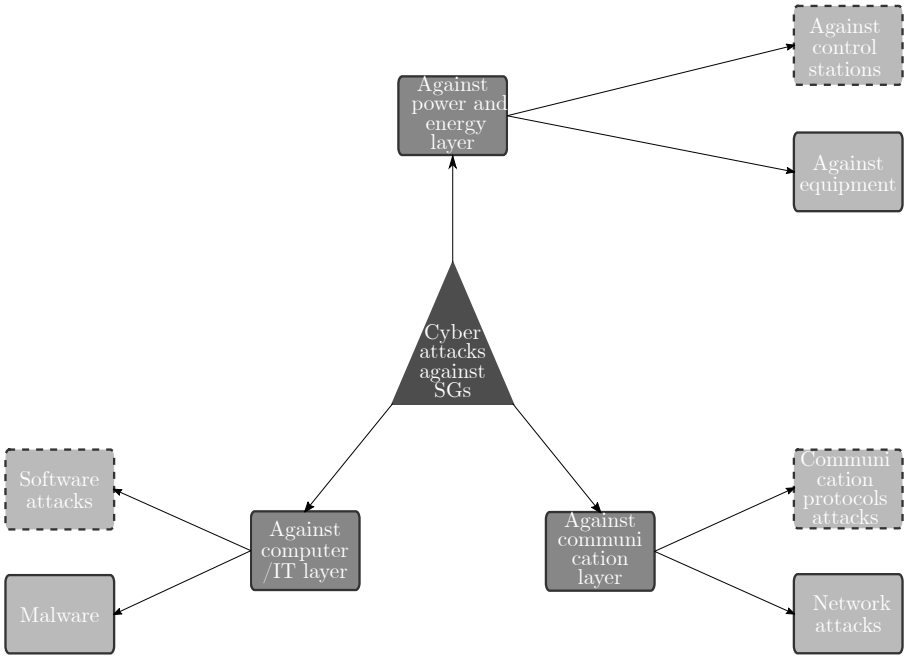

Figure 1: New classification of cyber attacks against SG

constructing the injected vector that contains the false measurements, a linear model of the SE was adopted in order to avoid high computationally demanding nonlinear models. A DC SE based FDIA was presented by Esmalifalak et al. [9] and in which Independent Component Analysis (ICA) was used in order to deduce the Jacobian matrix describing the topology of the power system from line measurements. The same technique was later adopted by Huang et al. [15]. A similar approach was followed by Yu et al. [36] using Principle Component Analysis (PCA) instead, to approximate the Jacobian matrix. Rahman et al. [31] applied a different technique based on collecting online and offline data to construct their FDIA with incomplete information about the SG.

- **AC SE based FDIA** Rahman et al. [32] proved that perpetrating a DC SE based FDIA can be easily detected if a nonlinear state estimator is used. Hug et al. [16] showed also implications of FDIA at Remote Transmission Units (RTU) on DC and AC SE pointing out that the use of a DC model by the attacker presents an advantage for the system operator that is no longer possible in the case of an AC SE based FDIA. Thus, work on AC SE based FDIA is being carried out within the scientific community. Recent work of Chin et al. [7] proposes formal description of necessary conditions to launch a blind AC SE based FDIA. The developed AC SE based FDIA based on a geometric approach, is completely stealthy for DC SE but approximately stealthy for AC SE. AC SE based FDIA is a novel and challenging research topic. For interested readers, a recent and comprehensive review of FDIAs against power systems was presented by Liang et al. in [22].

5.1.2 Attacks against Equipment. Causing physical damage is the utmost goal of an adversary once access to the Process Control System (PCS) has been gained in order to disturb the normal operation of the running process. A list of the different attacks against physical facilities was presented by Larsen [21]:

- **Inertial Attacks** are caused by operating speed variation of heavy equipment which is the most common cause of physical failure in large processes.
- **Exclusion Attacks** occur when physical interconnections in a PCS are broken.
- **Resonance Attacks** are provoked when an adversary induces repeatedly small variations until reaching the resonance.
- **Wear Attacks** are carried out by introducing malicious commands in the PCS to decrease the lifespan of the equipments.
- **Surge Attacks** damage equipment by exceeding boundaries of process variables or result in DOS due to emergency shutdowns.
- **Latent Abilities Attacks** consist in exploiting unused latent abilities of some equipment in order to cause a physical damage.

5.2 Attacks against Computer/IT Layer in SGs

5.2.1 Software Attacks. Software used in ICS is assumed to be built upon trustworthy algorithms. However, vulnerabilities may raise from the implementation [19] as well as from the programming language used in control applications [37].

Some software related attacks are presented in the following:

- **Buffer Overflows** are common exploits consisting in storing data in a buffer beyond its capacity to replace existing code with a malicious one. They can target servers in SCADA systems

but also field devices running RTOS systems [37] where fixed memory allocation time requirements can be used by attackers.
- **Format String Vulnerabilities** are bugs that allow to specify format string to format function [33] which may result in writing malicious values in a specific memory address.
- **Dangling Pointers** point to an invalid memory i.e. a deallocated memory that used to hold an object before deletion.
- **SQL Injections** are malicious SQL statements to manipulate databases and historians and lead to catastrophic damage [37].

5.2.2 Malware. Malware are malicious software exploiting vulnerabilities in ICT used extensively in ICS. Due to the spread of malware, a distinct subcategory was allocated to them. Consequences of malware propagation in a simulated SCADA system were demonstrated by Fovino et al. [11]. In the following, some of the main types of malware are shortly stated for the sake of completeness:
- **Virus** is a malware that replicates itself and spread among hosts on the same network. Attached to a legitimate program, it may modify the system software and corrupt data unnoticeably.
- **Worm** is a self-replicating stand-alone malicious program. It may exploit vulnerabilities on targets to spread on the network.
- **Trojan** is a malware that resembles to a legitimate software to mislead a user into executing it. In fact, trojans spread via interaction with the user contrarily to worm and viruses.
- **Malicious Bot** is a malware that executes automated tasks interacting with other network services. A botnet is a network of compromised hosts used to cast broad-based attacks.

5.3 Attacks against Communication Layer in SGs

5.3.1 Communication Protocols Attacks. The communication structure of the SG may have security flaws [34]. Existing communication protocols such as Modbus, Profibus, DNP3, ICCP do not integrate security solutions [23]. Some attacks targeting communication protocols in the SG is presented in the following.
- **Modbus** is a widely used protocol in ICSs. As Modbus was not designed with integrated security solutions, it may encounter several attacks that were presented in details by Huitsing et al. [17] and that we will summarize in the following. Slave reconnaissance targets confidentiality as it allows the interception of information from field devices. Direct slave control implies however the fabrication of a replacement of a legitimate master to take control of one or more field devices. Response delay consists in delaying response messages of slave devices to deliver out-of-date information to the master. Rogue interloper involves attacking a computer with the appropriate (serial or Ethernet) adapters to an unprotected communication link. More examples of Modbus/TCP protocol attacks can be found in [6].
- **Distributed Network Protocol (DNP)3** is a protocol widely used for the SCADA communication in North America and Asia. Different attacks may target the DNP3 protocol as no encryption nor authentication are used [8]. Passive network reconnaissance consists in gathering information about network topology and device functionality via capturing DNP3 messages. Baseline response replay includes fabrication of a master and simulation of responses of devices to master when adversary have knowledge of normal DNP3 traffic patterns. Rogue interloper occurs if attacker installs a MITM device between the master and substations to read, modify and fabricate DNP3 traffic.
- **IEC 61850** is a standard recommended by the International Electrotechnical Commission (IEC) for Ethernet-based communications in automated substations. It has some security mechanisms described in IEC 62351-4 and IEC 62351-6. However, multicast protocols (Generic Object Oriented Substation Event and Sample Values) used in IEC 61850 may be subject to spoofing, DOS, etc.
- **Inter-Control Center Protocol (ICCP)** is a data sharing protocol used to exchange time-critical data between control centers but also with business partners. ICCP can be exploited to create buffer overflows as presented in LiveData ICCP server [37].

5.3.2 Network Attacks. Heterogeneous networking technologies are used in SG. Injection and modification attacks can easily affect wireless networks without appropriate routing. Inherent security flaws may affect applications built on Internet. Data transmitted via the sensor network may be subject to spoofing, and modification affecting the normal functioning of the SG. More details about networking problems and possible solutions can be found in [23].
- **Denial Of Service (DOS)/ Distributed Denial Of Service (DDOS) Attacks.** DOS attacks refers to the inability of a legitimate user to access a resource or a network due to malicious actions. The adversary deploys multiple machines each sending small streams of attack traffic to compromise a specific target. In a SG, DOS and DDOS may target smart meters, networking devices, communication links and utility business servers [26]. DOS attacks compromise the availability of resources by, for instance, jamming the communication between two hosts. To cite just a few of the well-known DOS and DDOS:
  - **TCP-SYN Flood Attack** is based on the conventional structure of a TCP connection as it generates a large number of half-open TCP connection (before receiving the reply packet with SYN/ACK from the server) resulting in an over-consuming of the available resources.
  - **Ping of Death** consists in sending a malformed ICMP packet that contains a large size of data to a target host that gets over-flooded when trying to respond.
  - **ICMP/UDP Flood Attack** occurs when a large number of ICMP/UDP packets are sent to a host resulting to the latter overload due to massive responses.

  Another type of DOS attacks can exploit the connectivity of the network by flooding it with high volume of connections that consumes the OS resources. Those attacks can also cause data to be lost or delayed in reaching the destination [1]. Out-of-date data can lead to wrong control commands computed with erroneous SE. Contrarily to conventional IT systems where DOS attacks do not typically have significant negative consequences if managed timely, in ICS, DOS attacks may lead to disasters [26].
- **MITM Attacks.** MITM attacks occur when an adversary intercepts traffic between two hosts without their knowledge. Data intercepted can be sent and/or received by the malicious actor. MITM is a type of eavesdropping exploiting RT processing of data between the affected parties. Encryption may however help deal with MITM attacks.

- **Replay Attacks.** An adversary first captures valid packets transmitted between targets via MITM attacks and then replays them, with or without modification, against the victims. However, in both cases, this may disrupt or even damage the network.

6 CONCLUSIONS AND FUTURE WORK

The interconnected nature of the Smart Grid (SG) introduces vulnerabilities, that when exploited by attackers, may result in catastrophic consequences. In this light, a new classification of cyber-attacks is proposed in the present paper to unveil the various threats that endanger the SG. The suggested categories are based on the different layers of the Smart Grid Architecture Model (SGAM). We distinguish three categories of attacks. The first one groups attacks against power and energy layer. The second one consists of attacks against the computer/IT layer. Attacks against communication protocols are grouped in the third category. The new classification proposed in the present contribution provides a perspective on cyber-physical security of the SG and forms the necessary knowledge basis for mastering the current security challenges . Future work will include a further extension of the new classification to include attacks against regulations and market as well as proposing adequate counter-measures towards protecting the SG against the investigated cyber-attacks.

ACKNOWLEDGEMENT

This research was partially supported by the Federal Ministry of Education and Research (BMBF) within the framework of the project "Neue EnergieNetzStruktURen für die Energiewende" ENSURE (FKZ 03SFK1N0).

REFERENCES

[1] Ehab Al-Shaer and Mohammad Ashiqur Rahman. 2016. *Security and Resiliency Analytics for Smart Grids.* Springer. https://doi.org/10.1007/978-3-319-32871-3

[2] Fadi Aloul, AR Al-Ali, Rami Al-Dalky, Mamoun Al-Mardini, and Wassim El-Hajj. 2012. Smart grid security: Threats, vulnerabilities and solutions. *International Journal of Smart Grid and Clean Energy* 1, 1, 1–6.

[3] Robert Lipovsky Anton Cherepanov. 2017. (2017). https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf

[4] Alvaro A Cárdenas, Saurabh Amin, Zong-Syun Lin, Yu-Lun Huang, Chi-Yen Huang, and Shankar Sastry. 2011. Attacks against process control systems: risk assessment, detection, and response. In *Proceedings of the 6th ACM symposium on information, computer and communications security.* ACM, 355–366.

[5] Smart Grid Coordination CEN-CENELEC-ETSI. 2015. Group: Smart grid reference architecture (November 2012). *URI: https://ec. europa. eu/energy/sites/ener/files/documents/xpert_group1_reference_architecture. pdf.*

[6] Bo Chen, Nishant Pattanaik, Ana Goulart, Karen L Butler-Purry, and Deepa Kundur. 2015. Implementing attacks for modbus/TCP protocol in a real-time cyber physical system test bed. In *Communications Quality and Reliability (CQR), 2015 IEEE International Workshop Technical Committee on.* IEEE, 1–6.

[7] W. L. Chin, C. H. Lee, and T. Jiang. 2017. Blind False Data Attacks against AC State Estimation based on Geometric Approach in Smart Grid Communications. *IEEE Transactions on Smart Grid*, 1–1. https://doi.org/10.1109/TSG.2017.2708114

[8] Samuel East, Jonathan Butts, Mauricio Papa, and Sujeet Shenoi. 2009. A Taxonomy of Attacks on the DNP3 Protocol. *Critical Infrastructure Protection III*, 67–81.

[9] M. Esmalifalak, H. Nguyen, R. Zheng, and Zhu Han. 2011. Stealth false data injection using independent component analysis in smart grid. In *2011 IEEE International Conference on Smart Grid Communications (SmartGridComm).* 244–248. https://doi.org/10.1109/SmartGridComm.2011.6102326

[10] Terry Fleury, Himanshu Khurana, and Von Welch. 2008. Towards a taxonomy of attacks against energy control systems. In *International Conference on Critical Infrastructure Protection.* Springer, 71–85.

[11] Igor Nai Fovino, Andrea Carcano, Marcelo Masera, and Alberto Trombetta. 2009. An experimental investigation of malware attacks on SCADA systems. *International Journal of Critical Infrastructure Protection* 2, 4, 139 – 145. https://doi.org/10.1016/j.ijcip.2009.10.001

[12] NIST Smart Grid. 2010. Introduction to NISTIR 7628 guidelines for smart grid cyber security. *Guideline, Sep.*

[13] Veit Hagenmeyer, Hüseyin Kemal Çakmak, Clemens Düpmeier, Timm Faulwasser, Jörg Isele, Hubert B Keller, Peter Kohlhepp, Uwe Kühnapfel, Uwe Stucky, Simon Waczowicz, et al. 2016. Information and Communication Technology in Energy Lab 2.0: Smart Energies System Simulation and Control Center with an Open-Street-Map-Based Power Flow Simulation Example. *Energy Technology* 4, 1, 145–162.

[14] Gregory Hale. 2017. (2017). http://www.isssource.com/ukraine-attack-an-insiders-perspective/

[15] Y. Huang, M. Esmalifalak, H. Nguyen, R. Zheng, Z. Han, H. Li, and L. Song. 2013. Bad data injection in smart grid: attack and defense mechanisms. *IEEE Communications Magazine* 51, 1, 27–33. https://doi.org/10.1109/MCOM.2013.6400435

[16] G. Hug and J. A. Giampapa. 2012. Vulnerability Assessment of AC State Estimation With Respect to False Data Injection Cyber-Attacks. *IEEE Transactions on Smart Grid* 3, 3, 1362–1370. https://doi.org/10.1109/TSG.2012.2195338

[17] Peter Huitsing, Rodrigo Chandia, Mauricio Papa, and Sujeet Shenoi. 2008. Attack taxonomies for the Modbus protocols. *International Journal of Critical Infrastructure Protection* 1, 37–44.

[18] NAMUR Interessengemeinschaft Automatisierungstechnik der Prozessindustrie e.V. c/o Bayer Technology Services GmbH. 2015. Automation Security 2020-Design, Implementation and Operation of Industrial Automation Systems. (2015).

[19] Hubert B Keller, Oliver Schneider, Joerg Matthes, and Veit Hagenmeyer. 2016. Reliable, safe and secure software of connected future control systems-challenges and solutions. *AT-AUTOMATISIERUNGSTECHNIK* 64, 12, 930–947.

[20] Eric D Knapp and Joel Thomas Langill. 2014. *Industrial Network Security: Securing critical infrastructure networks for smart grid, SCADA, and other Industrial Control Systems.* Syngress.

[21] Jason Larsen. 2008. Breakage. *Black Hat Federal.*

[22] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Y. Dong. 2017. A Review of False Data Injection Attacks Against Modern Power Systems. *IEEE Transactions on Smart Grid* 8, 4, 1630–1638. https://doi.org/10.1109/TSG.2015.2495133

[23] Jing Liu, Yang Xiao, Shuhui Li, Wei Liang, and CL Philip Chen. 2012. Cyber security and privacy issues in smart grids. *IEEE Communications Surveys & Tutorials* 14, 4, 981–997.

[24] Yao Liu, Peng Ning, and Michael K. Reiter. 2011. False Data Injection Attacks Against State Estimation in Electric Power Grids. *ACM Trans. Inf. Syst. Secur.* 14, 1, Article 13, 33 pages. https://doi.org/10.1145/1952982.1952995

[25] Bill Miller and Dale Rowe. 2012. A survey SCADA of and critical infrastructure incidents. In *Proceedings of the 1st Annual conference on Research in information technology.* ACM, 51–56.

[26] Yilin Mo, Tiffany Hyun-Jin Kim, Kenneth Brancik, Dona Dickinson, Heejo Lee, Adrian Perrig, and Bruno Sinopoli. 2012. Cyber–physical security of a smart grid infrastructure. *Proc. IEEE* 100, 1, 195–209.

[27] A. Monticelli. 2000. Electric power system state estimation. *Proc. IEEE* 88, 2, 262–282. https://doi.org/10.1109/5.824004

[28] Sajid Nazir, Shushma Patel, and Dilip Patel. 2017. Assessing and augmenting SCADA cyber security: A survey of techniques. *Computers & Security* 70, 436 – 454. https://doi.org/10.1016/j.cose.2017.06.010

[29] F. Pasqualetti, F. Dörfler, and F. Bullo. 2013. Attack Detection and Identification in Cyber-Physical Systems. *IEEE Trans. Automat. Control* 58, 11, 2715–2729. https://doi.org/10.1109/TAC.2013.2266831

[30] Andrew Paverd, Andrew Martin, and Ian Brown. 2014. Security and Privacy in Smart Grid Demand Response Systems. In *Smart Grid Security*, Jorge Cuellar (Ed.). Springer International Publishing, Cham, 1–15.

[31] M. A. Rahman and H. Mohsenian-Rad. 2012. False data injection attacks with incomplete information against smart power grids. In *2012 IEEE Global Communications Conference (GLOBECOM).* 3153–3158. https://doi.org/10.1109/GLOCOM.2012.6503599

[32] M. A. Rahman and H. Mohsenian-Rad. 2013. False data injection attacks against nonlinear state estimation in smart power grids. In *2013 IEEE Power Energy Society General Meeting.* 1–5. https://doi.org/10.1109/PESMG.2013.6672638

[33] Julian Rrushi. 2009. Composite intrusion detection in process control networks. Università degli Studi di Milano.

[34] Dong Wei, Yan Lu, M. Jafari, P. Skare, and K. Rohde. 2010. An integrated security system of protecting Smart Grid against cyber attacks. In *2010 Innovative Smart Grid Technologies (ISGT).* 1–7. https://doi.org/10.1109/ISGT.2010.5434767

[35] Z. Xiao, Y. Xiao, and D. H. c. Du. 2013. Non-repudiation in neighborhood area networks for smart grid. *IEEE Communications Magazine* 51, 1 (January 2013), 18–26. https://doi.org/10.1109/MCOM.2013.6400434

[36] Z. H. Yu and W. L. Chin. 2015. Blind False Data Injection Attack Using PCA Approximation Method in Smart Grid. *IEEE Transactions on Smart Grid* 6, 3 (May 2015), 1219–1226. https://doi.org/10.1109/TSG.2014.2382714

[37] B. Zhu, A. Joseph, and S. Sastry. 2011. A Taxonomy of Cyber Attacks on SCADA Systems. In *2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing.* 380–388. https://doi.org/10.1109/iThings/CPSCom.2011.34