J Netw Syst Manage
https://doi.org/10.1007/s10922-018-9458-z

REPORT

Specialized CSIRT for Incident Response Management in Smart Grids

Rafael de Jesus Martins[1] · Luis Augusto Dias Knob[1] · Eduardo Germano da Silva[1] · Juliano Araujo Wickboldt[1] · Alberto Schaeffer-Filho[1] · Lisandro Zambenedetti Granville[1]

Received: 29 November 2017 / Revised: 5 April 2018 / Accepted: 16 April 2018

Abstract Power grids are undergoing a major modernization process, which is transforming them into Smart Grids. In such cyber-physical systems, a security incident may cause catastrophic consequences. Unfortunately, the number of reported incidents in power grids has been increasing in the last years. In this article we advocate that the adoption of Computer Security Incident Response Teams (CSIRTs) is necessary for the proper management of security incidents in Smart Grids. CSIRTs for Smart Grids must cover different parts of the grid, thus consisting of specialized response teams for handling incidents not only on the physical infrastructure, but also on the Smart Grid equipment and on the IT infrastructure. We thus propose an incident classification to assist the implementation of CSIRTs for Smart Grids, considering the specific concerns of the different response teams. We evaluate attack classifications available in the literature and review a well-known database of Smart Grid security incidents.

✉ Rafael de Jesus Martins
rjmartins@inf.ufrgs.br

Luis Augusto Dias Knob
luis.knob@inf.ufrgs.br

Eduardo Germano da Silva
eduardo.germano@inf.ufrgs.br

Juliano Araujo Wickboldt
jwickboldt@inf.ufrgs.br

Alberto Schaeffer-Filho
alberto@inf.ufrgs.br

Lisandro Zambenedetti Granville
granville@inf.ufrgs.br

[1] Institute of Informatics, Federal University of Rio Grande do Sul (UFRGS), Porto Alegre, Brazil

Published online: 26 April 2018

Keywords Power grid · Computer security · Incident classification · SCADA systems · AMI

1 Introduction

Smart Grids can be defined as the next generation of the power grid, in which electric distribution, generation, and transmission are integrated with data communications and pervasive computing. As a result, Smart Grids offer increased control, efficiency, reliability, security, as well as bidirectional power and data communication [1]. Furthermore, concepts such as renewable energy sources, responsible energy usage, and customer awareness are also captured by the notion of Smart Grid.

A Smart Grid is typically divided into two subsystems:

- Supervisory Control and Data Acquisition (SCADA) allows remote control and monitoring of resources, devices, and industrial processes. This subsystem is highly distributed and used to control devices geographically dispersed. Control and acquisition of centralized data is critical to the functioning of the subsystem [2].
- Advanced Metering Infrastructure (AMI) allows gathering power measurement information from smart meters installed on the customer premises. Generally, the data collected in the smart meters is related to the power consumption, which is sent to a central controller through a secure connection and can be used for various purposes, such as demand management [3].

To ensure the proper operation of all grid components, possibly against malicious individuals, security becomes a key concern [4]. Therefore, understanding the possible vulnerabilities, risks, and attack motivations is essential to protect the Smart Grid from cyber-attacks that may compromise the electrical infrastructure and affect the economy and the safety of the population [5].

In computer security, an incident is an event that affects directly or indirectly confidentiality, integrity, or availability (the CIA triad) of the system or its data. In many companies, these occurrences are treated by a Computer Security Incident Response Team (CSIRT), using a set of standards and guidelines for incident management [6]. These standards define the procedures to recognize, analyze, and respond to security incidents with minimum damage and low cost of recovery. One of the key parts of the deployment of CSIRT is the analysis of the scope where the team will operate within an organization. Once defined the scope, a review of the main existing vulnerabilities is conducted to create a taxonomy for classifying incidents in representative classes. This is essential to reduce the recovery time after an incident.

The management of Smart Grid can be divided into three main areas of concern: *power grid physical infrastructure* (e.g., relays and fuses), *Smart Grid equipment* (e.g., field devices and smart meters), and *Information Technology* (e.g., communication protocols and servers). Each of these areas is typically managed by different teams, and the organization should be able to forward attacks and

vulnerabilities to the correct maintainers. In this article, we argue that Smart Grids can benefit from the use of an incident management infrastructure with the implementation of a CSIRT that covers not only the communication network, but also the resilience and integrity of the electrical grid and its equipment. For that purpose, we introduce in this paper a taxonomy to assist the implementation of a CSIRT for Smart Grids that takes into account the concerns of the different response teams. Other industrial control systems could also benefit from a similar approach, though the present work focuses solely on Smart Grids and on the specificities they exhibit. In the process of defining our proposed taxonomy, we evaluate attack classifications available in the literature and review a well-known database of Smart Grid security incidents.

The remainder of this article is organized as follows. In Sect. 2, we classify the attacks against Smart Grids reported in the literature considering security principles and target Smart Grid areas of concern. In Sect. 3, we present concepts regarding incident response management, which is essential to base our taxonomy for Smart Grid-specialized CSIRT. In Sect. 4, we present a classification of incidents obtained from a well-known cyber-security incident database for SCADA systems, and then propose our taxonomy. Finally, in Sect. 5, concluding remarks and future directions are presented.

2 Categorization of Smart Grids Attacks

All processes and services that we rely on, such as water and sewage systems, telecommunication infrastructures, air, sea, and land traffic control, are highly dependent on electricity supplied by power grids. Power grids comprise several subsystems, also known as domains, that ensure the generation, transmission, distribution, and accounting of electrical energy [7]. Because of the importance and characteristics of these cyber-physical systems, any threat to their operation may result in catastrophic consequences, such as the destruction of equipment, heavy economical losses, or even put lives in danger [8].

Most of the existing power grids have been designed several years ago without much concern about basic security requirements, such as confidentiality, integrity, and availability. Although power grids were originally conceived to operate in completely isolated environments, nowadays these systems are highly interconnected and often linked to the Internet [7]. As such, most vulnerabilities resulting from poor Smart Grids design in terms of security are related to the rise of new types of malware and viruses that can spread through the network, including Stuxnet, Havex, Flare, and Night Dragon, to name but a few.

We argue that, given the importance of Smart Grid and its subsystems, any security threat to their correct operation needs to be identified and dealt as rapidly as possible. A comprehensive taxonomy of attacks can assist in reducing the time for detecting and mitigating attacks targeted to the power grid. Smart Grids present unique requirements and characteristics because they rely on a physical infrastructure, general IT components, and Smart Grid-specific equipment. Thus, a taxonomy for classifying attacks in Smart Grids must be tailored to this environment.

Furthermore, we target at a taxonomy with a high-level of abstraction, instead of describing attacks in detail. Our proposal intends to allow the classification of specific attacks under generalized categories. In addition, we define a taxonomy that can be easily expanded to adapt to new types of attacks that continuously appear. Finally, the taxonomy must tolerate incompleteness of information: in several cases, incident reports often omit the consequences of an attack. Thus, the taxonomy must also allow the classification of attacks targeted to the power grid, even when there is few information available about the incident.

One of the basis of our taxonomy encompasses, first, classifying the key vulnerability of Smart Grids addressed in the literature. Such a classification helps have a better landscape on vulnerabilities to then propose a taxonomy. Taking the observations discussed above in mind, we reviewed the state-of-the-art on security in Smart Grids, seeking to identify vulnerabilities of its many subsystems. Several investigations describe attacks targeted to the power grid and its inherent vulnerabilities [9, 10]. Others present SCADA vulnerabilities for each system layer [8]. We also take into account proposals of generic attack taxonomies for cyber-physical systems [11], as well as studies that discuss specific attacks to the power grid [12]. In Table 1 we summarize the state-of-the-art classifying Smart Grid vulnerabilities according to two main dimensions: security principles (CIA triad) in each row, and Smart Grid areas of concern in each of the three main columns. Each column is further detailed considering the corresponding component affected (e.g., Master Terminal Units (MTUs), Remote Terminal Units (RTUs), field devices, communication protocols, smart meters, and the electric equipment in the power grid itself).

Attacks aiming to disrupt the *confidentiality* (row A in Table 1) premises of the Smart Grid may compromise privileged information regarding the utility company and the customer alike. Understanding the habits and necessities of the customers is needed, so the utility company can offer more tailored services [1]. Unfortunately, there are still several systems that do not use any kind of encryption in communication [12]. In these systems, where commands and responses are transmitted in clear text, a cyber-attacker can eavesdrop (item 1.1-A in Table 1) information about the field devices, obtain access credentials, or compromise customer *confidentiality* [9]. Moreover, an attacker may be able to discover the network address and open communication ports of power grid components using Port Scanning and Ping Sweep (items {1.2, 2.1, 2.2}-A in Table 1), or even using Phishing techniques (item 1.2-A in Table 1), spyware programs like Virus/Malwares (items {1.2, 2.1}-A in Table 1), and brute force (items {1.2, 2.1, 2.2}-A in Table 1) to find out access credentials to components in the control center. Additionally, traffic analyzers could break the *confidentiality* in the communication between the equipment in the AMI subsystem, such as concentrators and smart meters, thus compromising the privacy of the user's energy usage profile [13]. No *confidentiality* attacks targeting the Smart Grid physical infrastructure were found in the literature (item 3.1-A in Table 1); this was somehow expected because of the lack of Information and Communication Technology (ICT) deployed in such equipments, serving solely as electrical infrastructure for the Smart Grid.

Table 1 Taxonomy of security attacks in the Smart Grid, according to the scope of affected equipment and area

	Information technology (1)		Smart grid equipment (2)		Physical infrastructure (3)
	Protocols (1.1)	Servers, PCs, etc. (1.2)	MTU, RTU (2.1)	Field devices, smart meters (2.2)	Relays, fuses, etc. (3.1)
Confidentiality (A)	Eavesdropping	Phishing, port scanning, ping sweeps, brute force, virus/malware	Port scanning, ping sweeps, brute force, virus/malware	Port scanning, ping sweeps, brute force	N/A
Integrity (B)	Man-in-the-middle, unauthorized access, spoofing	SQL injection, virus/malware, unauthorized access, spoofing, replay	Virus/malware, unauthorized access, spoofing, replay	Tampering, virus/malware, unauthorized access, spoofing, replay	Interference, energy theft
Availability (C)	Equipment theft, interruptions, black hole	Human interference, equipment failed, denial-of-service	Human interference, equipment failed, denial-of-service	Human interference, equipment failed, denial-of-service	Equipment failure

Cyber-attacks such as man-in-the-middle, tampering, and unauthorized access can compromise the *integrity* (row B in Table 1) of the components in the power grid and of the data exchanged. These allow a cyber-attacker to modify the data transmitted by smart meters, field devices, or even substations [10, 14]. Attacks on the integrity of the data can hide electricity thefts and corrupt information through added interference (item 3.1-B in Table 1), or induce wrong responses to unnecessary demands caused by false information about the functioning of the power distribution system. In this context, mechanisms to handle unauthorized modification, insertion, or destruction of information in SCADA systems are not implemented or are weak. This characteristic can also be observed in widely used communication protocols, such as Modbus [15] or DNP3 [16], which offer weak packet integrity assurance. These protocols do not provide security mechanisms to prevent an attacker from sending forged messages, as well as modifying, reordering, replaying, or destroying messages [10] (items {1.1, 1.2, 2.1, 2.2}-B in Table 1). Moreover, the lack of adequate access control in the majority of SCADA systems may allow an attacker, for example, to manipulate data in the company server using SQL injection techniques [8] (item 1.2-B in Table 1).

Finally, *availability* (row C in Table 1) is also a major concern for the operation of Smart Grids. That is so because of the real-time characteristics of some domains, which collect operational and usage statistics from system components. Attacks to the availability of power grid services and resources, such as Denial-of-Service (DoS) [17] or Black Hole [18], targeted to company servers, substations, field devices, or smart meters may have a large impact because of the importance of control and monitoring functions [19] (items {1.1, 1.2, 2.1, 2.2}-C in Table 1). For example, a Distributed DoS (DDoS) attack can isolate a power substation or prevent operators from accessing SCADA servers and intentionally delay the transmission of a time-critical message to violate its timing requirement. This could possibly interrupt the energy supply or, even worse, cause severe damage to power equipment [9]. Furthermore, cyber-attacks that interrupt the energy supply to substation components may have the same effects of a DDoS attack if the company responsible for maintaining the system does not enforce resilience policies. Lastly, partial or total equipment failure (item 3.1-C in Table 1) may be induced by an attacker, rendering relevant information unavailable until the equipment is repaired or replaced by the utility company.

3 Incident Response Management

Incident Response Management (IRMA) is a critical component for the Information Security Management System (ISMS), which operates as an information repository in order to simplify and accelerate the mitigation of security incidents. Several recognized publications, including the ISO/IEC 27000-series [20] and RFC2350 standards [21], describe the importance of implementing procedures and controls for incident management. Understanding what composes incident management for industrial systems and the importance of their role in countering both natural and

man-made hazards [22] is needed to base our contributions presented in the remaining of this paper.

In general, IRMA—usually described as a set of procedures for handling information security incidents—is divided into well-defined stages. Although there are differences among existing best practice guidelines, such as NIST800-61 [23] and ISO/IEC 27035 [20], the process can be summarized in the following main stages: (1) prepare, (2) detect, and (3) learn. While the stages *prepare* and *detect* deal primarily with how to organize and execute Incident Response, *learn* seeks to provide feedback to the system with the information acquired throughout the process.

IRMA requires the interaction among several parts of an organization; as such, the creation of an organized group known as CSIRT is highly recommended. CSIRTs aim to minimize and prevent the spreading of damages from computer security incidents. CSIRTs can range from one to several security experts, be composed of specialists as diverse as malware and forensics experts to attorneys and public relation staff, in charge of controlling all stages of IRMA. In addition, CSIRTs can provide services not only to organizations, but also to third parties such as governments or customers located in CSIRTs' operating area.

Created as a reaction to the impact caused by the worm developed by Robert Morris back in 1988, the first CSIRT [24], then called CERT (Computer Emergency Response Team), was implemented jointly by the Defense Advanced Research Projects Agency (DARPA) and Carnegie Mellon University in Pittsburgh. Other terms that can be found in the literature and are used as synonyms of CSIRT include CIRT (Computer Incident Response Team) [25] and CSIRC (Computer Security Incident Response Capability)] [23].

CSIRTs may differ in their purpose, and this directly influences the services provided by them. Among the possible types of CSIRT, we can list:

- Corporate Team, which improves and maintains a corporation's information infrastructure;
- Information Technology (IT) Vendor, which improves the security of its products;
- Network Service Provider Team, which provides a response team to customers for security incidents;
- National Coordination Center, which maintains a national integration point of contact to several CSIRTs.

From the mission and purposes of the CSIRT, a range of services can be offered, and these services can be summarized into three main categories:

- Reactive services, which are triggered by and event or request, are the core core component of CSIRT work;
- Proactive services, which provide assistance and information to help prevent and reduce the number of incidents in the future;
- Security quality management services, which augment existing and well established services that are independent of incident handling and traditionally

performed by other areas of an organization such as the IT, audit, or training departments [25].

The success of a CSIRT depends on the overall quality of the services it provides. It is essential that the services offered are aligned with the organization requirements. CSIRT that operate in line with such requirements can develop a more effective IRMA and thus help diminish or mitigate the damage caused by future attacks.

By integrating Industrial Control Systems (ICS) (e.g., SCADA and AMI systems) to the Internet, it became even more crucial to handle incidents in Smart Grids. Thus, a few national organizations, primarily in the US and Europe, have provided guidelines for the creation of CSIRTs in the context of ICS. Specifically, it is worth mentioning two documents created and maintained by the Homeland Security Department—"Developing an Industrial Control Systems Cybersecurity Incident Response Capability" [26]—and ENISA—"Good practice guide for CERTs in the area of Industrial Control Systems" [27].

Most documents that recommend the establishment of CSIRTs describe the requirement for a well-defined classification of security incidents. However, such documents do not explicitly define the prerequisites for an efficient categorization of incidents. Thus, one of our contributions is to present a categorization to manage a CSIRT for Smart Grids based on the types of attacks investigated in the previous section, taking into account the different response teams that may be involved. In addition, in the next section, we introduce our taxonomy for reported incidents in Smart Grids, according to the main security dimension affected. The attack categorization, combined with the dimension-ratio each attack historically shows to affect the most, outlines the incident classes and corresponding response teams in a Smart Grid specialized CSIRT.

4 Incident Classification for the RISIDATA Incident Catalog

Mapping and classifying the historical incidents in power grids and SCADA systems are prerequisites for suggesting how specialized CSIRTs for Smart Grids should operate. In Sect. 4.1, we introduce the dataset of incidents that we have used to base our classification. Further ahead, we present our incident classification, which showcases what CSIRTs are to handle each incident, in Sect. 4.2.

4.1 RISI Dataset

The Repository of Industrial Security Incidents (RISIDATA) [28] is a database of cyber-security incidents that have affected SCADA systems, cyber-related incidents, as well as events such as DoS attacks and malware infiltrations. RISIDATA's community is responsible for adding incidents to the database. This information is reviewed by researchers and some data is anonymized, for example, related to incident's exact event location, or details about the affected company. Incidents reported in this database contain information such as: when and where that the event

occurred, industry type (e.g., power grids, water sewage, oil refineries), a brief description about the incident, and the impact of the event on the environment, people, and cyber-physical system. The database also uses a reliability rating for reported incidents; for the statistical analysis, all but the incidents reported and confirmed by trustworthy, firsthand witness, or by official documents available (e.g. Nuclear Regulatory Commission reports or court documents), are excluded, therefore making the database suitable (in comparison to other sources) to academic analysis.

Because companies not always disclosure official reports on incidents occurred in power grids and cyber-physical systems, gathering a reliable overview of these incidents is not a straight-forward task. Therefore, RISIDATA stands as one of the few publicly available databases of security incidents in SCADA systems, emphasizing its importance as an asset for research in the area. Although there are other reports of same nature as of RISIDATA (e.g., Dell Annual Security Report [29]), these do not have the same level of detail. Additionally, in order to enrich our data sample for incidents occurred in Smart Grids, we included our search to cover incidents that occurred on other kinds of industries but that are still applicable to power grids, since many field devices can be used in several environments. On one hand, this expansion enlarges our sample size, allowing our classification to better represent the scale of incidents for power grids and similar industries; on the other hand, our classification still considers particularities of the Smart Grid (such as its specific equipments), since it is the main scope of this work, rendering the classification not directly applicable for other industries.

We analyzed the confirmed incidents in SCADA systems as follows. First, we cataloged the confirmed incidents related to the power sector, totalizing 36 incidents. In order to increase our dataset, we also included the confirmed incidents in RISIDATA in the 2005–2014 period, independently of the industry type. Hence, we achieved a total of 120 confirmed incidents. We analyzed in detail each event and used the taxonomy presented in Table 1 to classify these events according to their scope of impact (Information Technology equipment, Smart Grid equipment, or Physical Infrastructure). Due to the complexity and impact of some incidents, some events were classified into more than one category in the taxonomy, e.g., the blackout occurred in Florida in 2008 [30] that affected the power grid availability and integrity. Thus, we cataloged a total of 156 events that are presented in Fig. 1.

In Fig. 1, the three main columns (CIA triad) depict how often each security principle was affected the most by each type of attack, which are mapped on the left. Further to the left, these incidents are grouped into seven categories; these categories represent our classification of the incidents, helping identify which CSIRT should act in each event. On the right-side, it is shown which of the three areas of the Smart Grid each incident affects; an attack type that impacts more than a single area will thus appear replicated in the figure for each area it affects.

This data shows the increasing number of incidents related to cyber-physical infrastructures. Moreover, it is also possible to observe the increasing number of incidents that affected the IT infrastructure of these systems, which reached its peak in the 2011–2012 period, with 25 confirmed events.

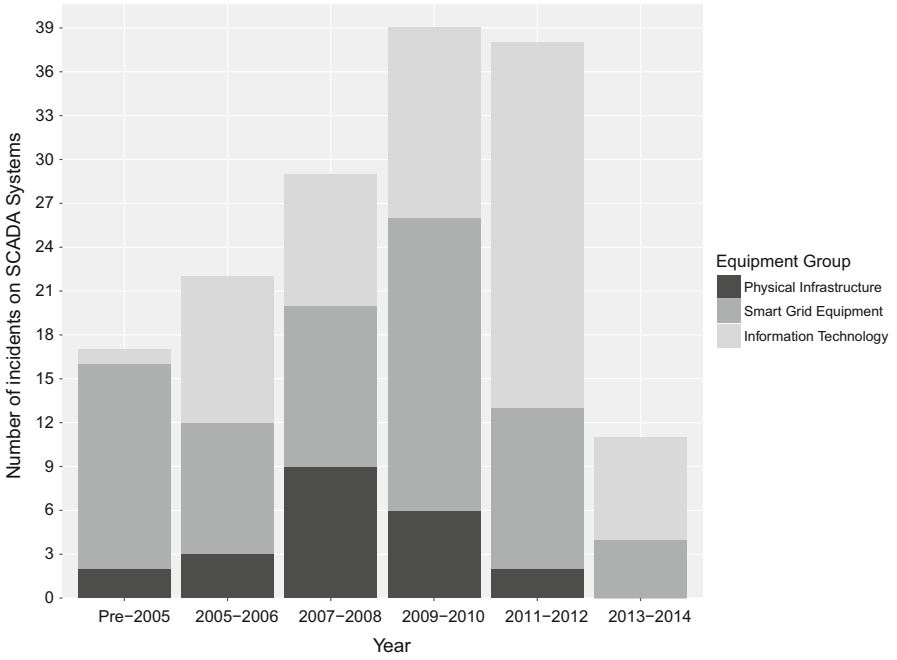

Fig. 1 Number of security incidents in SCADA systems per year, according to RISIDATA database

The proliferation of attacks targeted to the IT infrastructure confirms the fact that these systems are becoming more connected, directly or indirectly, to the Internet, exposing the vulnerabilities of SCADA systems. This is an important alert about how cyber-physical systems are vulnerable and how cyber-terrorists are turning their attention to attack these infrastructures.

4.2 Incident Classification

After reviewing the literature and the RISIDATA database, we sorted out the events on well-defined categories of security incidents thus defining our proposed taxonomy. We attempted to maintain our classification simple while covering all areas of a Smart Grid, from physical equipment to the communication protocols. Our taxonomy is shown at the bottom of Fig. 2, which presents a multilayer overview of the data obtained from the RISIDATA database. To accomplish it, we first cataloged the data according to the main dimensions of information security; second, we categorized each incident according to the incident classification. The categorization of each incident was done manually, and therefore requires a specialist for further expanding the classified dataset, or for reproducing it, for example.

In the database, we found 13 different types of attacks, presented separately in Fig. 2, which also highlights the targeted equipment group. According to the diagram, it is possible to notice a concentration of attacks involving integrity and

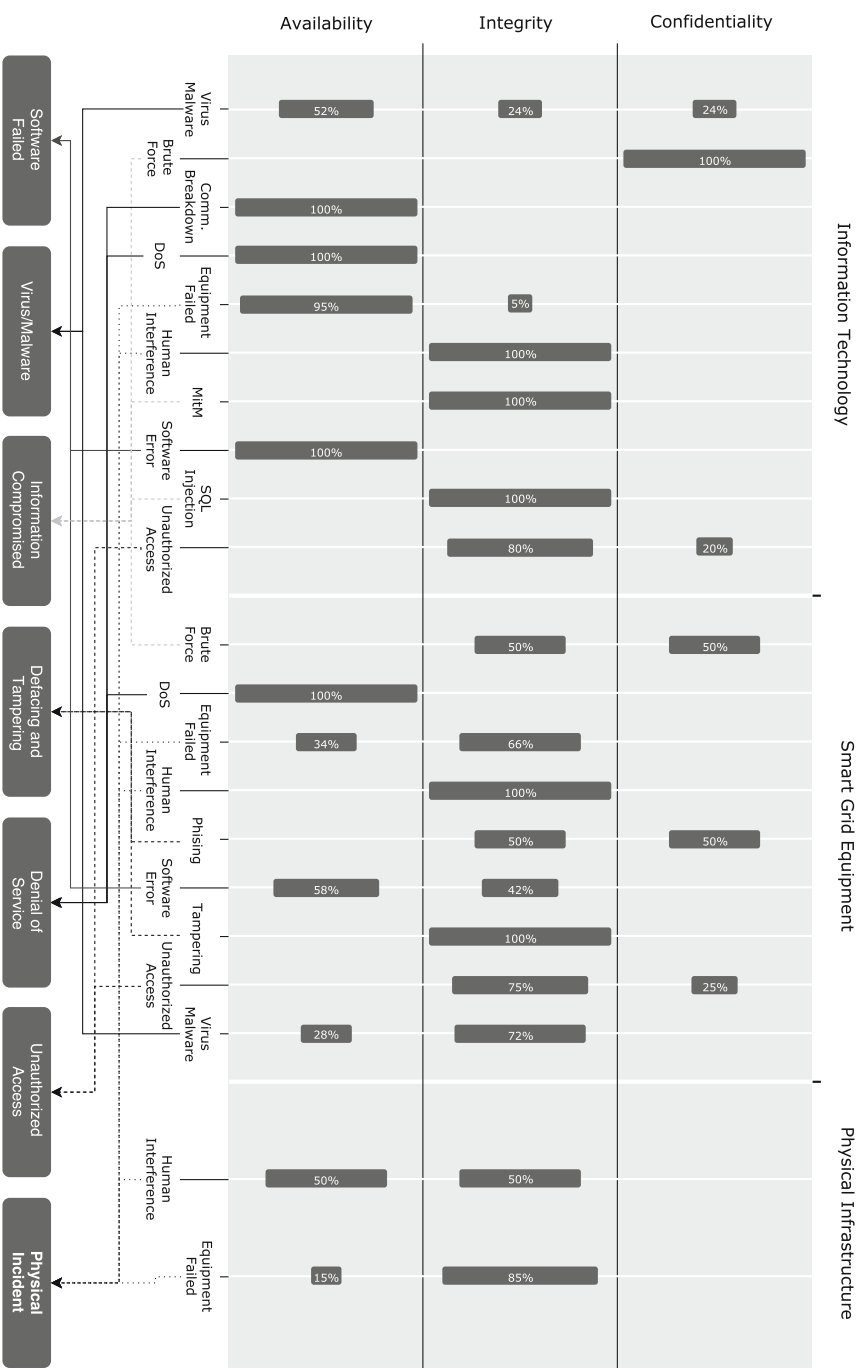

Fig. 2 Multilayer classification of incidents according with the main dimension affected and the attack categorization

availability, whereas there were no reported attacks attempting to violate confidentiality in the physical infrastructure. This can be partially explained by the unwillingness of companies to disclose incidents involving data confidentiality breaches, either due to legal or commercial reasons.

The classification also takes into consideration that a type of incident may affect the operation of one or more areas of the power grid and, consequently, requires the involvement of more than one response team. An example is equipment failure, which may occur in the physical infrastructure, IT, and even in grid components. Hence, depending on its nature, an equipment failure can mobilize a single response team or all teams of a CSIRT specialized for Smart Grids.

Compared to the classification shown in Table 1, a few types of attacks do not stand out either because they are difficult to detect (such as eavesdropping, port scanning, and interference) or due to privacy issues, such as cable theft.

A more detailed description of all cataloged incident classes contained in Fig. 2 is presented below. In addition, we also indicate which teams can act in each kind of incident that may occur, facilitating the forwarding of people to handle an event occurred on power grid.

- *Software failure* Failures caused by intentional or non-intentional actions, which can occur in management, control, or sensor software and operational systems. This kind of incident can mobilize teams responsible for maintaining the IT infrastructure and Smart Grid equipments;
- *Virus/malware* Software-based incidents that support the invasion or modification of the system. This category seeks to address incidents where the virus/malware is recognized before an attack is performed. Similarly to Software Failure, this kind of incident is a responsibility of teams that maintain the IT infrastructure or support Smart Grid equipment;
- *Compromised information* Access to privileged information that should not be available, including physical access to documents and servers. The majority of incidents classified within this category will mobilize the team responsible for the IT infrastructure. However, this kind of security incident may propagate to RTUs and field devices, which are managed by the Smart Grid equipment team;
- *Defacing and tampering* Alterations in the functioning of devices or software, e.g., smart meter tampering or website defacing. If the incident is recognized as Defacing, the service reestablishment will be conducted by the IT team. If it is recognized as Tampering, the incident will be treated by the team specialized on Smart Grid equipment;
- *Denial-of-service* Attempt to make a service or equipment unavailable, including Black Holes, Equipment Isolation or DDoS. This kind of security incident may occur on the IT infrastructure or on Smart Grid equipments. Thus, the team responsible for neutralizing this event will be mobilized according to the incident nature;
- *Unauthorized access* Unauthorized access to information, servers and equipment. Similarly to the previous class, Unauthorized Access may occur on the IT infrastructure or on Smart Grid equipment. The teams respective will be responsible for handling this kind of incidents;

- *Physical incident* Incidents that occur in the physical equipment, either due to natural causes or human interference, including equipment failures. This incident category can occur in all areas of the electrical system. Thus, a physical incident can mobilize all teams in a Smart Grids specialized CSIRT.

It is important to notice that, because our classification is based on reported incidents, we indicate the CSIRT responsible for reacting to each classified incident. Complementary to the reactive support, some classes of incidents may also be proactively tackled by their responsible team. For example, *Software Failure* incidents may arise from intentional or non-intentional actions, triggering the response from the CSIRT; alternatively, the team could find the critical faults through reviewing the software code, fixing the problem before an incident even occurs. Our classification is thus intended to base the categorization of incidents, and the implementation of the responsible CSIRTs, but is not to be taken as absolute or immutable. The permanent reevaluation of the adopted taxonomy and its responsible teams is vital for their lasting success in a Smart Grid.

5 Related Work

The proper management of security incidents in Smart Grids should not be solely relied on CSIRTs. In fact, it is equally important to look at the very characteristics of the Smart Grid that make it a target for malicious users, and what role the widespread standardization of the cyber-physical systems plays in securing these systems. Lastly, we also cite some computing techniques that have been recently proposed as defensive mechanism for incident management caused by attempts from intruders against the system.

Unfortunately, legacy SCADA protocols were developed focused only on performance, placing in background security aspects [31]. For example, the IP-versions of Modbus and DNP3 offer weak packet confidentiality assurance. Thus, these protocols allow, for example, the information exchange between SCADA devices to be transmitted in clear text. Although SCADA systems were originally conceived to operate in completely isolated environments, nowadays these systems are highly interconnected and often linked to the Internet. This trend was strongly motivated by the necessity to perform maintenance and to access remotely SCADA components but it also potentially enables malicious individuals to access the system [32]. Due to the importance of these cyber-physical systems, an targeted cyber-attack can result in catastrophic consequences.

In addition to the International Electrotechnical Commission (IEC), there are also other efforts that focus on standardizing cyber-physical system and several professional organizations have been developing standards to improve the security of SCADA systems. For example, The Institute of Electrical and Electronics Engineers Power Engineering Society (IEEE-PES) has a working group for addressing issues of risk assessment of information security in SCADA networks. The Object Linking and Embedding for Process Control (OPC) Foundation is also another organization working towards open connectivity in industrial automation

using open standards. OPC has developed standards for implementing data access, alarms, event management, and even Web access to SCADA network devices [10]. Furthermore, The National Institute for Standards and Technology (NIST) released a complete guide to ICS security. NIST also focuses efforts on enhancing the security of master stations [7].

Unfortunately, several SCADA systems currently in operation have vulnerabilities in their mechanisms of basic security, such as access control and user authentication. Although the adoption of reliable mechanisms of authentication and access control in this context is feasible, costs of development and deployment restrain the incorporation of those service to the SCADA systems. In addition, even secure systems might have vulnerabilities occasioned by misconfiguration, errors, or by intruders. Hence, the number of researches that propose Intrusion Detection Systems (IDSes) as a complementary approach of security for protecting SCADA systems is increasing [33].

Other techniques are also proposed for detecting intrusions in SCADA environments. A process-aware approach to detect intrusion is proposed by [34]. An interesting aspect of this paper is the evaluation of the impact of different realistic attack scenarios and the discussion of responses to these attacks. [35] exploit the predictable and regular nature of SCADA communication patterns to detect intrusion in field devices. The authors proposed a distributed and lightweight IDS suitable for implementation across multiple resource constrained SCADA devices in the Smart Grid. This approach uses the Bloom Filter data structure for memory efficiency and incorporates the physical state of the power grid for greater robustness. [36] designed an IDS that relies on the Honey Token based Encrypted Pointers to protect SCADA networks from cyber-attacks. These honey tokens inside the frame serve as a trap for the cyber-attacker. This IDS is designed for detecting intrusions and for recovering the system using reverse engineering approach.

6 Conclusion

Analyzing cyber-security incidents in Smart Grids is essential to prevent failures and ensure the resilience of the grid. In the event of an incident, quickly identifying and repairing the affected sectors of the grid is mandatory in minimizing financial losses, and overall customers' satisfaction. In this article we advocate the adoption of CSIRTs for proper incident management in Smart Grids. As a result, the handling of specific security incidents remains under the responsibility of specialized response teams, dealing with incidents not only on the power grid physical infrastructure, but also on the Smart Grid equipment and on the IT infrastructure.

Despite the importance of power grids and similar industrial systems, it is generally difficult to find reliable information about incidents that have affected the operation of the different parts of a Smart Grid. Even then, RISIDATA arises as a publicly available, well-rounded database for incidents reported in all types of industrial control systems and processes. We built on the RISIDATA database to evaluate incident scenarios in Smart Grids, and demonstrated how the specialized CSIRTs can forward the requests among several distinct groups of maintainers,

highlighting how the classification of these incidents can help in their assignment to the corresponding team.

The task of keeping a Smart Grid secure from incidents, both nature and man-made, is not one to be achieved easily. Moreover, due to factors usually rooted in financial causes, much of the modernization process in turning a power grid into a Smart Grid is built upon legacy structure and hardware, perpetuating vulnerabilities that may have already been addressed by their more modern counterparts. In future work, we plan to focus our analysis in the networking shortcomings of the Smart Grid, which tends to continually grow as a target for malicious activity, due to the modernization of the grid.

Acknowledgements This work is supported by ProSeG - Information Security, Protection and Resilience in Smart Grids, a research project funded by MCTI/CNPq/CT-ENERG # 33/2013.

References

1. Yan, Y., Qian, Y., Sharif, H., Tipper, D.: A survey on smart grid communication infrastructures: motivations, requirements and challenges. IEEE Commun. Surv. Tutor. **15**(1), 5–20 (2013)
2. Nicholson, A., Webber, S., Dyer, S., Patel, T., Janicke, H.: Scada security in the light of cyber-warfare. Comput. Secur. **31**(4), 418–436 (2012)
3. Rahimi, F., Ipakchi, A.: Demand response as a market resource under the smart grid paradigm. IEEE Trans. Smart Grid **1**(1), 82–88 (2010)
4. Bou-Harb, E., Fachkha, C., Pourzandi, M., Debbabi, M., Assi, C.: Communication security for smart grid distribution networks. IEEE Commun. Mag. **51**(1), 42–49 (2013)
5. Chen, P.-Y., Cheng, S.-M., Chen, K.-C.: Smart attacks in smart grid communication networks. IEEE Commun. Mag. **50**(8), 24–29 (2012)
6. Tãÿndel, I.A., Line, M.B., Jaatun, M.G.: Information security incident management: current practice as reported in the literature. Comput. Secur. **45**(0), 42–57 (2014)
7. Stouffer, K., Falco, J., Scarfone, K.: Guide to industrial control systems (ICS) security. In: NIST special publication, pp. 800–882 (2011)
8. Zhu, B., Joseph, A., Sastry, S.: A taxonomy of cyber attacks on scada systems. In: Proceedings of the 2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing, ser. ITHINGSCPSCOM '11, pp. 380–388. IEEE Computer Society, Washington (2011)
9. Wang, W., Lu, Z.: Survey cyber security in the smart grid: survey and challenges. Comput. Netw. **57**(5), 1344–1371 (2013). https://doi.org/10.1016/j.comnet.2012.12.017
10. Igure, V., Laughter, S., Williams, R.: Security issues in SCADA networks. Comput. Secur. **25**(7), 498–506 (2006)
11. Fleury, T., Khurana, H., Welch, V.: Critical Infrastructure Protection II. Towards a Taxonomy of Attacks Against Energy Control Systems, pp. 71–85. Springer, Boston (2008)
12. Silva, E., Knob, L., Wickboldt, J., Gaspary, L., Granville, L., Schaeffer-Filho, A.: Capitalizing on SDN-based SCADA systems: an anti-eavesdropping case-study. In: 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM), pp. 165–173 (2015)
13. Finster, S., Baumgart, I.: Privacy-aware smart metering: a survey. IEEE Commun. Surv. Tutor. **16**(3), 1732–1745 (2014)
14. Wermann, A., Bortolozzo, M., Silva, E., Schaeffer-Filho, A., Gaspary, L., Barcellos, A.: ASTORIA: a framework for attack simulation and evaluation in smart grids. In: Network Operations and Management Symposium (NOMS), 2016 IFIP/IEEE, (2016, to appear)
15. Swales, A.: Open modbus/tcp specification. Schneider Electr. **29**, 1–25 (1999)
16. Clarke, G.R., Reynders, D., Wright, E.: Practical modern SCADA protocols: DNP3, 60870.5 and related systems. Newnes (2004)

17. Needham, R.M.: Denial of service. In: Proceedings of the 1st ACM Conference on Computer and Communications Security, ser. CCS '93, pp. 151–153. ACM, New York (1993). https://doi.org/10.1145/168588.168607
18. Al-Shurman, M., Yoo, S.-M., Park, S.: Black hole attack in mobile ad hoc networks. In: Proceedings of the 42nd Annual Southeast Regional Conference, ser. ACM-SE 42, pp. 96–97. ACM, New York (2004). https://doi.org/10.1145/986537.986560
19. Ericsson, G.: Cyber security and power system communication—essential parts of a smart grid infrastructure. IEEE Trans. Power Deliv. **25**(3), 1501–1507 (2010)
20. Disterer, G.: ISO/IEC 27000, 27001 and 27002 for information security management. J. Inf. Secur. **4**(02), 92 (2013)
21. Brownlee, N., Guttman, E.: RFC 2350-expectations for computer security incident response. Internet RFCs (1998)
22. Chen, R., Sharman, R., Rao, H.R., Upadhyaya, S.J.: Coordination in emergency response management. Commun. ACM **51**(5), 66–73 (2008). https://doi.org/10.1145/1342327.1342340
23. Grance, B.K.T., Kent, K., Kim, B.: Computer security incident handling guide, recommendations of the national institute of standards and technology NIST800-61 (2004). https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf. Accessed 20 Apr 2018
24. Ruefle, R., Dorofee, A., Mundie, D., Householder, A., Murray, M., Perl, S.: Computer security incident response team development and evolution. IEEE Secur. Priv. **12**(5), 16–26 (2014)
25. West-Brown, M.J., Stikvoort, D., Kossakowski, K.-P., Killcrece, G., Ruefle, R.: Handbook for Computer Security Incident Response Teams (CSIRTs). Technical Report, Software Engineering Institute, Carnegie-Mellon University, Pittsburgh (2003)
26. Stouffer, K., Falco, J., Scarfone, K.: Guide to industrial control systems (ICS) security. NIST Spec. Publ. **800**(82), 16–16 (2011)
27. Dufkova, A., Budd, J., Homola, J., Marden, M.: Good practice guide for certs in the area of industrial control systems. In: European Network and Information Security Agency (ENISA) (2013)
28. RISIDATA: RISI: the repository of industrial security incidents (2016). http://www.risidata.com. Accessed 20 Apr 2018
29. Dell Incorporated: Dell security annual threat report. Technical Report, Dell Incorporated (2015). https://software.dell.com/whitepaper/dell-network-security-threat-report-2014874708. Accessed 19 Jul 2017
30. Time: Florida's blackout: a warning sign? Time (2008)
31. Chikuni, E., Dondo, M.: Investigating the security of electrical power systems scada. AFRICON **2007**, 1–7 (2007)
32. McClanahan, R.H.: SCADA and IP: is network convergence really here? IEEE Ind. Appl. Mag. **9**(2), 29–36 (2003)
33. Barbosa, R.R.R.: Anomaly detection in SCADA systems: a network based approach. Ph.D. dissertation, University of Twente, Enschede (2014). http://doc.utwente.nl/90271/. Accessed 20 Apr 2018
34. Cardenas, A.A., Amin, S., Lin, Z.-S., Huang, Y.-L., Huang, C.-Y., Sastry, S.: Attacks against process control systems: risk assessment, detection, and response. In: Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, ser. ASIACCS '11, pp. 355–366. ACM, New York (2011). https://doi.org/10.1145/1966913.1966959
35. Parthasarathy, S., Kundur, D.: Bloom filter based intrusion detection for smart grid scada. In: 2012 25th IEEE Canadian Conference on Electrical Computer Engineering (CCECE), pp. 1–6 (2012)
36. Asif, M., Al-Harthi, Y.: Intrusion detection system using honey token based encrypted pointers to mitigate cyber threats for critical infrastructure networks. In 2014 IEEE International Conference on Systems, Man and Cybernetics (SMC), pp. 1266–1270 (2014)

Rafael de Jesus Martins is an undergraduate student in computer engineering at the Federal University of Rio Grande do Sul (UFRGS), in Brazil. His current research interest include Internet of Things, Smart Grids and Mobile Edge Computing (MEC).

Luis Augusto Dias Knob received the B.Sc. degree from University of Passo Fundo (UPF) in 2010, and M.Sc. degree in computer science from the Federal University of Rio Grande do Sul (UFRGS) in 2016. He is pursuing the Ph.D. degree at the Pontifical Catholic University of Rio Grande do Sul (PUCRS),

Brazil. He is a Professor with the Federal Institute of Rio Grande do Sul (IFRS), Sertão, Brazil. His current research interest include Internet of Things, Sensor Networks, Edge Computing and Software-Defined Networking.

Eduardo Germano da Silva received his M.Sc. degree in computer science in 2016 from Federal University of Rio Grande do Sul (UFRGS), in Brazil. He achieved his bachelor's degree in Information and Communication Technologies at the Federal University of Santa Catarina (UFSC), in 2013. His current research interests include Smart Grids, SCADA systems, Software-Defined Networking and Intrusion Detection Systems.

Juliano Araujo Wickboldt is an Associate Professor at the Federal University of Rio Grande do Sul (UFRGS) in Brazil. He holds both M.Sc. (2010) and Ph.D. (2015) degrees in computer science from UFRGS. Juliano was an intern at NEC Labs Europe in Heidelberg, Germany for one year between 2011 and 2012. In 2015, Juliano was a visiting researcher at the Waterford Institute of Technology in Ireland. His research interests include softwarized networking and 5G technologies.

Alberto Schaeffer-Filho is an Associate Professor at Federal University of Rio Grande do Sul (UFRGS), Brazil. He holds a Ph.D. in Computer Science from Imperial College London (2009), and his areas of expertise are network/service management, network resilience, and smart grids. He is a member of the IEEE and the Brazilian Computing Society (SBC).

Lisandro Zambenedetti Granville is Associate Professor at the Federal University of Rio Grande do Sul (UFRGS), Brazil. He holds a Ph.D. in Computer Science from UFRGS (2001), and his areas of expertise are network and service management, network virtualization, and visualization of network management information. He is co-chair of the Network Management Research Group (NMRG) of the Internet Research Task Force (IRTF) and president of the Brazilian Computer Society (SBC).