

Risk Management Framework for the Power Grid Cyber-Physical Security

Riadh W. Y. Habash¹, Voicu Groza¹, and Kevin Kurr²

¹*School of Electrical Engineering and Computer Science, University of Ottawa, Ottawa, Ontario, Canada.*

²*Kylowave Inc., Ottawa, Ontario, Canada.*

Authors' contributions: *Please write this section*

Authors may use the following wordings for this section: This work was carried out in collaboration between all authors. " 'Author Riadh. W. Y. Habash, Voicu Groza and Kevin Kurr' designed the study, performed the statistical analysis, wrote the protocol, and wrote the first draft of the manuscript. 'Author Riadh. W. Y. Habash' managed the literature searches..... All authors read and approved the final manuscript."

Received 1st March 2013

Accepted xxxxxxxxxxxx 2013

Published xxxxxxxxxxxx 2013

Research Article

ABSTRACT

Aims: This paper addresses critical security challenges of the smart power grid due to the tight coupling between cyber and physical systems. It features approaches to inform utilities, policymakers, researchers, and consumers about practices to reduce the risks from cyber attacks.

Study Design: The paper introduces key cyber-physical systems and standards of the smart grid; identifies the security threats; and shows the need for protection at various levels of the power grid. A risk-based approach has been proposed, which could be implemented to achieve the vision of a secure smart grid infrastructure.

Place and Duration: The study was carried out in Ottawa, Ontario, Canada during the period of January 2012 to January 2013.

Methodology: Risk in the context of the smart grid, security threats, priorities, and countermeasures have been presented and a combined framework for risk management that can be translated into continuous security improvement programs has been proposed.

Conclusion: The proposed framework calls for a coordinated assessment of cyber and physical risks keeping the whole grid security goals in mind. Integrated risk management approaches are significantly needed to efficiently guide resource allocations and optimize practices at all levels of the smart grid platform to identify the risk, measure it, minimize it, and finally engineer out the risks by the use of available resources, to an acceptable and approved standards.

Keywords: *Smart grid, standards, cyber-physical systems, security, risk management.*

*Corresponding author: E-mail: rhabash@site.uottawa.ca;

1. INTRODUCTION

Electric power systems are very complex interconnected networks which include a series of independently operating regional grids that would greatly benefit from the optimization that comes with interconnection provided by the smart grid. The smart grid has been described by IEEE [1] as “a next-generation electrical power system that is typified by the increased use of information and communication technologies (ICT) in the generation, delivery, and consumption of electrical energy”.

The objective of transforming the current power grid into a smart grid is to provide reliable, secure, and high-quality electric power to digital societies in an environmentally friendly and sustainable way [2, 3]. However, there are lots of grid assets that run on legacy systems that cannot be replaced overnight, and with the rise of the smart grid, more of them are being connected to existing utility information technology (IT) systems, adding succeeding layers of functionality and capability that connect, in one way or another, to the internet at large. ICT is the key, but it is only a means to an end. What is not explicitly stated here, but is equally important, is that a fully developed smart grid concept includes in addition to smart meters, technologies at both the transmission and distribution levels and extends to both hardware and software, such as monitoring and control systems, as well as primary equipment like transformers and relays. Under this model, the smart grid should be adaptive, with less reliance on operators, especially in responding rapidly to load changing conditions; efficient, by reducing the cost to produce, deliver, and consume electricity; predictive, by identifying potential outages before they occur; integrative, in terms of real-time communications and control functions; interactive between customers, suppliers, and markets; reliable, by reducing the cost of interruptions and power quality disturbances; and secure, by reducing the probability and impact of attacks.

The smart grid will introduce millions of intelligent computing components that communicate in two-way communication [4]. As such, how to address networking security risks are critically important in the design of communication networks for the smart grid. Potential networking intrusion caused by intentional attackers may lead to a variety of consequences [5], from customers' information leakage to a cascade of failures, such as power outage and destruction of infrastructures.

There have been several literature reviews and surveys touching upon the topics of smart grid security [6-10]. This paper features approaches to inform utilities, policymakers, researchers, and consumers about practices to reduce the risks from cyber attacks in the pursuit of the smart grid. Various cyber and physical technologies have been identified in Section 2. Section 3 presents standards that guideline the implementation of the smart grid. Section 4 discusses risk in the context of the smart grid. Cyber attacks, security priorities, and countermeasures have been presented in Section 5. Section 6 proposes a risk management strategy to mitigate the anticipated security risks. Finally, Section 7 concludes the paper with future research directions.

2. CYBER-PHYSICAL SYSTEMS

Cyber-physical systems (CPS) are integrations of hardware, software, networking and protocols, control, and physical processes. Innovation of the electric grid is being modernized and tends to deal with the challenges more proactively by using state-of-the-art technological advances in the domain of CPS [11]–[13]. While the smart grid system is basically made up of four traditional components including generation, transmission, distribution, and utilization, many new applications that rely on ICT infrastructures are common between these components. In the distribution component, customers use smart

devices (for example, smart appliances, electric vehicles) and probably renewable energy sources such as solar panels and wind turbines, and their usage of electricity will be measured by smart meters. Fig. 1 shows the typical components of the smart power grid.

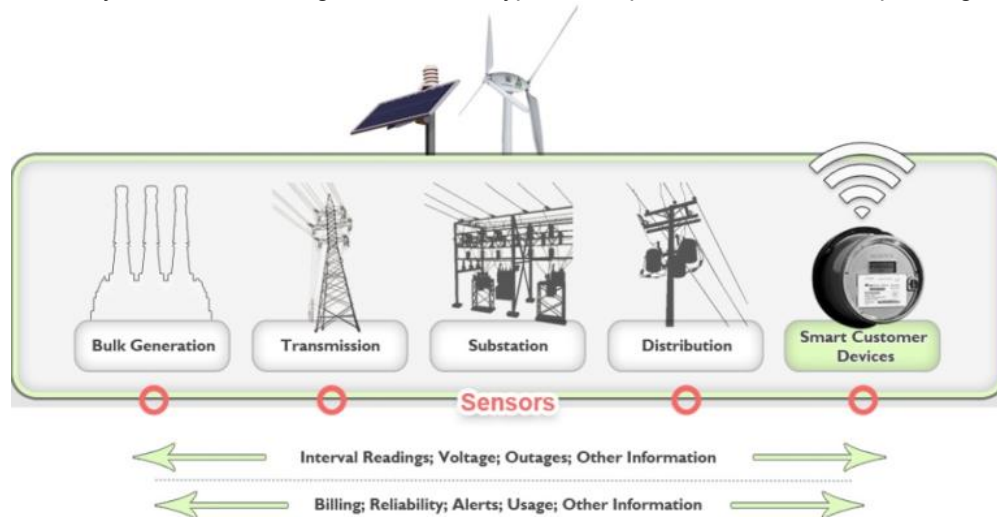


Fig. 1. Typical components of a typical smart power grid.

2.1 Information and Communication Technologies

A communication system is the key component of the smart grid infrastructure [14]. With the integration of advanced technologies and applications for achieving a smarter electricity grid infrastructure, a huge amount of data from different applications will be generated for further analysis, control and real-time pricing methods. Hence, it is very critical for electric utilities to define the communication infrastructure requirements to handle the output data and deliver a reliable, secure, and cost-effective service throughout the total system [15]. Fig. 2 provides an overview of the smart grid communication landscape.

Various ICTs supported by two main communications media, wired and wireless, can be used for data transmission within the smart grid. Wireless networks are commonly used in the current smart grid deployments. The wireless solutions can be either licensed or unlicensed, depending on the needs of the utility. For the highest reliability, licensed should be the choice. Each of the above options has their advantages and disadvantages, but what is consistently true is the need to have a scalable security solution [16].

Two types of information infrastructure are needed for information flow in a smart grid: first flow is from electrical appliances to smart meters and second from smart meters to utility's data centers. As suggested in [17], the first data flow can be accomplished through power line communication or wireless communications, while cellular technologies or the internet can be used for the second flow. Table 1 shows the main communications technologies and their specifications.

Advanced metering infrastructure (AMI) is viewed as a foundational-enabling technology for the smart grid. The implementation of AMI solutions (smart meters/modules, AMI server, meter data management (MDM) and software, core AMI transport infrastructure and backhaul communications) in the power distribution system has the potential to benefit both energy suppliers and consumers. The smart meter is one of the core components of the AMI that is in constant communication with the electric utility, retrieving real-time prices and

transmitting real-time demand upstream. The energy suppliers may benefit by more efficient meter reading, less maintenance cost, and outage location identification. Consumers will also have new opportunities to reduce their energy costs by taking advantage of real-time energy pricing, off-peak rates, and other available programs. In general, AMI solutions can be built around: wireless, power line carrier (PLC), and fiber optics. Part of the issue is that there will not be fiber, or even wired Ethernet, everywhere. Thus, some part of the communication must be wireless, bringing us to the point that radio frequency (RF) devices inherently require additional security considerations.

There are also many data exchange protocols used between entities such as transmission control protocol (TCP)/Internet protocol (IP), hypertext transfer protocol (HTTP), and file transfer protocol (FTP) which are widely used in the global information technology domain.

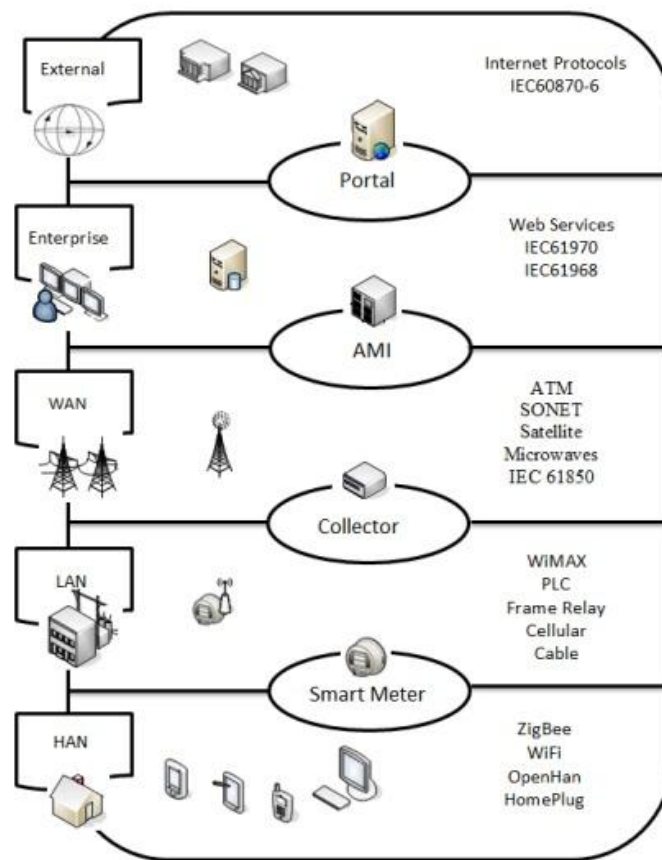


Fig. 2. Smart grid communication infrastructure and examples of technologies.

2.2 SCADA System

The control system within the electric grid consists of multiple mechanisms used to manage the grid's reliability and efficiency. The grid's control mechanisms can be divided into two main systems: centralized control centers and those distributed into the substations [18].

The centralized control which is at the core of the smart grid is configured by the supervisory control and data acquisition (SCADA) system, which collects measurements and device statuses from field devices, forwards operator commands to various field devices, and manages historic data about system operations. The SCADA communications occurs between the SCADA servers and software-based remote terminal units (RTU) located within each substation. It uses the IEC 61850 standard to access data from substation and field devices. The SCADA server polls the status of the substation's various devices every second and displays the acquired information to the operator through the human machine interface (HMI).

SCADA has been used before the advent of the network system. With the smart grid, there are several cases that added additional network environment to legacy SCADA system. Accordingly, the importance of network security increases continuously.

Table 1. Main communication technologies for the smart grid

Technology	Specifications	Suitability for Smart Grid
GSM	900-1800 MHz; 14.4 Kbps; 10 km.	Suitable for AMI; demand response (DR), and home area network (HAN)
3G	1.92-1.98 GHz, 2.11-2.17 GHz; 10 km.	Licensed; suitable for AMI; DR, and HAN; costly fee!
WiMax	2.5 GHz, 3.5 GHz, 5.8 GHz; 5 km (NLOS), 50 km (LOS)	DR; Wireless automatic meter reading (WMAR) as part of utility AMI.
ZigBee	868-915 MHz, 2.5 GHz; 250 Kbps; 50 m; 1 mW.	Unlicensed; most suitable standards for smart grid low- power residential network domain: HAN.
GPRS	900-1800 MHz; 170 Mbps; 10 km.	AMI; HAN; DR.
PLC	1-30 MHz; 3 Mbps;	AMI and HAN

GSM: Global system for mobile communication. 3G: Third generation. WiMax: Worldwide inter-operability for microwave access. GPRS: General packet radio service.

2.3 Substations

In any grid, there are thousands of transmission and distribution substations which have various levels of automation, where automation is indirectly related to security because increased automation implies increased computer-controlled electronics and software, which tends to increase the potential for cyber security weaknesses.

Accessing the substation could be through the user interface and/or intelligent electronic devices (IEDs). Cyber security of IEDs in the substations has been recognized as a critical issue for the smart grid [19]. There are possible cyber-physical system vulnerabilities in a substation including unsecured standard protocols and unauthorized remote access to IEDs. Some substation IEDs and user interfaces have a web server therefore it may provide a remote configuration change and control with default passwords. Even if firewalls and cryptography schemes are used for security, weak security key management cryptography and misconfigured firewalls are still exposed to intruders.

3. SMART GRID STANDARDS

There are a variety of technological solutions for smart grid that have been developed or are still in the development process. However, the key challenge is that the overall grid system is lacking widely accepted standards and this fact limits the integration of smart meters, smart devices, and renewable energy sources and constrains the interoperability between them. The adoption of interoperability standards for the overall system is a critical prerequisite for making the smart grid a reality. Seamless interoperability, robust information security, increased safety of new products and systems, compact set of protocols and communication exchange are some of the objectives that can be achieved with smart grid standardization efforts [20]. There are many regional, national, and international attempts towards achieving this goal. An overview of currently implemented smart grid standards is given in Table 2.

Table 2. Smart grid standards

Standard	Description
IEEE P2030	Interoperability with end-use applications.
IEEE P1901	Power line communications for appliances.
IEEE 929-2000	Utility interface of distributed generation (DG) systems.
IEEE 1547-2003	Interconnecting DG and storage information.
IEC61970	Energy management for enterprise applications.
IEC 61969	Energy management for DG.
IEC 61968	Integration of a utility enterprise.
IEC 61850	Communications for transmission, distribution, and substations.
IEC 60870-6/TASE.2	Data exchange between utility control centers.
ITU-T G.9955/G.9956	Physical/data link specification within AML.
IEC 62351	Security for IEC 61850.
IECTC57	Control and communications.
ISO/IEC 15408	IT security.
HomePlug	Connecting appliances within HAN.
ISA100.11a	Wireless systems.
ANSI 12.18	Data transportation via infrared within AML.
ANSI C12.19	Meter data communications.
Z-Wave	Wireless communications.
ZigBee	Wireless communication based on IEEE 802.15.
NISTIR 7628	Cyber security.
PRIME	Multi-vender interoperability within AML.
G3-PLC	Interoperability and cyber security.

4. RISK IN THE CONTEXT OF SMART GRID

Risk in the context of smart grid may be defined as the probability of a threat agent exploiting vulnerability to cause harm to a computer, network, system, or utility, and result in operational and business consequences. Cyber security risk is difficult to measure even in a static environment because it is a complex function of threat, vulnerabilities, and consequences. The following equation attempts to correlate elements of risk [21-23].

$$R = P_A \times (1 - P_E) \times C \quad (1)$$

R represents the level of risk assumed, or the level of risk that still remains after accounting for threat, consequence and protection mechanism. It is a value between 0 and 1 representing the combined probability that the system will be attacked, the effectiveness of the system, and the consequence of a successful attack.

P_A is the likelihood of attack, with a maximum of 1 if the probability of attack is set at 100%. With the level of threat against the grid is high, it is safe to say that the probability of an attack on grid infrastructure is large.

P_E is the probable effectiveness of the security in place to protect the system. While $(1 - P_E)$ measures the lack of security mitigation (vulnerability). The vulnerability depends on the grid's cyber supporting infrastructure. This typically entails all the computers, software platforms, networks, protocols, and other resources required to support grid control and monitoring functions. The grid supporting infrastructure is currently overwhelmed with vulnerabilities due to its heavy dependency on legacy systems, which were not designed from a security perspective. C is a value between 0 and 1 that rates the consequence of a successful attack. The risk of a cyber attack is dependent on the impact that the attack has on the power systems. This will mostly be determined by how the various cyber vulnerabilities impact the grid's various power applications. P_E may be expanded to

$$P_E = P_I \times P_N \quad (2)$$

Where, P_I is the probability of interception and P_N is the probability of neutralization of a given threat. P_I determines how likely an attack is to be discovered and a response initiated. Once a response has been initiated, P_N helps determine how effective that response will be in stopping the attack.

Like the rest of the variables in Eq. (1), C is a value between 0 and 1 indicating the impact a successful attack would have on the system. It is important to understand what assets would have the largest impact if lost, damaged or destroyed and then protect them accordingly.

In general, three parameters attributes to help determine consequences: geographical size of the impact C_A (international, national, regional, local); time to recover C_T (permanent, years, months, days, hours); and cost to recover C_C (very high, high, medium, low, very low). Understanding the asset and knowing the impact values for each attribute makes it possible to calculate C using Eq. (3).

$$C = 1 - (1 - C_A) \times (1 - C_T) \times (1 - C_C) \quad (3)$$

5. CYBER-PHYSICAL SECURITY

Security refers to the degree of protection afforded to the system from deliberate attacks. Smart grid security involves an architecture that includes security from the beginning, consists of more than just protective devices such as firewall, and engages processes as well as products. This includes physical assets (power, sensing, control, and communication technologies), policy, market, and management; and IT including cyber and data. Interconnection among all above requires secure automated information exchange and intelligent decision throughout the entire power grid.

5.1 Cyber Attacks

Threats to smart grid critical infrastructure could be of many forms as shown in Table 3 [26]-[31]. To make an analysis based on attack, we may build a frame of main risk factors for cyber-physical security that may cover any sector of the smart grid. The ISO/IEC Standard 15408 (Table 2) (Common Criteria—Fig. 3) includes a security risk model showing the value relationship of owners to their assets.

Table 3. Forms of cyber attacks on the smart grid

Form	Description
Protocol	ICCP, IEC 61850, DNP3, could be potentially exploited to launch attacks if they are not secured properly.
Routing	Attack on the routing infrastructure of the Internet.
Intrusion	Exploiting vulnerabilities in the software and communication infrastructure of the grid such as gaining access to substation HMI bypassing security controls (firewalls, system passwords).
Denial of Service (DoS)	Attacks that target availability by flooding the communication network or the server with huge volumes of traffic, thus denying service to users.
Malware	Malicious software that exploits vulnerabilities in system software and hardware.
Application	Attack on EMS, such as power consumption auto-monitoring, economic dispatch, optimal power flow, adaptive protection, relay protection schemes, electricity real-time pricing, etc.
Insider	An insider abuses their current system.

To launch an attack, a threat agent must first exploit entry points, and upon successful entry an adversary can deliver specific attacks on the grid infrastructure. The extensive grid networks provide potential entry points including access through infected devices and poorly configured firewalls.

Research on the SCADA testbed has identified numerous cyber vulnerabilities and contributed to the production of SCADA-specific security assessment methodologies [24]. A control system malware called Stuxnet was found in July 2010 [25]. Steps of Stuxnet attack after intrusion attempts are based on change of the file system, setting, and status. This malware, targeting vulnerable SCADA systems to induce physical consequences, raises new questions about power grid security.

Fig. 4 presents a scenario for a possible Stuxnet intrusion into the SCADA systems. Such systems are not usually connected to the Internet, but the Stuxnet worm could spread via infected mountable drives plugged into USB ports. It is common to find a network bridge between SCADA systems and corporate networks (TCP/IP), which might be used to extract data for producing reports. This creates scenarios where the SCADA networks are not completely isolated anymore. Stuxnet makes complex modifications to the infected system. By taking control of the environment, the worm may run equipment and adjust settings. In extreme circumstances, it could even cause complete failure or explosions. Protecting against attacks on SCADA networks is a challenging task, given the wide range of attack mechanisms, the decentralized nature of the control, and the lack of coordination among various systems in the electric grid.

Another cyber vulnerabilities exist at wireless devices used in AMI located on the customers' premises which are outside the utility's physical security perimeter; accordingly, they are at high risk of compromise. Attackers can extract data from the memory of these

devices including secret keys used for network authentication and device memory to insert malicious software. Once the device is compromised it can be used to attack other parts of the smart grid by communicating through the network. Many compromised smart meters or data collector nodes could be programmed by the attacker to simultaneously send messages that cause power demand to be reduced and then to be increased dramatically. These phony messages could cause grid instability and power outages.

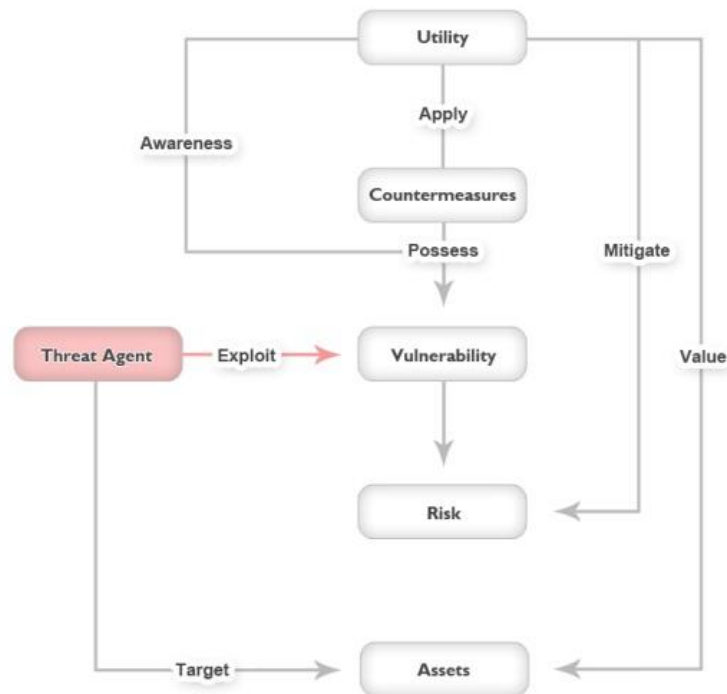


Fig. 3. Security model based on ISO/IEC Standard 15408.

5.2 Security Priorities

In general, information security requirements for a system include three high-level security priorities: confidentiality, integrity, and availability. Confidentiality prevents an unauthorized user from obtaining secret or private information. Integrity prevents an unauthorized user from modifying the information. Availability ensures that the resource can be used when requested [10] and is the most important security objective. Integrity of data is clearly important in general, but since so many different types of interactions are taking place in the smart grid, the integrity requirements will need to be specific to a particular application. Attacks targeting availability, or DoS attacks, attempt to delay, block or corrupt the communication in the smart grid. Attacks targeting data integrity can be regarded as more sophisticated attacks. The target of the attacks can be customer's information, corporation data, and electric market information where confidentiality is critical.

5.3 Countermeasures

Utilities need to analyze the potential threats in order to verify which apply to its environment. Such analysis may help in the selection of suitable countermeasures needed to reduce the relevant risks to acceptable levels. Countermeasures are usually implemented for the purpose of reducing vulnerabilities and meeting security policy requirements. The challenge is to establish countermeasures that restrict a threat agent from exploiting a known threat against vulnerabilities. It is important to note that any security countermeasure implemented in the smart grid should not impede power availability. Key management and secure communication architecture are vital countermeasures for cyber security. Shared secret keys or multi-factor authentication may be used to achieve secrecy and authenticity for communication.

Efforts have been made in the power community to develop secure protocols for power grids. Distributed network protocol 3 (DNP3) is currently extensively-used for substations. Security functionalities has been implemented for DNP3 by modifying the original protocol to introduce security mechanisms to the DNP3 stack and by inserting a security layer between the TCP/IP layer and the DNP3 protocol stack. Another protocol, IEC 61850, comes without its own security mechanisms but relies on IEC 62351.

Network approaches are primary countermeasures to detect, mitigate and eliminate DoS attacks that actively lead to network traffic dynamics. However, they are much less effective to deal with attacks targeting integrity and confidentiality that cause negligible effect on the network performance. Encryption is an elementary cryptographic method to achieve secure communication and information protection for any information system [32].

Special attention should be paid to insider threats within utilities and those organizations that provide services using consumer energy consumption information.

Another way to fight attacks is to bring more of the smart grid into the realm of standards-based technologies, where there is a depth of expertise and support for securing critical networks.

6. SECURITY RISK MANAGEMENT

Having framed the security risk context, we now move to measures and manage those risks. Risk management is about discovering critical assets and realizing their weaknesses, loss expectation, and the suitable risk mitigation approaches for ensuring their sustained value. Consequently, risk management involves choosing among alternatives to reduce the effects of risks.

Risk management efforts can address infrastructure and application perspectives of the smart grid domains including customer (HAN), grid (power system, LAN and WAN), and services (data and enterprise). Infrastructure enhancements will primarily involve conventional cyber security protections such as cryptography, access control, and authentication mechanisms that can provide both adequate security, high availability, and can be easily integrated with legacy systems.

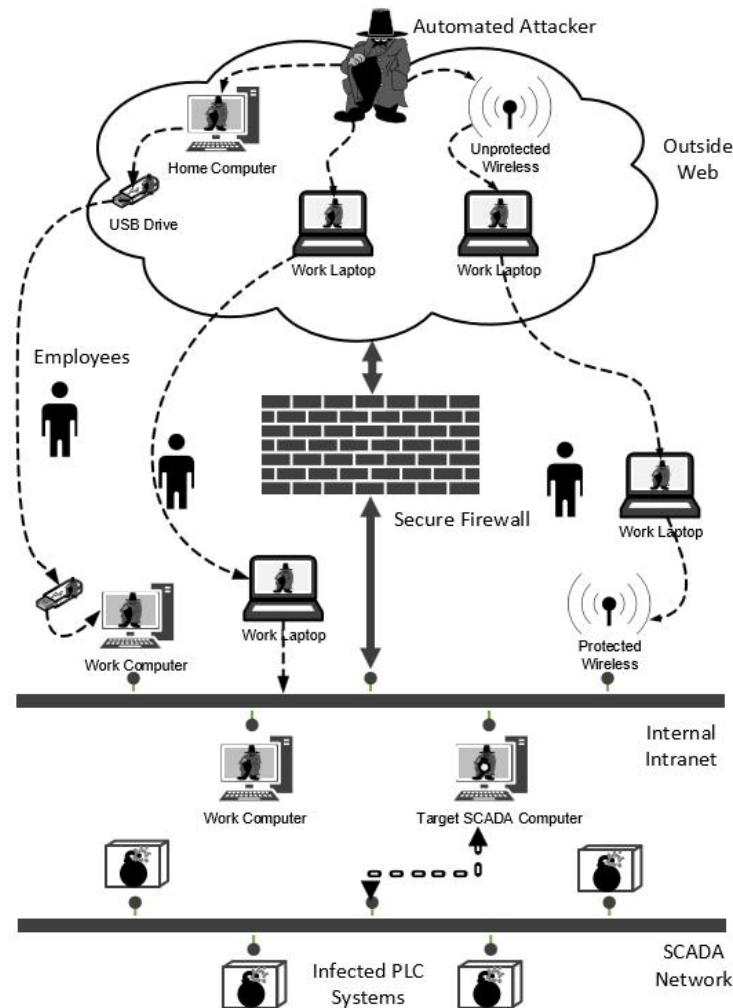


Fig. 4. Scenario for a possible Stuxnet intrusion into the SCADA systems.

6.1 Unified Framework

For the utility, security start with defining a risk management framework that will be used to identify threats and vulnerabilities; assess the effectiveness of existing controls in mitigating the risks; recommend new controls to mitigate the risks to a level acceptable to the utility and public; periodically repeat this process to account for changes in the threat situation; and set up policies that address human behaviour, which is the basis for all security risks.

Inspired by CAN/CSA Q-634-91 [33], Fig. 5 presents a unified framework for risk management in all domains. This combined framework demands interactive and step-wise actions to reduce the overall risks. Such a framework calls for a coordinated assessment of cyber and power grid risks keeping the whole grid security goals in mind. When a risk is identified, a risk strategy can be applied whether to avoid it, accept it, or reduce its impact. More than one risk strategy may be applied in a given situation. While best strategies are applicable to all environments, utilities may discover that some are less relevant to a

particular situation. The specific implementation details differ according to the purpose, technology road map, available resources, and other factors.



Fig. 5. Risk management framework for the smart grid.

The unified process of risk management comprises of several steps including: risk identification and threat characterization; risk analysis; risk planning including level of risk acceptance; risk prioritization based on objectives; periodical risk tracking; risk monitoring including countermeasures; and risk communication to the management, stakeholders, and organization. The risk management process must enable sound decision making. Since threats cannot be totally eliminated, the process must focus on vulnerabilities and risk actions.

The most important elements in the risk management process in relation to improve security of the smart grid are risk identification and assessment of control effectiveness. Conventional vulnerability assessment techniques such as penetration testing and vulnerability scanning are not suitable for this environment as they often trigger failures in legacy systems. Approaches to achieve safer and more reliable assessments are needed to ensure that critical cyber-physical assets are protected from attacks.

In view of the integration of the cyber and physical assets, unified and interoperable solutions are essential to assure communication and information among various systems of different media and topologies found in the smart grid.

Even though power systems are increasingly being designed and implemented using cyber standard hardware and software platforms and network protocols, they need to fulfill very different risks, priorities, performance, and reliability requirements as shown in Fig. 6.

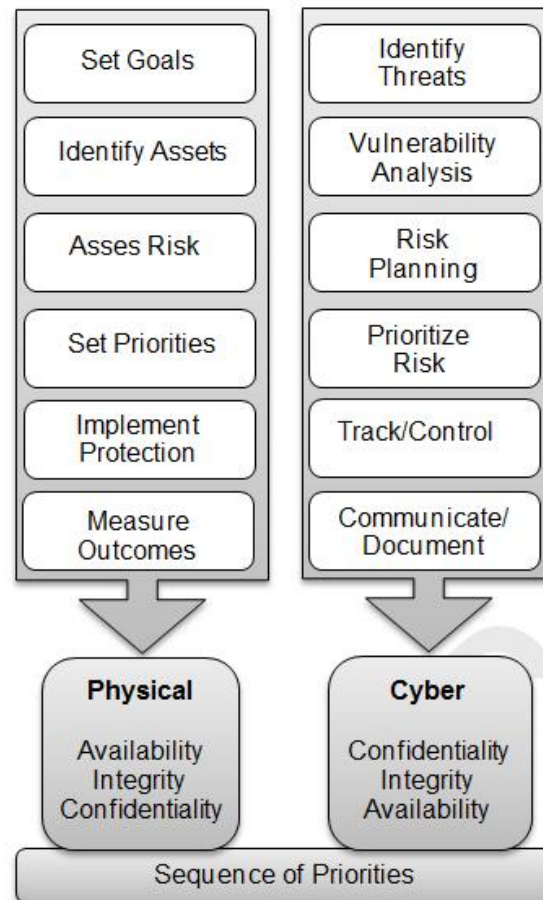


Fig. 6 Risk management based on priorities for physical and cyber assets.

6.2 Risk Impact

The criticality of cyber vulnerabilities should be evaluated based on their ability to impact either the physical power system or supporting cyber functions such as system outage, billing, or market data. The concept of impact has been discussed in [34]. The evaluation of the physical system should include analysis of the power applications and their ability to impact the power system. This analysis may be carried out using power system simulation techniques to quantify steady state and transient performances including power flows and variations in grids stability parameters in terms of voltage, frequency, and rotor angle [10].

Developing a secure system requires that both applications and supporting infrastructure are designed to be attack resilient. Therefore, it is critical to address redesign the grid's basic control mechanisms and algorithms to provide an initial layer of attack resilience throughout the grid [35]. Finally, being able to translate the risk assessment into continuous security improvement programs is a key part of the cyber-physical security agenda.

7. CONCLUSION AND FUTURE RESEARCH

Integrated risk management approaches are significantly needed to efficiently guide resource allocations and optimize practices at all levels of the smart grid platform to identify the security risk, measure it, minimize it, and finally engineer out the risks by the use of available resources. The risk management process will proactively monitor risks throughout the system and modify processes as appropriate.

Incorporating attack prevention, detection, mitigation, and resilience is among the most important research and development needs for the emerging smart grid. Research initiatives are required to accelerate the development of standards, protect cyber-physical infrastructures, secure critical information, and resilience power system applications. The research need to quantify the potential impact of a cyber-attack on the power grid in terms of load loss, stability interruptions, equipment damage, and financial cost. The ultimate goal is to develop a risk modeling framework that incorporates system planning and operational studies with the dynamics of the physical system and the cyber-based control network.

Finally, a collaborative effort by utilities, research community, and policy makers is required to achieve the vision of a secure smart grid infrastructure.

COMPETING INTERESTS

Authors have declared that no competing interests exist.

REFERENCES

1. IEEE 2030-2011, IEEE Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), End-Use Applications, and Loads, STD97148, STDPD97148, September, 2011.
2. Office of the National Coordinator for Smart Grid Interoperability. NIST framework and roadmap for smart grid interoperability standards, release 1.0. NIST Special Publication 1108, 2009.
3. Santacana E, Rachliffe G, Tang Le, Feng X. Getting smart. IEEE Power Energy Mag. 2010;March/April:41-8.
4. The Smart Grid Interoperability Panel-Cyber Security Working Group. Smart grid cyber security strategy and requirements. NIST IR-7628;Feb 2010.
5. Metke AR, Ekl RL. Smart grid security technology. Proc of Innovative Smart Grid Tech (ISGT).Jan. 2010.
6. Ericsson GN. Cyber security and power system communication—Essential parts of a smart grid infrastructure, IEEE Trans Power Del. 2010; 25(3):1501–7.
7. Yan Y, Qian Y, Sharif H, Tipper D. A survey on cyber security for smart grid communications. IEEE Communications Surveys and Tutorials. 2012;7(3):998–1010.
8. McDaniel P, McLaughlin S. Security and privacy challenges in the smart grid. IEEE Sec Privacy. 2009;7(3):75–7.
9. Khurana H, Hadley M, Lu N, Frincke DA, Smart-grid security issues. IEEE Sec Privacy. 2010;Jan/Feb:81–5.
10. Wang W, Lu Z. Cyber security in the smart grid: survey and challenges. Computer Networks. 2013;November:1344-71.

11. Hoffman M, Daim TU. Building energy efficiency technology roadmaps: A case of Bonneville power administration (BPA). *Proc Technol Manag. Global Future*. 2006: 1503–27.
12. King RL. Information services for smart grids. *Proc IEEE PES Gen Meet*. 2008;1–6.
13. Li F, Qiao W, Sun H, Wan H, Wang J, Xia Y, Xu Z, Zhang P. Smart transmission grid: vision and framework. *IEEE Trans Smart Grid*. 2010;1(2):168-77.
14. Gungor VC, Lu B, Hancke GP. Opportunities and challenges of wireless sensor networks in smart grid. *IEEE Trans Ind Electron*. 2010;57(10):3557–64.
15. Güngör VC, Sahin D, Kocak T, Ergüt S, Buccella C, Cecati C, Hancke GP. Smart grid technologies: communication technologies and standards. *IEEE Trans Ind Inform*. 2011;7(4):529-39.
16. Gunther EW, Snyder A, Gilchrist G, Highfill DR. Smart grid standards assessment and recommendations for adoption and development. EnerNex Corporation, Draft 0.83 03/1/2009.
17. Peizhong Y, Iwayemi A, Zhou C. Developing ZigBee deployment guideline under WiFi interference for smart grid applications. *IEEE Trans Smart Grid*. 2011;2(1):110–20.
18. Hahn A, Ashok A, Sridhar S, Govindarasu M. Cyber-physical security testbeds: architecture, application, and evaluation for smart grid. *IEEE Trans Smart Grid*. 2013;4(2):847-55.
19. Ten C-W, Hong J, Liu C-C. Anomaly detection for cybersecurity of the substations. *IEEE Trans Smart Grid*. 2011;2(4):865-73.
20. Gungor VC, Sahin D, Kocak T, Ergüt S. Smart grid communications and networking. *Türk Telekom Tech. Rep*. 2011;April:11316-01.
21. Clements SL, Kirkham H, Elizonda M, Lu S. Protecting the smart grid: a risk-based approach. *IEEE Power Energy Society General Meeting*. San Diego, 24-29 July, 2011.
22. Ray PD, Harnoor R, Hentea M. Smart power grid security: a unified risk management approach. *IEEE Int Carnahan Conf Security Tech. (ICCST)*, San Jose, CA, pp. 276-285, 5-8 Oct. 2010.
23. Govindarasu M, Hann A, Sauer P. Cyber-physical systems security for smart grid. *PSERC Publication 12-02*, 2012.
24. Permann MR, Rohde K. Cyber Assessment Methods for SCADA Security. *Instrumentation, Systems and Automation Society (ISA)*, Tech. Rep., 2005.
25. Vijayan J. Stuxnet renews power grid security concerns, [Computerworld, 2010: http://www.computerworld.com/s/article/9179689/Stuxnet_renews_power_grid_security_concerns].
26. Yaar A, Perrig A, Song D. A path identification mechanism to defend against DDoS attacks. *Proc IEEE Symposium on Security and Privacy*, 2003.
27. Mirkovic J, Reiher P. A taxonomy of DDoS attack and DDoS defense mechanisms. *SIGCOMM Comput Commun Rev*;2004:39–53.
28. Strasser M, Capkun S, Popper C, Cagalj M. Jamming-resistant key establishment using uncoordinated frequency hopping. *Proc IEEE Symp Security and Privacy*. 2008;May:64–78.
29. Popper C, Strasser M, Capkun S. Jamming-resistant broadcast communication without shared keys. *Proc. of the 18th USENIX Security Symposium (Security '09)*, Aug. 2009.
30. Liu Y, Ning P, Dai H, Liu A. Randomized differential DSSS: jamming-resistant wireless broadcast communication. *Proc. 29th IEEE Conf Comp Comm (INFOCOM '10)*, March 2010.

31. Sidhu TS, Yin Y. Modelling and simulation for performance evaluation of IEC61850-based substation communication systems. *IEEE Trans Power Delivery*. 2007;22(3):1482–9.
32. Mo Y, Kim TH-Jin, Brancik K, Dickinson D, Lee H, Perrig A, Sinopoli B. Cyber-physical security of a smart grid infrastructure. *Proc. IEEE*. 2012:195-209.
33. CAN/CSA Q-634-91. Risk Analysis Requirements and Guidelines, Quality Management. A National Standard of Canada, November, 1991.
34. Ten C-W, Liu C-C, Manimaran G. Vulnerability assessment of cybersecurity for SCADA systems. *IEEE Trans Power Syst*. 2008;23(4):1836–46.
35. Sridhar S, Hahn A, Govindarasu M. Cyber physical system security for electric power grid. *Proceedings of the IEEE*. Jan. 2012.

© 2013 Habash et al.; This is an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/3.0>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.