Infrastructure Security for Smart Electric Grids: A Survey

Naran M. Pindoriya, Dipankar Dasgupta, Dipti Srinivasan and Marco Carvalho

Abstract The deployment of smart grid technologies is drawing significant attention in the electric power industry. The term "smart grid" refers to modernization of the electric grid using digital technology that includes an advanced sensing and metering infrastructure, high speed, fully integrated two-way communications, and a supporting information infrastructure. In particular, the smart grid combines matured electric grid infrastructure with information and communication technology to offer better grid performance in terms of overall system efficiency and reliability. It supports a two-way energy and information flow, facilitates the integration of time-varying energy sources and new dynamic loads, and amongst other things. However, along with these potential benefits, smart grid also brings new challenges in ensuring security of the grid and the information infrastructure that connects and controls it. This chapter presents a brief survey of various essential components of smart grid and some of the security challenges that encompass virtually all aspects of its operation.

Keywords Smart grids · Smart grids security · Survey · Smart grids architecture · Advanced metering infrastructure

N. M. Pindoriya · D. Srinivasan
Department of Electrical and Computer Engineering,
National University of Singapore (NUS), Singapore 117576, Singapore

D. Dasgupta
Department of Computer Science, University of Memphis, Memphis, TN 38152-3240, USA

M. Carvalho (✉)
Florida Institute of Technology, Melbourne, FL 32901, USA
e-mail: mcarvalho@fit.edu

V. Pappu et al. (eds.), *Optimization and Security Challenges in Smart Power Grids*,
Energy Systems, DOI: 10.1007/978-3-642-38134-8_8,

1 Introduction

In electric power industry, the primary focus has always been in maintaining safety and reliability of the grid infrastructure when deploying new power-related equipment. Traditionally the communication and information technologies are considered of secondary importance, often seen as just another device to help achieve power system reliability. However, with the increasing adoption of smart grid technologies, the information infrastructure is becoming critical to the operation and the reliability of the power system. Equipped with this modernized full digital technology and smarter features to handle such complexity, the traditional electric grid is elevated as or referred as smart grid. It transforms the entire electricity value chain, the way electricity is transmitted, distributed, consumed, and charged. A reliable, resilient, secure, flexible, and manageable standards-based information and communication network is the backbone of a smart grid (Pothamsetty and Malik 2009).

Communication network provides the intelligent link between the major elements or domains across entire electrify delivery system. This means distributed intelligent information processing is needed for critical decision-making and performance control, both locally and globally at the entire grid. Adding intelligence throughout the newly networked grid presents many benefits, including improved electric grid reliability and power quality; improved responsiveness; increased transmission and distribution efficiency; and potentially reduced costs for the service providers and customers. It also provides the communication platform for new applications; and builds a suitable economy that ensures future prosperity. Such benefits of reliability and efficiencies in electric grid can be established with the centralized energy and information management, smart devices and applications that enable a finer level of visibility, control and automation.

The key attributes of the smart grid are (U.S. Department of Energy 2009a): the deployment of technologies to enable customers in active involvement; the support distributed power generation and storage; the provisioning of stable power quality; the optimization of power generation, distribution, and consumption. It is also expected that smart grid should anticipate automatic response to system disturbances and load fluctuations; and operate resiliently against physical, cyber attacks, and natural disasters and exhibit self-healing ability.

However, because of increasing adoption of distributed intelligence and broadband communications would also add a new layer of complexity and effectively introduce new challenges. A prerequisite for a safer and secure smart grid is the interoperability of security controls and compliance with standards and regulations. Some of the main security challenges related to smart grid technologies, standards, regulations and management are discussed in this chapter.

2 Overall Architecture of Smart Grid

The smart grid emerges through the integration of advanced information and communication technologies (ICT) into the entire electricity value chain—right from generation to the end users. Dynamic two-way digital communication is possible through ICT at all levels of power grid. The conceptual model of smart grid by the U.S. National Institute of Standards and Technology (NIST), as shown in Fig. 1, defines seven important domains (NIST 2010): bulk generation, transmission, distribution, customers, operations, markets and service providers, along with all the intercommunications and energy/electricity flows among each domain.

Each domain is comprised of important smart grid components connected to each other through two-way communications and energy/electricity paths. The architecture overview based on the three layers—physical power/energy, communication, and application is depicted in Fig. 2. The end-to-end architecture with more details is represented in Leeds (2009).

There are several key elements in detailed logical model such as networks (wired and wireless), functional subsystems (such as the supervisory control and data acquisition (SCADA), etc.), endpoints (e.g., computers in the back offices, monitored and/or controllable substation devices), and overlays (such as distributed security functions and elements) (Metke and Ekl 2010).

The smart grid can be represented as a network of many systems and subsystems, as well as a network of networks, where each domain is expanded into three smart grid foundational layers:

- Physical power/energy layer (generation, transmission, substation, distribution systems, and energy consumer/end users)
- Communication layer (data transport, communications infrastructure and networks)

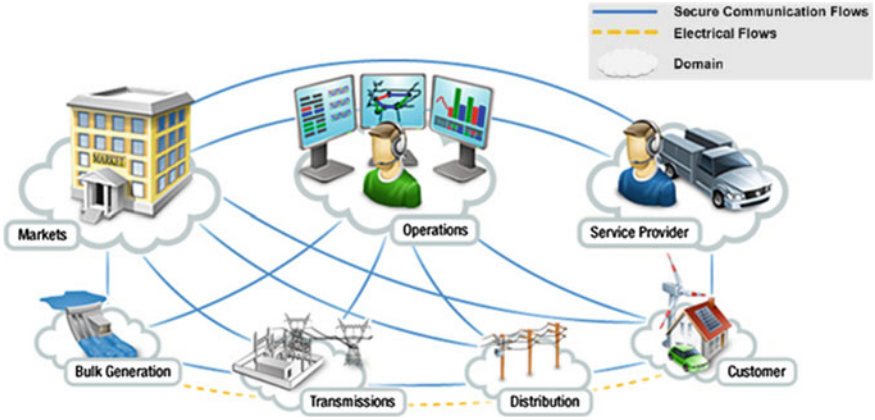

Fig. 1 Smart grid conceptual model by NIST

- Application layer (applications e.g., demand response control, billing, outage control, load monitoring, real-time energy markets, and a new range of customer services).

Of these three layers, the communication layer is the new enabling infrastructure of the power/energy layer that makes the electric grid “smarter”. It interconnects a variety of systems and critical devices (such as smart meters, sensors, grid components, and energy management systems (EMS)), physical power/energy layer to application layer, to allow every part of the grid to communicate both up and down the energy supply chain.

The communication layer leverages the same internet technologies that have transformed other high-tech industries. These internet technologies are now enabling distributed intelligent systems to be deployed in the electric grids for many purposes, including remotely monitoring, control, analysis, reporting, forecasting, recovery, and others.

Moreover, to help with the development of required standards, the power industry is gradually adopting different technologies (or rather networks) for the partitioning of the communication layer of the smart grid. Devices and applications in each domain are network end points.

Examples of applications and devices in the customer domain include smart meters, smart appliances, smart thermostats, energy storage, plug-in hybrid electric vehicles (PHEV), and distributed generations (e.g., solar energy as photovoltaic (PV), wind turbines, etc.). Applications and devices in the transmission or distribution domain include phasor measurement units (PMUs) in a transmission line substation, substation controllers, distributed generation, and energy storage.

Applications and devices in the operations’ domain include SCADA systems and computers or smart screen at the operations centre. Applications in the operations, market, and service provider domains are similar to those in Web and business information processing. The following technology solutions must be developed and implemented to achieve the vision of the smart grid (NETL 2010):

- Information and communications networks
- Advanced metering infrastructure (AMI)
- Customer side systems and demand response (DR)
- Distribution management system/distribution automation (DMS)
- Transmission enhancement applications and grid optimization
- Distributed energy resources (DER) and storage.

2.1 Information and Communication Networks

On the basis of Smart Electric Grid functional requirements, the network should provide the capability to enable an application in a particular domain to communicate with an application in any other domain over the information network, with proper management control as to who and where applications can be interconnected.

Therefore, the key element of the smart grid is the installation of a completely new two-way information and communication network between the energy suppliers and their customers. This network can be constructed by employing various architectures, with one of the most common being local concentrators that collect data from groups of meters and transmit that data to a central server via a backhaul channel. A variety of communication media and technologies that can be considered to provide part or all of this architecture are includes the copper wiring or optical fiber, hybrid fiber coax, power line carrier (PLC) technology, broadband over power lines (BPL), wireless technologies, internet, etc.

These networks include the Enterprise Network that connects control center applications to markets, generators, and with each other. Local area networks (LAN) are used to identify the network of integrated smart meters, field components, and gateways that form the logical network between distribution substations and a customer's premises; wide area network (WAN) connect the network of upstream utility assets, including-but not limited to-power plants, distributed storage, substations, and so on.

Field area networks (FAN) connect devices, such as intelligent electronic devices (IEDs) that control circuit breakers and transformers; and, home area network (HAN) enable smart appliances, and ultimately smart homes and buildings; as well as the advanced metering infrastructure (AMI) and feedback on demand response. As Fig. 2 shows, the interface between the WAN and LAN consists of substation gateways, while the interface between LAN and HAN is provided by smart meters. These networks may be implemented using public (e.g., the Internet) and non-public networks in combination. Both public and non-public networks will require implementation and maintenance of appropriate security and access control to support the smart grid (NIST 2010).

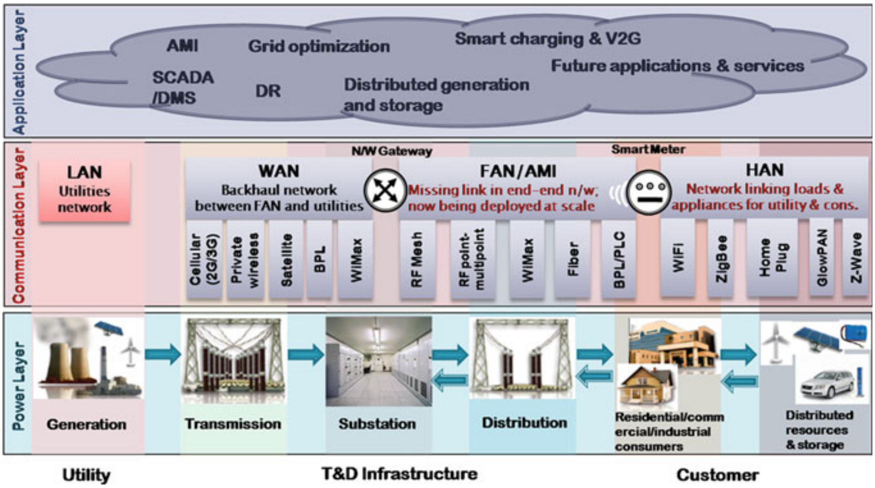

Fig. 2 Simplified three-layer architecture model for smart grid (Leeds 2009)

Low speed transmission SCADA and EMS applications have been successfully integrated among regional transmission organizations, generators, and transmission providers. But these applications need further improvement to fully utilize the integrated, high-speed communications system required by the smart grid. PLC technology has been in use for many years in utility industry. Originally focused on the internet access and voice over internet protocol (VOIP) for consumers, BPL carrier technologies is becoming increasingly accepted and successfully deployed to meet utility needs for DER, automated meter reading (AMR), DR, and consumer portal applications, as well as video monitoring (primarily for security), and other high-speed data applications. Wireless technologies are also currently being developed and demonstrated, but they are not yet used in the grid communication infrastructure on either the system or the user side.

BPL is a technology that allows data to be transmitted over utility power lines. BPL has been implemented in the U.S. and other countries on medium voltage distribution lines, but it has not been applied to HV lines. BPL signals have less attenuation on HV lines and can, therefore, travel longer distance. These are also more amenable to noise-mitigation techniques than distribution lines.

2.2 Advanced Metering Infrastructure (AMI)

One of the important components of AMI is the smart meter. Earlier meters are being replaced by their smarter counterparts, which provide many more capabilities, such as taking usage data in shorter intervals, sending meter readings back to the billing system, alerting in case of power failure, monitoring power quality etc. Public networks (such as the Internet) enabling communications between the service provider and consumers is an integral part of the AMI. Smart meters are envisioned to reside on customer site and send information via the data network to the utility company. Conversely, the utility company can also use the same infrastructure to send commands, updates or new configurations to the remote meters.

An important AMI building block is the data reception and management system (FERC 2013), where the data is collected, processed, and made accessible to the service provider. Integrated home energy management software and related display units simplify user interaction with the AMI system.

An AMI system requires significantly greater bandwidth than automated meter reading (AMR) systems and is more sophisticated than older AMR standards. Besides monitoring, AMI offers efficient control and improved visibility. Energy consumer can utilize smart power sockets and smart appliances to better control consumption, in coordination with the smart meter.

For example, using pool pumps, charging PHEV, heating water, etc. require high power consumption. If many users choose to perform these activities at the peak hour, it may compromise the functionality of the system. AMI components enable users to make smart and mutually beneficial decisions with the utility company, and provide users with the means to actively manage their own consumption. AMI helps the customer to take advantage of real-time pricing, off-peak rates and other programs offered by utility companies. AMI system can render a host of information including tamper notification, swell events, peak KW readings etc.

2.3 Transmission and Distribution Management and Control

The transmission systems and the centralized generating assets are required to be enable a more reliable and efficient infrastructure. In Smart Grid, we can have wide area monitoring systems (WAMS) that will make use of integrated advanced sensors and phasor measurement units (PMU). WAMS will enable the development and deployment of advanced Grid applications for improved situation awareness. It will also facilitate the system operators' to respond immediately and accurately to any disturbance in the system (U.S. Department of Energy 2009b). Development of advanced operational algorithms and compatible controlling mechanisms may enable the design of resilient and seal-healing capabilities for the Grid.

The North American Synchro Phasor Initiative (NASPI) organization has undertaken a PMU installation roadmap, and standardization of voltage levels for PMUs. PMU is used to read voltages, currents, frequency and other information with very high accuracy, speed and synchronization. These measurements are also known as synchro phasors. Measurements are highly synchronized and time-aligned by means of accurate GPS- synchronized clocks. A more accurate picture of the large grid system can be formed, for example, by combining measurements from various PMU sites.

Applications can process these high dimensional data read from various points and provide grid operators with features to visualize the state of the grid in a comprehensive manner and with high fidelity. These applications will also be able to aid experts to notice evidence of changing conditions and nascent grid anomalies. With sophisticated data visualization and analysis software, these new measurements can be used to drive power system planning and forensic analysis (U.S. Department of Energy 2009b).

2.4 Distributed Energy Resources and Energy Storage

Smart grid will allow integration of various sources such as wind turbines, micro turbines, photovoltaic (PV) arrays, etc. Plug-in hybrid electric vehicle (PHEV) could also act as a temporary energy source if necessary. All these sources are time-varying and distributed in nature. These will help the utility to a great extent to satisfy dynamic load, especially at the peak hour. Enhanced communication and automation is required for large-scale deployment of DER and to integrate these time-varying sources into their grid without creating instability and load balancing problems.

To render the energy demand instantaneously and in a stable manner, the DER integration will require backup source for generation and energy storage system. All these will help the utility to meet the peak demand without investing huge amount of resource for a comparatively very short time period. This will result in reduced energy cost for customers and encourage utility companies to help and reward cooperating parties involved in generation and charging/discharging activities. It will also enhance the integration of non-dispatchable generation resources into the power grid. Besides PHEV, other existing options for energy storage are batteries, pumped storage hydroelectric, compressed air storage, flywheel storage, thermal storage, and magnetic superconducting storage.

3 Smart-Grid Standards and Interoperability

In order to realize the promise of smart grid, it is critically important to define and adopt an appropriate set of standards, as they directly affect the interoperability, compatibility, reliability, and efficiency of the overall system. Standards define specifications for languages, communication protocols, data formats, linkages within and across systems, interfaces between software applications and between hardware devices, and much more. One key requirement of the smart grid is the interoperability of the cyber systems used to manage the power systems. Interoperability can be defined as the ability of two or more networks, systems, devices, applications, or components to exchange and readily use information—securely, effectively, and with little or no inconvenience to the user (IEEE 1990).

The Smart Grid will be a system of interoperable systems. Standards are essential for each interface to support many different Smart Electric Grid applications and also needed for data networking and cyber security throughout the grid. Security standards are used to establish requirements on the security operations of energy service providers (e.g., utilities, generators, system operator, etc.) as well as smart grid device manufacturers. Many power industry standards organizations, for example, the National Institute of Standards and Technology (NIST), the North American Electrical Reliability Corporation (NERC), the International Society of Automation (ISA), the National Infrastructure Protection Plan (NIPP), and the American National Standards Institute (ANSI), are assisting in the development of frameworks for both smart grid standards and security requirements. The NIST has primary responsibility for coordinating development of an interoperability framework allowing smart grid technologies to communicate and work together. The Electric Power Research Institute (EPRI), Institute of Electrical and Electronics Engineers (IEEE), and International Electrotechnical Commission (IEC) are also working alongside NIST to develop guidelines for smart grid security and interoperability. The NIST has identified five "foundational" sets of standards for smart grid interoperability and cyber security that are ready for consideration by federal and state energy regulators. Over 100 standards have been identified by IEC, focus on information models and protocols critical to reliable and efficient grid operations as well as cyber security.

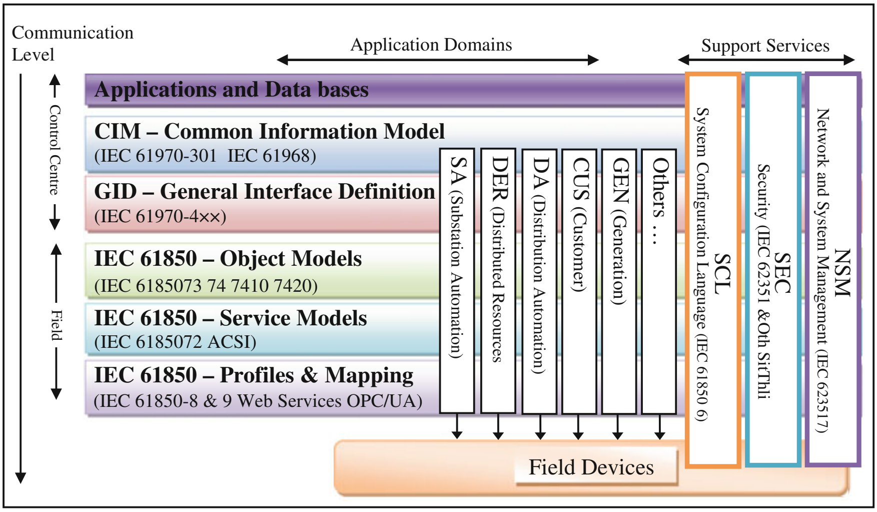
Communication Level
Application Domains
Support Services
Control Centre
Field
Applications and Data bases
CIM – Common Information Model
(IEC 61970-301 IEC 61968)
GID – General Interface Definition
(IEC 61970-4××)
IEC 61850 – Object Models
(IEC 6185073 74 7410 7420)
IEC 61850 – Service Models
(IEC 6185072 ACSI)
IEC 61850 – Profiles & Mapping
(IEC 61850-8 & 9 Web Services OPC/UA)
SA (Substation Automation)
DER (Distributed Resources
DA (Distribution Automation)
CUS (Customer)
GEN (Generation)
Others ...
SCL
System Configuration Language (IEC 61850 6)
SEC
Security (IEC 62351 &Oth SifThi
NSM
Network and System Management (IEC 62517)
Field Devices

Fig. 3 IEC 61850 Models and Common Information Model (CIM) (CSWG 2010)

These standards will be further updated to achieve efficient and secure intersystem communications as Smart Electric Grid requirements and technologies evolve. The core IEC standards and their functions are given below (IEC 2013). The specialized communication standards developed by IEC are illustrated in Fig. 3.

- IEC 61970 and IEC 61968: Providing a common information model (CIM) necessary for exchanges of data between devices and networks, primarily in the transmission (IEC 61970) and distribution (IEC 61968) domains. CIM standards are integral to the deployment of a smart grid scenario, in which many devices connect to a single network.
- IEC 61850: Facilitating substation automation, distributed generation (solar PV, wind power, fuel cells, etc.), SCADA communication and distribution automation as well as interoperability through a common data format.
- IEC 60870-6: Facilitating exchanges of information between control centers.
- IEC 62351: Addressing the cyber security of the communication protocols defined by the preceding IEC standards. Cyber security is such a major concern with smart grids, which are especially vulnerable to attack because of the two-way communication between devices and the utility grid.

These five IEC standards were among the 25 smart grid-relevant standards identified as "ready for implementation" in the *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0*, which was issued in January 2010 (NIST 2010).

However, these specifications required a cyber security review that could not be completed until NIST finalized its initial *Guidelines for Smart Grid Cyber Security*, which were published in early September 2010 (CSWG 2010). CIM enables vertical and lateral integration of applications and functions within the Smart Grid. IEC 61850 and its associate standards are emerging as favorites for WAN data communication, supporting TCP/IP, among other protocols, over fiber or a 1.8-GHz favor of WiMax.

The communication and interoperability standards developed by IEEE (2013) are IEEE 802.3 (Ethernet), IEEE 802.11 (WiFi), IEEE 802.15.1 (Bluetooth), IEEE 802.15.4 (Zigbee), IEEE 802.16 (WiMax). Moreover, the most relevant ANSI standards for interoperability of AMI systems include ANSI C12.19 (metering "tables" internal to the meter) and ANSI C12.22 (communications for metering tables). ANSI C12.22 and its associate standards are viewed as the favorite LAN standard, enabling a new generation of smart meters capable of communicating with their peers as well as with their corresponding substation gateways over a variety of wireless technology.

NIST has developed very important guidelines related to cyber security information technology and secure interoperability. Two documents of particular interest for the Smart Electric Grid are: NIST SP-800-53 (recommended security controls for federal information systems) and NIST SP-800-82 (Guide to industrial control systems (ICS) Security). Broadly speaking, there are four levels of cyber security standards (Cleveland et al. 2008):

1. Media related standards—Specific to fiber optics, microwave, WiFi, wires, telephones and cellphones
2. Transport related standards—Internet standards including Ethernet, Internet Protocol (IP), Transport Control Protocol (TCP), Hyper Text Transfer Protocol (HTTP)
3. Application related standards—Hyper Text Markup Language (HTML), EXtensible Markup Language (XML), IEC 61850, Common Information Model (CIM)
4. Security related standards—Advanced Encryption Standard (AES 256), Public Key Infrastructure (PKI), secret keys, and certificates.

4 Smart Grid Security and Cyber Security

The Smart Electric Grid will require the development and deployment of several new technologies, such as smart meters, sensors, extensive computer network connectivity for a two-way communication infrastructure that supports the new sophisticated features like real-time information and control for electric power grid. However, such increasing network connectivity and telecommunication capabilities, in smart grid, require both physical security and cyber security management to safeguard the critical infrastructure elements across entire electricity delivery system. Cyber security, in particular, has always been a concern for utility IT experts, but has become a more significant issue due to the increasing penetration of smart grid technology. These technologies expand the application of network information systems to utility and customer assets that previously required manual operation and were not remotely accessible. Securing the assets of electric power delivery systems, from the control centers to the substations, to the feeders and even to customer meters, require an end-to-end security infrastructure that protects the large number of communication assets (control center-based SCADA, RTUs, PLCs, power meters, digital relays, and bay controls) used to operate, monitor, and control power flow and measurement. Security of energy systems and electronic information in the IT and telecommunication infrastructure includes the confidentiality, integrity, and availability on all related cyber physical systems.

- **Integrity** of telemetry data and control commands is the most critical security requirement for the proper functioning of the smart grid and support the consisting and accuracy in delivery and billing. It includes assurance that data has not been modified without authorization, source of data is authenticated, timestamp associated with the data is known and authenticated, and quality of data is known and authenticated.
- **Availability** is generally considered the next most critical security requirement, although the time latency associated with availability can vary 4 ms for protective relaying, sub-seconds for transmission wide-area situational awareness monitoring, seconds for substation and feeder SCADA data, minutes for monitoring non-critical equipment and some market pricing information, hours for meter reading and longer term market pricing information, and days/weeks/months for collecting long term data such as power quality information.
- As the smart grid reaches into homes and businesses, and as customers increasingly participate in managing their energy and their information is more easily available in cyber website, **confidentiality** and **privacy** of their information have increasingly become a concern. Unlike power system reliability, customer privacy is a new issue. Not only this, electric market information and general corporate information, such as human resources, internal decision-making, etc. have some confidential proprietary value.

A lack of adequate security in the electric power industry could pose threats of service disruption, which can impede safe and efficient functioning of the electric grid. The most common malicious attack includes both attempts to physically tamper with a meter, and disruption of the supporting communications infrastructure. Security is not just about preventing attacks or system compromises; it is also about preventing the accidental or malicious leakage of information. Particularly for real-time operations, it is crucial to “live through” any attacks or compromises to the information infrastructure, and to recover with minimal disruption to the power system operations—including power system reliability, efficiency, and cost.

Because of the large variety of communication methods and performance characteristics, as well as because no single security measure can counter all types of threats, it is expected that multiple levels of security measures needs to be implemented. Added layers of security controls, policies, and procedures are necessary to prevent, detect and manage security risks in power grids.

Security of information exchanges will also require end-to-end security from the sender of the information all the way across through all intermediate paths to the final receiver of the information. Accordingly, information security must address not only fixed assets and devices but also the virtual paths and information flow from end to end. This end-to-end aspect of security makes it far more difficult to assess the control risks—threats, vulnerabilities, and impacts—as well as to determine the most appropriate security solutions. The NIST smart grid cyber security coordination task group (CSCTG) was established to ensure consistency in the cyber security requirements across all the smart grid domains and components.

Thus the most critical infrastructure necessary to create a reliable high-performance smart grid is the information and communications networks. Functional requirement of communication infrastructure is that the network should enable an application in a particular domain to communicate with an application in any other domain in the information network, with proper management and control over who and where applications can be interconnected.

4.1 AMI Security

The operational imperatives for AMI Cyber Security (AMI-SEC) Task Force (2008) recognize the existence of gaps in risk management between AMI and traditional information and communications technology (ICT) systems. Typically, AMI lies at the intersection of physical and logical infrastructures. AMI's resiliency not only demands security and continuity, but rethinking the relationship of systems to services. Without proper security in AMI systems, electricity distribution will be unreliable and interruptible both on a physical and logical scale. An AMI system's potential exposures may exist in control functions in the form of remote service disconnects and management of devices in home area networks (HAN). These potential exposures exemplify the increased risk against the grid as a whole. AMI-SEC Task Force (2008) was developed the security domain model to boundary the complexity of specifying the security requirement to implement a robust, secure AMI solution as well as serve as a tool to guide utility companies in their AMI implementation. The "services" provided in Table 1 are described for security domains (AMI-SEC-ASAP 2008).

4.2 Substation Security

Substations, transmission and distribution domains include the devices such as circuit breakers, power transformers, phase-shifting transformers, capacitor banks, switches, etc. It may also contain various electronic automation and communication devices used to measure, monitor, and control the substation components.

The increasing level of automation envision in smart grids, are likely may open the door for malicious activities. In other words increased automation, if not performed with comprehensive security evaluation, can result in new vulnerabilities related to the substation devices. Potential consequences of exploitation of vulnerabilities

Table 1 Various applications and associated services

Security domain	Description
Utility Edge Services	All field services including monitoring, measurement and control to be controlled by the Utility provider
Premise Edge Services	All field service applications including monitoring, measurement and control controlled by the customer (customer has control to delegate to third party)
Communications Services	These applications relay, route, and perform field aggregation, field communication aggregation, field communication management information
Management Services	Provide support services for automated and communication services (includes device management)
Automated Services	Allow unattended collection, transmission of data and performs the necessary translation, transformation, response, and data staging
Business Services	Support core business applications (includes asset management)

resulting from substation automation are grid instability, power outages, destruction of generators, which are highlighted in U.S. Department of Energy (2009b).

To automate substation without introducing new security vulnerabilities, and important security goals should be given high priority. Authentication and authorization must be enforced to prevent intruders and unauthorized operator users from accessing and tampering with distribution devices, running unauthorized commands.

The transformation must also ensure integrity and confidentiality of telemetry data, control protocols and other administrative information. It must also emphasize the protection of upstream assets. The processes used to manage energy routing from plant to consumer and fidelity of the energy delivery systems are defined by the telemetry and control systems security zone.

4.3 SCADA Security

SCADA systems now are becoming increasingly connected to the public Internet, which enables the fielding of new equipments such as intelligent electronic devices (IEDs). Such deployments, however, are likely to make the SCADA system more vulnerable (Ericsson 2010). Remote device monitoring is the key to enhancing the reliability of the electric power grid. The substations along the electricity supply chain contain many remote terminal units (RTUs) and IEDs.

However, the monitored data from these substations can only be relied upon if the integrity of the data is assured. The various new issues related to SCADA system have been emphasized in the CIGRÉ working groups JWG D2/B3/C2.01 “Security for Information Systems and Intranets in Electric Power Systems” (Ericsson et al. 2007) and D2.22 “Treatment of Information Security for Electric Power Systems” (Ericsson et al. 2010).

There is a need to perform case-by-case technical assessments of all vendor products, studying provide expose and the protocols they use so that their security can be assured within the greater cyber security context. Security for such devices is being standardized according to the IEC 62351 standards.

4.4 Communication Link Security

As wireless devices are inexpensive and provide significant advantages over wired counter parts, they are being prevalent in current Smart Grid deployments. Many AMI implementations are using mesh networks because its reliability and redundancy. However, their security aspects are not publicly available at this point and most of these implementations are based on IEEE 802.15.4 protocol and there are known vulnerabilities with its implementations.

4.5 Security Protocol Design Challenges

The incorporation of advanced ICT in power grid will require many communication protocols. It is likely that many of these protocols will be based on customized versions of existing protocols, borrowed from other domains. However, the adaptation and use of technologies from different domains require an appropriate mapping and match at several abstract levels, including the conceptual level, system policy level, formats and algorithms level and implemented tools level. A detailed discussion and case study of such adaptations can be found at Khurana et al. (2007).

If for a particular level or application, requirements for the power grid are significantly unique, new protocol should be designed from scratch. Protocols should also be modular and must provide multiple levels of defense, so that they can be easily replaced with newer modules in case of discovery of a flaw. Computational and communication overhead of the protocol must be evaluated. Error handling is another important area that required significant attention while designing protocols. Protocol must guarantee the authenticity of the messages and try to optimize other issues.

4.6 Cryptographic Key Management

Managing and protecting keys is a problematic task for many users. Cryptographic functions are computationally expensive, too, especially for smart devices with limited physical resources. So, we can follow the approach of Computational Grid (C-Grid), to some extent. Still, for power grid (P-Grid), much customization is required. Federated authentication services like single sign-on may also be used.

4.7 Error Handling Challenges

Systems that do not perform error checking of invalid inputs are susceptible to crush and execute arbitrary code at some point. On the other hand rigorous bounds checking and error management can sometimes lead to problems, too. So, balance must be maintained so that the system does not execute alien code and can survive from distributed DoS attacks.

4.8 Challenges due to Ad Hoc Automation

Although the envisioned Smart Grid deployment has not been completed yet, the current grid is being automated and updated in different parts on a regular basis. New smart meters are being deployed for operational conveniences. Many of these improvements are being carried out without any comprehensive security assessment. These smart devices have lifecycle of several years. Competition to be the first to market, many of the vendors are rushing and not providing considerable care in comprehensive security consideration.

4.9 Smart Grid Security Challenges: Summary

There are many security challenges need to be addressed as the power grid is fully integrated to the cyber infrastructure, we summarize some important smart grid security challenges in Table 2.

5 Conclusions

The basic framework of Smart Electric Grid and most significant technologies/elements that must be developed and implemented to achieve the vision of the Smart Electric Grid are briefly discussed in this chapter. To achieve efficient and secure intersystem communications and to properly manage and control the power system, one key requirement of the Smart Electric Grid is the standards related to interoperability and cyber security.

Various organizations are actively involved in the development of these important standards. This chapter briefly surveyed the different standards for Smart Electric Grid. Moreover, one critical aspect of the Smart Electric Grid related information and communications infrastructure is the physical and cyber security. Infrastructure security that includes the protection of networks and servers from unauthorized accesses and malicious attacks are discussed.

Table 2 Summary of important smart grid security challenges

Specific problem	Description of problem
Privacy of usage data (McDaniel and McLaughlin 2009; IEEE 2010a)	• Usage data and statistics will be of paramount importance to entities for business intelligence and also to malicious hackers for launching targeted and well informed attacks. Existing policies do not describe all possible scenarios • Government need to establish a national regimen for consumer protections
Vulnerabilities and exploitation restriction (McDaniel and McLaughlin 2009; IEEE 2010b; INL 2009)	• General-purpose operating systems doing real time control is far riskier than well tested finite state machines implemented in special purpose hardware. Limits must be imposed on systems to limit worst-case behaviors. These limit conditions must be locally controlled and must not be remotely programmable • Hackers may gain unauthorized access to Smart Meters to manipulate its functionalities and make the grid unstable and cause financial loss • Extraction of data and encryption key from device memory was demonstrated
Communication networks and links vulnerability (IEEE 2010a; INL 2009)	• Most mesh networking protocols are based on IEEE 802.15.4 standard which is reported to be susceptible to a set of known types of attacks • As the vendors of wireless AMI technology are in a rush to develop and deploy market, security may not receive sufficient emphasis
Key management (IEEE 2010a; Khurana et al. 2007; Sugwon and Myongho 2010)	• Currently, it's not feasible to operate Cryptographic key management or similar services for 5.5M smart meters. Key management is required to be planned for various communication modes, such as master-to-IED, peer-to-peer and broadcast • Analogous C-Grid tools can be used in P-Grid to facilitate single sign-on based access to a multitude of resources across organizational boundaries. Scaling such accesses requires federated approaches where the organizations agree on a common authentication and authorization system for accessing data and resources
Intrusion detection (IEEE 2010b; Khurana et al. 2007; Sugwon and Myongho 2010)	• Organizations need to define security policies, deploy monitoring systems supported by advanced IDSs, and set up mechanisms for forensic analyses and development of a communication process to share incident data with other organizations and a response in a coordinated fashion
Operational cost (IEEE 2010b)	• Operational cost of a million-node network, where significant portion of resources need to be invested in monitoring and continuous analyzing of threats and compromises, is another challenging issue

(continued)

Table 2 (continued)

Specific problem	Description of problem
Development cost effectiveness (Sugwon and Myongho 2010)	• Implementing complex security functionalities on embedded microprocessor based platform is not feasible because of these devices' limited computational ability. Besides security functions, these devices also have to receive network packets and are vulnerable to Kernel live-lock resulting from too much interrupt handling. For capturing high-rate arriving packets, an expensive alternative is to use specialized hardware such as network processors in the monitoring cards. Some dedicated hardware, possibly FPGA-based co-processors or hardware accelerators or graphic processor may be used to for cryptographic functionalities. One less expensive alternative is to use Chip-level MultiThreading processor, such as ARM11 MPCode (quad-core)
Transition (Sugwon and Myongho 2010; Kouril et al. 2006)	• Transition is another challenging task involving finding workarounds for already deployed IEDs with limited processing capabilities and lack of security features. For such devices, there are two transition scenarios for achieving security: "bump-in-the wire (BITW)" and "bump-in-the stack (BITS)" solutions • Transition cost will also be very high for setting up smart metering infrastructure. But some interesting findings suggest that end consumers are willing to make onetime payment of $48 on average or $13 per month. This will offset the transition expense to great extent
Error handling (IEEE 2010b; Khurana et al. 2010)	• Only the input sequences that are within defined safety boundaries should be allowed • Common techniques include back off timers, limits on number of events reported, event reporting compression and suppression techniques, and both in-band and out-of-band reporting. Increased complexity in the error management process, leads to an increase in edge cases as well • Protocols having no mechanism to handle malformed or unexpected packets may fail or possibly execute arbitrary code
Fault and failure modeling (IEEE 2010b)	• Our current modeling capability is also limited. We need to model faults and failures more accurately with respect to security incidents. We must also undertake analyses assuming a substantial number of faults and failures in wide array of combinations
Recovery after failure (McDaniel and McLaughlin 2009; IEEE 2010b)	• Comprehensive recovery strategies must also be developed through close collaboration between utility companies and vendors • A backup plan is necessary that will allow some level of power operations when the computers don't work properly

(continued)

Table 2 (continued)

Specific problem	Description of problem
Efficiency (IEEE 2010a)	• Efficiency and scalability must meet varying real-time requirements based on the location. Constrained network and devices must also be considered
Evolvability (IEEE 2010a; Khurana et al. 2010)	• The design should be modular, so that it can be easily upgraded later on with minimal disturbance to other components working properly
Data management (Khurana et al. 2007)	• Managing and accessing large amount of energy usage and business related data at control center are challenging issues. To utilize this data several C-Grid techniques such as data federation, data virtualization and integration and data location services can be realized
Load management (Khurana et al. 2007)	• Energy can be treated as a resource and its delivery to an appliance can be treated like a task. Now we can utilize C-Grid's task scheduling techniques to efficiently perform load management in the P-Grid
Breaching of trust (IEEE 2010a)	• Most of the control systems' design decisions are based on implicit trust. So, methods to deal with untrustworthy participants are required
Security protocol design challenges (Khurana et al. 2010; Sugwon and Myongho 2010)	• Security goal should aim for complete guarantee for message authenticity and integrity from protocols. The grid applications require high performance, high availability, timeliness, comprehensive security design, adaptable and evolvable designs etc. So, protocols must be developed considering these fundamental constraints • For power grid a potential approach is to use existing protocols upon customization for P-Grid. New protocols could be designed, too, if requirements are fairly unique. In Khurana et al. (2010), design principles are proposed considering traditional tools, known cyber attacks and protocol goodness properties • Computation and communication overhead should also be analyzed thoroughly for designing efficient protocols. Error handling, detection of cyber attack & proper responses and evolvability should also be considered carefully to design a highly available protocol. The design should be modular, so that it can be upgraded easily
System complexity (INL 2009)	• Risk resulting from cyber attack depends on threats, vulnerabilities and consequences which is very difficult to estimate. The size and dynamic nature deteriorates the scenario by adding up more complexity and uncertainty. It is hard to predict how an attack can be manifested given the adversary is reasonably intelligent. Emphasis on cost minimization and market capturing than security analyses in the face of incomprehensible threats may result in deployment of vulnerable systems

(continued)

Table 2 (continued)

Specific problem	Description of problem
SCADA automation without proper security (INL 2009)	• SCADA Security assessment has been conducted in the past and several vulnerabilities have been found. Among 17,325 transmission substations in the US and Canada, 81 % and 57 % of distribution substation have some form of automation and these are increasing day by day. Study found that new vulnerabilities are introduced which are associated with substation automation
PMU Vulnerabilities (INL 2009)	• NASPI (North American SynchroPhasor Initiative) security has not yet been sufficiently explored. In Smart Grid there are many physically unprotected potential entry points. Wireless networks can be easily sniffed by attackers and these are susceptible to Man-in-the-Middle attacks. There are weaknesses in security mechanisms to prevent these attacks
Massive deployment of intelligent sensors (Jain and Chapman 2010)	• Large scale deployment of new tiny devices, called Heterogeneous System on a Chip (HSoC), is proposed to sense and autonomously reconfigure power system. Three layered sensor is envisioned. VLSI implementation details of the first two layers, powers system sensing and decision making layers. In addition to detection of failures in power system, handling of chip faults are also addressed
Cooperation among various organizations (Khurana et al. 2007)	• Collaboration and sharing among various organizations is needed to fight against intrusion and malicious activities
Lack of comprehensive security strategy (U.S. Department of Energy 2009a; IEEE 2010b)	• We must develop security architecture appropriate to the Smarter Grid's needs. The power engineering community must welcome security community and work together

References

AMI-SEC-ASAP (2008) AMI-SEC-ASAP, AMI system security requirements-v1.01, December 2008. http://osgug.ucaiug.org/utilisec/amisec/default.aspx. Accessed 15 March 2011

Cleveland F, Small F, Brunetto T (2008) Smart grid: interoperability and standards—an introductory review. Utility Standard Board, September 2008

CSWG (2010) Cyber Security Working Group (CSWG) of the smart grid interoperability panel (SGIP)—NIST. Introduction to NISTIR 7628. Guidelines for smart grid cyber security. September 2010. http://www.nist.gov/smartgrid/upload/nistir-7628_total.pdf

Ericsson GN (2010) Cyber security and power system communication—essential parts of a smart grid infrastructure. IEEE Trans Power Delivery 25(3):1501–1507

Ericsson G, Torkilseng A, Dondossola G, Jansen T, Smith J, Holstein D, Vidrascu A, Weiss J (2007) Security for information systems and intranets in electric power systems. Tech. Brochure (TB) 317 CIGRÉ

Ericsson G, Torkilseng A, Dondossola G, Piètre-Cambacédès L, Duckworth S, Bartels A, Tritschler M, Kropp T, Weiss J, Pellizzonni R (2010) Treatment of information security for electric power utilities (EPUs). Tech. Brochure (TB), CIGRÉ

Federal Energy Regulatory Commission (FERC) (2013), http://www.ferc.gov/eventcalendar/Files/20070423091846-EPRI%20-%20Advanced%20Metering.pdf

IEEE (1990) IEEE standard computer dictionary: a compilation of IEEE standard computer glossaries, New York

IEEE (2010a) Smart grid security issues, Computer and reliability societies, IEEE, January/February 2010

IEEE (2010b) The smarter grid, Computer and reliability societies, IEEE, January/February 2010

IEEE (2013) Approved IEEE smart grid standards. http://smartgrid.ieee.org/standards

INL (2009) INL/EXT-09-15500, Study of security attributes of smart grid systems—current cyber security issues, April 2009. http://www.inl.gov/scada/publications/d/securing_the_smart_grid_current_issues.pdf. Accessed 15 March 2011

International Electrotechnical Commission (IEC) (2013) http://www.iec.ch/

Khurana H, Khan MMH, Welch V (2007) Leveraging computational grid technologies for building a secure and manageable power grid. 40th annual Hawaii international conference on system sciences

Khurana H, Bobba R, Yardley T, Agarwal P, Heine E (2010) Design protocols for power grid cyber-infrastructure authentication protocols

Jain VK, Chapman GH (2010) Massively deployable intelligent sensors for the smart power grid. IEEE 25th international symposium on defect and fault tolerance in VLSI systems (DFT)

Kouril D, Matyska L, Procházka M (2006) Improving security in grids using the smart card technology. Grid computing, 7th IEEE/ACM international conference

Leeds DJ (2009) The smart grid in 2010: market segments, applications and industry players. GTM Research, July 2009

McDaniel P, McLaughlin S (2009) Security and privacy challenges in the smart grid. http://www.patrickmcdaniel.org/pubs/sp-smartgrid09.pdf. Accessed on 15 March 2011

Metke AR, Ekl RL (2010) Security technology for smart grid networks. IEEE Trans Smart Grid 1(1):99–107

National Energy Technology Laboratory (NETL) (2010) Understanding the benefits of the smart grid. Report (DOE/NETL-2010/1413), June 2010

NIST (2010) Report on NIST framework and roadmap for smart grid interoperability standards, release 1.0, January 2010. http://www.nist.gov

Office of the National Coordinator for Smart Grid Interoperability, National Institute of Standards and Technology (2010) NIST framework and roadmap for smart grid interoperability standards. Release 1.0 (NIST SP 1108), January 2010. http://www.nist.gov/public_affairs/releases/upload/smartgrid_interoperability_final.pdf. Accessed 15 March 2011

Pothamsetty V, Malik S (2009) Smart grid leveraging intelligent communications to transform the power infrastructure. CISCO Systems, white paper, February 2009

Sugwon H, Myongho L (2010) Challenges and direction toward secure communication in the SCADA system. Communication networks and services research conference (CNSR)

The North American SynchroPhasor Initiative (NASPI) (2013) www.naspi.org

U.S. Department of Energy (2009a) Smart grid system report, July 2009

U.S. Department of Energy (2009b) Study of security attributes of smart grid systems—current cyber security issues. Report by U.S. Department of Energy (DOE), Office of Electricity Delivery and Energy Reliability, April 2009