SECURITY COMMUNICATIONS NETWORK FOR INTEROPERABLE SMART GRID

JINWEN ZHU

Department of Engineering Technology
Missouri Western State University Saint Joseph, USA
E-mail: jzhu@missouriwestern.edu

Abstract- The ever increasing electric energy demand, together with the complex and nonlinear nature of the electric power distribution network, have caused serious power network issues in recent years. The promotion of modernized electric network (smart grid) that integrating control, automation, communication, information, and power technologies to deliver sustainable energy has been widely recognized. A smart grid system consists of many different subsystems that might have over millions of consumers and devices, the demand of its reliability is extremely critical. An interoperable communication network and its security is a key for the success of the emerging smart grid to deliver efficiently quality and reliable energy. In this paper, some of the key communications and their security challenges for realizing interoperable smart grid are presented. First, the background of smart grid system is introduced and the interoperability is addressed. Then, smart grid interoperable reference model (SGIRM) is described, and finally communication network and security measures for interoperability is presented. The aim of this paper is to offer a guideline of communication network and security requirements for interoperable smart grid.

Keywords- security, communication network, smart grid, interoperability, electrical power system

I. INTRODUCTION

The ever increasing electric energy demand, together with the complex and nonlinear nature of the electric power distribution network, have caused serious power network issues in recent years. In addition, the existing power grid suffers from the lack of pervasive and effective communications, monitoring, and automation, which further increase the possibility of region-wide system breakdown. Many nations urged to modernize their existing power grids to enhance their grids efficiency and reliability [1].

The modernized power network, the smart grid, "is an automated, widely distributed energy delivery network characterized by a two-way flow of electricity and information, capable of monitoring and responding to changes in everything from power plants to customer preferences to individual appliances" [2]. The smart grid conceptual model consisting of power system network, communication network, as well as seven domains is shown in Fig. 1 [3].

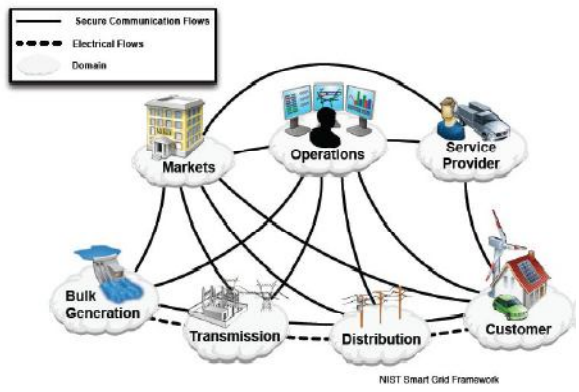

Figure 1. Smart grid conceptual model

The smart grid is a power system infrastructure requires both a complex two-way communication infrastructure, sustaining power flows between intelligent components, and sophisticated computing and information technologies for improved efficiency, reliability, and safety [4] [5]. With the increasing integration of renewable and alternative energy sources, plug-in hybrid and electric vehicles, as well as other energy equipment recently, thesmart grid becomes a large-scale distributed two-way power system characterized by different technologies and topologies [6][7]. Integration of energy technology and information and communications technology is necessary to achieve seamless operation for electric generation, delivery, and end-use benefits to permit two-way power flow with communication and control.

However, a heavy dependence oncommunicationsand networking systemsraises vulnerabilities of SmartGrid, which in turn increases therisk of compromising reliable and secure power system operation[8].It is important to note that the key to achieving the potential advantages of the smart grid is the successful design and implementation of a interoperable, reliable, and securecommunication infrastructure [9] [10]. This is a very challenging task since the communication network is an integration of various network segments that are responsible for maintaining the communications among a vast number of nonhomogeneous equipment including power facilities and end-user devicesthat are geographically spread. Moreover, the smart grid will generate data in vast quantities. To manage, store, and effectively use this data, the power system, communications, and information technologies should be coordinated using a system of systems

approach; that is, achieve interoperable security communications across smart grid technologies.

II. SMART GRID INTEROPERABILITY

Interoperability is the capability of two or morenetworks, systems, devices, applications, or components toexternally exchange and readily use information securely andeffectively [2].
Smart grid interoperability provides organizationsthe ability to communicate effectively and transfer meaningfuldata, even though they may be using a variety of differentinformation systems over widely different infrastructures,sometimes across different geographic regions and cultures.
Smart grid interoperability is usually associated with thefollowing [2]:

- Hardware/software components, systems, andplatforms that enable machine-to-machinecommunication to take place.
- Data formats, where messages transferred bycommunication protocols need to have a well-definedsyntax and encoding.
- Interoperability on the content level; a commonunderstanding of the meaning of the content beingexchanged.

Interoperability of the smart grid will allow utilities, consumers, and other stakeholders to purchase hardware and software in the marketplace and readily incorporate it into different areas of the smart grid so that it will work with other smart grid components. As the power system is upgraded with more flexibility, integrated communications, and advanced controls, it will enable large-scale integration and interoperability of a greater diversity of technologies and end-use applications.
The interface interoperability within the infrastructure is organized such that [2]

- The system can be easily customized for particular geographical, application-specific,or business circumstances, but
- Customization does not prevent necessary communications between elements of the infrastructure.

This interoperation will include a preponderance of monitoring and control activities, enabling two-way flow of electricity and information for the production, transportation, and consumption of electric energy. The diversity of evolving smart gridtechnologies intended for use across the entire power gridpresents significant challenges to achieving interoperability.Business processes, competition, relationship with partners,and different strategies should consider the need for interoperability.

III. SMART GRID INTEROPERABILITY REFERENCE MODEL

The smart grid interoperability reference model (SGIRM) [2] defines theinterfaces between functional domains of the power grid from each of the perspectives and describes therelationships among the domains, including the characteristics of the data that flow between them. Theconstraints, issues, and impacts on interoperability at these interfaces are considered for each domain. Withthis information, optimal design criteria for the interoperability of smart grid implementations can be planned.The SGIRM allows for extensibility, scalability, and upgradeability [2].

The SGIRM is a conceptual representation of the smart grid architecture from threehigh-level perspectives: 1) power systems; 2) communications; and 3) information technology. The SGIRM contains both entities and relationships within the environment of the smart grid and definesinterfaces in a technology-agnostic manner. Smart grid interoperability is meant to be achieved by consideration of these three perspectives. The goal of each perspective's architecture is to address interoperability among the elements of the smart grid. While the three technologies share this common goal, each perspective contains unique aspects addressed from its individual architectural-specific technology purposes.
The smart grid three interoperability architectural perspectives (IAPs)primarilyrelate to logical, functional considerations of power systems,communications, and information technology interfaces forsmart grid interoperability. A summary of the threeperspectives follows [2]:

- Power systems IAP (PS-IAP): The emphasis of thepower system perspective is theproduction, delivery,and consumption of electric energy includingapparatus, applications, and operational concepts. Thisperspective defines seven domains common to allthree perspectives: bulk generation, transmission,distribution, service providers, markets,control/operations, and customers.
- Information technology IAP (IT-IAP): The emphasis of the information technology perspective is the control of processes and data management flow. The perspective includes technologies that store, process, manage, and control the secure information data flow
- Communications technology IAP (CT-IAP): Theemphasis of the communications technologyperspective is communication connectivity amongsystems, devices, and applications in the context of thesmart grid. The perspective includes communicationnetworks, media, performance, and protocols.

Each of these perspectives is comprised of domains,entities, and either interfaces or data flows. The reference model ispresented functionally, is expandable, and is not intended to beprescriptive or restrictive. It is imperative that interoperabilityis maintained as smart grid technologies and architecturesevolve.

The IAPs of the SGIRM are comprised of domains,entities, and interfaces or data flows [2].

1) Domains common to all of the SGIRM IAPs are asfollows:
   a) Bulk generation. The generators of electricity inbulk quantities. May also store energy for laterdistribution.
   b) Transmission. The carriers of bulk electricity overlong distances.
   c) Distribution. The distributers of electricity to andfrom customers.
   d) Service providers. The organizations providingservices to electrical customers and utilities.
   e) Markets. The operators and participants inelectricity markets.
   f) Control/operations. The management of themovement of electricity.
   g) Customers. The end users of electricity.
2) Entities (devices, communication networks, computersystems, software programs, etc.) are generallylocated inside a domain and are connected to eachother through one or more interfaces. Each perspectivehas entities that more closely map to its technology.However, each entity can map to an appropriate entityor entities in another perspective.
3) Interfaces are logical connections from one entity toanother that support one or more data flowsimplemented with one or more data links.
4) Data flows are used instead of interfaces in the IT-IAP.These data flows are application-levelcommunications from entities that provide data toentities that consume data.

A. Power System Interoperability

Smart grid interoperability from a power systemsperspective represents a complex system with the main goal ofassuring electric power is delivered to all customers with highreliability and availability, at high power quality, and at a costthat makes electric power an economical form of energy [2]. Todo so, the power system operator needs to assure that, for eachfraction of a second, the amount of electric power produced isequivalent to the amount of power consumed. If this equationis not balanced, power system issues may occur inmilliseconds. These issues include equipment damage and lossof electric power to customers. Simultaneously, the amount ofreactive power produced and consumed must be balanced. Thesmart gridis focused on optimizing the solutions necessaryto maintain these balances.

B. Information technology interoperability

The smart grid is both an evolution of power equipment technology and the advancement of sophisticated computer monitoring, analysis, optimization, and control from exclusively central utility locations to the distribution and transmission grids [2]. It thus brings many of the concerns of distributed automation that should be addressed from an IT perspective, such as interoperability of data exchanges, computer network security, data communication requirements, and integration with existing and future devices, systems, and applications.

C. Communications technology interoperability

The communications technology perspective of the SGIRM supports a broad set of networks. The graphical view shown in Fig. 2 provides the relationships of variousnetworks to the smart grid bulk generation, transmission,distribution, and customer domains. In some cases, multiple names may be used for the same functional subnetwork [2]. Forexample, customer premises networks (CPNs) vary in size andnumber of connected devices but are typically classified ashome area networks (HANs), business area networks (BANs),or industrial area networks (IANs), and there is a demarcationof these networks from networks used in the distributiondomain. Some communication paths are between end pointswithin the same domain and other communication paths arebetween domains, and may include a series of subnetworks. The public Internet provides communication capabilities that span all four of the illustrated domains and though the implementer (e.g., utility or RTO) may not want to use the public Internet or regulators may choose to not allow its use, it remains an architectural alternative. Use or non-use of the public Internet in certain communication paths is left to the implementer. It also shows the end-to-end communications security and management layers, cutting across each smart grid communication domain.

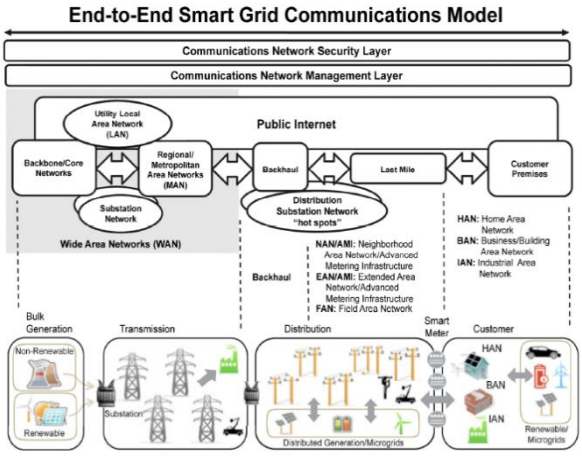

Figure 2. End-to-end smart grid communications model

IV. SECURITY COMMUNICATIONS NETWORK FOR INTEROPERABILITY

The deployment of the smart grid will be a continuing evolution and not a single event; therefore, there is a need to adapt legacy protocols to new communication technology capabilities.

Interoperability in CT has generally been improved by use of a functionally layered protocol in accordance with the International Organization for Standardization (ISO) Open Systems Interconnect (OSI) reference model [11]. Within the OSI model, functions are placed into seven layers, and layers are connected with service interfaces as shown in Fig. 3.

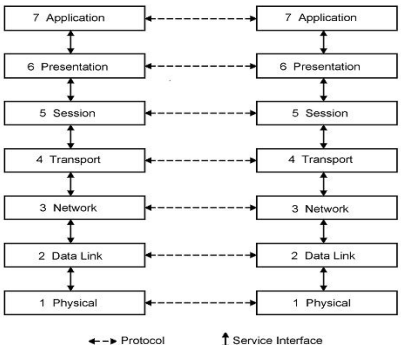

Figure 3. OSI reference model

This layering simplifies the task of replacing one communication technology with an alternate technology. For example, transport protocols have been designed to operate over a wide variety of data link types that comply with the service interface. Many of these communication links may exist within the smart grid for many years to come. In evolving existing protocols and applications to a layered communications architecture, implementers may need to adapt the existing protocol to conform to the transport layer of a modern layered communication network.

A. Communication Interoperability Architecture

The CT-IAP presented in Fig. 4[2] can include new technologies asthey become available, and it also can be used to develop target architectures by the developers. It is a visualrepresentation of most relevant smart grid communications systems, subsystems, and key elements with ageneric, flexible, and dynamic architecture that will evolve as technology progresses.

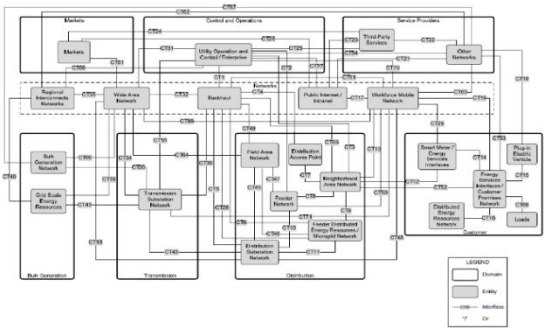

Figure 4. Communication technology IAP

The CT-IAP displays domains, entities, and interfaces from the communications technology perspective. The CT-IAP domains provide a view of the electric power system close to that of existing electric utilities' view that emphasizes the production, delivery, and consumption of electrical energy. These CT-IAP domains are as follows: Bulk Generation, Transmission, Distribution, Customer, Service providers, Control and operations, Markets.

Within each domain (intra-domain) or between domains (inter-domain), the entities are connected to each other through one or more interfaces. The number of interfaces connecting one or more entities represents the available (and future) and most relevant interconnection alternatives.

The communications entities are either wireline or wireless network systems or relevant communications system elements that stand out as important in the context of the whole system architecture. The interfaces are further defined as generic interconnections that establish the minimum level of interoperability requirements between two or more entities. The interfaces are then further specified in terms of performance requirement, security level, protocol layer, and other more specific needs that will be identified in the future.

The entities are connected with communication links represented by lines between the two entities; thus, this line represents "interface" or "connectivity" between two entities. It should be noted that the single line between two entities does not mean that there is only one or a single interface. The line represents an "aggregation" of interfaces between the two entities.

The CT-IAP is not meant to give the level of details required for the designer of the lower communications protocol layer, but it provides the generic and standard framework elements and an overarching view ofwho they are, what they are, where they are, how they are connected to each other, with coded entities andinterfaces that can be later detailed and refined for particular needs. Therefore, it is technology- andprotocol-agnostic to allow the flexibility provided by a generic and standard-based interoperabilityreference model.

B.Security Communications Network

Any large smart grid communications system will be made up of a number of different communications technologies and subnetworks. The information used for smart grid monitoring and control will have communications requirements that will vary widely depending on the smart grid applications. A rigorous method for categorizing an application's communications requirements in the context of the smart grid will aid in the design of a unified smart grid communications system.

B.1 Data classification and security services

Once data over the communication link is classified, security controls will be determined according to the level of availability, integrity, and confidentiality protection, which ensures data isprotected in the most cost-effective manner.Availability provides timely and reliable access to the useful information. Integrity protects against improper information modification/repudiationor destruction to ensure the correctness of information.Confidentiality provides only authorized access to information. Table I shows the relationship between security services and types ofattacks [2].

Attack	Security Services			
	Confidentiality	Integrity	Availability	Accountability
Access	X	-	-	X
Modification	-	X	-	X
Denial of service	-	-	X	-
repudiation	-	X	-	X

B.2 Tier classifications and level of assurance in communication links

Level of assurance refers to the level of certainty that a service can be provided to meet the use case requirements. This would include quantitative and qualitative use related to the direct or indirect impact of actions facilitated by the communications links.

Level of assurance, minimum latency, and impact on operations are three aspects to make a quantitative and/or qualitative evaluation of the requirements for the particular applications. The tier or latency class relates to the reliability of the network with respect to services to be provided.The technology chosen must meet the requirements defined under each tier class. Tier classes 1, 2, or 3 are defined by the level of assurance, minimum latency, and impact on operations [2].

- Tier 1 (critical). This is data that is critical to the operation, control, and safe operation of the smart grid.
- Tier 2 (important). This is data that is important with limited control in operations of the smart grid.
- Tier 3 (informative). This is data that is informative but not necessarily important for operations of the smart grid.

Table II shows the level of assurance used to define the tier class priority hierarchy [2].

TABLE II. TIER CLASS AND LEVEL OF ASSURANCE

	Tier class 1 (critical)	Tier class 2 (important)	Tier class 3 (informative)
Level of assurance	High	Medium	Low
Priority	1	2	3
Descriptions	— Control or safety relevant — Potential for loss of life or injury, and potential damage to assets — Low, low-low latency (relaying) — Medium, high latency (distribution)	— Control — Potential damage to assets — Medium, high latency	— Informative — No potential damage to assets — High or high-high latency

The three tier or latency classes that relate to thereliability and trustworthiness of the networks with respect to services to be provided are as follows [2]:

- Tier class 1 for low-low (two levels) and low (one level) latency applications, includes potential for loss of life and damage to assets and relates to control and safety-relevant actions.
- Tier class 2 for medium latency applications, includes potential damage to assets and no risk to personnel.
- Tier class 3 for high (one level) and high-high (two levels) latency applications and offers no damage to assets and no risk to personnel.

B.3 Security and Key management for communications

The security categorization drives the requirements for the communications for trustworthiness includingresiliency, reliability, and fault tolerance. In establishing the appropriate security categorization with respect tothe tier class, it sets a baseline for a target for a potential impact that can define the goal for the designer to usein selection of the appropriate components.

Key management is another critical process to ensure thesecure operation of the Smart Grid.The role of key management is to provide a mechanism to automatically generate, update, and delete keysto be used for protecting a communication channel between peers that exchange information over thechannel.

A concept of unified key management function (UKMF) is providedhere as an example key management framework. UKMF works across multiple communication protocols within the same communication layer or across multiple communication layers and is suitable for lowprocessing power devices such as smart meters. A

fully unified UKMF model is shown in Fig. 5 [2]. In the fully unified model, allprotocols that require ciphering keys are managed by UKMF. There are several protocols that can be used to realize the UKMF.

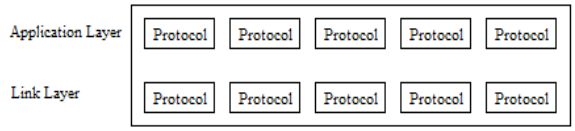

Figure 5. Fully unified UKMF model

CONCLUSION

The transition of the traditional power grid into the smart grid, especially with the integration of microgrid, requires enhancements of the communication system. The integration of different technologies and topologies promotes the requirements for interoperable security communication infrastructures. After an introduction on smart grid, the interoperability concept is described.Then, smart grid interoperable reference model (SGIRM) defining three integrated architectural perspectives -power systems, communications technology and informationtechnology, and the three corresponding interoperability architectural perspectivesare discussed. The security communicationscharacteristics including confidentiality, integrity, availability, assurance and security key management for smart grid interoperability are finally addressed.

REFERENCE

[1] V. C. Gungor, Bin Lu, and Gerhard P. Hancke, "Opportunities and Challenges of Wireless Sensor Networks in Smart Grid," Industrial Electronics, IEEE Transactions on, Vol. 57, No. 10, pp. 3557-3564, 2010.

[2] IEEE Std P2030, "Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), and End-Use Applications and Loads," 2011.

[3] NIST, "Framework and Roadmap for Smart Grid Interoperability Standards, Release 2.0," February 2012.

[4] U.S. Department of Energy, "The smart grid: An introduction," Washington, DC, Sep. 2008.

[5] S. M. Amin and B. F. Wollenberg, "Toward a smart grid," IEEE Power Energy Mag., vol. 3, no. 5, pp. 34–41, Sep./Oct. 2005.

[6] M. Liserre, T. Sauter, and J. Y. Hung, "Future energy systems: Integrating renewable energy sources into the smart power grid through industrial electronics," *IEEE Ind. Electron. Mag.*, vol. 4, no. 1, pp. 18–37, Mar. 2010.

[7] A. Y. Saber and G. K. Venayagamoorthy, "Plug-in vehicles and renewable energy sources for cost and emission reductions," *IEEE Trans. Ind. Electron.*, vol. 58, no. 4, pp. 1229–1238, Apr. 2011.

[8] W. Wang, Z. Lu, "Cyber security in the Smart Grid: Survey and challenges," *Computer Networks*, vol. 57, pp. 1344–1371, 2013.

[9] V. C. Gungor and F. C. Lambert, "A survey on communication networks for electric system automation," Comput. Netw., vol. 50, no. 7, pp. 877– 897, May 2006.

[10] X. Fang, S. Misra, G. Xue, and D. Yang, "Smart grid - the new and improved power grid: A survey," *IEEE Commun. Surveys Tutorials*, 2012.

[11] ISO/IEC 7498-1, "Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model," 1994.

★★★