Intl J Engg Sci Adv Research 2015 Sep;1(3): 240-252

Smarter Way to Electricity: Smart Grid A Survey of Communication Networks Reliability & its Security

Isha
Computer Science & Engineering Department
Rama University, Kanpur, India
Isha.singh268@gmail.com

***Abstract*: Around the world, electrical power systems are facing a drastic change stimulated by the urgent requirement to decarbonise electricity supply, to allow the minimum use of aging resources and to make effective application of information and communication technologies (ICTs). These entire goals find a single path; 'Smart Grid.' A smart grid can be defined as an electricity network which is digital and other advanced technologies so as to monitor and manage the transport of electricity from all generation sources to meet the varying electricity demands of end-users. Smart grids co-ordinate the needs and capabilities of all generators, grid operators, end-users and electricity market stakeholders to operate all parts of the system as efficiently as possible, and maximize system reliability, resilience and stability by minimizing costs and environmental impacts. A Smart Grid incorporates the features of advanced ICTs to convey real-time information and facilitate the almost instantaneous stability of supply and demand on the electrical grid. The aim of this paper is to provide a basic discussion of the Smart Grid concept, the comparison between the smart grid and the traditional grid, communication technologies involved in smart grid and its related reliability and security aspects.**

Keywords: Smart Grid, Framework, Communication Technologies, Reliability and Security

1. INTRODUCTION

"A brain is a society of very small, simple modules that cannot be said to be thinking, that are not smart in themselves. But when you have a network of them together, out of that arises a kind of smartness". [1]

– Kelvin Kelly, author of Out of Control: The New Biology of Machines, Social Systems, and the Economic World.

The increment in energy requirements with the need for carbon footprint reduction and the push for more energy management are driving governments, utilities and consumers to seek for a smarter way of managing the current electricity grid [2, 3]. The result is the introduction of Smart Grid as the evolutionary approach that can bring the 'smartness' to the traditional power grid in order to achieve the mentioned objectives. Several concepts of the smart grid, such as dynamic pricing, distributed generation, and demand management, have significantly impacted the operation of ICT services, in particular, communication networks and data centres. Ongoing energy-efficiency and operational expenditures reduction efforts in communication networks and data centres have gained another dimension with those smart grid concepts [4].

Electricity is observed as the most versatile form of energy available and is used by majority of people around the world through a series of tried-and-tested technologies. Our traditional power systems are based on centralized generation plants that supply end-users via long-established, unidirectional transmission and distribution systems. These systems have served us well, in many cases for more than a hundred years, but times are changing. There is demand for cleaner energy in societies to combat climate change and thus demand for electricity is rising. Hence it can be inferred that more electricity must be generated from a greater variety of sources. Wind, solar, biofuel, and geothermal plants will all be needed, as well as coal, gas and nuclear, with significant consequences for the power system. The quality of power in the grid can be enhanced with new variations by introducing the mix of renewable, thermal and nuclear power plants. The availability of wind and solar power is affected by the changing weather patterns, and the emergence of distributed power generation (rooftop solar panels, for example) will complicate matters further, requiring local networks to receive as well as deliver power. The existing power supply infrastructure is unable to manage such complexity, and needs to change. It needs to be equipped with advanced communications and information technologies to monitor, analyse and organize the supply and demand of electricity. This is what is meant by a smart grid [5].

Thus the essence of the smart grid vision can be given is "a fully-automated power delivering network that can ensure a two-way flow of electricity and information between the power plants and appliances and all points in between." This next evolution of the power grid will involve the expansion and integration of advanced communications and information technology into all aspects of utility operations. The increased functionality associated with the integration into information systems also comes with increased exposure, and a key consideration is to ensure cyber security, especially as systems that have traditionally been physically-isolated, closed and proprietary evolve towards more networked, open architectures based on IP standards.

Smart grid can vary, but generally speaking, this term refers to the use of digital information and controls technology to improve the reliability, security, and overall efficiency of

the electric grid. Proponents suggest that this will be accomplished by offering consumers and utilities incentives to work together to create a more responsive and less polluting system. A popular description of the smart grid invokes the idea of an "energy Internet" with a two-way flow of energy, in much the same way that the Internet allowed greater interactivity and selectivity in the flow of information. Just as we have seen television programming move away from broadcast to cable to video-on-demand and DVR technology, proponents of the smart grid imagine that we will see energy flow onto and off the grid as customer and utility exchange information, a marked contrast from today's one-way, utility-to-customer energy system [1].

1. What is Smart Grid?

A smart grid can be defined as an electricity network which is digital and other advanced technologies so as to monitor and manage the transport of electricity from all generation sources to meet the varying electricity demands of end-users. Smart grids co-ordinate the needs and capabilities of all generators, grid operators, end-users and electricity market stakeholders to operate all parts of the system as efficiently as possible, and maximize system reliability, resilience and stability by minimizing costs and environmental impacts.

For the purposes of this roadmap, smart grids include electricity networks (transmission and distribution systems) and interfaces with generation, storage and end-users. While many regions have already begun to "smarten" their electricity system, all regions will require significant additional investment and planning to achieve a smarter grid. Smart grids are an evolving set of technologies that will be deployed at different rates in a variety of settings around the world, depending on local commercial attractiveness, compatibility with existing technologies, regulatory developments and investment frameworks [6].

2. Difference between Traditional and Smart Grid

The existing utility grid is a one direction grid or a centralized grid in which power flows, from generation resources through the transmission-distribution system to the customer. Generation may or may not be located in the same geographic area as the load being served, which can often require transmission from distant locations.

Existing utility grids may or may not include Supervisory Control and Data Acquisition (SCADA) sensors, computing, and communications to monitor grid performance. Utility systems may depend instead on separate reporting systems, periodic studies, and standalone outage management applications fig.1 and Table 1 shows the difference between the two.

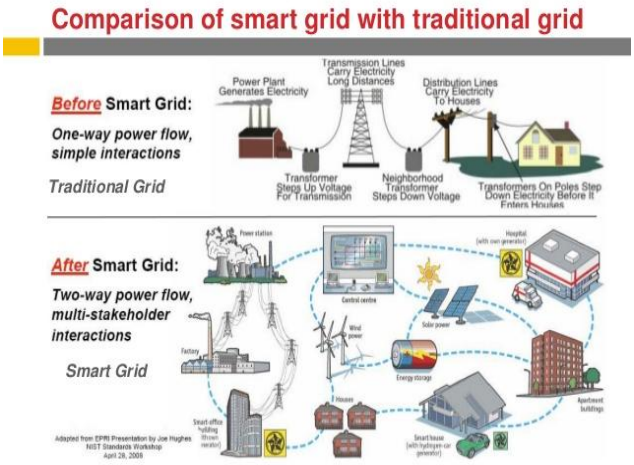

Figure 1 Comparison of smart grid with traditional grid

Information to the customer is generally limited to a periodic bill for services consumed in a prior time period or billing cycle. Utility web sites may or may not provide customers will access to their usage data. Energy usage is usually presented as an aggregate kWh value for a specific billing cycle, which may or may not align with monthly calendar boundaries.

The first step to transform the existing grid into a smart grid requires the addition of generation options throughout the grid at bulk power transfer points, substations, other distribution locations and on the customer side of the meter. Adding generation throughout the grid allows power sources to be located closer to their point of use, reducing investment in transmission and distribution, and in many cases reducing energy losses. Implementation of widespread, smaller generation resources diversifies supply, reduces risks of major outages, and improves overall reliability.

Sensors, remote monitoring, automated switches, reclosers, upgraded capacitor banks, and other equipment may be integrated into the grid to provide end-to-end monitoring and control of the transmission and distribution network. Equivalent additions on the customer side of the meter would include automated control systems and smart appliances with embedded price and event-sensing and energy management capability. Sensors provide the information to better understand grid operation, while control devices provide options to better manage system operation.

The last stage necessary to transform and create a smart grid is the addition of communication systems to support information flows that fully link both the utility and customer sides of the grid.

Table 1 Difference between Traditional and Smart Grid

Traditional Grid	Smart Grid
Electric machinery	Digital
One-way communication	Two-way communication
Centralized power generation	Distributed power generation
A small number of sensors	Full grid sensor layout
Manual monitoring	Automatic monitoring
Manual recovery	Automatic recovery
Failures and power outages	Adaptive and Islanded
Few user options	More user options

Characteristics and framework of Smart Grid

A Smart Grid employs innovative products and services together with intelligent monitoring, control, communication, and self-healing technologies. It incorporates the electricity grid and communication technologies [7]. It is envisioned to provide modern electrical services that transcends from Generation domain to the consumer end. The Smart Grid characteristics and functionalities can thus be summed up as follows [2, 3, 8]:

The literature [9-12] suggests the following attributes of the Smart Grid:

1) Integration of all generation and storage options: It better facilitates the connection and operation of generators of all sizes and technologies and accommodates intermittent generation and storage options [13]. It accommodates and facilitates all renewable energy sources, distributed generation, residential micro-generation, and storage options, thus significantly reducing the environmental impact of the whole electricity supply system. It will provide simplified interconnection similar to 'plug-and-play.'

2) Enabling active participation by consumers: Smart Grid allows consumers to play a part in optimizing the operation of the system and provides consumers with greater information and choice of supply. It enables demand response and demand-side management through the integration of smart meters, smart appliances and consumer loads, micro-generation, and electricity storage (electrical vehicles) and by providing customers with information related to energy use and prices. It is anticipated that customers will be provided with information and incentives to modify their consumption pattern to overcome some of the constraints in the power system.

3) Enabling new products, services and markets: Examples include linking of energy buyers to sellers, brokers, integrators and aggregator services and also Plug-In Hybrid Electric Vehicles (PHEV) and Vehicle to Grid services. It opens access to the markets through increased transmission paths, aggregated supply and demand response initiatives, and ancillary service provisions.

4) Provision of power quality for the digital economy: It provides power quality of the electricity supply to accommodate sensitive equipment that enhances with the digital economy.

5) Optimization of asset utilization: It optimizes and efficiently operates assets by intelligent operation of the delivery system (rerouting power, working autonomously) and pursuing efficient asset management. This includes utilizing assets depending on what is needed and when it is needed.

6) Anticipating and responding to system disturbances: It assures and improves reliability and the security of supply by anticipating and responding in a self-healing manner, and strengthening the security of supply through enhanced transfer capabilities.

7) Operating resiliently against attack and natural disasters: It operates resiliently in disasters, physical or cyber attacks and delivers enhanced levels of reliability and security of supplying energy.

4.1 Framework

A platform is provided by communication architecture to build the automated and intelligent management functions in power systems. The functional requirements of communication architectures depend on the expected management tasks. To better understand our research goals on the communication networks that support the system management, we discuss the framework of smart grid.

4.1.1 Smart grid reference model

In the smart grid, many distributed renewable energy sources will be connected into the power transmission and distribution systems as integral components. The typical renewable energy sources include wind, solar, small hydro, tidal, geothermal, and waste.

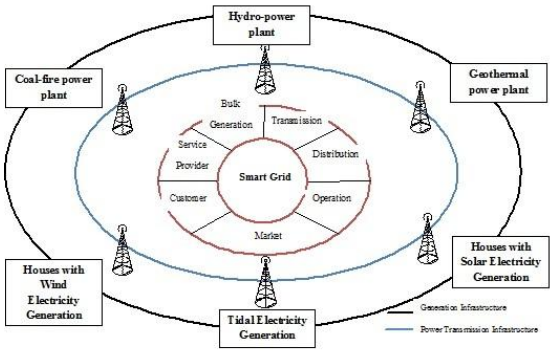

Figure 2 Framework of Smart Grid [16]

These sources generate extra electricity that supplements the electricity supply from large power plants and, when the electricity generated by distributed small energy sources exceeds the local needs, the surplus is sold back to the power grid. With the addition of renewable energy sources, bi-directional dynamic energy flows are observed in the power grid. We illustrate in Fig. 2 the framework of smart grid. A co-

located communication infrastructure is required to coordinate the distributed functions across the entire power system so as to effectively manage complex power system that involves an enormous number of diversely functional devices. This system consists of seven functional blocks [14,15], which are, namely, bulk generation, transmission, distribution, operation, market, customer, and service provider [16].

1. Bulk generation

Oil, coal, nuclear fission, flowing water, sunlight, wind, tide, etc resources are used to generate electricity. Smart grid is capable of storing surplus electricity generated at times of resource richness and can be stored up for redistribution at times of resource scarcity. The bulk generation domain and the transmission domain are connected. Market domain and operation domain communicate with bulk generation through a market service interface over internet and over the wide area network respectively. It is required to communicate key parameters like generation capacity and scarcity to the other domains. It comprises of electrical equipments including RTUs, programmable logic controllers, equipment monitors, and fault recorders.

2. Transmission

After the generation, electricity is transmitted to the distribution domain via multiple substations and transmission lines. The transmission is typically operated and managed by a RTO or an ISO. The RTO is responsible for maintaining the stability of regional transmission lines by balancing between the demand and supply. Small scale energy generation and storage are also supported by transmission domain. To achieve self-healing functions and enhance wide area situational awareness and control, a lot of information will be captured from the grid and sent to the control centers. The control centers will also send responses to the devices in remote substations. The bidirectional communications between control centers and substations are handled in the transmission domain too.

3. Distribution

The dispatch of electricity to end users in the customer domain is implemented by making use of the electrical and communication infrastructures that connect the transmission and customer domains. This domain includes distribution feeders and transformers to supply electricity. It interacts with many different equipment, such as DERs, PEVs, AMI, and sensors with communication capability. The distribution domain takes the responsibility of delivering electricity to energy consumers according to the user demands and the energy availability. In order to provide quality electricity, the stability of this domain is monitored and controlled.

4. Operation

This domain maintains efficient and optimal operations of the transmission and distribution domains using an EMS in the transmission domain and a DMS in the distribution domain. It uses field area and wide area networks in the transmission and distribution domains to obtain information of the power system activities like monitoring, control, fault management, maintenance, analysis and metering. The information is obtained using the SCADA systems. The operations domain may be subdivided into sub-domains for transmission, distribution, and RTO/ISO operations. These sub-domains may be controlled by different organizations.

5. Market

The balance between the supply and the demand of electricity is maintained by the market domain. This domain consists of retailers who supply electricity to end users, suppliers of bulk electricity, traders who buy electricity from suppliers and sell it to retailers, and aggregators who combine smaller DER resources for sale. Effective communications between the bulk producers of electricity, the DERs and the market is essential to match the production of electricity with its demand.

6. Customer

Customers consume, generate (using DERs), or store electricity. This domain includes home, commercial or industrial buildings. It is electrically connected to the distribution domain and communicates with the distribution, operation, service provider and market domains. The customer domain also supports the demand response process. To allow customers to actively participate in the grid, a two-way communication interface between the customer premises and the distribution domain in required. This is generally referred to as an ESI and is present at the customer premises. A communication network within the customer premises is required to allow exchange of data and control commands between the utility and the smart customer devices. This network is referred to as a home area network. It is expected to support applications such as remote load control, DER monitoring and control, IHD support for customer usages, reading of non-energy meters, and integration with building management systems.

7. Service provider

Service providers provide electricity to customers and utilities. They manage services like billing and customer account management for utility companies. It communicates with the operation domain to get the metering information and for situational awareness and system control. It must also communicate with HANs in the customer domain through the ESI interface to provide smart services like management of energy uses and home energy generation. Table 2 gives the description of various smart grid domains.

Table 2 Description of Smart Grid domains [14]

Smart Grid Domain	Description
Customers	The end users of electricity. May also generate, store, and manage the use of energy. Traditionally, three customer types are discussed, each with its own domain: home, commercial/building, and industrial
Markets	The operators and participants in electricity markets.
Service Providers	The organizations providing services to electrical customers and utilities
Operations	The managers of the movement of electricity.
Bulk Generations	The generators of electricity in bulk quantities. May also store energy for later distribution.
Transmission	The carriers of bulk electricity over long distances. May also store and generate electricity.
Distribution	The distributors of electricity to and from customers. May also store and generate electricity.

5. Communication Technologies in Smart Grid

Smart grid requires a communication system to handle a large amount of data from various applications in a secure and cost effective way. Two types of communication technologies can be employed for data transmission by smart grid, wired and wireless. Low cost and easy deployment are the main advantages of wireless communication over wired communication, *i.e*. wireless communication is more popular in smart grid systems [17].

Table 3 Networking Technologies used in Smart Grid [20]

WAN	LAN	HAN	Access	Multimedia
SONET/SDH	Ethernet	ZigBee	PSTN	MPLS
WDM/DWDM	Wireless Ethernet	Home Plug	xDSL	
Digital Trunked Radio	GbE/10GbE	6LoWPAN	Cable Modem	
RoIP		OpenHAN	FTTH	

5.1. Wide Area Networking Technologies [20]

Customarily, two types of information in a smart grid system should be transferred. The first data is from sensors to smart meters and the second is from smart meters to data center. The first data connection can be performed via power line or wireless communications and popular systems for second information are cellular networks and internet [18]. In this section, we review some communication technologies which can be used for smart grid systems [19]. Table 3 summarizes network technologies used in smart grid.

1. SONET/SDH

SONET (Synchronous Optical Network) and SDH (Synchronous Digital Hierarchy) are critical digital transport networks that allow the combination of high- speed data services. A common number of aggregate transmission rates, especially at higher rates, are both defined in them. However, they are quite different at lower multiplexing levels. SDH is widely used in electric utilities as the backbone of transmission networks in Smart Grid as well as in carriers. It provides carrier- level reliability with short restoration time in case of path failures. SDH also has been put into use by many electric utilities for fibre and microwave systems throughout the world.

2. WDM/DWDM

WDM (Wavelength Division Multiplexing) is a technology which enables a number of optical carrier signals being integrated onto a single optical fiber by using different wavelength of laser light. In the power grid, WDM can be used to update current SDH devices. DWDM (Dense WDM) allows data transmits at more than one wavelength on each fiber pair of an optical fiber channel and allows data transmits in different formats including IP, ATM, SONET/SDH and Ethernet. Thus, DWDM- based networks can carry multiple types of data at different rate on an optical fiber channel.

3. Digital trunked radio

Digital trunked radio uses unguided electromagnetic waves to transmit information as well as wireless transport of data. A trunked radio system is a complex type of computer-controlled two- way radio system that allows sharing of relatively few radio frequency channels among a large group of users. Efficiency is the main object of this kind of system, and it can provide Smart Grid with electric utility network with disaster management.

4. RoIP

Radio over IP (RoIP) is a new generation technology focusing on data transmission over microwave radio, which is with IP addressing. RoIP networks can use all types of IP infrastructure including public Internet, private network, or local network. RoIP is a new way to improve the efficiency of two- way radio technology and allows it to communicate with desk and mobile phones. Besides, RoIP can also improve the stability of Smart Grid when disaster occurs.

5.2. Local Area Networking Technologies

1. Ethernet

Ethernet is a LAN technology with many advantages including superior versatility, speed and compatibility which make it a good choice for substation automation system. A trend to create LANs in substations appears due to the increased number of intelligent electronic devices (IEDs).

2. Wireless Ethernet

Wireless Ethernet, also known as wireless LAN technologies provide stable, high speed point- to- point and point- to- multipoint communication. 802.11 standard defines three non- interoperable technologies: Frequency Hopping Spread Spectrum (FHSS), Direct Sequence Spread Spectrum (DSSS) and Infrared (IR). It is superior to implement wireless LANs over wired LAN due to it's easy to setup, its cost-efficiency and it provides mobility of devices. Wireless Ethernet is able to be chosen for multiple applications in Smart Grid like distribution substation automation and protection system.

3. GbE/10GbE

Gigabit Ethernet (GbE) is an extension of the IEEE 802.3 Ethernet standard. It can be used in high- speed local area network backbones and server connectivity with its lower cost of ownership because applications do not need to change and re- training of technical support people will not be necessary. The need to interconnect Ethernet LANs to SONET/SDH wide area networks is growing as the increasing deployment of Ethernet in the LAN. The next part will talk about HAN technologies.

5.3. Home Area Networking Technologies

1. ZigBee

ZigsBee is designed to emphasize the unique needs of low-cost, low- power wireless sensor and control network. ZigBee is a specification for a suite of high- level communication protocols using small digital radio for wireless personal area networks. The ZigBee allows networking using multiple topologies, like star, tree and mesh. The technology is intended to be simpler and cheaper. Its open standard platform that integrates multiple products and systems is ZigBee's main advantage. ZigBee now has a Smart Energy Application Profile that is specifically designed for utility application within HAN.

2. Home Plug

HomePlug is a union name for various power line communications specifications that support networking over existing home electrical wiring. Some specifications exist under the Home Plug moniker, each offering unique performance capabilities and coexistence or capability with other Home Plug specifications. The Home Plug applications are based on PLC (Programmable Logic Controller) or BPL (Broadband- Over- Powerline) technology. PLC/BPL brings new interest to Smart Grid technology. For example, the energy consumer can control plug- in electric vehicle charging or other smart energy devices they are using.

3. 6LoWPAN

6LowPAN (IPV6 over LoW Power wireless Area Network) is the name of the working group in the Internet area of the IETF (Internet Engineering Task Force). 6LoWPAN is an international open standard that allows in- home wireless Internet. 6LoWPAN has defined encapsulation and header compression mechanisms that allow IPv6 packets to be sent to and received from over IEEE 802.15.4 based networks, which means IP protocol is a stable technology supporting various applications and

communication technologies.

4. Ope nHAN

OpenHAN (Home Area Network) is a proposed standard for home area network and home grids that is aimed to standardize powerline networking interoperation from a utility point of view and ensure reliable communications co- extant with AC power outlets. OpenHAN enables utility control of standards, customer coordination and operational states. OpenHAN is the basis of automated demand response in which there is a link between the customer's smart meters and the appliances. And residents are able to let the appliances run the system during time when electricity is cheap or expensive.

5.4. Access Technologies

1. PSTN

PSTN (Public Switched Telephone Network) is the union of the world's circuit- switched telephone networks that are operated by national, regional, or local telephone operators and provides infrastructure and services for public telecommunications. PSTN consists of telephone line, fiber optical cables, microwave transmission networks, cellular networks, communication satellites, and undersea telephone cables interconnected by switching centers which allows any telephone in the world to communicate with any other. The core of PSTN now is digital and it includes mobile phones as well as fixed telephones.

2. xDSL

DSL (Digital Subscriber Line) is an aggregate of technologies that provide Internet access by transmitting digital data over the wires of a local telephone network. xDSL includes a series of DSL technologies, ADSL (Asymmetric Digital Subscriber Line), SDSL (Symmetric Digital Subscriber Line), SHDSL (Symmetric High- speed Digital Subscriber Line), G.SHDSL (Group of Single- pair High- speed Digital Subscriber Line), IDSL (Internet Digital Subscriber Line) and VDSL (Very- high- data- rate Digital Subscriber Line).

3. Cable Modem

Cable Modem is a type of network bridge and modem that provides two- way data communication via radio frequency channels on a hybrid fiber- coaxial (HFC) and RFoG (Radio Frequency over Glass). Cable Modem is mainly used to deliver broadband Internet access in the form of cable Internet by taking the advantage of the high bandwidth of a HFC and RFoG network.

4. FTTH

FTTH (Fiber to the home) is a technology that offers a broadband optical fiber connection to consumer sites. It has been a decade since FTTH became a better solution of the telecommunication industry and it provides nearly unlimited bandwidth to the home users. Passive Optical Network (PON), which permits a single optical fiber to be separated into 128 times without active electronic repeaters, is the key to FTTH.

This kind of point- to- multipoint network does not require any electronics between the consumers and the central office.

5.5. Multimedia Networking Technologies

1. MPLS

MPLS is a mechanism in high- performance telecommunications networks that directs data from one network node to the next based on short path labels rather than long network addresses to avoid complicated search in a routing table. MPLS technology provides some new capabilities in IP networks including the support of VPN (Virtual Private Networks), the support of IP routing on network switches and traffic engineering. The next part will talk about some special issues in Smart Grid.

6. Reliability and Security in Smart Grid

6.1. Defining risk and reliability terminology

Risk, according to [21], is the exposure to the possibility of loss, injury, or other adverse or unwelcome circumstance; a chance or situation involving such a possibility. In the context of risk analysis (e.g., [22]), risk is often more formally defined as: [23]

$$\text{Risk} = \text{Exposure} \times \text{Vulnerability} \times \text{Cost} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (1)$$

Exposure is the extent to which a particular object or system is exposed to potential hazards. When expressed probabilistically, exposure is the probability that a particular object will be contacted by a hazard. Vulnerability, in this context, is the probability that an object fails, given that it is contacted by a hazard. Often exposure and vulnerability are combined into an overall probability that a particular component will fail. "Cost" refers to the total system cost that would result from the failure of a particular component. In the case of interconnected infrastructures, this cost needs to account for not only the immediate impact of the component failure (the cost of the transformer, for example), but also the costs incurred from potential cascading failures that might be triggered by a particular outage or set of outages. It is common in risk analysis to use data on historical outages and simulations to assess the expected value of (1) over some range of potential set of failures. This expected value is often reported as a measure of system reliability.

Reliability: Reliability is an important attribute ensuring high performance of the product, since it directly and significantly influences the product's performance and ultimately its life cycle cost and the economics of its use. Poor reliability in design, manufacturing, construction, and operation would directly increase warrant costs, liabilities, refits, and repair costs. Therefore, performance engineering can be considered synonymous with improving attributes like reliability, durability, quality, availability, safety and efficiency. A product having these attributes is expected to perform well and yield minimum life cycle costs, which not only include design and development costs and manufacturing costs, but also maintenance costs over the product's entire life [24].

Reliability clarifies the operational health and level of instability of the entire system [25]. In old power infrastructure, growing energy consumption and peak demand are some of the reasons that produce unreliability issues for the power grid [26]. Using the modern and safe communication and information technologies, faster and healthier control devices such as sensors for the entire grid from suppliers to customer resources will considerably strengthen the system reliability [26]. Reliability of the grid can be improved by deployment of sensors that prepare immediate situational awareness. Sensors now being widely used in the transmission grid allow the system to detect and response failures and anomalies in shortest period of time. Sensors in the grid could also detect when a transformer is spoiling and notice to replace it before a failure happens [27].

In the communications industry, reliability is typically measured as the fraction of time that a particular service (such as a web server) is available. Other reliability measures include the fraction of data packets that successfully reach their intended destination, or the latency associated with packet delivery. In the electricity industry, reliability is often measured differently at the distribution (retail service) level and at the bulk transmission/generation (bulk) level. At the distribution level, two of the most common reliability metrics are the System Average Interruption Frequency Index (SAIFI) and the System Average Interruption Duration Index (SAIDI) [28]. SAIFI measures the average frequency of outages per customer and SAIDI measures the average duration of outages, over a one year period, per customer. At the bulk grid level, a common reliability metric is the expected amount of electric energy demand that goes unserved over a specified period (often referred to as the Loss of Load Expectation, LOLE). These reliability indices can be defined as: [23]

System average interruption frequency index (SAIFI), [29]

SAIFI describes how often an average customer will experience a sustained interruption (greater than five minutes). It is defined as:

$$\text{SAIFI}=\frac{\sum \text{Total Number of Customers Interrupted}}{\text{Total Number of Customers Served}}, \quad \text{SAIFI}=\frac{CI}{N_T}$$

where *CI* is the number of customers interrupted and *NT* is the total number of customers served for the area.

System average interruption duration index (SAIDI),

SAIDI is defined as the total duration of an interruption for an average customer over a specific period. The index is defined as:

$$\text{SAIDI}=\frac{\sum \text{Customer Interruption Duration}}{\text{Total Number of Customers Served}}, \quad SAIDI = \frac{CMI}{N_T}$$

where *CMI* is the customer minutes interrupted. In terms of load-based indices, the average system interruption frequency index (ASIFI) is often used to measure performance in areas

with few consumers and concentrated loads. ASIFI is defined as:

$$\text{ASIFI}= \frac{\sum Total\ Connected\ kVA\ of\ Load\ Interrupted}{Total\ Connected\ kVA\ Served}$$

$$ASIFI = \frac{\sum Li}{L_T}$$

where, ASIFI is the ratio of total connected kVA of load interrupted and the total connected kVA served. SAIDI and SAIFI are two of the most common reliability indices used in the industry.

Customer average interruption during index (CAIDI),

CAIDI is defined as the average time required to restore service. It can be defined as:

$$\text{CAIDI}=\frac{\sum Customer\ Interruptions\ Duration}{Total\ Number\ of\ Customers\ Interrupted},$$

$$\text{CAIDI}= \frac{SAIDI}{SAIFI}$$

Customer total average interruption duration index (CTAIDI),

This index represents the total average time in the reporting period that customers who actually experienced an interruption were without power. This index is hybrid of CAIDI and is similarly calculated except that those customers with multiple interruptions are counted only once. This can be defined as:

$$\text{CTAIDI}= \frac{\sum Customer\ Interruption\ Duration}{Total\ Number\ of\ Customers\ Interrupted},$$

$$\text{CTAIDI}= \frac{\sum T_{iN_i}}{CN}$$

where CN is total Number of Customers who have Experienced a Sustained Interruption during the reporting period.

Customer average interruption frequency index (CAIFI),

CAIFI is defined as the average frequency of sustained interruptions for those customers experiencing sustained interruptions. The customer is counted once regardless of the number of times interrupted for this calculation. This can be defined as:

$$\text{CAIFI}= \frac{\sum Total\ Number\ of\ Customers\ Interrupted}{Total\ Number\ of\ Customers\ Interrupted}, \quad \text{CAIFI}= \frac{\sum N_i}{CN}$$

Average service availability index (ASAI),

ASAI is defined as The average service availability index represents the fraction of time (often in percentage) that a customer has received power during the defined reporting period. This can be defined as:

$$\text{ASAI}= \frac{Customer\ Hours\ Service\ Availability}{Customer\ Hours\ Service\ Demand},$$

Customers experiencing multiple interruptions ($CEMI_n$),

$CEMI_n$ is defined as the ration of individual customers experiencing more than n sustained interruptions to the total number of customers served. This can be defined as,

$$CEMI_n= \frac{Total\ Number\ of\ Customers\ that\ experience\ more\ than\ n\ sustained\ interruptions}{Total\ Number\ of\ Customers\ Served}$$

Average system interruption frequency index (ASIFI),

The calculation of this index is based on load rather than customers affected. ASIFI is sometimes used to measure distribution performance in areas that serve relatively few customers having relatively large concentrations of load, predominantly industrial/commercial customers. Theoretically, in a system with homogeneous load

distribution, ASIFI would be the same as SAIFI. This can be defined as,

$$\text{ASIFI}= \frac{\sum Total\ Connected\ kVA\ of\ Load\ Interrupted}{Total\ Connected\ kVA\ Served}, \quad \text{ASIFI}= \frac{\sum L_i}{L_T}$$

Average system interruption duration index (ASIDI),

The calculation of this index is based on load rather than customers affected. This can be defined as:

$$\text{ASIDI}= \frac{\sum Connected\ kVA\ Duration\ of\ Load\ Interrupted}{Total\ Connected\ kVA\ Served}$$

Monetary average interruption frequency index (MAIFI),

This index indicates the average frequency of momentary interruptions. This can be defined as:

$$\text{MAIFI}= \frac{\sum Total\ Number\ of\ Customer\ Momentary\ Interruption}{Total\ Number\ of\ Customers\ Served},$$

$$\text{MAIFI}= \frac{\sum IM_i N_{mi}}{N_T}$$

There are a number of established methodologies and industry tools (e.g., GEMARS [30]) designed for reliability analysis for power systems. However, there is tremendous uncertainty about how to model the impact of smart grid in reliability analysis tools. This section gives the review of system reliability analysis in protection mechanism.

6.1.1. System Reliability Analysis

In the context of bulk power system, North American Electric Reliability Corporation (NERC) define system reliability as the ability of a system to meet the electricity needs by maintaining continuity and stable supply of electricity, even when unexpected equipment failures or other factors occurred [31]. System reliability is a topic that cannot be neglected, it is important in power grid research, design and development. A major blackout incident was happened in Malaysia (13 January 2005) due to circuit breaker failure in protecting the busbar, resulting 6,230 MW (54%) total load loss in the affected region and 3.5million customers were affected in this incident [32]. Hence, there is an emerging need in improving the system reliability, and it is expected that the

future smart grid will provide enhancement with better system reliability operation and smarter failure protection mechanism.

There are several methods in ensuring system reliability, (i) by ensuring the reliability of distributed generation (DG) in distribution network, (ii) by ensuring the reliability of measurement infrastructure and (iii) by ensuring the network reliability before implementation. Besides that, (iv) by enabling substation to have the ability to perform decision-making is also another key to ensure system reliability [33].

Ensuring Reliability of DG: It is expected that the embedded or dispersed or distributed generation (DG) such as small scale generation from renewable energy resources, will be widely be used in smart grid. As the integration of DG into distributed network increases, the risk in distributed network increases. The risk compromises of distribution network reliability and stability, resulting from the use of fluctuant and intermittent renewable resources. To analyze the reliability of DG, Chen *et al.*, [34] proposed a method that use simulation model which gradually increase of local generators in smart grid, to mitigate the cascading failures resulted from DG. The model concept is, as loads in distribution network are being served locally by individual local generators (similar to Microgrid architecture), less power flow interruptions within entire power grid, this enhances the reliability and stability of smart grid. They obtained satisfactory result which dramatically reducing the likelihood of cascading failures in smart grid.

Ensuring Reliability of Measurement Infrastructure: To enable smart grid operation, a smart measurement infrastructure is required. It served as the input for smart grid with monitoring and sensing ability, to observe network healthiness, reliability and stability. A phasor measurement unit (PMU) is one of smart measurement unit. PMUs have been widely used in wide-area measurement system (WAMS) for monitoring, control and protection function in smart grid. To analyze the reliability of WAMS, Wang *et al*., [35] presented a quantify reliability evaluation method for WAMS, using combined Markov modeling and state enumeration techniques to evaluate WAMS reliability. The proposed idea of reliability evaluation covers the backbone communication network in WAMS and also the overall WAMS from a hardware reliability viewpoint. For verification, the WAMS evaluation method was demonstrated in the IEEE 14-bus system. It was proven that the evaluation method to be dependable in providing useful information to improve the reliability of WAMS and recognize the reliability of WAMS-based control scheme which require different information set. Besides that, Vaiman *et al.*, [36] introduced a Region of Stability Existence (ROSE) concept, which could continuously and automatically monitor system condition in realtime by computing the power system stability margins accurately. Their approach is illustrated in ISO New England's transmission network, with data set of (i) State Estimator (SE) data, (ii) Supervisory Control and Data Acquisition (SCADA) data and (iii) PMU measurements, used in ROSE computation. Their results of study indicated that the approach is effective and efficient in improving the reliability in ISO New England's transmission net work and could be used to prevent major blackouts.

3. *Ensuring Network Reliability before Implementation:* The more accurate and precise a simulation platform can be used to emulate the actual case. Therefore, the behavior and performance of smart grid can be understood better. Simulation of system reliability provides the preview of the system advantages, weaknesses and potential short coming before implementation. This ensure the system to be implemented is reliable and stable, through the evaluation and decision making based on the simulation results. But the question is how to create a simulation system which is accurate, precise, wide, flexible, adoptable and scalable? Godfrey *et al.*, [37] proposed a wide modelling method of targeting in smart grid applications with co-simulation, which focuses on communication and power network in smart grid to provide the means to examine the effect on communication failures. Their simulation method enables the investigation of wide range of smart grid issues with high capability and accuracy in addressing the communications latency adversely impact to the expected behavior later in power system.

In addition, Ghosn *et al.*, [38] designed an agent-oriented architecture for simulation, primarily focuses on self-healing problem, with an incremental method that begins with simulating a local Microgrid. Their architecture enables scalable and adaptable design that grows hierarchically into a more complete model. Such architecture also enables smart grid developer and designer to understand the weaknesses, potential short coming issues and identify the way to improve the electrical grid. With their agent –oriented architecture, they able to present software design issues that must be considered in producing a system that is flexible, adaptable and scalable.

Yusof *et al*., [39] presented a teleprotection simulation lab which enhances the learning process of the teleprotection system and it allows proactive measures to be taken before any unwanted incidents occur. The overall reliability and performance of the teleprotection system has been improved. With the simulation lab, it allows their R&D team to test and evaluate the performances of various telecommunication aided protection schemes comprehensively under a controlled lab environment.

Ensure Network Reliability by Empowering Substation with Decision Making: By empowering substation with the ability to perform decision making, the system could response by itself first without waiting for instruction from control network. This enables the substation to resolve the issue in the shortest possible time and ensure the reliability of the network. However, safety and precaution is necessary, the failure in performing the right decision is crucial. To ensure network reliability while minimizing failure in decision making, Overman *et al.*, [40] defined a multilevel framework trust model with reasonable compromises in both the failure and reliability. They suggested that distributed decision making ability to substation and/or field devices, by pre-load the substation and/or field devices with sufficient information for autonomous action, in the event of system failure without having to wait for instruction from control network. In their research, they have proven that by pre-loading the substation and/or field device with a set of "next actions to be taken" instructions, when attached in distributed rather than hierarchical communication architecture, the proposed model

could significantly increase the grid reliability, while at the same time reduce real time impact from loss of reliable control.

6.2. Security

Security aspect in smart grid is a challenging task of wits, pitting security attackers versus assets holders. Security in SG is of no exception to this paradigm. Information and communication technologies (ICT) are the primary enablers of the smart grid while carrying the risk of increasing security vulnerabilities of the grid, and allowing attackers to easily access the power system to either manipulate internal operation or steal state secrets and Intellectual property. Attacks may initiate from various parts of the power system including smart meters, advanced metering infrastructure (AMI), electric transportation infrastructure (e.g., plug-in hybrid electric vehicle, PHEV, charging stations), energy storage subsystem, wide area measurement and situational awareness component distribution automation subsystem, or supervisory control and data acquisition (SCADA) network, and target vital components of the smart grid [41]. Cyber security is intended as one of the crucial challenges for SG [42], [43], [44]. Vulnerabilities usually allow an attacker to break a system, corrupts user privacy, aquire access to control software, and modifies load conditions to destabilize the grid in unexpected ways [43]. We must take a note that the advanced infrastructure employed in SG on one hand encourages us to exercise more powerful mechanisms to defend against cyber attacks and handle failures effciently, on the other side opens so many new vulnerabilities. Hence in the following, it is going to be discussed countless new security and privacy issues due to the deployment of many smart meters, sensors, and PMUs, together with some solutions.

Security in Smart Metering: The security issue arrives from the recently deployed smart meters in large quantity. Smart meters are very attractive point for malicious hackers, since vulnerabilities can effortlessly be monetized [45]. Hackers or attackers who compromises a smart meter can immediately alter their energy costs or change generated energy meter readings to make money. A common consumer cheating in traditional power grid is that customers turn a physical meter upside down inside the electrical socket so as to cause the internal usage encounters to run backward. Due to the usage of smart meter, such attack can even be done with remote PCs. Moreover, wide usage of smart meters may provide a potentially many number of opportunities for adversaries. For example, inserting false information could mislead the electric utility into making incorrect decisions about regiona or local usage and capacity. Let us consider a simple but effective Denial-of-Service (DoS) attack. An adversary establishes the demand request of a smart meter, and keeps requesting a large amount of electricity. Within the framework of SG, it can be possible that the utility disconnects all the appliances connected to the meter so that all the power services for this user are refused. Deployment of smart meters in large not only leads to a large number of opportunities for adversaries, but also opens up the door to the cyber attacks which could lead to broad effects and even severe disasters. Let us take an example given by Anderson and Fuloria [46]. An ideal attack on any target country is to corrupt its citizens electricity supply. till now, the only effective way to do that involves attacks on generation, transmission, and distribution electrical system, which are now increasingly well defended. However, the rise of smart meters changes this game. The scenario is that a country where there are millions of smart meters, controlled by a few of their central utility controller. The attacker can also compromise these controllers and can send the set of commands that will cause meters to interrupt the electric supply. Such attack could cause severe disastrous results. In order to improve the security of smart metering systems, researchers have found many possible attacks and proposed some solutions. Cleveland [47] illustrates the security requirements i.e (integrity, confidentiality, availability, and accountability) and other related threats to the main components of an advanced metering infrastructure (AMI) of SG. McLaughlin et al. [48] dissusses an adversary's means of defrauding the electrical grid by altering AMI systems, and validated the effectiveness of such attacks by doing penetration testing on commodity devices. They found that not only is theft still possible in AMI systems, but that current AMI devices introduce a list of new vectors for achieving it. To protect the attacker from forging the reading of smart meter and guarantee the meter reading accuracy, Varodayan and Gao [49] gives a secure technique for power suppliers to echo the meter readings they receive from smart meters back to the customers so that particular users can verify the integrity of the smart meter. Furthermore, their process can also guarantee information-theoretic confidentiality, hence solving the confidentiality leak introduced by the redundant measurement. Berthier et al. [50] investigated the practical essentialities for monitoring and intrusion detection through a thorough analysis of the numerous threats targeting an AMI. They specified that specification-based detection technology has got the potential to meet the industrial requirements and constraints of an AMI. However, such technology puts a excessive development cost.

2. **Privacy in Smart Metering:** Smart meters in AMI also have unintended outcomes for customers privacy. NIST found out that the big benefit give by the SG, i.e. the ability to get richer data to and from consumer meters and other electric appliances, is also its Achilles heel from a privacy viewpoint [51],[44]. The more obvious privacy trouble is that the power usage information stored in the meter reacts as an information-rich side channel, and can be reused by interested groups to get personal data like consumer energy usage habits, behaviours, activities, likings, and even beliefs [52],[53], [45]. A little monitoring test on a private residence conducted in [16] reflected that personal information can be approximated with high accuracy, even with proportionally unadvanced hardware scheme, and algorithms. To tackle with privacy propaganda of smart meters in AMI, some proposals have been proposed. Li et al. [54] gives a very distributed incremental data aggregation approach, in which data is aggregated at all smart meters. Homomorphic encryption is used to secure the data in transit. Hence, intermediate meters cannot notice any intermediate or final outcome. Li et al. [55] proposed to compress the smart

meter data and use random sequences in the compressed sensing to boost the privacy and integrity aspects of the meter readings to enhance the security. A privacy-preserving protocol for energy billing and for performing general calculations on fine grained energy meter readings is proposed by Rial and Danezis [56]. The Zero-knowledge proofs are utilized particularly to ensure that the fee is correct without disclosing any energy consumption data. Costas and Kalogridis [57] anonymizes smart metering data so that information obtained from it cannot be easily attached with an identified person thus effectively deals with privacy problem. Kalogridis. [51] protects smart metering data privacy by a load signature moderation system. Authors discussed a model in which the amount of utility energy required may hide the consumers demand, by properly configuring the power router to determine the power given or required by a battery. Such type of system allows users to control (upto a certain extent) their energy usage, security, and home energy privacy.

3. Security in Monitoring and Measurement: High deployment of monitoring and measurement devices (e.g. sensors, Meters and PMUs) could also gives rise to system vulnerabilities. The effective functioning of SG is widely dependent on the widely-deployed accurate measurement devices. Such measured information are typically transmitted to a control utility center, such as Supervisory Control and Data Acquisition (SCADA) Systems [58]. State estimators in the utility center estimate the power grid status by analysing the measurement data and power system models. Therefore, it is very vital to guarantee the integrity of the data in SG. A usual attack to corrupt data integrity is the stealth attack (also called false-data injection attack), which was first interpreted by Liu et al. in [59]. It disscussed that an attacker can change the state estimated data without triggering bad-data alarms in the control center. Xie et al. [60] reflected that with the knowings of the system configuration, such attacks will circumvent the false data measurement detections in the SCADA systems, and may give rise to profitable financial misconduct. So, In order to know that how difficult it is to do a successful false-data injection attack on a particular measurements, Sandberg. [61] expalis security indices to measure the less effort required to reach attack goals while refusing false data alarms in the power grid utility control center. Yuan. [62] successfully developed the abstraction of a special type of false data injection attacks load redistribution attacks, and analyzed their worst damage to power grid operation in different time move with different attacking resource limitations. To protect the system from such attacks, scientists have defined various approaches. Early we disscussed that the control center of power grid uses state estimators to estimate the power grid state. In [63], it is shown how one can fully protect a state estimator from such hidden attacks by encrypting a adequate number of measurement devices. Dan and Sandberg [64] expanded the research in [63], [61] and defined two algorithms to keep encrypted appliances in the system to maximize their utility's system security.

4. Security in Information Transmission: It is widely famous that the communication technologies that we are utilizing are often not secure enough themselves and can easily be attacked. Hence most of the security and privacy issues which are there in the general communication networks (e.g. Internet and wireless networks) can also exist in SG Especially, we have to take more care of wireless communication technologies since wireless networks are expected to be the more vulnerable and functional deficit networks in SG. For example, wireless mesh networks (WMNs) are considered very reliable because they provide multihop redundant communication paths, but WMNs are vulnerable to attacks by only intelligent adversaries. ZigBee is known widely as a low-cost, low-power, wireless networking technology, found on the IEEE 802.15.4 standard. However, there also exist vulnerabilities associated with IEEE 802.15.4 implementations [65].

Security attacks on information transmission in SG can be classified in three major types based on their motto [66].

1) Network Availability: Malicious attacks on intending network availability can be called as DoS attacks. They attempt to slow down, block, or even manipulate information transmission so as to make network resources unavailable to terminals that are in need to exchange information in SG. As shown out by NIST [67], the high priority is of designing the information transmission networks that should be robust to attacks which are targeting network availability, because the network unavailability may outcome in the loss of real-time monitoring of critical smart grid infrastructures and power system disasters.

2) Data Integrity: Data integrity attacks generally intend to deliberately manipulate or corrupt information shared within the SG, its elements and may be highly damaging in the SG

3) Privacy of Information: Information privacy attacks just intend to eavesdroping on communications in SG elements so as to acquire desired information, like consumer account number and their energy usage. Initially, the work was done by Li et al. [68], who investigated the fundamental limit, i.e, how much channel capacity is essential to promise the secured communications among SG elements, from the perspective of information theory, and found the situation of a single meter and or Gaussian noise communication channel with an eavesdropper.

Thus to improve the security and privacy of information transmission in SG, researchers have exhibited several solutions. Lu et al. [69] suggested that the strong authentication protocol design and intrusion detection mechnism as the countermeasures to tackle and protect the SG network against attacks targeting data integrity and information privacy .Further, Khurana et al. [70] proposed a bunch of designs and talked practices which can often ensure the correctness of standards for authentication in SG. Such design principles encompass names, unique encoding, explicit trust considerations, implementations of timestamps, protocol boundaries, deliverance of secrets, and clear-cut security parameters.

II. CONCLUSION

Networking technologies advancements enhance the smart grid to be more efficient, robust and reliable power system. In this review, we have presented and characterized communication network architectures, performance

requirements and research challenges for intelligent power system management. For a network to work properly, the management of networking in smart grid is a key factor. The communication network must be capable of delivering the correct message with guarantee within the stipulated time frame. Some problems about the reliability and security of network in smart grid still need more attention, though few solutions are available. System reliability analysis and failure in protection mechanism are considered in order to realize a reliable and stable smart grid operation. Although smart grid enable power grid to be empowered with intelligent and advanced capabilities, it also opens up many new challenges and risks. Communication reliability and security must be provisioned with the delay constraint. Reliability and security are thus very challenging problems in the communication network

REFERENCES

[1] Harris, C. and Meyers, J.P. - "Working Smarter, Not Harder: An Introduction to the "Smart Grid"", in Electrochemical Society Interface, page 45, 2010
[2] SmartGrids – Strategic Deployment Document for Europe's Electricity Network of the Future, European Technology Platform, April 2010.[7] NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0, Office of the National Coordinator for Smart Grid Interoperability, U.S Department of Commerce, January 2010.
[3] Joe Miller. "Understanding the Smart Grid: Features, Benefits and Costs." Illinois Smart Grid Initiative. July 8, 2008.
[4] Melike Erol-Kantarci, and Hussein T. Mouftah, "Energy-Efficient Information and Communication Infrastructures in the Smart Grid: A Survey on Interactions and Open Issues", IEEE Communication Surveys & Tutorials, vol.17, no.1, pp. 179-197, First Quarter 2015.
[5] ABB Back ground Information, Smart grids: An Introduction to Smart Grids. Technology Roadmap: Smart Grids, International Energy Agency, 2011.
[6] A White Book on Smart Grid, Faculty of Information Technology, Mathematics and Electrical Engineering, Norwegian University of Science and Technology, 2011.
[7] F. Bagnan Beidou, Walid G. Morsi, C.P. Diduch and L. Chang. "Smart Grid: Challenges, Research Directions and Possible Solutions"2nd IEEE International Symposium on Power Electronics for Distributed Generation Systems (PEDG), 2010.
[8] Mitsubishi Electric (2013) Environmental technology R&D achievements.
[9] National Energy Technology Laboratory US (2009) A compendium of modern grid technologies.
[10] European Commission (2009) ICT for a low carbon economy.
[11] World Economic Forum (2009) Accelerating smart grid investments.
[12] Harris A (2009) Smart grid thinking. Eng Technol 4 (9):46-49.
[13] [National Institute of Standards and Technology, NIST framework and roadmap for smart grid interoperability standards, Release 1.0.
[14] E.W. Gunther, A. Snyder, G. Gilchrist, D.R. Highfill, Smart grid standards assessment and recommendations for adoption and development.
[15] Wenye Wang, Yi Xu and Mohit Khanna, "A Survey on the communication architectures in smart grid", Elsevier Journal on Computer Networks, vol. 55, pp. 3604-3629, 2011.
[16] Gungor, V.C., B. Lu and G.P. Hancke, 2010. Opportunities and challenges of wireless sensor networks in smart grid, IEEE Trans. Ind. Electron., 57(10): 3557-3564.
[17] Wenpeng, L., D. Sharp and S. Lancashire, 2010. Smart grid communication network capacity planning for power utilities, in Proc. IEEE PES, Transmission Distrib. Conf. Expo., 19-22: 1-4.
[18] Abolfazl Azari, "Survey of Smart Grid from Power and Communication Aspects", Middle-East Journal of Scientific Research, vol. 21(9), pp. 1512-1519, 2014.
[19] Zheng QIN, "A Survey of Networking Issues in Smart Grid", 2013.
[20] New Oxford American Dictionary. Oxford University Press, USA, 2010.
[21] Louis Anthony Cox. Evaluating and improving risk formulas for allocating limited budgets to expensive risk-reduction opportunities. Risk Analysis, DOI: 10.1111/j.1539-6924.2011.01735.x, 2011.
[22] Paul Hines, Jason Veneman, Brian Tivnan Smart Grid: Reliability, Security, and Resiliency. University of Vermont/MITRE Working Paper. January, 2014.
[23] K. B. Misra, "Role of Performance Engineering in Sustainable Development", Principles of Sustainable Development, vol. 3, Encyclopedia of Life Support Systems.
[24] Lo, C.H. and N. Ansari, 2011. The Progressive Smart Grid System from Both Power and Communications Aspects, IEEE Communications Surveys and Tutorials, pp: 1-23.
[25] La Commare, K. and K.J. Eto, 2004. Understanding the cost of power interruptions to U.S. electricity customers (Lawrence Berkeley National Laboratory, LBNL-55718.
[26] Güngör, V.C., D. Sahin, T. Kocak, S. Ergüt, C. Buccella, C. Cecati and G.P. Hancke, 2011 Smart grid technologies: Communication technologies and standards, IEEE Transactions on Industrial Informatics, 7(4): 529-539.
[27] P1366/d8, mar 2012 - ieee draft guide for electric power distribution reliability indices.
[28] Arif Islam, "Smart Grid Reliability Assessment Under Variable Weather Conditions", Graduate Theses and Dissertation, Scholar Commons University of South Florida, 2010.
[29] Mars: Ge concorda multiple area reliability simulator. Technical report, GE Energy Consulting, 2014.
[30] C. S. Bogorad and L. M. Nurani, "NERC'S DEFINITION OF THE BULK ELECTRIC SYSTEM", Spiegel & Mcdiarmid LLP, (2012).
[31] Z. B. Shukri, "WADP System Protection", Asia-Oceania Regional Council of CIGRE, (2012).
[32] Lee-Cheun Hau, Jer-Vui Lee, Yea-Dat Chuah and An-Chow Lai, "Smart Grid – The Present and Future of Smart Physical Protection: A Review", International Journal of Energy, Information and Communications, vol. 4, Issue 4, pp. 43-53, August 2013.
[33] [34] X. Chen, H. Dinh and B. Wang, "Cascading Failures in Smart Grid - Benefits of Distributed Generation", Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on, (2010), pp. 73-78.
[34] [35] Y. Wang, W. Li and J. Lu, "Reliability Analysis of Wide-Area Measurement System", IEEE Transactions on Power Delivery, vol. 25, no. 3, (2010), pp. 1483-1491.
[35] [36] M. Vaiman, M. Vaiman, S. Maslennikov, E. Litvinov and X. Luo, "Calculation and Visualization of Power System Stability Margin Based on PMU Measurements", 2010 First IEEE International Conference on Smart Grid Communications (SmartGridComm), (2010), pp. 31-36.
[36] [37] T. Godfrey, S. Mullen, R. C. Dugan, C. Rodine, D. W. Griffith and N. Golmie, "Modeling Smart Grid Applications with Co-Simulation", 2010 First IEEE International Conference on Smart Grid Communications (SmartGridComm), (2010) October 4-6, pp. 291-296.
[37] [38] S. B. Ghosn, P. Ranganathan, S. Salem, J. Tang, D. Loegering and K. E. Nygard, "Agent-Oriented Designs for a Self Healing Smart Grid", 2010 First IEEE International Conference on Smart Grid Communications (SmartGridComm), (2010), pp. 461-466.
[38] [39] H. A. Yusof, A. Musa, A. Q. Ramli and M. I. Ridwan, "Teleprotection simulation lab: Understanding the performance of telecommunication aided protection systems under impaired telecommunication network conditions", 2012 IEEE International Conference on Power and Energy (PECon), (2012), pp. 655-660.
[39] [40] T. M. Overman and R. W. Sackman, "High Assurance Smart Grid: Smart Grid Control Systems Communications Architecture", 2010 First

IEEE International Conference on Smart Grid Communications (SmartGridComm), (2010), pp. 19-24.
[40] [41] Melike Erol-Kantarci and Hussein T. Mouftah, "Smart Grid Forensic Science: Applications, Challenges, and Open Issues", IEEE Communication Magazine, pp.68-74, January 2013.
[41] [42] T. Baumeister. Literature review on smart grid cyber security, Technical Report, 2010.
[42] [43] A. R. Metke and R. L. Ekl. Security technology for smart grid networks. IEEE Transactions on Smart Grid, 2010.
[43] [44] National Institute of Standards and Technology. NIST framework and roadmap for smart grid interoperability standards, release 1.0, January 2010.
[44] [45] P. McDaniel and S. McLaughlin. Security and privacy challenges in the smart grid. IEEE Security & Privacy, 2009.
[45] [46] R. Anderson and S. Fuloria. Who controls the off switch? IEEE SmartGridComm10, pages 96102, 2010.
[46] [47] F. M. Cleveland. Cyber security issues for advanced metering infrastructure (AMI). IEEE Power and Energy Society General Meeting: Conversion and Delivery of Electrical Energy in the 21st Century, pages 1-6, 2008.

[47] [48] S. McLaughlin, D. Podkuiko, and P. McDaniel. Energy theft in the advanced metering infrastructure. 4th Workshop on Critical Information Infrastructures Security, 2009.
[48] [49] D. P. Varodayan and G. X. Gao. Redundant metering for integrity with information-theoretic confidentiality. IEEE SmartGridComm 2010, 345349, 2010.
[49] [50] R. Berthier, W. H. Sanders, and H. Khurana. Intrusion detection for advanced metering infrastructures: Requirements and architectural directions. IEEE Smart Grid Communication 2010, 350355, 2010.
[50] [51] G. Kalogridis, C. Efthymiou, S. Z. Denic, T. A. Lewis, and R. Cepeda. Privacy for smart meters: Towards undetectable appliance load signatures. IEEE SmartGridComm2010, 2010.
[51] [52] H. S. Cho, T. Yamazaki, and M. Hahn. Aero: Extraction of users activities from electric power consumption data. IEEE Transcations on Consumer Electronics, 2010.
[52] [53] M. A. Lisovich and S. B. Wicker. Privacy concerns in upcoming residential and commercial demand-response systems. the TRUST 2008 Spring Conference, 2008.
[53] [54] F. Li, B. Luo, and P. Liu. Secure information aggregation for smart grids using homomorphic encryption. IEEE SmartGridComm2010. 2010.
[54] [55] H. Li, R. Mao, L. Lai, and R. C. Qiu. Compressed meter reading for delay-sensitive and secure load report in smart grid. IEEE SmartGridComm2010, 2010.
[55] [56] A. Rial and G. Danezis. Privacy-preserving smart metering.
[56] [57] C. Efthymiou and G. Kalogridis. Smart grid privacy via anonymization of smart metering data. IEEE SmartGridComm2010, 2010.
[57] [58] National Communications System. Technical Information Bulletin 04- 1, Supervisory control and data acquisition (SCADA) systems. 2004.
[58] [59] Y. Liu, P. Ning, and M. Reiter. False data injection attacks against state estimation in electric power grids. ACM CCS, 2009.
[59] [60] L. Xie, Y. Mo, and B. Sinopoli. False data injection attacks in electricity markets. IEEE SmartGridComm, pages 226-231, 2010.
[60] [61] H. Sandberg, A. Teixeira, and K. H. Johansson. On security indices for state estimators in power networks. the First Workshop on Secure Control Systems, 2010.

[61] [62] Y. Yuan, Z. Li, and K. Ren. Modeling load redistribution attacks in power systems. IEEE Transaction on Smart Grid, 382392, 2011.
[62] [63] R. B. Bobba, K. M. Rogers, Q. Wang, H. Khurana, K. Nahrstedt, and T. J. Overbye. Detecting false data injection attacks on DC state estimation. the First Workshop on Secure Control Systems2010, 2010.
[63] [64] G. Dan and H. Sandberg. Stealth attacks and protection schemes for state estimators in power systems. IEEE SmartGridComm2010, 2010.
[64] [65] Department of Energy, Office of Electricity Delivery and Energy Reliability. Study of security attributes of smart grid systems - current cyber security issues 2009.
[65] [66] Z. Lu, X. Lu, W. Wang, and C. Wang. Review and evaluation of security threats on the communication networks in the smart grid. Military Communications Conference2010, 2010.
[66] [67] The Smart Grid Interoperability Panel - Cyber Security Working Group. Guidelines for Smart Grid cyber security: Vol. 1, Smart Grid cyber security strategy, architecture, and high-level requirements. NISTIR 7628.
[67] [68] H. Li, L. Lai, and R. C. Qiu. Communication capacity requirement for reliable and secure state estimation in smart grid. IEEE SmartGrid-Comm2010, 2010.
[68] [69] Z. Lu, X. Lu, W. Wang, and C. Wang. Review and evaluation of security threats on the communication networks in the smart grid. Military Communications Conference2010, 2010.
[69] [70] H. Khurana, R. Bobba, T. Yardley, P. Agarwal, and E. Heine. Design principles for power grid cyber-infrastructure authentication protocols .Hawaii International Conference on System Sciences, pages 1-9, 2010.