Journal of Renewable Energy and Sustainable Development (RESD) Volume 5, Issue 1, June 2019 - ISSN 2356-8569
http://dx.doi.org/10.21622/RESD.2019.05.1.003

The Challenges and Risks Facing ICT in the Management and Operation of the Smart Grid

Tarek M. Attia
National Telecom Regulatory Authority (NTRA), K28, Cairo-Alex. Desert Road, Smart Village, Giza, Egypt.
tattia@tra.gov.eg

Abstract **-** The Smart Grid integrates the traditional electrical power grid with information and communication technologies (ICT). Such integration empowers the electrical utilities providers and consumers and improves the efficiency and the availability of the power system while constantly monitoring, controlling and managing the demands of customers. Through the Smart Grid, the power system becomes smart by communicating, sensing, controlling and applying intelligence. It also keeps the environment free from pollution; minimizes the cost; and ensures effective operations against all types of hazards and danger. Smart Grid is a huge complex network composed of millions of devices and entities connected with each other through wireless communications techniques including Home Area Networks (HANs) and Wide Area Networks (WANs). Such a massive network comes with many security concerns and vulnerabilities. This paper highlights the complexity of the Smart Grid network and the challenges that exist in securing the smart power grid and the countermeasures and solutions applied for information and communication networks to secure Smart Power Grid. The paper concluded by overviewing the key functions and benefits of using the Smart Grid technology and how this affects human livelihood, economy and the environment.

Keywords **-** Smart Grid, Information and Communication Technologies (ICT), Challenges and Risks, Security and Privacy.

I. INTRODUCTION

The basic concept of Smart Grid is to add monitoring, analysis, control, and communication capabilities to the national electrical delivery system to maximize the throughput of the system while reducing the energy consumption. The Smart Grid will allow utilities to move electricity around the system as efficiently and economically as possible. It will also allow the home owner and business to use electricity as economically as possible.

Recent advancement in communication and information technologies turned the way of operations in different fields such as healthcare, industries, transportation, environment, logistics, power grids, banking, etc.… and the Smart Grid can be considered one of the main applications of Internet of Things (IoT) Technology.

Smart Grid technologies have been used to distribute and upgrade electricity through two-way communications and pervasive computing capabilities for improving reliability, control, safety and efficiency. Smart Grid delivers electricity between consumers and suppliers and control digital appliances to save energy and increase efficiency, reliability and transparency. It provides protecting and automatic monitoring for interconnected elements. It covers generators via transmission network and distribution system for industries and home users with their thermostats and other intelligent appliances [1].

Smart Grids provide electricity demand from the centralized and distributed generation stations to the customers through transmission and distribution systems. The grid is operated, controlled and monitored using ICT. These technologies enable energy companies to seamlessly control the power demand, allow for an efficient and reliable power delivery at reduced cost and reduce transmission losses. These technologies recover fault automatically and reduce transmission lines. Smart Grid technologies are effective and beneficial for modern power systems in terms of technical solutions and economical point of view. They can integrate the renewable energy and distributed sources. The system is real time and two ways with theft detection capabilities. Various different technologies have been adopted by Smart Grid such as sensor networks, wireless mesh networks and intelligent and other interconnected technologies.

Basically, the Smart Grid concept is to provide grid observability, create controllability of assets, and enhance security and performance with cost-effective operations, maintenance and system planning. Through Smart Grid technology, the new grid is

http://dx.doi.org/10.21622/RESD.2019.05.1.003

expected to provide self-corrective, reconfiguration and restoration capabilities.

An intelligence Smart Grid system autonomously collects real-time data, analyzes them by using information about cyber security, computational intelligence, electricity generation, substations, distribution and consumer consumption, and provides secure, safe and reliable control. Data information from various terminals iselectrically interconnected with a utility domain that is handled by the Supervisory Control and Data Acquisition (SCADA) system which has recently begun to spread in the world, especially in developed countries, as a practical model. Electrical information network protocol is a part of SCADA that helps in monitoring, controlling, configuration and troubleshooting the electric power networks. It can track disturbance in real time which means power grid should be responsive, awake and communicative with every node in the network [13].

Recently, the increasing demand for power transfers over long distance has emphasized the significance of stability in the power grid. Stability is referred to the ability of the grid to withstand disturbances through the nature of disturbance of interest. To address these challenges, power industries and government have been established to overcome and handle the issues with designing future grids. There are many challenges that hinder the efficiency of Smart Grid operation. Security remains one of the most important issues in Smart Grid systems given the danger and inconvenience residents and companies alike might encounter if the grid falls under attack. To understand the importance of exploring security and privacy issues in the Smart Grid which is one of the IoT applications, one must first take a look at the existing state of the IoT device deployments in the world. A study by Hewlett-Packard [2] on commercialized IoT deployments found that 80% of such devices violate privacy of personal information (e.g., name, date-of-birth, etc.), 80% failed to require passwords of sufficient complexity and length, 70% did not encrypt communications and 60% had security vulnerabilities in their user interfaces.

Three main security objectives must be incorporated in the Smart Grid system [3]: 1) availability of uninterrupted power supply according to user requirements, 2) confidentiality of user's data, and 3) integrity of communicated information.

The remainder of this paper is organized as follows. Section 2 provides a brief background about Smart Grid technologies. Section 3 discusses the key threats and challenges of Smart Grids. Section 4 explains the countermeasures and security solutions of Smart Grid. Section 5 provides a brief discussion of the key functions and benefits of the Smart Grid, and Section 6 summarizes the paper contributions.

II. SMART GRID TECHNOLOGIES

The National Institute of Standards and Technology (NIST) proposed a Smart Grid architecture composed of seven domains (bulk generation, transmission, distribution, customers, service providers, operations and markets) as shown in figure 1[4]. Each domain includes different Smart Grid actors. The Smart Grid infrastructure is divided into smart energy subsystem, information subsystem and communication subsystem. The Smart Grid can be viewed as having two main components; system component and network component.

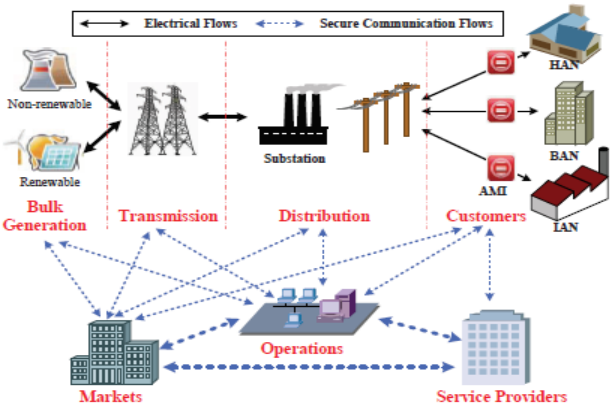

Fig .1 Domains of a mart rid [NIST]

1. System Components

The major system components in Smart Grid are Renewable Energy Resources, Distributed Energy Resources, Smart Meter, Electrical Household Appliances, Electric Utility Center for monitoring and controlling operation and Service Providers.

- Electrical Household Appliances are assumed to be able to communicate with smart meters via a HAN facilitating efficient power consumption management to all home devices.

- Renewable Energy Resources are solar, nuclear, coal and wind energy that supply home appliances with local generated electricity.

- Smart Meter is a stand-alone embedded system. Each smart meter contains a micro controller that has a memory, analogue/digital ports, timers, real-time clock and serial communication facilities. Smart meters register the power consumption periodically and transmit it to the utility server, connect or disconnect a customer power supply and send out alarms in case of abnormality. Some smart meters are equipped with relays that can be interfaced directly with smart home appliances to control them; for example, turn off the air conditioner during peak periods. Furthermore, the smart meter can be used in demand side management.

- Electric Utility Center interacts with smart meters to regulate power consumption. It also sends consumption related instructions to smart meters and collects sub-hourly power usage reports and emergency/error notifications using GSM/GPRS/3G/4G or WiMAX technology.

- Service Providers establish contracts with users to provide electricity for individual devices. Service providers interact with internal devices via messages relayed by the smart meter. To establish such interaction, service providers should register with the electric utility and obtain digital certificates for their identities and public keys. The certificates are then used to facilitate secure communications with users.

2. Network Component

In general, Smart Grid communication technologies are divided into 5 main areas: sensing and measurement, advanced components, decision support and improved interfaces, standards and interacted communications [1]. Smart Grid distributes the electricity between traditional and distributed generation resources to the residential, industrial and commercial consumers.

Through communication infrastructure, the smart monitoring and metering approaches provide real-time energy consumption. Via communication infrastructure, the Smart Grid intelligent devices, dedicated software and control centers interact with each other. The role of communication infrastructure is crucial for effective Smart Grid operations. Smart Grid incorporates two types of communication: Wide Area Network (WAN) and Home Area Network (HAN). A HAN connects the in-house smart devices across the home with the smart meter. The HAN can communicate using ZigBee, Wi-Fi, wired or wireless Ethernet, or Bluetooth. On the other hand, a WAN is a bigger network coverage that connects the smart meters, service providers and electric utility. The WAN can communicate using WiMAX, GSM/GPRS/3G/4G and 5G (in the near future), or fiber optics and power line communication (PLC).

ZigBee, Ethernet, Wi-Fi, GSM, General packet radio services (GPRS), 3G, 4G and WiMAX are promising wireless and wired technology are currently used as integrated Smart Grid systems for communication management due to some distinctive advantages. For example, ZigBee WSNs are employed due to their low improved scalability, reliability and low cost [5]. Long Term Evolution (LTE), WiMAX and 4G are also among the new generation of wireless communication technologies with significant area of wider application in Smart Grid operational realizations. From the perspective of broadband communication system performance, LTE and 4G are more advantageous because of their bidirectional communications characteristic with wider network potential coverage suitable for widespread terminal access and remote control [6].

Technologies used for communication have a wide application field intensity according to the coverage range and data transmission rate. These technologies are shown in Table1. In order to find opportunities in real life applications of the designed model, a module must be determined for data transmission to be carried out smoothly in the Smart Grid.

The smart meter acts as a gateway between the in-house devices and the external parties to provide the needed information. The electric utility manages the power distribution within the Smart Grid, collects power usage from smart meters, and sends notifications to smart meters once required.

http://dx.doi.org/10.21622/RESD.2019.05.1.003

Table 1 Comparison between Different Communication Technologies [1, 3, 5, 6].

Technology	Frequency Band	Data Rate	Coverage Range	Limitations
GSM	900, 1800MHz(licensed)	Up to 14.4Kb/s	1–10km	Very low data rates
GPRS	900, 1800MHz(licensed)	Upto170Kb/s	1–10km	Low data rates
3G	1900, 2100MHz(licensed)	384Kb/s -2Mb/s Up to 168 Mb/s (HSPA+)	1–10km	Costly spectrum fees, Latency
4G	900,1900,2100, 2600MHz (licensed)	Up to 300Mb/s	Up to 5km	Costly spectrum fees
WIMAX	2.5GHz,3.5GHz,5.8GHz	Up to100Mb/s	10-50km(LOS) 1–5km(NLOS)	Not widespread
PLC	1–30 MHz	NB-PLC: 500 Kb/s BB-PLC: 200 Mb/s	NB-PLC: 150 km BB-PLC: 1.5 km	Noisy channel environment
WI-FI	Unlicensed frequency bands (2.4GHz and 5GHz)	Up to 150Mb/s	30–250m	High interference, Short range, High power consumption
ZigBee	868–915MHz, 2.4 GHz	250Kb/s	30–50m	Low data rates, Short range

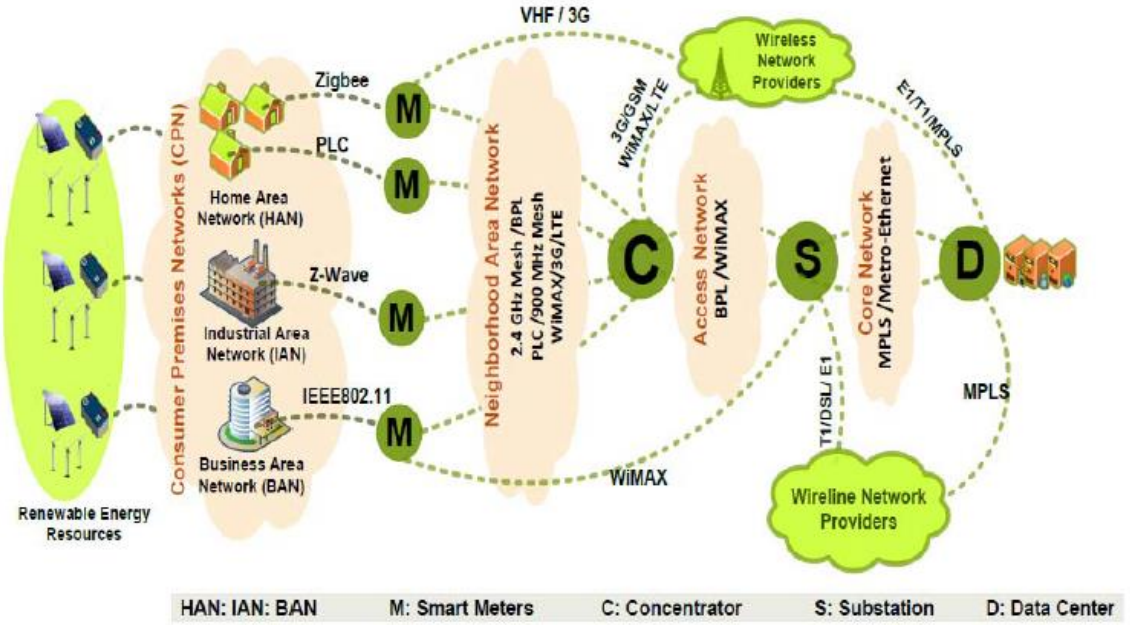

Fig .2 Basic network architecture [3]

The smart meter receives messages from devices within HAN and sends them to the appropriate service provider. Figure 2 illustrates the basic network architecture [3]. Note that while HANs are used in residential homes, Industrial Area Networks (IANs) and Business Area Networks (BANs) are used within industrial sites and business offices, respectively.

These technologies are designed to support Smart Grid applications in terms of controlling and monitoring operations as SCADA, Energy Management Systems (EMS), Distribution Management Systems (DMS), Enterprise Resource Planning Systems (ERPS), distribution feeder automation, generation plant automation, physical security, etc.

III. KEY THREATS AND CHALLENGES

Smart Grid is a mixture of different legacy systems paired with new technologies and architectural approaches, based on different standards and regulations that all need to be integrated into a

communication network to support the challenges of the future electricity network. To support this objective, the cyber security architecture for Smart Grid communications is presented on the basis of cyber security and architecture requirements, dependency on legacy installations, and the regulations and industry standards. The Smart Grid can offer enormous economic benefits, but it faces many challenges, some of which are briefly described below.

1. Identity Management

A Smart Grid has several intelligent devices that are involved in managing both the electricity supply and network demand. These intelligent devices may act as attack entry points into the network. Moreover, the massiveness of the Smart Grid network makes network monitoring and management extremely difficult.

Access control is related to identity management, mutual authentication is needed to ensure that both suppliers and consumers can be sure of the other party's identity. Identity verification is about linking identities to real world properties, e.g. the physical location of a sensor, or the full name and postal address of an object.

2. Objects safety and security

The Smart Grid consists of a very large number of perception objects that spread over large geographic area, it is necessary to prevent the intruder's access to the objects that may cause physical damage to them or may change their operation. There are some limitations for the objects, for example [7]:

- Computational and energy constraint: Most of the time, Smart Grid devices are battery driven and devices that are using low-power CPUs have low clock rate. Therefore, computationally expensive cryptographic algorithms (that require fast computation) cannot be transferred directly to such low powered devices.

- Memory constraint: Smart Grid devices are built with limited RAM and Flash memory compared to the traditional digital system (e.g. PC, Laptop, etc.), and use Real Time Operating System or lightweight version of General-Purpose Operating System. They also run system software and proprietary services. Therefore, security schemes should be memory efficient. However, traditional security algorithms are not designed specifically considering the memory efficiency, because the traditional digital system uses sizeable RAM and hard drive. Those securities schemes might not get enough space in memory after booting up the operating system and system software. Therefore, conventional security algorithms cannot be used directly for securing devices.

- Tamper Attacks: Smart Grid devices might be deployed in the remote regions and are left unattended. An attacker might tamper with the Smart Grid devices by device capture. Later, they can extract the cryptographic secrets, modify programs, or replace them with malicious nodes. Tamper resistant packaging is one way to defend against these attacks [2].

3. Data confidentiality

Smart meters autonomously collect massive amounts of data and transport them to the utility company and service providers. These data include private consumer information that might be used to deduce consumer's activities, devices being used and times when the home is vacant.

Data confidentiality refers to the prevention of data access by unauthorized persons or entities. Maintaining data availability involves ensuring that no person or entity could deny access to those authorized users and systems [14]. The sensor devices perform independent sensing or measurements and transfer data to the information processing unit over the transmission system. It is necessary that the sensor devices should have proper encryption mechanism to guarantee the data integrity at the information processing unit. The Smart Grid network determines who can see the data, thus, it is necessary to guard the data against external hackers.

4. Network security

The data from sensor devices is sent over wired or wireless transmission network. The transmission system should be able to handle data from a large number of sensor devices without causing any data loss due to network congestion, ensure proper security measures for the transmitted data and prevent them from external interference or monitoring [15]. There are some limitations for the security of the network, for example:

- Scalability: The number of Smart Grid devices is growing continuously and more devices are getting connected with the global information network. Current security schemes lack of the scalability property; therefore, such schemes are not suitable for Smart Grid devices.

- Diversity of devices: Diversity of the devices within the Smart Grid network ranges from the low-end RFID tags to full-fledged PCs. Therefore, it is hard to find a single security scheme that accommodates even the simplest of devices.

- Diversity of communication medium: Smart Grid devices connect to the local and public network via a wide range of wireless links. Therefore, it is difficult to find a comprehensive security protocol considering both the wireless and wired medium properties.

- Multi-Protocol Networking: Smart Grid devices might use a proprietary network protocol (e.g., non-IP protocol) for communication in proximal networks. At the same time, it might communicate with a Smart Grid service provider over the IP networking. These multi-protocol communication characteristics make traditional security schemes unsuitable for Smart Grid devices [2].

- Dynamic network topology: A Smart Grid device might join or leave a network at anytime from anywhere. The temporal and spatial device adding and exiting characteristic makes a network topology dynamic. Existing security model for the digital systems does not cope with these types of sudden network topological changes. Hence, such a model does not fit in with the smart device security.

5. Interoperability and Standardization

Many manufacturers provide devices using their own technologies and services that may not be accessible by others. The standardization of the Smart Grid network is very important to provide better interoperability for all objects and sensor devices and all components of Smart Grid. Using IP standards in Smart Grids offer a big advantage as they provide compatibility between the various components. However, devices using IP are inherently vulnerable to many IP-based network attacks such as IP spoofing, Tear Drop, Denial of Service (DoS), and others [7].

It can be envisaged that in a complex system such as Smart Grid, heterogeneous communication technologies are required to meet the diverse needs of the system. Therefore, the standardization of communications for Smart Grid means making interfaces, messages and work flows interoperable. Instead of focusing on or defining one particular technology, it is more important to achieve agreement on usage and interpretation of interfaces and messages that can seamlessly bridge different standards or technologies. In other words, one of the main aims of communication standardization for Smart Grids is ensuring interoperability between different system components rather than defining these components (meters, devices or protocols).

6. Deficiency of Policies and regulations

some countries already build smart cities with Smart Grids but still they are not clear to set the policies, regulations, guidelines and standards. The implementation of Smart Grids is another challenge because of its complicated design, planning and maintenance and operations. Only well organization with professional staff government organization can perform these tasks effectively. Inefficient and unorganized communication between teams might cause a lot of bad decisions leading to much vulnerability [1].

To educate the customers about Smart Grid operations and other services is another challenge. Cyber security technologies are not enough to achieve secure operations without policies, regulation and training.

7. Network Availability

Smart Grid services must be available at all times and Remote access to grid devices should be monitored and controlled. Since Smart Grid uses IP protocol and TCP/IP stack, it becomes subject to DoS attacks and to the vulnerabilities inherent in the TCP/IP stack. DoS attacks might attempt to delay, block, or corrupt information transmission in order to make Smart Grid resources unavailable.

8. Efficiency and Scalability

Ensuring system availability is a high priority in critical systems like the Smart Grid which requires that several key issues be addressed. First, the system

must be efficient in its use of computation and communication resources so that resources do not get dominated and all requests can be handled. Second, the system must have adequate redundancy built into it so that, if sub-systems fail or are compromised, then the entire system does not collapse. Third, the system should support auxiliary security functions that may be deployed in the Smart Grid communication system to detect and to respond to cyber-attacks [8]. Fourth, the system must have good error management built in to ensure proper handling of failures (e.g., those resulting from bad messages).

9. Impact of Interference due to Transmission Lines on Wireless Medium

One of the concerns in using wireless communication along power lines is the interference from high-voltage transmission lines. Electromagnetic noise generated around high-voltage power lines is an undesirable disturbance, which can affect wireless data transmission. This noise can be observed as an additive signal to the original one, and it can interrupt, obstruct, degrade, or limit the performance of communication systems [9].

10. Limitations based on software

These limitations include for example:

- Dynamic security patch: Installing a dynamic security patch on the Smart Grid devices and mitigating the potential vulnerabilities is not a straightforward task. Remote reprogramming might not be possible for the Smart Grid devices, as the operating system or protocol stack might not have the ability of receiving and integrating new code or library.

- Embedded software constraint: Operating systems, which are embedded within the Smart Grid devices, have thin network protocol stacks and might lack enough security modules. Therefore, the security module designed for the protocol stack should be thin, but robust and fault tolerant.

11. Jamming and Access Restriction

A jamming attack is used to prevent meters from connecting with the utility company through stuffing the wireless media with noise. This can be implemented in two methods: continuous noise signal emission causing the channel to remain blocked; and noise signal emission only in response to the sensing of normal radio channel signals. Smart meters are affected in two corresponding ways: The channel can always be seen as engaged by carriers; and data packets are prevented from being received [10].

12. Frequency Spectrum scarcity

The Smart Grid devices require dedicated spectrum to transmit data over the wireless medium. Due to limited spectrum availability, an efficient dynamic cognitive spectrum allocation mechanism is required to allow millions of sensors to communicate over the wireless medium.

IV. COUNTERMEASURES AND SOLUTIONS

Security is a major challenge because the Smart Grid systems are controlled through the digital communications network, where important and private data are disseminated and stored. So, there is a need for a proper mechanism to ensure security and privacy in systems. The security and cyber securities are major challenges of recent Smart Grids systems.

Having overviewed the major challenges and vulnerabilities of Smart Grid, this section outlines some measures and solutions on cyber security for Smart Grid communications [3]:

1. Identity should be verified through strong authentication mechanisms

Organizations should implement an implicit deny policy such that access to the network is granted only through explicit access permissions. Moreover, each object/sensor needs to have a unique identity over the Internet. Thus, an efficient naming and identity management system is required that can dynamically assign and manage unique identity for such numerous objects.

2. Malware protection on both Embedded and General-purpose systems

Embedded systems are intended to only run software that is supplied by the manufacturer. The manufacturer is required to embed in its products a secure storage that contains keying material for software validation. Using a key, the system can validate any newly downloaded software prior to running. However,

general purpose systems are intended to support third party software. For this system, up-to-date and frequently updated antivirus software along with host-based intrusion prevention are required.

3. Network Intrusion Prevention System (IPS) and Network Intrusion Detection System (IDS)

technologies should augment the host-based defence to protect the system from outside and inside attacks. It is important to guarantee the real time performance and continuous operation features in a Smart Grid communication system.

4. Vulnerability assessments

They must be performed at least annually to make sure that elements that interface with the perimeter are secure. In some instances, user actions can open potential system vulnerabilities. As such, awareness programs should be put in place to educate the network users about security best practices for using network tools and applications.

5. Public Key Infrastructure (PKI)

Devices must use PKI to secure communication. However, there are some constraints regarding cryptography and key management. Current devices do not have enough processing power and storage to perform advanced encryption and authentication techniques, communications in a Smart Grid system will be over different channels that have different bandwidths, and connectivity, where all devices, certificate authorities, and servers must be connected at all times.

6. Special design and operation of Smart Grid

Security must be part of the Smart Grid design. Otherwise, security of devices becomes vendor specific; the fact that might produce many vulnerabilities because of incompatibility issues. Moreover, third-party companies can help for managing communication and data security issues of data transfer if network communications become a burden to the utilities.

7. Robust Authentication Techniques for Smart Grid includes

- Authentication protocol: A robust authentication protocol is needed while communicating between Smart Grid parties. The protocol must operate in real-time abiding with some constraints such as minimum computational cost, minimum communication overhead, and robustness to attacks, especially DoS attacks.

- Devices must know the sources and destinations they communicate with: This is accomplished through mutual authentication techniques using Transport Layer Security (TLS) or Internet Protocol Security (IPsec). In addition, devices should support Virtual Private Network (VPN) architectures for secure communication.

8. Customer training

The government of any country must take the initiative for trainings and programs where customers will be taught about Smart Grids, its benefits and potentials. Print and electronic media are the main sources to educate customers and highlight the advantages and the benefits of using Smart Grid technologies.

9. Services resilient

With the very large numbers of sensors and actuators expected, it is inevitable that some fail, either through hardware faults, electrical noise or even mishandled upgrades. Services need to be designed to be resilient in the face of such failures. This needs to happen at multiple levels of abstraction. Resilience is also important for handling rapid changes in demand without overloading the platforms the services are running on. Resilience is also key to handling cyber-attacks. One approach to counter this is defense in depth with successive security zones for detecting intrusion and raising the alarm. Continuous monitoring can be combined with machine learning techniques for spotting unusual signs of behavior.

Cyber-attacks on Smart Grid devices are inevitable and the resilience of devices and networks must be carefully considered. Separation of valuable network assets may be the best way to protect them from attacks.

10. Privacy measures

Smart Grid should only collect the data needed from the huge amount of transferred data to achieve their goals and it is necessary to take proper privacy

measures and prevent unauthorized access. Some potential design principles are proposed to address privacy issues in the Smart Grid:

- An organization should ensure that information security and privacy policies and practices exist and are documented and followed. Audit functions should be present to monitor all data accesses and modifications.
- Organizations should ensure the data usage information is complete, accurate, and relevant for the purposes identified in the notice.
- Privacy policies should be made available to service recipients. These service recipients should be given the ability to challenge an organization's compliance with their state privacy regulations and organizational privacy policies as well as their actual privacy practices.
- Only personal information that is required to fulfil the stated purpose should be collected from individuals. Treatment of the information should conform to these privacy principles.
- Personal information should be used only for the purposes for which it was collected and should not be disclosed to any other parties except for those identified in the notice, or with the explicit consent of the service recipient.
- Personal information in all forms, should be protected from unauthorized modification, copying, access, use, loss, theft, or disclosure and notice should be announced before collecting and sharing personal information and energy use data.
- Information should only be used or disclosed for the purpose for which it was collected and should only be disclosed to those parties authorized to receive it. Personal information should be aggregated or anonymized wherever possible to limit the potential for computer matching of records.

V. THE KEY FUNCTIONS AND BENEFITS OF THE SMART GRID

The Smart Grid has to operate in a highly efficient manner, with higher liability and enhanced power quality. This key feature offers a lot of advantages and future perspectives in the power energy domain. One of the main characteristics of Smart Grid is to keep a self-healing feature while relying on more renewable energy based generations systems such as solar and wind.

Customers will have better control and responsibility toward their power consumption. Due to its self-healing action, long outages will not occur. Smart Grids will be more efficient and economical than the existing power system because they will facilitate more renewable energy source integration. Figure 3 is an overview of Smart Grid key functions [11].

Monitoring and forecast of the supply-demand balance can be done in order to maintain the balance of supply and demand in energy production and consumption in the Smart Grid. Storing energy with photovoltaic cells and PV power units offers a wide range of opportunities in the network control in the provision of supply-demand balance in the micro-grid network [11]. The status of materials that are used in power generation and distribution of transmission is important for continuity of electrical energy. Also, energy can be used efficiently by coordinating production, transmission, distribution and storage.

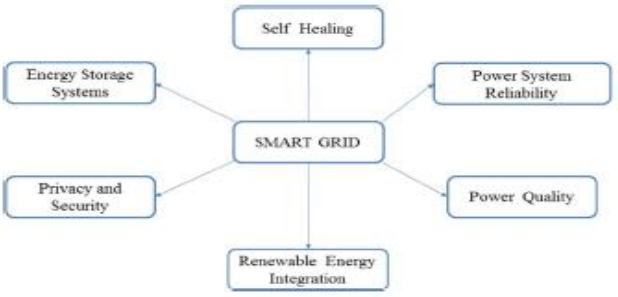

Fig .3 Key functions of Smart Grid

Providing security of supply in the network raises the issue of energy efficiency. The customer also has a great responsibility alongside energy efficiency starting from subscriptions until delivery to the subscriber in an optimized way. Subscriber will contribute to this process by the selection of equipment and using it at convenient times. Keeping in mind the balance of the entire system constructed by the network structure will disclose itself. Consumers would support more longevity of the network and the effective protection minimizing technical losses by changing habits and drawing energy from the network overtime. Average energy consumption from the main supply and demand of energy taken under the energy efficient use of resources can be done with Smart Grid

management. In case of the production of renewable energy more efficiently, the use of energy storage is an alternative idea. Giving priority to renewable energy sources will reduce carbon emissions (CO2). The balance of supply and demand in the network can be met by storing the energy while providing priority to renewable energy sources.

The grid will gain a dynamic structure by providing a controlled flow of power in distribution networks.

There are many benefits by using Smart Grid networks instead of traditional Grid, for examples:

- Reduce energy consumption costs by reducing energy consumption at peak time and to define the amount of energy that must be purchased based on real data and production plans.
- Reduce energy consumption by comparing energy consumption with production level: when a reduction in the production output is not matched by a corresponding reduction in energy usage, this must trigger energy managers to seek the waste source, and then take action to remove it [12].
- Improving the efficiency and the availability of the power system while constantly monitoring, controlling and managing the demands of customers.
- Improving maintenance management efficiency by identifying patterns in energy consumption and taking proactive maintenance considers when energy consumption goes consistently out of range.
- Improving the environmental effect and reputation of the factory by measuring and reducing the CO2 footprint of production processes.
- Continuous improvement of energy efficiency at the production level by decentralizing decision-making.
- Monitoring power quality in factories by monitoring energy in real-time and informing the energy provider about power fluctuations occurrences.
- Increasing energy-aware process design in both the short and the long term by integrating energy data into process design to reduce energy waste.
- Improving the economics of self-generated power by the efficient use of renewable energy; for example, using weather forecasting to build production schedules relying on energy that is expected to be generated and requiring energy for production [12].

VI. FUTURE RESEARCH DIRECTION

Future research efforts involving ICT for Smart Grid management and control functions should focus on a number of critical issues. Since Smart Grid concept use distinct and advanced communication architectures, therefore issues regarding operational readiness, communication security, system responsiveness, management of increased number of communication nodes in the network, the routing protocols in communication networks for Smart Grid between in-home smart appliances, smart meter and the operator's control center, ease of system deployment and extended network coverage should be given preference. Future research on sensor design and measurement in intelligent network architecture should focus more on a high degree of sensitivity, security and reliability that ensures higher information integrity at the consumer terminal, as well as reliable feedback for central control of the tool and management system. The achieving of these functions highly depend on innovations of new and advanced microelectronic technologies and control methods, improved energy conversion and storage systems and applications of integrated power electronics devices. Further studies are needed to enhance the security level of the grid including integrity and confidentiality of the transmitted data, and enhancing universal policies and regulations for secure communication technology. Finally, there is also need to improve the time required to perform speedy fault diagnosis which can basically be achieved by improvement in interfaces and decision support technologies.

VII. CONCLUSIONS

Traditional power systems are moving towards digitally enabled Smart Grids which will enhance communications, improve efficiency, increase reliability and reduce the costs of electricity services. Smart Grid technology is a beneficial technology for power system stability, customer's satisfaction, load distribution and all types of grid operations. The emergence of Smart Grid technologies will give favorable environment for future, better power

supplies services. Clearly, securing the Smart Grid communication infrastructure will require the use of standards-based state-of-the-art security protocols.

The massiveness of the Smart Grid and the increased communication capabilities make it more prone to cyber-attacks. Since the Smart Grid is considered a critical infrastructure, vulnerabilities and challenges should be identified and sufficient measures and solutions must be implemented to reduce the risks to an acceptable secure level. This paper was used to identify interesting multiple issues of importance to Smart Grid cyber security. This paper also surveyed the challenges, threats and vulnerabilities in Smart Grid networks, and the solutions needed as countermeasures to these challenges. An observed trend was that many of the attacks were almost identical in their function, but they are simply applied to the grid in different ways.

REFERENCES

[1] R.M. Larik, M.W. Mustafa and S.H. Qazi. “Smart Grid Technologies in power systems: An overview.” Research Journal of Applied Sciences, Engineering and Technology, vol. 11(6), pp 633-638, 2015.

[2] M. Hossain, M. Fotouhi, and R. Hasan. “Towards an analysis of security issues, challenges, and open problems in the Internet of things.” 2015 IEEE World Congress on Services, New York, 2015, pp. 21-28.

[3] F. Aloul, A.R. Al-Ali, R. Al-Dalky, M. Al-Mardini and W. El-Hajj. “Smart Grid Security: Threats, vulnerabilities and solutions.” International Journal of Smart Grid and Clean Energy, vol. 1, No. 1, September 2012.

[4] J. Liu, Y. Xiao, S. Li and W. Liang. “Cyber security and privacy issues in Smart Grids.” IEEE Communications Surveys & Tutorials, vol. 14, No. 4, Fourth Quarter, pp.981-997, 2012.

[5] S. Elyengui, R. Bouhouchi and T. Ezzedine. “The enhancement of communication technologies and networks for Smart Grid applications.” International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), vol.2, Issue 6, pp. 107-115, November-Dec.2013.

[6] Y.S. Mohammed, N. Bashir, A. Mohammed and A.K. Benjamin. “Information and communication technology for control and management in power systems Smart Grid.” International Journal of Engineering and Innovative Technology (IJEIT), vol. 2, Issue 5, pp. 214-220, November 2012.

[7] R. Khan, S.U. Khan, R. Zaheer and S. Khan. “Future Internet: The Internet of things architecture, possible applications and key challenges.” in 10th International Conference on Frontiers of Information Technology Proceedings, 2012, pp. 257-260.

[8] Ye Yan, Yi Qian, H. Sharif and D. Tipper. “A survey on cyber security for Smart Grid communications.” IEEE Communications Surveys & Tutorials, vol. 14, No. 4, pp.998-1010, Fourth Quarter 2012.

[9] A. Pawar and S. Rahane. “Opportunities and challenges of wireless communication technologies for Smart Grid applications.” International Journal of Computer Networking, Wireless and Mobile Communications (IJCNWMC), vol. 3, issue 1, pp. 289-296, Mar 2013.

[10] C. Lopez, A. Sargolzaei1, H. Santana1 and C. Huerta. “Smart Grid cyber security: An overview of threats and countermeasures.” Journal of Energy and Power Engineering, vol. 9, pp. 632-647, 2015.

[11] R. Bayindir, I. Colak and K. Demirtas. “Smart Grid technologies and applications.” Renewable and Sustainable Energy Reviews (66), pp.499-516, December 2016.

[12] F. Shrouf and G. Miragliotta. “Energy management based on IoT: Practices and framework for adoption in production management.” Journal of Cleaner Production, pp.1-12 (2015).

[13] P. Thapa, S. K. Acharya, H.I. Chang, S. Park, H.S. Jung, O.I. Whan, G.C. Park and J. Lee. “A high-speed intelligence Smart Grid system by using MIMO channel capacity.” International Journal of Advances in Computer Networks and Its Security(IJCNS), vol. 7, issue 1, pp. 113-117, April 2017.

[14] I. Ali, S. Sabir and Z. Ullah. "Internet of things security, device authentication and access control: A review." International Journal of Computer Science and Information Security (IJCSIS), vol. 14, No. 8, pp.456-466, August 2016.

[15] T. Attia. "Challenges and opportunities in the future applications of IoT technology." 2nd MENA Regional ITS Conference, Egypt on 18 – 21 February 2019, pp.1-15.