Available online www.jsaer.com

***Journal of Scientific and Engineering Research*, 2021, 8(9):21-30**

Review Article

ISSN: 2394-2630
CODEN(USA): JSERBR

Smart Grid

Matthew N. O. Sadiku[1], Uwakwe C. Chukwu[2], Abayomi Ajayi-Majebi[3], Sarhan M. Musa[1]

[1]Roy G. Perry College of Engineering, Prairie View A&M University, Prairie View, TX, USA
[2]Department of Engineering Technology, South Carolina State University, Orangeburg, SC, USA
[3]Department of Manufacturing Engineering, Central State University, P.O. Box 1004, Wilberforce, OH, USA
Email: sadiku@ieee.org; uchukwu@scsu.edu; ajayi-majebi@centralstate.edu; smmusa@pvamu.edu

Abstract This chapter presents a brief overview on smart power grid. It begins by discussing the characteristics of smart grid. It covers the basic enabling technologies. It discusses the problem of electromagnetic interference on smart grid. It addresses the unique security requirements or objectives of smart gird. It covers some applications of smart grid and its future. It presents some benefits and challenges of smart grid.

Keywords Smart grid, smart city, smart everything

Introduction

To sustain our modern society, we need an uninterrupted supply of electricity. The world's annual electricity generation was 20,250 TWh in the year 2012 and is expected to be 25,500 TWh in the year 2020 [1]. In the traditional power system, electricity is being generated and transmitted through a one-way transmission and distribution system called the grid. The basic structure has not changed for about 100 years. It is known to be inefficient and unreliable. As a result of its low efficiency, the power industry is faced with unprecedented challenges and opportunities. Experiences have shown that it is not suitable for 21st century.

The US Department of Energy (DOE) is charged with modernizing the nation's electricity grid to improve its reliability and efficiency. The ongoing modernization of the electric power grid is commonly referred to as the "smart grid." The word "smart" in smart grid refers to the notion of a power grid with intelligence. The main objective of the smart grid is to bring reliability, flexibility, efficiency, and robustness to the power system. Smart grid does this by introducing two-way data communications into the power grid. Thus the smart grid consists of the power infrastructure and communication infrastructure, which correspond to the flow of power and information respectively. This enables intelligent operation of the smart grid. But this introduces security-related challenges [2,3].

Characteristics of Smart Grid

The term "grid" is traditionally used for electricity generation, electricity transmission, electricity distribution, and electricity control. A "smart grid" is an enhancement of the traditional electric power grid. It is also known as "intelligent grid," or''The Grid 2.0." It is the modernization of the power delivery system. It is a transformation of the legacy unidirectional electric grid into automatic intelligent system of bidirectional exchange of electric power and information. A smart grid may be defined as any combination of enabling technologies, hardware, software, or practices that collectively make the delivery infrastructure (or the grid) more reliable, more versatile, more secure, more accommodating, more resilient, and ultimately more useful to consumers [4]. A smart grid basically consists of overlaying the physical power system with the information

system. A conceptual model of the smart grid based on NIST (National Institute of Standards and Technology (NIST) is shown in Figure 1 [5].

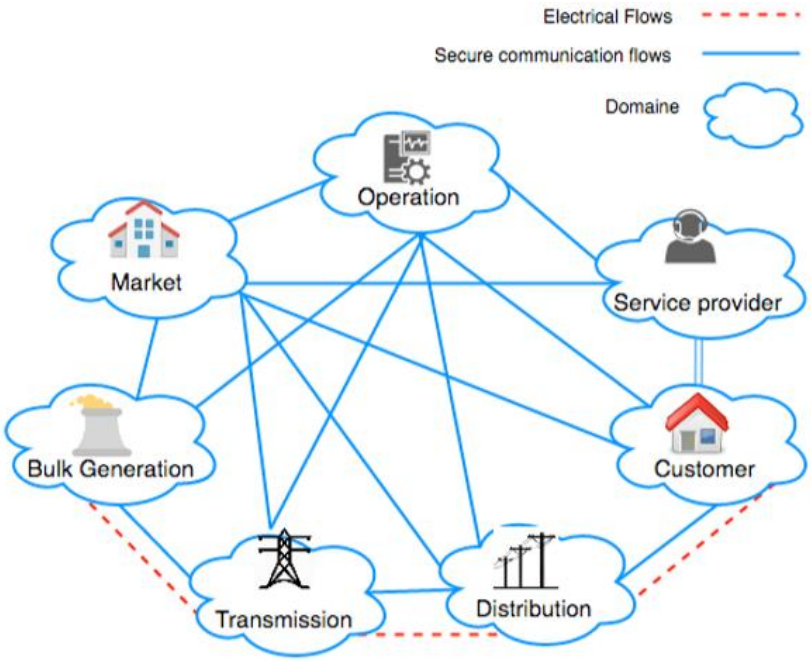

Figure 1: A conceptual model of the smart grid based on NIST [5]

From the technical point of view, the smart grid can be divided into three major systems [6]:

- *Smart infrastructure system:* This is the energy, information, and communication infrastructure underlying the smart grid. This allows two-way flow of electricity and information. This implies that the users may put back electricity into the grid. The system enables multiple entities (such as intelligent devices, dedicated software, control center, etc.) to interact.
- *Smart management system:* This provides advanced management and control services. Efficient management is fundamental for efficient operation of smart grids. Management of smart grid includes the development and implementation of smart metering, real time pricing, efficient management of renewable energy sources, and management of transmission and distribution networks.
- *Smart protection system:* This provides advanced reliability analysis, fault protection, and security services. The existing infrastructure has become vulnerable to several security threats.

Fundamental Technologies

The smart grid is made possible by applying sensors, smart meters, and field automated devices to the electrical power grid. The grid can predict, adapt, and reconfigure itself reliably and efficiently. It will be able to handle uncertainties in schedules, power transfer across regions, managing and resolving unpredictable events, and meeting the demand for reliable supply [7].

Indispensable to the functioning of a smart grid are considerations dealing with: energy storage, advanced meters and sensors, grid-friendly plug-in hybrids, grid-friendly loads, substation and distribution automation, communications, data-intensive analysis, visualization and human interface, and renewable energy integration [8]. Smart grids employ novel load shaping strategies based on energy storage and dynamic pricing. A consumer would sign up for a nominal quota of energy from the grid. If the usage exceeds the quota the consumer is faced with a higher electricity price. If these strategies are implemented with low complexity and in a distributed fashion, scalability to large number of consumers is possible [9].

The smart grid architecture has five major components: power architecture, communication networks, wireless sensor networks, Supervisory Control and Data Acquisition (SCADA), and smart meters [10].

- *Power Architecture:* Generation, transmission, and distribution are the three main subsystems of the electric power system. The smart grid utilizes several technologies to produce, distribute and monitor

energy usage to customers. The power infrastructure generates and distributes power to consumers. Energy from distribution substation is received by the Home Area Network (HAN) and distributed to all home appliances.

- *Communication Networks:*. Over the years, the power industry operated their own communications infrastructure to control power grids. The trend has shifted toward using shared public communication networks. Smart grids need communication networks to convey sensing and control data for improving the efficiency of energy generation, transmission, and delivery. The power and communication systems are becoming more and more interdependent. The smart grid is the next generation electric power system that depends on modern communication networks and supports electricity generation, transmission, and consumption. It is the emerging intelligent power systems that depend on Information and Communication Technology (ICT). The communication network includes the physical network architecture and network protocols. All components are connected by the several communication technologies such as Wide Area Networks, WiMax, and HAN. The communication infrastructure controls the power infrastructure and makes it intelligent, efficient, and reliable. It is vital that communications are secured, devices are protected, and privacy is respected. The communication system measures, collects, stores, and communicates between all devices.
- *Wireless Sensor Networks* (WSNs): A wireless sensor network (WSN) usually consists of a large number (hundreds or thousands) of sensor nodes deployed over a geographical region. The wireless sensor nodes are compact, light-weighted, and battery-powered devices that can be used in virtually any environment. Wireless sensor networks enable both utilities and customers to transfer, monitor, predict, and manage energy usage effectively and costly. They have been confirmed as one of the most promising technologies for many smart grid (SG) applications due to their low complexity and inexpensive costs. They have been recognized as a promising technology that can enhance various aspects of today's electric power systems, including generation, delivery, and utilization.
- *SCADA*: Smart grid may also be regarded as a combination of several micro grids. Each micro grid operates autonomously within its system supervisory control and data acquisition (SCADA) system. SCADA is a control system for smooth managing large-scale, automated industrial operations. When applied to electric power industry, it can help the industry to save time and money, reduce operational costs, and improve efficiency. It provides real-time monitoring and automation for smart power grid. SCADA is now used extensively in the electricity sector and integrated with external systems. It is the controlling system as well as the communication network in smart grid [11].
- *Smart Meters:* For customers, the first step towards the smart grid is the installation of smart meters. Smart meters are wireless, high-tech, digital communication devices that will replace the old, analog electricity meters and allow remote electricity readings. They are essentially digital meters that read remotely over a secure wireless network. A smart meter is a significant smart grid infrastructure with capabilities for facilitating real-time energy consumption and billing, voltage and frequency data measurement, loads connections and disconnections, diagnostic information communication and efficient energy usage. The smart meter, the home area network (HAN), advanced sensors, control systems, standardized software interfaces and information management systems allow information gathering and dissemination between user-ends and utilities and collectively constitute the advanced metering infrastructure (AMI) [12]. AMI includes Supervisory Control and Data Acquisition (SCADA) Center, smart meters, and Wireless Sensor Networks. This allows for automatic reading of power consumption of the customers. Utilities can automate billing from a centralized interface.

EMI on Smart Grid

Traditionally, the power lines operate at very low frequency and high power while communication systems operate at very high frequency and very low voltage. The interaction of electronic devices with broadband power line technology (PLC) used for high frequency operations leads to electromagnetic interference (EMI). All power grid devices are exposed to electromagnetic (EM) fields of natural or manmade origin, radiated directly into devices or conducted via the power, signal or ground connections. The smart grid now comes with

critical challenges, prominently among others, of the electromagnetic compatibility (EMC) issues which if not addressed would hinder the sole purpose of smart grid.

Electromagnetic interference (EMI) is a disturbance caused by electromagnetic induction, electrostatic coupling, or conduction, thereby affecting the performance of a device, transmission channel, or a system.

As illustrated in Figure 2 [13], there are two types of electromagnetic interference [14]: (1) Radiated interference, (2) Conducted interference. The radiated electromagnetic interference consists essentially of the common mode noise, differential mode noise and mixed mode noise signals. Conducted interference is a major issue in most power electronic systems due to significant leakage current generated by fast switching and stray components of the system.

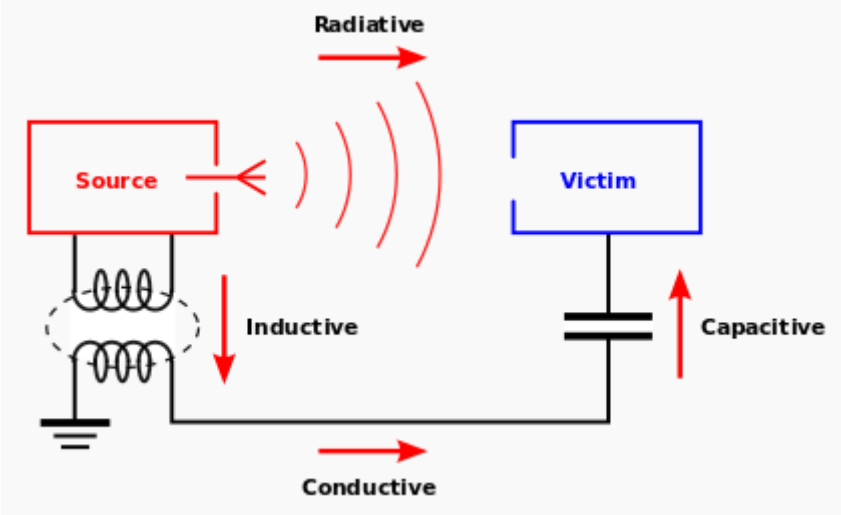

Figure 2: EMI coupling modes [13]

Comparing the modern power switches used in power supplies with those from older generations, the new switches have significantly reduced switching times, leading to faster rise and fall times for the voltage and current waveforms. These fast edges produce significant energy at surprisingly high frequencies, and are the root cause of all EMI problems in switched-mode power supplies. The sources of electromagnetic interference in smart grid are the power system infrastructure, communication systems and information technology systems. The operation and interaction of devices in these units introduces EMI to the system which poses a threat to the efficient utilization and performance of the smart grid. These devices can be narrowed down to the following [15,16]: (1) Power electronic interfaces (PEI), (2) Smart Meter, (3) Power line technology (PLC), (4) Flexible AC transmission systems (FACTS), (5) Other communication technologies. Here we consider EMI on each of these devices.

- *EMI in Power Electronic Interface:* The traditional energy sources has negative effects on the environment, hence the introduction of renewable energy sources (such as wind, solar, hydro, photovoltaic, fuel cell) to facilitate distributed generation. Renewable energy resources cannot be directly integrated into the grid because of their varying output characteristics, hence the increased use of power conversion devices which depends on the application of power electronic interfaces which are susceptible to electromagnetic interference. In power electronics, the two major sources of EMI are dv/dt and di/dt during switching times. The presence of group of converters leads to the aggregation of sources of interference in power electronic interface and the transfer of interference over distant circuitry on input and output of the converters.
- *EMI in Smart Meter:* The smart meter is an advanced energy meter that measures the consumption and facilitates the connection between the consumer and the power utilities. It uses a two-way communication to provide real time information on energy consumption which helps in controlling and monitoring the meter and also helps the utility to optimize power generation, transmission, and distribution as required and demanded. Smart meters emit electromagnetic radiation, like cell phones

and other high-tech electronic devices. But there is no agreement among scientific experts as whether the radiation is harmful or not.

- *EMI in Power Line Communications:* Power line carries power from the generation point to distribution unit through to the consumers using electrical cables usually at 50 Hz or 60 Hz frequency. Due to it availability everywhere, it was proposed as a means of communication. Also, it gives the utility the opportunity to oversee their own communication infrastructure. This system is referred to as power line communication system. However, the viability of this new technology is been questioned, due to some challenges it seems to be facing. PLC is susceptible to electromagnetic interference and can also be a source.
- *EMI in Flexible AC transmission systems* (FACTS): FACTS devices generate a high frequency steady state electromagnetic noise due to continuous transient switching of power electronic components such as thyristor valve. FACTS devices consist of components such as DC-AC inverter, interfacing inductor banks, harmonic blocking transformer, step-up transformer, associated control hardware and software. These are the culprit FACTS devices that are responsible for high electromagnetic disturbances that make the operation of FACTS devices worrisome despite their important roles in renewable energy integration and control. Fundamentally, FACTS controllers are based on controlled switching power-electronic devices used for power conversion and compensation. For high flexibility and wide substation load variation tolerance, new FACTS-based equipment is finding increasing applications in bi-directional transmission system's reactive power generation and absorption control.

Security of Smart Grid

The nation's security, economic prosperity, and the well-being of the citizens depend on reliable and secure energy infrastructure. For every nation, government and private industry work together to protect critical infrastructure.

With the heavy reliance on computer communication networks to manage its energy usage, a smart grid becomes exposed to vulnerabilities and cyber attacks. The potential impact of cyber attacks is vast. Potential threats from a broad range of cyber attacks on the smart grid have become a serious concern. Cyber security is critical to sustainable modern grid. Security is crucial attribute of the smart grid. It is the degree of protection provided by the grid against potential loss or damage. Security issues arise as smart power grids become targets of cyber security threats. With the rapid expansion of the Internet of things, the potential for malicious attacks on the smart grid is on the increase. A breach in the security of the smart grid can be fatal for its reliability [17].

The smart grid has unique security requirements or objectives [18]. The security objectives have been availability, authentication, confidentiality, nonrepudiation, and integrity.

- *Availability*: This refers to the ability of the smart grid to maintain correct operation even during adverse conditions. This usually gets the highest priority when it comes to power. Access to the smart grid should be available and reliable to all users. Power systems should be available 100% of the time. Attacks targeting availability of service generally leads to Denial of Service (DoS).
- *Authentication*: This usually involves using username and password to validate the identity of the user. Authentication and integrity can help the smart grid protect against common cyber attacks such as impersonation, forgery, and man-in-the-middle.
- *Confidentiality*: Data secrecy is important especially for privacy-sensitive data such as user personal information and meter readings. Confidentiality ensures that information in smart grid is restricted only to authorized people.
- *Nonrepudiation*: This is an assurance of the responsibility to an action. The source should not be able to deny having sent a message, while the destination should not deny having received it. This security objective is essential for accountability and liability.
- *Integrity*: This assures that data, devices, and processes are free from tampering. Data should be free from injection, deletion, or corruption. When integrity is targeted, nonrepudiation is also affected.

Security threats within the smart grid usually attempt to compromise one or more security objectives. As the smart grid depends on computer networks, it is vulnerable to various security and privacy issues. A cyber attacker can penetrate a smart grid using variety of attacks. The physical layer security for smart grid deals unauthorized access, with malicious attacks, privacy issues, and voltage regulation [19]. Figure 3 shows some security threats towards communication networks in the smart grid [20].

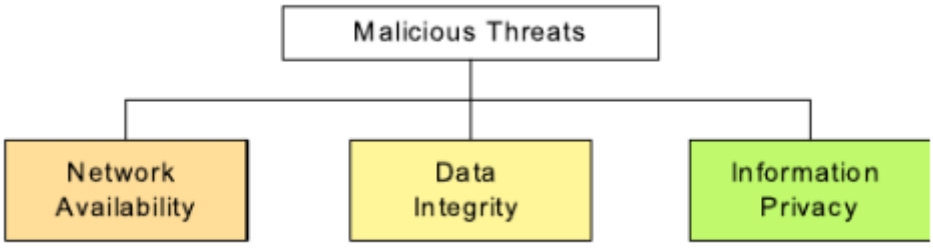

Figure 3: Security threats towards communication networks in the smart grid [20]

- *Unauthorized Access*: This broad threat covers a wide range of issues including access to data, devices, systems, and networks. Access control should include authentication, network access, and device authentication.
- *Malicious Attacks*: Individuals can attack the communication infrastructure and cause damages to the smart grid. Malicious attacks can be classified as eavesdropping, jamming, and injecting [21]. A malicious, unauthorized individual can eavesdrop on the data transmission and access critical information, thereby violating the confidentiality requirements. Jamming blocks the information flow. An injecting attack inserts bad data into the network with the intension of misleading the control center.
- *Privacy Issues*: Any personal information that may be available through the smart grid should be secured. This includes personal name, address, account number, bill history, the IP address of the meter, and service provider. We must strike a balance between security and privacy.

Computer networks do not exist in isolation. The human factor plays a unique role in cyber-defense operations. Average hackers, disgruntled former employees, terrorists, and foreign nations could be responsible for cyber attacks. To curb the flow of malicious attacks, analysts must monitor and protect smart grids [22].

To secure a smart grid, it is important to have several mechanisms in place. These include authentication protocols, cryptographic algorithms, and firewalls [23].

- *Authentication*: This confirms the identity of an entity that tries to access the network.
- *Firewalls*: Network firewalls protect the smart grid assets against malicious cyber attacks.
- *Intrusion detection*: Anomaly detection uses event correlation to identify cyber intrusions. The ability to prevent, detect, and tolerate intrusions is necessary in the smart grid systems.
- *Encryption*: Providing encrypted communications among smart grid devices should be a basic requirement.

Smart Grid Applications

Applications of smart grid technologies can be found every where in the world. Smart grid has worldwide applications, with each nation having slightly different goals in pursuing smart grid technologies.

Electricity uses are evolving: positive energy buildings, electric mobility, variable intensity urban lighting, storage batteries, etc. New uses include renewable energies, electric vehicles, and connected houses.

- *Renewable Energy Sources* (RES): To feed the energy appetite of the world, renewable energy technologies are becoming feasible and offer alternative generation options. Renewable energy sources (RESs) and energy storage systems (ESSs) are the key technologies for smart grid applications. The most rapidly expanding renewable resources are expected to be wind and solar. Smart grid technologies enable high levels of renewables to be included in an electricity system.
- *Plug-In Electric Vehicles* (PEVs): An area with the potential for increased electricity consumption is transportation. A growing number of automobile manufacturers are introducing plug-in EVs, which can

drastically reduce our dependence on oil and emit no air pollutants when running in all-electric modes. The smart grid will have the infrastructure needed to enable the efficient use of this new generation of PEVs. The key factor for acceptance of PEVs in the marketplace will be the availability of charging stations [24].

- *Smart Home:* Smart homes should be regarded as the building blocks of smart cities and intelligent communities. It is becoming a reality in the developed world with energy efficiency and reduction in carbon footprints riding high on the agenda of most the governments and states. The main objectives of a smart home are to improve the quality of life, increase automation, facilitate energy management, and minimize environmental emissions. Smart homes automate electrical devices and control the environment inside [25].

Future Smart Grids

Smart gird is the subject of great public interest as a means to enable a more efficient and renewably powered electricity grid infrastructure. Utility companies are fully aware of the difficulties involved in transitioning their infrastructure towards an uncertain future. Future smart grids will likely to be more tightly integrated with the cyber infrastructure for sensing, control, scheduling, dispatch, and billing. In the future, distributed generation from intermittent sustainable energy sources coupled with rising local demand are expected to present a significant challenge to current electricity grids.

The security and privacy of future smart grid and smart metering networks is important to their eventual acceptance by the public. Smart meter users will need to be reassured that their data is secure. Smart meters and other intelligent energy technologies can improve energy efficiency and possibly reduce power costs.

Visions of smart grids abound for the evolution of the electricity grid. This vision is often presented as a technological solution for greening power systems. Planning and designing of smart grids by designers and engineers bring together various elements to form a vision of the future of electricity consumption. Automated control of consumer electricity loads is a key component of future smart grid [26].

The future of smart grid will be revolutionized by three D's: decentralization, digitalization, and decarbonization. The development of a smart grid is an evolutionary process. Utilities, technology providers, universities, regulatory bodies, and R&D organizations must work together to move the process forward. The US Department of Energy is pushing for more innocvations in smart grid technologies. More research and development is needed to support smart grid deployment throughout the United States. At present, Europe, the United States, Japan and other developed countries have researched the construction of smart grid and advanced metering standard infrastructure. Their ultimate goal will be to completely automate the smart grid, from power generation to distribution.

Benefits and Challenges

The smart grid is an intelligent power grid designed to handle distributed resources using communication technology employing smart meters and control system. Key benefits of smart grid include uninterrupted supply of power, reduced transmission and distribution loss, secure grid, and market based electricity pricing. It holds a great promise for a cleaner, more efficient power; healthier air; and lower greenhouse gas emissions. It promotes clean energy, controls energy consumption pattern, and brings security to the grid. The most valuable promise of smart grid is the reliability and security of the power system. The smart grid offers several benefits to both the power grid and the energy consumers such as: reduction in transmission congestion, reduced blackouts and forced outages, self-diagnosis, self-healing, peak demand shaving, increased system capacity, increased power system security and reduced vulnerability, and ease in managing hybrid and electric vehicles. Some of the benefits of the smart grid are shown in Figure 4 [27].

One challenge utility industry faces is the cost of deploying cybersecurity measures. Although public conversations have increased public awareness of the risks to the smart grid, the thinking of most people has not changed much. The human factor is the weakest link in cybersecurity since several cybersecurity breaches are caused by individuals.

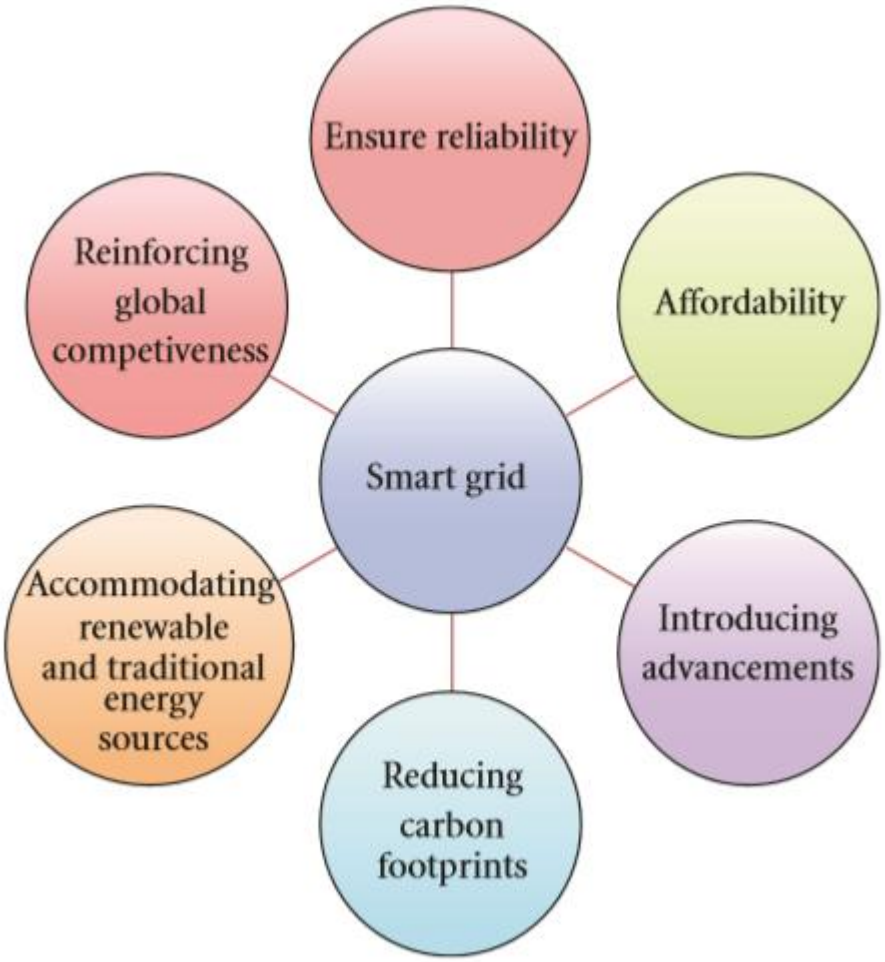

Figure 4: Some of those benefits of the smart grid [27]

Defending against cyber-attacks on SCADA systems is challenging due to the wide range of attack mechanisms, the decentralized nature of the control, deregulation, and the lack of coordination among various entities in the electric grid. Load shaping is one of the important and challenging issues in power grid. With energy storage in place, the consumer can optimize the energy consumption by varying charging and discharging flow depending on the demand and price. This accomplishes optimal load shaping.

Electricity service providers face some challenges in implementing smart meters. Replacing the present meters as well as handling the huge amount of data generated by the meter is challenging. There are no standards of advanced metering system. The assurance of equipment interoperability is essential to smart grid development.

Conclusion

The energy sector (electricity, natural gas, and petroleum) is one of 16 critical infrastructure sectors designated by the Department of Homeland Security. Our modern society depends on critical infrastructure sectors, especially the energy sector. The US power grid has long been considered a logical target for a major cyberattack.

Electricity is a necessity in the modern world. The smart grid is the latest development for the electric power system. It is commonly regarded as a digital upgrade of the existing power system. It is a mechanism for providing bidirectional communication and control between electricity providers and consumers.

The future smart grid should enhance the security and reliability of the power system. The implementation of smart grid will be a long continuous process because it involves technological and financial investment. It also involves international effort. The government of each nation will need to develop a policy for implementing

smart grid. As the smart grid moves in people's living room, the focus will significantly change to marketing to consumers.

The smart grid is no doubt the future of the power system with its flexibility, reliability, efficiency and "smartness" bringing inexplicable possibilities to the power grid. For more information about smart grid, one should consult books in [1, 4, 7, 28-35] and many others available on Amazon.com. One should also consult a related journal: *IEEE Transactions on Smart Grid.*

References

[1]. B. M. Buchholz and Z. Styczynski, *Smart Grids – Fundamentals and Technologies in Electricity Network*s. Heidelburg, Springer-Verlag, 2014, p. 19.

[2]. J. Hastings, D.M. Laverty, and D. J. Morrow, "Securing the smart grid," *Proceedings of Power Engineering Conference* (UPEC), 2014.

[3]. M.N.O. Sadiku et al., "Smart grid — An introduction", *International Journal of Electrical Engineering & Technology* (IJEET), vol. 7, no. 1, pp. 45-49, Feb. 2016.

[4]. F. P. Sioshansi (ed.), *Smart Grid: Integrating Renewable, Distributed, and Efficient Energy*. Oxford, UK: Academic Press, 2012, pp. xxix, xxx, 393.

[5]. Z. Elmrabet et al., "Cyber-security in smart grid: Survey and challenges," https://arxiv.org/ftp/arxiv/papers/1809/1809.02609.pdf

[6]. X. Fang et al, "Smart grid – the new and improved power grid: A survey," *IEEE Communications Survey and Tutorials*, vol. 14, no. 4, Fourth Quarter, 2012, pp. 944-980.

[7]. J. Momoh, *Smart Grid Fundamentals of Design and Analysis.* Hoboken, NJ: John Wiley & Sons, 2012, p. 1, 130.

[8]. M. A. El-Sharkawi, *Electric Energy - An Introduction*. Boca Raton, FL: CRC Press, 3rd edition, 2013.

[9]. T. Jiang, Y. Cao, L. Yu, Z. Wang, "Load shaping strategy based on energy storage and dynamic pricing in smart grid", *IEEE Trans. on Smart Grid*, vol. 5, no. 6, Nov. 2016, pp. 2868-2876.

[10]. E. Y. Dari and M. Essaaidi, "An overview of smart grid cyber-security: State of the art study," *Proceedings of the 3rd International Renewable and Sustainable Energy Conference*, 2015, pp. 1-7.

[11]. M. N. O. Sadiku, Y. Wang, S. Cui, S. M. Musa, "SCADA in power systems," *International Journal of Software & Hardware Research in Engineering*, vol. 6, no. 2, February 2018, pp. 23-27.

[12]. M. N. O. Sadiku, S.M. Musa, A. Omotoso, and A.E. Shadare, "A primer on smart meters," *International Journal of Trend in Research and Development,* vol. 5, no. 4, 2018, pp. 65-67.

[13]. M. N. O. Sadiku, *Elements of Electromagnetics.* New York: Oxford University Press, 7the edition, 2018, pp. 732-737.

[14]. A. E. Shadare, M. N. O. Sadiku, and S.M. Musa, "Electromagnetic compatibility issues in critical smart grid infrastructure," *IEEE Electromagnetic Compatibility Magazine*, vol. 6, Quarter 4, 2017, pp. 63-70.

[15]. A. A. Omotoso, M. N. O. Sadiku, and S. M. Musa, "Effects of electromagnetic interference on smart grid," *Proceedings of the 2019 International Conference on Scientific Computing*, Las Vegas, 2019, pp. 190-192.

[16]. "Electromagnetic compatibility," *Wikipedia*, the free encyclopedia https://en.wikipedia.org/wiki/Electromagnetic_compatibility

[17]. M. N. O. Sadiku, Y. P. Akhare, and S. M. Musa, "Cybersecurity in smart grid," *Journal of Scientific and Engineering Research*, vol. 6, no. 8, 2019, pp. 146-152.

[18]. K. Tazi, F. Abdi, and M. F. Abbou, "Review on cyber-physical security of the smart grid: attacks and defense mechanisms," *Proceedings of the 3rd International Renewable and Sustainable Energy Conference*, 2015, pp. 1-6.

[19]. M. Tembely, M. N. O. Sadiku, and S.M. Musa, "Smart grid cybersecurity," *Journal of Multidisciplinary Engineering Science and Technology*, vol. 3, no. 9, Sept. 2016, pp. 5574-5576.

[20]. Z. Lu et al., "Review and evaluation of security threats on the communication networks in the smart grid," *Proceedings of MILCOM 2010 Military Communications Conference*, October-November, 2010.

[21]. X. Wang et al., "Physical layer security in wireless smart grid," *Security and Communication Networks*, vol. 8, 2015, pp. 2431-2439.
[22]. R. S. Gutzwiller, "The human factors of cyber network defense," *Proceedings of the Human Factors and Engineering Society 59th Annual Meeting*, 2015, pp. 322-326.
[23]. J. Xie, A. Stefanov, and C. C. Liu, "Physical and cyber security in a smart grid environment," *WIREs Energy and Environment*, vol. 5, Sept/Oct, 2016, pp. 519-542.
[24]. K. M. R. Eswa, "Smart grid-future for electrical systems," *International Journal of Electrical and Electronics Research*, vol. 3, no. 2, April-June 2015, pp. 603-612.
[25]. M. N.O. Sadiku, S.M. Musa, and R. Nelatury, "Smart homes," *Journal of Scientific and Engineering Research*, vol. 3, no. 6, 2016, pp. 465-467.
[26]. D. A. Ghanem and S. Mander, "Designing consumer engagement with the smart grids of the future: Bringing active demand technology to everyday life," *Technology Analysis & Strategic Management*, vol. 26, no. 10, 2014, pp. 1163-1175.
[27]. S. Iyer, "Cyber security for smart grid, cryptography, and privacy," *International Journal of Digital Multimedia Broadcasting*, 2011.
[28]. C. C. Liu, S. McArthur, and S. J. Lee (eds.), *Smart Grid Handbook*. John Wiley & Son, 3 volumes, 2016.
[29]. Y. Xiao, *Security and Privacy in Smart Grids.* Boca Raton, FL: CRC Press, 2018.
[30]. A. B. M. S. Ali (ed.), *Smart Grids; Opportunities, Developments, and Trends*. London, UK: Springer-Verlag, 2013.
[31]. L. C. Beard, *Smart Grids for Dummies*. John Wiley & Sons, 2010.
[32]. S. T. Mak, *New Technologies for Smart Grid Operation*. Bristol, UK: IOP Publishing, 2015.
[33]. E. D. Knapp and R. Samani, *Applied Cyber Security and the Smart Grid: Implementing Security Controls into the Modern Power Infrastructure.* Waltham, MA: Elsevier, 2013.
[34]. I. E. Reid and, H. A. Stevens (eds.), *Smart Meters and the Smart Grid: Privacy and Cybersecurity Considerations.* Nova Science Pub., 2012.
[35]. P. Barker and R. F. Price (eds.), *Cybersecurity for the Electric Smart Grid: Elements and Considerations*. Nova, 2012.

About the Authors

Matthew N. O. Sadiku is a professor emeritus in the Department of Electrical and Computer Engineering at Prairie View A&M University, Prairie View, Texas. He is the author of several books and papers. His areas of research interest include computational electromagnetics and computer networks. He is a fellow of IEEE.

Uwakwe C. Chukwu is an associate professor in the Department of Industrial & Electrical Engineering Technology of South Carolina State University. He has published several books and papers. His research interests are power systems, smart grid, V2G, energy scavenging, renewable energies, and microgrids.

Abayomi Ajayi-Majebi is a professor in the Department of Manufacturing Engineering at Central State University in Wilberforce, Ohio. In 2015 he was honored by the White House as a Champion of Change for his significant contributions to the engineering education of minority students. He is a senior member of both the Society of Manufacturing Engineers and the American Society for Quality.

Sarhan M. Musa is a professor in the Department Electrical and Computer Engineering at Prairie View A&M University, Texas. He has been the director of Prairie View Networking Academy, Texas, since 2004. He is an LTD Sprint and Boeing Welliver Fellow. His areas of research interest include computational electromagnetics and computer networks.