Posted on Authorea 22 Sep 2022 — CC-BY 4.0 — https://doi.org/10.22541/au.166385207.71655799/v1 — This a preprint and has not been peer reviewed. Data may be preliminary.

Cyber Security in Smart Grids, Threats, and Possible Solutions

Diptiben Ghelani[1]

[1]Department of Computer Engineering, Gujrat Technological University

September 22, 2022

Abstract

The integration of telecommunications in the energy grid, which is paving the way for Smart Grids, calls into question how the energy sector has historically ensured safe operations. New cyber security concerns exist, particularly in the areas of privacy, connection, and security management, which must be addressed effectively. Existing cyber security technologies and best practices are mostly derived from the old telecommunication context, where safety and availability requirements are less stringent. Lessons on how the oil and gas sector has coped with security concerns in the introduction of integrated operations can be used to Smart Grids. Smart Grids, on the other hand, face a somewhat different reality due to their wide geographic dispersion and large number of end-users. This study makes a contribution by providing an overview of cyber security problems for Smart Grids, as well as a plan for addressing these challenges in the near future. However, because many of the communication technologies now advocated for use by a smart grid are cyber-vulnerable, this might result in inconsistent system operations, resulting in wasteful spending and possibly disaster for both utilities and customers. We review the cyber security needs and potential vulnerabilities in smart grid communications in this study, as well as survey existing cyber security solutions for smart grid communications.

American Journal of Applied Scientific Research
2022; X(X): XX-XX
http://www.sciencepublishinggroup.com/j/ajasr
doi: 10.11648/j.XXXX.2022XXXX.XX
ISSN: 2471-9722 (Print); ISSN: 2471-9730 (Online)

SciencePG
Science Publishing Group

Cyber Security in Smart Grids, Threats, and Possible Solutions

Diptiben Ghelani

Department of Computer Engineering, Gujrat Technological University, Ahmedabad, India

Email address:
Shezi1131@gmail.com

To cite this article:
Diptiben Ghelani. Cyber Security in Smart Grids, Threats, and Possible Solutions. *American Journal of Applied Scientific Research*. Vol. x, No. x, 2022,

Received: May, 10, 2022; **Accepted**: August, 20, 2022; **Published**: September, 10, 2022

Abstract: The integration of telecommunications in the energy grid, which is paving the way for Smart Grids, calls into question how the energy sector has historically ensured safe operations. New cyber security concerns exist, particularly in the areas of privacy, connection, and security management, which must be addressed effectively. Existing cyber security technologies and best practices are mostly derived from the old telecommunication context, where safety and availability requirements are less stringent. Lessons on how the oil and gas sector has coped with security concerns in the introduction of integrated operations can be used to Smart Grids. Smart Grids, on the other hand, face a somewhat different reality due to their wide geographic dispersion and large number of end-users. This study makes a contribution by providing an overview of cyber security problems for Smart Grids, as well as a plan for addressing these challenges in the near future. However, because many of the communication technologies now advocated for use by a smart grid are cyber-vulnerable, this might result in inconsistent system operations, resulting in wasteful spending and possibly disaster for both utilities and customers. We review the cyber security needs and potential vulnerabilities in smart grid communications in this study, as well as survey existing cyber security solutions for smart grid communications.

Keywords: Cyber Security, Smart Grids, Vulnerability, Telecommunication

1. Introduction

The electrical distribution system is being integrated with communication networks to produce a two-directional power and information flow infrastructure known as a smart grid [1]. The integration not only transitions power automation systems from antiquated proprietary technology to new communication technologies, but it also transforms closed power control systems into open data networks. The smart grid infrastructure may be more efficient, robust, and inexpensive to maintain and run by adding major new functionality, distributed intelligence, and state-of-the-art communication capabilities to the electrical grid. However, it not only benefits the power business in terms of performance, but it also poses significant dangers and difficult tasks in terms of securing smart grid systems from cyber security attacks. Given the large scale of a smart grid, it is logical to assume that the smart grid communication system's cumulative vulnerability is likewise vast [1]. Almost everyone agrees that a smart grid cyber security compromise may have massive effects. Demand response, for example, introduces substantial new cyber-attack vectors, like as malware that causes a big coordinated and immediate decline in demand. With the integration of communications networks into the electrical grid, cyber security issues must be addressed. Experts in cyber security must comprehend the grid, as well as the relevance of security solutions that can match the grid's stringent standards for availability, efficiency, and scalability. However, grid creators and operators must be aware of the grid's cyber security consequences [2].

2. Smart Grid Concept

The Smart Grid's concept entails a shift from "a limited number of highly managed devices" to "an Internet-like distributed environment" with a large number of devices. Though Cohen quotes one presenter at an IEEE meeting on the subject as saying, "We know how to safeguard the Internet," few at that meeting – or elsewhere – would agree.

There are several security issues linked with the Internet, yet solutions exist to alleviate or mitigate some of these issues. Cohen mentions the routing infrastructure and general purpose computing as examples of challenges. Legacy cyber security solutions designed for business networks are unlikely to meet the needs of a smart grid communication system operating safely in public data communication networks like the internet. Smart grid communication systems differ from traditional business network systems in terms of goals, objectives, and assumptions about what needs to be secured in cyber security. In a smart grid communication system [3], it is critical to ensure real-time performance and continuous operating features. Those apps were not created with the intention of being used on a corporate network. As a result, current security solutions must be embraced where they fit, such as communication networks inside a control centre and/or a substation, and new solutions must be developed to bridge the gaps where typical corporate network cyber security solutions do not function or apply. Updating a complicated system like the smart grid communication infrastructure has the potential to introduce new security vulnerabilities. The author offered a review of efforts on smart grid cyber security in [4]. Process Control System (PCS) Security, Smart Meter Security, Power System State Estimation Security, Smart Grid Communication Protocol Security, and Smart Grid Simulation for Security Analysis are the five categories that make up distinct components of the smart grid. A smart grid is a vast, complicated system that nevertheless needs extensive cyber security planning. In this part, we go over the history of a smart grid system in terms of SCADA systems, communication networks, and secure smart grid communications installations [5].

3. SCADA

The SCADA system is essential for monitoring and controlling a substation. It assists electric utilities with Distribution Automation (DA) and computerised remote control of Medium Voltage (MV) substations and power grids to improve supply dependability and save operating and maintenance expenses Sectionalizer Switchgears, Ring Main Units, Reclosers, and Capacitor Banks were designed for local use with little remote control in the past. RTUs now provide strong integrated solutions for upgrading remotely placed electric equipment by leveraging SCADA via dependable wireless communication channels. RTUs smoothly link with a wide range of high-performance control centres offered by major manufacturers globally via SCADA in a Distribution Management System (DMS). A high-performance IP Gateway or comparable node is generally used to connect to these Enterprise Management Systems (EMS) and DA/DMS control centres [6].

4. Networks of Communication

Electric utilities' operational and commercial demands necessitate a high-performance data communication network that can handle both current and future operating requirements. The heart of electric system automation applications is a communication network like this. It is critical to create a cost-effective and dependable network architecture. The benefits and drawbacks of a hybrid network architecture for electric system automation are described in [7]. Virtual Private Networks (VPNs) based on the internet, power line communications, satellite communications, and wireless communications (wireless sensor networks, WiMAX, and wireless mesh networks) are all covered. It gives a quick overview of the hybrid network architecture that may satisfy the requirements of diverse electric system automation applications. A smart grid communication network is being developed as a structured framework for electric utilities to use modern communication technologies for automation, making the decision-making process more efficient and direct [8].

Different communication networking technologies are used depending on the size and structure of smart grid systems. AMI systems can be meshed or point-to-point, with short local coverage or long-range communications [13], [14]. Fiber, wireless broadband, or broadband via power lines are all possibilities for backhaul options. Depending on the utility's intended dependability, speed, and coverage, WiMax, WLAN, WSN, cellular, and LMR are all viable options. Wireless communication systems might be licenced or unlicensed, depending on the utility's requirements. Licensed should be picked for maximum dependability. Each of the above approaches has its own set of benefits and drawbacks, but one thing that all of them have in common is the necessity for a scalable security solution [9].

5. Deployments

Smart grid implementations must adhere to strict security standards. All users and devices that may have an impact on the grid's operation will require strong authentication. Scalable key and trust management solutions, adapted to the unique needs of the Energy Service Provider, will be critical given the enormous number of customers and devices involved. Years of developing and maintaining massive secure network communication systems have taught us that:

Provisioning symmetric keys into thousands of devices can be prohibitively costly and unsafe. Large networks will necessitate the creation of key and trust management systems; these methods can be borrowed from other industries, such as land mobile radio systems and Association of Public-Safety Communications Officials (APCO) radio systems. With tens of thousands of secure devices, several APCO deployed systems provide state-wide wireless coverage. Trust management solutions based on public key infrastructure (PKI) technology might be tailored expressly for smart grid operators, alleviating the burden of providing security that complies to well-known security standards and guidelines. Over 1000 PMUs are scheduled to be implemented in three years [10]. Many more will be put in distribution networks to cope with the inconsistent electricity generated by rooftop solar and electric cars. PMUs will also start to show up at the terminals of generating equipment, transformers, and huge motors. They'll be installed in both business and residential buildings. One of the main reasons for redundancy in smart grid PMU systems is to satisfy the needs of being able to make software security fixes without losing data. These software fixes must be applied without causing data loss. The usefulness of PMUs for real-time grid operations may be shown in the energy company's experience during the Hurricane Gustav power island event [11].

6. Requirements

The control and communication systems are critical to the dependability of a smart grid. Communication technologies are getting increasingly sophisticated as smart grids evolve, allowing for increased control and dependability. To enable the additional functionalities, the smart grid will require increased levels of network connectivity. Meanwhile, increasing levels of connection should be accompanied by more advanced security mechanisms to address cyber security flaws and breaches. Several security protocols used by various tiers in communication networks to meet specific security needs; further information is available in [18]. In this section, we go over the high-level security requirements in general, as well as the major security requirements and vulnerabilities for smart grid communications in terms of privacy, availability, integrity, authentication, authorization, auditability, nonrepudiability, third-party protection, and trust [12].

6.1. Security Requirements at a High Level

One of the most significant obstacles confronting smart grid adoption, according to the Electric Power Research Institute (EPRI), is system cyber security. According to the EPRI Report, cyber security is a key concern since the threat of cyber attacks and events against this important sector is rising as it becomes increasingly linked. Not just planned assaults from disgruntled workers, industrial espionage, or terrorists, but also incidental breaches of the information infrastructure caused by user mistakes, equipment failures, and natural calamities must be addressed. Vulnerabilities might allow an attacker to get into a network, acquire access to control software, and change load conditions, causing the grid to become unstable in unanticipated ways. Various organisations are conducting high-level requirements for smart grid communication security, as well as the relevant standards. Many organisations are working on smart grid security requirements, including the North American Electrical Reliability Corporation-Critical Infrastructure Protection (NERC-CIP), International Society of Automation (ISA), IEEE 1402, National Infrastructure Protection Plan (NIPP), and the National Institute of Standards and Technology (NIST), [13] which is currently working on a number of smart grid cyber security programmes [10].

The Smart Grid Interoperability Panel (SGiP) Cyber Security Working Group, formerly the NIST Cyber Security Coordination Task Group (CSCTG), is one significant source of requirements. The NIST CSCTG was created to guarantee that cyber security standards are consistent across all smart grid domains and components. At the time of writing, the newest draught paper from the Cyber Security Working Group, NIST Interagency Report (NIST-IR7628), entitled Smart Grid Cyber Security Strategy and Requirements, is still in the works. Home-to-Grid (H2G), Building-to-Grid (B2G), Industrial-to-Grid (I2G), Transmission and Distribution (T&D), and Business and Policy Domain Expert Working Groups (DEWGs) have been created by NIST and the Department of Energy GridWise Architecture Council (GWAC) [14].

6.2. The Meeting of Two Traditions: Process Control vs. Telecommunication Networks

Both electricity distribution and communications networks are inherent components of vital infrastructure, and both are large-scale complex systems with the user's complexity disguised. Both have historically operated on a pay-per-use basis, and while certain flat-rate (e.g. per-month) telephony services exist, Cloud Computing is reviving the metered use paradigm for general computing. Both are built to be dependable and are based on a vast set of criteria. These networks, on the other hand, were plainly designed for very distinct reasons, with very different baseline needs, and they are used and propagated in very different ways. Hardware failures are the most common cause of events in electric power transmission, and a lack of monitoring can make pinpointing the specific location of the breakdown difficult. Electric power is commonly thought of as a unidirectional, homogenous service delivered from a central source, with capacity expansion being costly and time-consuming due to the construction of additional power plants and the stringing of high-voltage distribution lines. Incidents in communications networks are more frequently caused by software faults, either directly or indirectly, and complexity. It's tough to prevent and identify such errors [15]. The telecom sector is competitive, with multiple carriers providing services that are almost identical. This also means that the supply is spread, and the service is heterogeneous in the sense that many commodities are available through the same channel. Furthermore, because users consume and create data, telecom networks are bidirectional. Telecommunications service scaling may be rapid and inexpensive, as it frequently entails actions like replacing a server in a datacenter [3].

6.4. Security vs. Safety

The potential of a system to impact its surroundings in an unfavourable way is commonly referred to as safety, and the primary goal of safety mechanisms is to safeguard life, health, and the environment from harm. On the other side, security may be defined as the inability of the environment to adversely impact the system [4]. A security breach can result in a system functioning in a dangerous manner, and hence a security breach might result in a safety breach. The two properties, safety and security, are inextricably linked and must be addressed separately. The electricity grid has always been more concerned with safety than security. With the emergence of Smart Grids, which rely heavily on communications networks, security concerns must be addressed [16].

While telecom aspires for integrity, secrecy, and availability in that order, power grid and process control in general are concerned first and foremost with human safety, followed by continuous operation and protection of physical components. While telecom has a central server in the centre of the network with the greatest security level, the power grid must safeguard all edge nodes just as effectively as the central control systems. Technological foundation; compared to the amount of proprietary systems and technologies used in process control, the range of systems utilized in telecom is quite restricted. Rebooting is a popular means of correcting a problematic office computer; however it is not acceptable in the power grid since it causes an interruption in operation, which usually has significant cost effects [17].

6.5. Integrated Operations

Smart Grids are to the energy sector what Integrated Operations (IO) was to the oil and gas industry. IO meant switching from proprietary stand-alone systems in closed/physically isolated networks to standardised commercial-off-the-shelf (COTS) technologies integrated into communication networks. This move allows for remote control and assistance, as well as time and money savings, because only a few people can simultaneously monitor a big number of installations. Though this effect is beneficial to the power industry, it also leads to increased networking between supervisory control and data acquisition (SCADA) systems and general ICT infrastructure, resulting in a collision of two worlds in terms of requirements, vulnerabilities, threats, and appropriate countermeasures [18]. Offline proprietary systems have an almost nil attack surface since an attacker would have to be in the same geographical location as the target system and have comprehensive technical knowledge of the system in order to cause harm. COTS systems that are accessible from anywhere are vulnerable to a distinct set of attackers and dangers. And, while extensive technical expertise is still necessary, there are significantly more experts in COTS systems than there are in proprietary systems throughout the world. A wide community is also aware of current COTS system vulnerabilities and attack methods [19].

7. Stuxnet

The most well-known incident occurred in July 2010, when a new and complex piece of malware targeting industrial control systems was discovered. Stuxnet's purpose was to reprogramme certain industrial control systems and conceal any alterations. Despite the fact that the virus was discovered in July 2010, it was proved to have existed for at least a year before that. Stuxnet was designed to infect workstations in five firms, all of which had a presence in Iran. While the majority of infections were discovered in Iran, Stuxnet's capacity to self-replicate allowed it to infect devices outside of the target organisations. According to Symantec's investigations, there were roughly 100 000 compromised hosts on September 29th, 2010. They also discovered 40 000 distinct external IP addresses from over 155 countries, with Iran accounting for almost 60% of them [20].

7.1. Hackers Trigger a Power Outage

Hackers caused a power outage by hacking into computer systems, according to Computerworld. The outage occurred in January 2008, and it affected multiple cities in unidentified locations, with the goal appearing to be extortion. The advantages and hazards of disclosing the assault were carefully examined, and no more information was shared. The notorious Slammer virus infiltrated a computer network at a nuclear power facility in Ohio, United States, in 2003, and crippled a safety monitoring system for about five hours [18]. Because the plant was turned off, the infection did not do any damage. However, the compromised network was thought to be secured by a firewall, which was not the case. This incident served as a cautionary tale about what an outsider may do when attacking a process control system. A Californian offshore contractor employee was accused in August 2009 with hacking into a communications network that detected oil spills. He was unable to secure full-time employment and desired to retaliate against his former employer. Fortunately, his activities did not result in a leak, but he did inflict thousands of dollars in damage. The essay emphasises that safety systems, like any other computer system, have weaknesses, and that causing those safety systems to fail can result in disastrous consequences [21].

7.2. Features of Smart Grid

The smart grid is projected to increase grid resilience while also enhancing environmental performance. Resilience refers to an entity's capacity to withstand and recover rapidly from unforeseen occurrences [1]. Grid resilience has become a non-negotiable component in today's world, especially when power outages threaten the economy. By permitting extra distributed power supply, simplifying the integration of new resources into the grid, and offering remedial capabilities when breakdowns arise, the smart grid promises to bring flexibility and dependability. Furthermore, smart grid technologies are intended to enable electric cars to replace conventional vehicles, lowering customer energy consumption and grid energy losses [22].

7.3. The Notion of a Smart Grid

A smart grid, according to the National Institute of Standards and Technology (NIST) [2, is made up of seven logical domains that comprise both actors and applications: bulk generating, transmission, distribution, customer, markets, service provider, and operations. Applications are tasks done by one or more actors in each domain. Actors are programmes, devices, and systems. Figure 1 depicts the smart grid conceptual model and the interaction of actors from many domains over a secure channel. The end user is the primary actor in the customer domain. Customers are divided into three categories: residential, commercial/building, and industrial. These actors have the ability to create, store, and manage energy in addition to consuming it. This domain connects with the distribution, operation, service provider, and market domains and is electrically linked to the distribution domain [23].

Actors in the market sector are power market operators and participants. This domain keeps the supply and demand of electricity in check. The market domain interfaces with energy supply domains such as the bulk generating domain and distributed energy resources (DER) in order to match output with demand. Organizations that provide services to both electrical customers and utilities fall under the service provider domain. Billing, client accounts, and energy usage are all managed by these firms. The service provider interfaces with the operation domain for situational awareness and system control, as well as with the customer and market domains to offer smart services such allowing customers to interact with the market and generate energy at home. The managers of electricity transport are the actors in the operations domain. This area ensures that transmission and distribution activities are efficient and effective. Energy management systems (EMS) are used in transmission, whereas distribution management systems (DMS) are used in distribution. The transmission domain transports produced electrical power from the generating domain to the distribution domain across considerable distances via several substations. This domain may also be used to store and create energy [24].

8. Systems for Smart Grids

Advanced metering infrastructure (AMI), automated substation, demand response, supervisory control and data acquisition (SCADA), electrical vehicle (EV), and residential energy management are some of the dispersed and heterogeneous applications that make up the smart grid (HEM). We'll talk about three key and susceptible smart grid applications in this section: AMI, SCADA, and automation substation goes into the various uses in depth. Advanced metering infrastructure (AMI) is responsible for collecting, measuring, and evaluating energy, water, and gas use in both the consumer and distribution domains. It allows the user to communicate with the utility in both directions. The smart metre, the AMI headend, and the communication network are the three components [25]. Smart metres are digital metres with microprocessors and local memory that are used to monitor and collect power use from household appliances as well as transfer data in real time to the AMI headend on the utility side. An AMI headend is a metre data management system that is part of an AMI server (MDMS). Several communication protocols, such as Z-wave and Zigbee, describe communication between smart metres, household appliances, and the AMI headend [25].

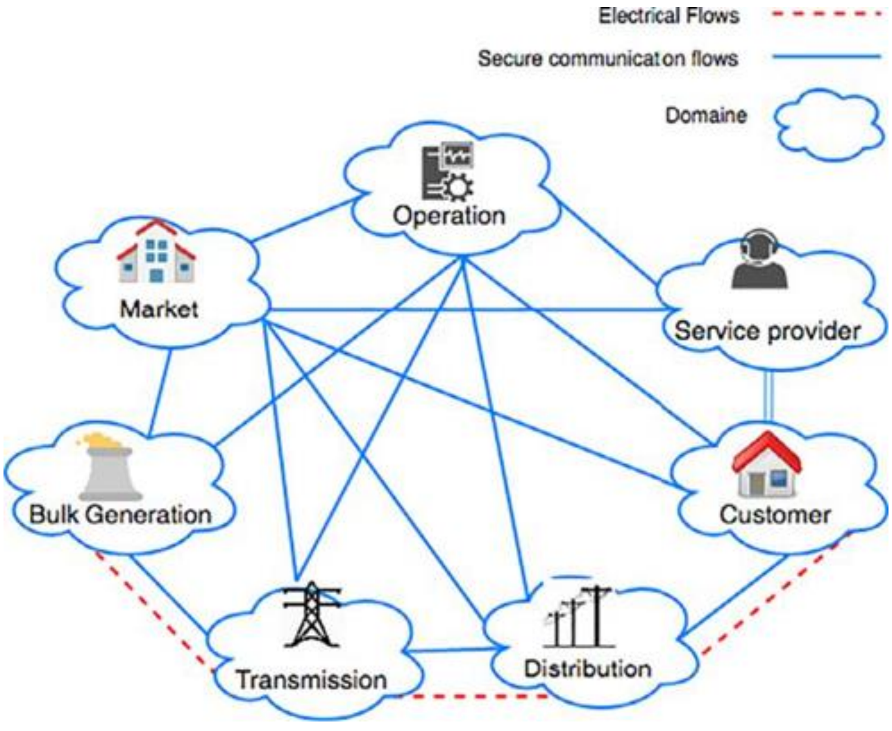

Figure 1. *NIST [2]-based smart grid conceptual model.*

8.1. Privacy

When derived client consumption data is produced in metering devices, privacy concerns must be addressed. Consumption data is a type of data that may be utilised to get insight into a customer's activity [26]. Customer privacy is harmed as a result of smart grid communications. Electricity use data, which is kept at the smart metre and then distributed, operates as an information-rich side channel, revealing consumers' patterns and actions. Power consumption fingerprints can be detected in certain activities, such as watching television. History has proven that when financial or political incentives align, behavioural data mining techniques evolve swiftly to reflect the interests of those who would profit from it. Utility corporations aren't the only ones that could violate your privacy. For example, the recently introduced Google PowerMeter service [34] collects real-time use data from deployed smart metres. Customers who sign up for the service get a personalised web page that shows local use [27].

8.3. Availability

Unauthorized individuals or systems cannot refuse authorised users access or usage because of availability. All IT aspects of the plant, including as control systems, safety systems, operator workstations, engineering workstations, production execution systems, and communication systems between these elements and the outside world, are included in smart grid systems. Denial-of-service (DoS) attacks are malicious assaults that aim to delay, obstruct, or even alter information transmission in order to make network resources inaccessible to communication nodes in the smart grid that require information exchange. Because IP-based protocols are generally expected to be used in at least part of the smart grid (e.g., IEC 61580 has already embraced TCP/IP as a component of its protocol stacks), and TCP/IP is prone to DoS attacks. In terms of attack types, prevention, and response, DoS assaults against TCP/IP have been widely explored in the literature [28].

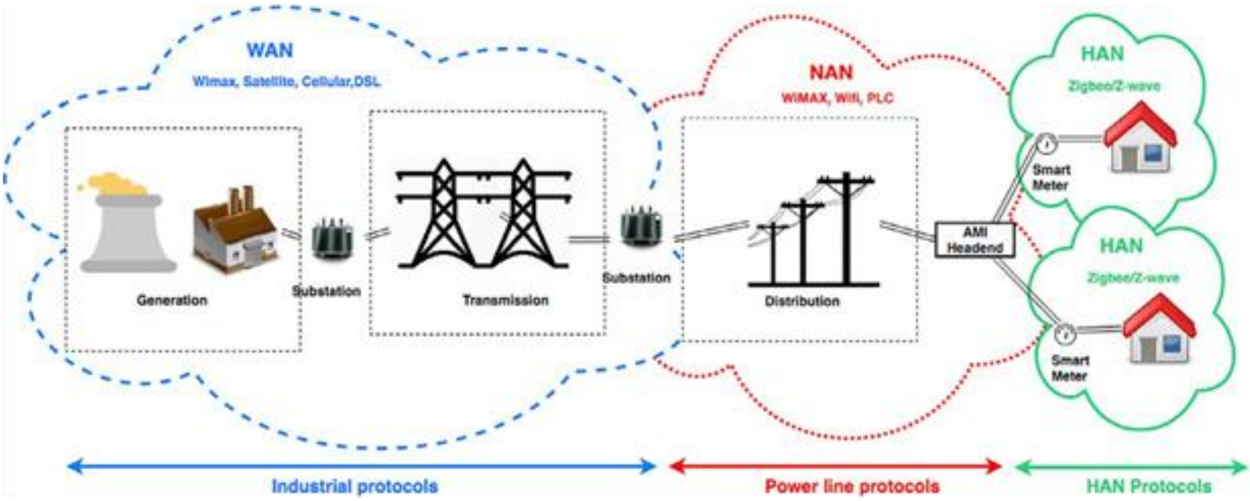

Figure 2. *The smart grid architecture is depicted in this diagram.*

The substation is an important part of the electrical grid. It's in the areas of generation, transmission, and dissemination. Receiving electricity from a producing plant, managing distribution, and limiting power surges are all roles it fulfils. It includes gadgets like a remote terminal unit (RTU), global positioning system (GPS), human-machine interface (HMI), and sophisticated electronic devices that control and distribute electrical energy (IEDs). For power system control, the substation delivers operating data to the SCADA. Many processes within the substation are automated in order to improve power system dependability. The IEC 61850 standard defines the communication between the automation substation and other transmission and distribution equipment [29].

8.2. Challenges

The smart grid is a collection of legacy systems, new technologies, and architectural approaches, all based on different standards and laws, that must be combined into a communication network to meet the problems of the future power grid. To help achieve this goal, the cyber security architecture for smart grid communications is being offered based on cyber security and architectural needs, legacy installation dependencies, and legislation and industry standards [30]. This section gives an overview of the roles and systems that will be classified in a future smart grid communication network [31]. It also includes techniques for creating security controls, allowing for the future development of a compliance procedure for smart grid communications' trustworthy connectivity. Internetworking, security policy and operations, security services, efficiency, and Internetworking are among the major challenges in developing and operating a secure smart grid communication system [32]. Because many applications and devices lack built-in security, the interconnected smart grid communication systems are riddled with vulnerabilities that vary across networks. This cannot be the model for a critical network like the smart grid. To minimise threats from interruption, interception, modification, and fabrication, smart grid cyber security defence layers should be built into the solution [33]. Keeping the network private, that is, where all transportation facilities are wholly owned by a utility, would greatly reduce the threat of intruders because there would be no way for intruders to access the network over the Internet. However, in today's highly connected world, having a completely separate network is not feasible. Reusing communication facilities, such as the Internet, makes good business sense [34]. A poorly secured smart grid connected to the Internet, as is common with commercial networks, exposes the grid to a variety of threats. Cyber-attacks from hostile groups attempting to disrupt the power supply are examples [35].

8.4. Services of Security

Developing, deploying, and integrating a secure smart grid solution will be just as important as managing and maintaining one. Security services will assist smart grid network operators in identifying, controlling, and managing security risks. Every aspect of a smart grid must be secure, according to EPRI. Without policies, ongoing risk assessment, and training, cyber security technologies will not be enough to ensure secure operations. It takes time to develop these human-centered procedures, and it takes time to ensure that they are done correctly. Smart grids require low-cost, high-performance security services, as well as mobility, security, and system integration expertise. These security services can be tailored to the needs of each utility to help them achieve their organisational goals [31].

9. Conclusion

Cyber-security is a fundamental and essential concern for IoT-based smart grid applications. Smart grid security challenges include data gathering and control devices such as PLCs, smart metres, IEDs, RTUs, and PMUs. Firewalls, attack scenarios, countermeasures, encryption, intrusion analysis, forensic analysis, and routers are among the network security problems. Cyber-attacks are classified to take into consideration crucial aspects of information security, allowing for a well-organized and practical approach to providing practical solutions for present and future assaults in smart grid applications. Furthermore, due to the features of smart grid applications, customised solutions for their unique needs must be developed. We may infer that practically all areas of IT technology in smart grid applications have potential vulnerabilities because of security threats in the general IT backdrop. As a result, cyber-security challenges in smart grid applications are being investigated further in order to protect against cyber-attacks and vulnerabilities. Researchers may learn more about smart grid cyber-security aims, needs, and future research trends in the publication. We also provide a brief overview of cyber-security concerns and defence options for smart grid applications. Furthermore, we evaluate current security studies on the smart grid and first describe the smart grid's background before discussing its benefits, features, and essential components. We next go through potential cyber-threat solutions for smart grid applications. Following that, we look at the future developments in smart grid security. The survey paper makes significant contributions by presenting particular solutions to vulnerabilities in IoT-based smart grid applications and highlighting potential research possibilities for scholars to propose future research directions.

References

[1] Faquir, D., et al., *Cybersecurity in smart grids, challenges and solutions.* AIMS Electronics and Electrical Engineering, 2021. 5 (1): p. 24-37.

[2] Kotut, L. and L. A. Wahsheh. *Survey of cyber security challenges and solutions in smart grids*. in *2016 cybersecurity symposium (CYBERSEC)*. 2016. IEEE.

[3] Line, M. B., I. A. Tøndel, and M. G. Jaatun. *Cyber security challenges in Smart Grids*. in *2011 2nd IEEE PES international conference and exhibition on innovative smart grid technologies*. 2011. IEEE.

[4] Liu, J., et al., *Cyber security and privacy issues in smart grids.* IEEE Communications Surveys & Tutorials, 2012. 14 (4): p. 981-997.

[5] Chen, T. M. *Survey of cyber security issues in smart grids*. in *Cyber Security, Situation Management, and Impact Assessment II; and Visual Analytics for Homeland Defense and Security II*. 2010. International Society for Optics and Photonics.

[6] Sayed, K. and H. A. Gabbar, *SCADA and smart energy grid control automation*, in *Smart energy grid engineering*. 2017, Elsevier. p. 481-514.

[7] Subramani, R. and C. Vijayalakshmi, *Global Journal of Engineering Science and Research Management.*

[8] Sayed, K., A. G. Abo-Khalil, and A. M. Eltamaly, *Wind Power Plants Control Systems Based on SCADA System*, in *Control and Operation of Grid-Connected Wind Energy Systems*. 2021, Springer. p. 109-151.

[9] Yadav, S. A., et al. *A review of possibilities and solutions of cyber attacks in smart grids*. in *2016 International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH)*. 2016. IEEE.

[10] Metke, A. R. and R. L. Ekl. *Smart grid security technology*. in *2010 Innovative Smart Grid Technologies (ISGT)*. 2010. IEEE.

[11] Yan, Y., et al., *A survey on cyber security for smart grid communications.* IEEE Communications Surveys & Tutorials, 2012. 14 (4): p. 998-1010.

[12] Burroughs, J. E., *Three Factors Leading to Failed Communications in Emergency Situations*. 2017, Walden

University.

[13] Brooks, C., *Critical Infrastructure Protection at the Local Level.* The Cyber Defense Review, 2019: p. 45-64.

[14] Barron, D. M., J. Hickey, and D. Bart, *Communications: Critical Infrastructure and Key Resources Sector-Specific Plan as Input to the National Infrastructure Protection Plan*. 2007, DEPARTMENT OF HOMELAND SECURITY WASHINGTON DC.

[15] De La Ree, J., et al., *Catastrophic failures in power systems: causes, analyses, and countermeasures.* Proceedings of the IEEE, 2005. 93 (5): p. 956-964.

[16] Birman, K., R. Van Renesse, and W. Vogels. *Adding high availability and autonomic behavior to web services*. in *Proceedings. 26th International Conference on Software Engineering*. 2004. IEEE.

[17] Josyula, V., M. Orr, and G. Page, *Cloud computing: Automating the virtualized data center*. 2011: Cisco Press.

[18] Padhy, R. P., M. R. Patra, and S. C. Satapathy, *Cloud computing: security issues and research challenges.* International Journal of Computer Science and Information Technology & Security (IJCSITS), 2011. 1 (2): p. 136-146.

[19] Mather, T., S. Kumaraswamy, and S. Latif, *Cloud security and privacy: an enterprise perspective on risks and compliance*. 2009: "O'Reilly Media, Inc.".

[20] Falliere, N., L. O. Murchu, and E. Chien, *W32. stuxnet dossier.* White paper, symantec corp., security response, 2011. 5 (6): p. 29.

[21] Lever, C., et al. *A lustrum of malware network communication: Evolution and insights*. in *2017 IEEE Symposium on Security and Privacy (SP)*. 2017. IEEE.

[22] Paul, S., et al. *A review of smart technology (Smart Grid) and its features*. in *2014 1st International Conference on Non Conventional Energy (ICONCE 2014)*. 2014. IEEE.

[23] Mahmood, A., M. Aamir, and M. I. Anis. *Design and implementation of AMR smart grid system*. in *2008 IEEE Canada Electric Power Conference*. 2008. IEEE.

[24] Becker, S., et al., *Features of a fully renewable US electricity system: Optimized mixes of wind and solar PV and transmission grid extensions.* Energy, 2014. 72: p. 443-458.

[25] Dai, Y., et al., *An improved framework for power grid vulnerability analysis considering critical system features.* Physica A: Statistical Mechanics and its Applications, 2014. 395: p. 405-415.

[26] Ghelani, D., *Conceptual Framework of Web 3.0 and Impact on Marketing, Artificial Intelligence, and Blockchain.*

[27] Ghelani, D. and T. K. Hua, *A Perspective Review on Online Food Shop Management System and Impacts on Business.*

[28] Featherston, S., *Empty categories in sentence processing*. Vol. 43. 2001: John Benjamins Publishing.

[29] Roostaee, S., R. Hooshmand, and M. Ataei. *Substation automation system using IEC 61850.* in *2011 5th International Power Engineering and Optimization Conference*. 2011. IEEE.

[30] Humayun, M., et al., *Cyber security threats and vulnerabilities: a systematic mapping study.* Arabian Journal for Science and Engineering, 2020. 45 (4): p. 3171-3189.

[31] Oak, R., Du, M., Yan, D., Takawale, H., & Amit, I. (2019, November). Malware detection on highly imbalanced data through sequence modeling. In Proceedings of the 12th ACM Workshop on artificial intelligence and security (pp. 37-48).

[32] Hua, T. K., & Biruk, V. (2021). Cybersecurity as a Fishing Game: Developing Cybersecurity in the Form of Fishing Game and What Top Management Should Understand. Partridge Publishing Singapore.

[33] Ughulu, D. (2022). The role of Artificial intelligence (AI) in Starting, automating and scaling businesses for Entrepreneurs. *ScienceOpen Preprints*.

[34] Ughulu, J. Entrepreneurship as a Major Driver of Wealth Creation.

[35] Ghelani, D., & Hua, T. K. (2022). Conceptual Framework of Web 3.0 and Impact on Marketing, Artificial Intelligence, and Blockchain. *International Journal of Information and Communication Sciences*, *7*(1), 10.

[36] Ghelani, D., & Hua, T. K. A Perspective Review on Online Food Shop Management System and Impacts on Business.

[37] Ghelani, D., Hua, T. K., & Koduru, S. K. R. (2022). A Model-Driven Approach for Online Banking Application Using AngularJS Framework. *American Journal of Information Science and Technology*, *6*(3), 52-63.

[38] Dr. John Ughulu. The role of Artificial intelligence (AI) in Starting, automating and scaling businesses for Entrepreneurs.. *ScienceOpen Preprints.* DOI: 10.14293/S2199-1006.1.SOR-.PP5ZKWJ.v1

[39] Gao, Y., et al. *Analysis of security threats and vulnerability for cyber-physical systems*. in *Proceedings of 2013 3rd International Conference on Computer Science and Network Technology*. 2013. IEEE.