Networking for Power Grid and Smart Grid Communications: Structures, Security Issues, and Features

Biswash Basnet[1], Varsha Sen[2]

Lane Department of Computer Science and Electrical Engineering, West Virginia University, Morgantown, USA

E-mail: [1]bb00126@mix.wvu.edu, [2]vs00039@mix.wvu.edu

Abstract

The evolution from traditional to smart grid systems has radically changed communication architectures. It enables secure, efficient, and resilient energy infrastructures. Unlike the centralized, unidirectional communication practices typical of traditional grids with minimal automation, modern smart grids use tiered, bidirectional networks allowing real-time control, integration of distributed energy resources (DER), and active consumer participation. The drive for this development arises from the growing use of renewable energy resources, electric vehicles, and sophisticated digital metering technologies. End-to-end communication architectures now underpin grid reliability, interoperability, and cybersecurity. This research explores the end-to-end architecture of traditional and smart grids, including access technologies, protocol layers (e.g., IEC 61850, Modbus, DNP3), and hierarchical network domains such as the Home Area Network (HAN), Neighbourhood Area Network (NAN), and Wide Area Network (WAN). Physical transmission mediums, key cybersecurity challenges, and standards like IEC 60870 are also discussed. Case studies of real implementations, emerging protocols, and security issues are analyzed to clarify directions toward intelligent, scalable, and self-healing grid communication infrastructures.

Keywords: Protocols, Cybersecurity, Grid Resilience, Interoperability, Automation, AMI, PMU, SCADA, DNP3.

DOI: https://doi.org/10.36548/rrrj.2025.1.008
Received: 15.04.2025, received in revised form: 17.05.2025, accepted: 05.06.2025, published: 17.06.2025

1. Introduction

Advances in digital communication and the growing need for sustainability, dependability, and real-time operational control are driving a major transformation in the electric power sector. Centralized generation, radial distribution, and limited system feedback are characteristics of traditional power grids, which were first developed in the early 20th century and operate on a hierarchical, top-down model. These systems have mostly relied on supervisory systems like Remote Terminal Units (RTUs) and SCADA (Supervisory Control and Data Acquisition), which use analog or serial digital technologies, for unidirectional communication [1]. Although centralized monitoring and control have been made possible by communication technologies created for conventional power systems, these technologies' scalability, responsiveness, and reliability are limited in the face of the continuous change brought about by the growing integration of distributed energy resources (DERs), electric vehicles, renewable energy, and homeowners [2]. A paradigm shifts towards a two-way, cyber-physical system that relies on reliable communication protocols, a variety of access networks, and real-time monitoring, control, and automation is marked by the rise of the smart grid, along with sophisticated control and protection systems, stability mechanisms, and resilience strategies [3]. Proactive fault detection, adaptive load balancing and control, and the safe integration of DERs, electric vehicles, and active prosumers within a dynamic energy ecosystem are all made possible by this evolution [4].

Network communication, which includes both wired (e.g., fiber optics, Ethernet/IP, leased lines, HomePlug, M-Bus, Power Line Communication [PLC]) and wireless (e.g., ZigBee [IEEE 802.15.4], Wi-Fi [IEEE 802.11], WiMAX, 4G/5G cellular, satellite) technologies that facilitate low-latency, secure, and scalable data exchange across generation, transmission, distribution, and consumer endpoints, is at the heart of this development [5]. Application-specific criteria like coverage, latency tolerances, bandwidth requirements, and environmental factors influence the choice of these communication modes. Wireless systems offer flexible and scalable deployment options that are perfect for distributed automation, smart metering, and remote monitoring, while wired systems are ideal for substations and backbone control due to their high reliability and immunity to electromagnetic interference.

Furthermore, layered communication protocols like TCP/IP and the OSI model, along with circuit switching and packet switching technologies, are necessary to achieve dependable and efficient grid operations. To improve interoperability and secure heterogeneous systems,

numerous standards and frameworks are being developed or improved, such as IEEE 802.15.4 (ZigBee) for low-power wireless communication, NERC CIP for grid cybersecurity, and IEC 61850 for substation automation [6]. The communication infrastructures supporting both conventional and contemporary smart grids are thoroughly examined in this paper. By contrasting intelligent and legacy architectures and categorizing communication protocols across hierarchical network layers, it investigates the development of networking technologies and their impact on grid modernization. A thorough analysis is conducted of key performance metrics, such as latency, bandwidth, scalability, and interoperability. Furthermore, the analysis assesses the application of critical cybersecurity frameworks and standards (such as IEEE 802.15.4, NERC CIP, and IEC 61850) in relation to their significance in guaranteeing timely, safe, and interoperable grid operations. By combining these components, this paper emphasizes how important communication systems are as a basis for demand-side management, fault location, distributed energy integration, and cyber-physical resilience.

2. Communication in Power Grids

2.1 Requirements for Power Grid Communications

The future grid demands a communication infrastructure that not only allows for real-time monitoring and control but also adaptation toward to the growing complexity from DERs, integration of renewables, and coordination between the physical and cyber realms. The key features of the resulting communication infrastructure are as follows [8].

1. **Bandwidth:** The network should support high-resolution, high-frequency data from PMUs, smart meters, DERs, and edge devices. Bandwidth will dynamically adjust in all three layers, i.e., the FAN, HAN, and WAN, to accommodate mission-critical applications such as SCADA, AMI, and underfrequency load shedding (UFLS).
2. **Latency:** The safeguard mechanisms require ultra-low and deterministic latency, under which the actions of the controls need to be implemented within a timescale of a millisecond. Differentiated Quality-of-Service (QoS) is also important in supporting applications with different degrees of delay tolerances, ranging from real-time fault isolation to periodical metering.
3. **Security:** There will be multi-layered security, including encryption, authentication, anomaly detection, and access controls utilized in end-to-end communication. These measures will protect against false data injection, tampering, and exfiltration of data through wired and wireless media.

4. **Scalability:** The design needs to support thousands of new devices, including IoT sensors and DER controllers, without affecting performance. Edge computing and distributed intelligence reduce latency and data congestion and allow for local control.
5. **Interoperability:** The implementation of open standards such as DNP3, IEC 61850, and Modbus provides compatibility with legacy systems and new systems. Hybrid architectures need to be capable of supporting both routable and non-routable protocols to provide flexibility in IP and serial network installations.

Real-time automation is constrained by these technical specifications. For instance, PMUs produce 30–60 messages in a single second, taking 10–50 milliseconds to respond, more than traditional systems can accommodate. In the lack of secure, low-latency, and interoperable infrastructure, grid resilience and automation remain vulnerable.

2.2 Traditional Power Grid

Conventional grids, developed in the 19th and 20th centuries, were designed for unidirectional power flow from central generation to consumers. The infrastructure for communication, being primitive, utilized low-speed digital or analog technologies for minimal controls and monitoring [8]. At the generation level, utilities utilized analog telephone lines, leased circuits, and microwave radio for telemetry and voice dispatch, with minimal bandwidth and flexibility for new automation, SCADA systems, developed in the latter portion of the 20th century, utilized remote terminal units (RTUs) and programmable logic controllers (PLCs) linked through RS-232 or RS-485 serial links [9]. These systems operated on poll-response models using Modbus, DNP3, and IEC 60870-5-101-based protocols, with rudimentary extraction of data and controls on serial or analog channels [10]. In transmission, Power Line Carrier Communication (PLCC) reigned in the transmission of protection signals on the transmission lines, saving infrastructure costs and ensuring timely coordination of substation states [11]. Although they are not IP-based and do not conform to layered structures, they carry essential telemetries of voltage, breaker status, and frequency, and are reported reliably. DNP3, developed in the 1990s, supported noisy, low-bandwidth environments and supplied timestamped event reporting, unsolicited messaging, and command acknowledgement, Consequently, it became the de facto standard in North American utilities. IEC 60870-5-101, utilized extensively in Europe and Asia, provided similar functionality over serial links, while IEC 60870-5-104 extended the same stack to IP-based WANs [12]. Such traditional, formal,

protocol-based messages between the substation and central control stations were introduced, forming the foundation for modern smart grid evolution [13]. However, these systems are incapable of supporting bidirectional flow of information, faster-than-real-time communications, and cybersecurity protections for the modern decentralized, automatic grid scenario.

While legacy grid communication systems were adequate for the centralized operation of the past, modern decentralized systems are woefully inadequate. Legacy protocols such as IEC 60870-5-101 and DNP3 were designed for unidirectional data transportation, precluding two-way, interactive operation with consumers and DERs. Hierarchical point-to-point SCADA topologies are not scalable, and integrating DERs, EVs, and smart appliances is impossible. Aging communication links, typically operating at 1200–9600 bps, cannot support PMU high-rate synchrophasor streams, which require 30–60 messages per second. Automation is incompletemanual fault detection and outage response are common, and FLISR functions are never enabled. Security is a significant issue as well; protocols such as Modbus and early DNP3 lack encryption and authentication, making the systems vulnerable to false data injection (FDI) and denial-of-service (DoS) threats [14]. The systems are based on fixed, vendor-specific configurations precluding interoperability and grid-wide observability. Even when a common standard is agreed upon, implementation discrepancies prevent smooth communications between devices. Furthermore, the absence of facilities for machine learning or real-time data analytics prevents an evolving response to developing threats and dynamic load conditions [15].

2.3 Comparison of Traditional and Smart Grid Communication Protocols

The transition to smart grids required a paradigm shift in communication protocols to support requirements like bidirectional data flow, real-time control, and advanced cybersecurity. Modbus, Distributed Network Protocol version 3 (DNP3), and IEC 60870-5-101 are some of the conventional grid communication protocols that were originally designed for centralized SCADA systems with unidirectional polling methods, high latency, and low bandwidth [16]. These traditional systems employed hierarchical or point-to-point topologies for communications and relied on manual access controls or perimeter defenses rather than embedded security.

In contrast, the recently developed standards, such as IEC 61850, Secure DNP3, and Manufacturing Message Specification (MMS), are intended for fast, event-based, and object-oriented communications via the Internet Protocol. For example, IEC 61850 provides Generic Object-Oriented Substation Event (GOOSE) messaging and Sampled Measured Value (SMV), supporting protection and automation functions with as little as sub-4 milliseconds delay [6]. The standard even provides Substation Configuration Language (SCL), supporting automatic configuration and vendor-neutral interoperability. In addition, modern protocols include a robust cybersecurity framework in the form of Transport Layer Security (TLS), Public Key Infrastructure (PKI), and Role-Based Access Control (RBAC), standardized in IEC 62351 [17]. These capabilities facilitate distributed intelligence, in-time monitoring, and scalability in the integration of Distributed Energy Resources (DERs) in Home Area Network (HAN), Neighbourhood Area Network (NAN), and Wide Area Network (WAN). Smart grid communication, despite advances, is plagued by real-world issues, primarily in the areas of interoperability, cybersecurity, and scalability. Furthermore, the large-scale implementation of advanced standards like IEC 61850 and technology requires enormous expenditure.

3. Smart Grid Communication Layers and Network Architecture

Smart grid communication is built on a layered architecture, categorized by coverage and function into three primary domains: Wide Area Network (WAN), Field/Neighborhood Area Network (FAN/NAN), and Premise Area Network (PAN), which includes Home Area Network (HAN) [8], [12]. This structure supports two-way electricity and information exchange, decentralized energy generation, automation, and predictive analytics for grid operation. WAN interconnects utility control centers, transmission substations, and power plants across cities or regions using high-speed communication technologies such as fiber optics, microwave links, and 4G/5G networks. WAN supports latency-sensitive applications like SCADA, PMU data streaming, and teleprotection. The adoption of 5G, offering ultra-low latency and high reliability, is currently being piloted to enhance WAN capabilities for real-time grid operations.

FAN/NAN consolidates advanced metering systems, field controllers, line sensors, and distribution substations in individual local areas or small municipalities. Technologies often employed are ZigBee, Wi-Fi, LTE, and Power Line Communication (PLC). PLC uses the existing electricity infrastructure for transmission; however, it is plagued by issues related to noise and signal degradation over long distances. Such networks gather information from

individual residential sites and transformers and send consumption information and working status to the central command center. HAN enables communication between smart meters, appliances, and Home Energy Management Systems (HEMS). Short-range, low-power technologies like ZigBee, Wi-Fi, and HomePlug allow consumers to monitor and control energy usage. ZigBee is favored for its mesh networking, low power consumption, and cost efficiency in HAN environments.

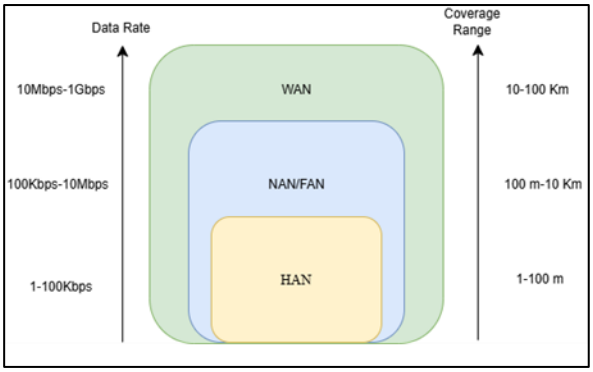

Figure 1. Data Rate vs. Coverage Range for HAN, NAN/FAN, and WAN

Every network layer has specific data rate, coverage, and latency requirements. WANs typically support bandwidths from 10 Mbps to 1 Gbps, while HANs operate in a bandwidth range of 10–100 kbps [1]. The reliability of smart grids relies on QoS differentiation, where critical control communications are prioritized over non-critical bulk data. In this context, concepts like packet switching, latency analysis, and buffer management are of utmost significance.

Table 1. Comparison of Communication Requirements across HAN, NAN, and WAN

Parameter	**HAN (Home Area Network)**	**NAN (Neighbourhood Area Network)**	**WAN (Wide Area Network)**
Coverage Range	1-100 meters	100-10000 meters	10-100 km
Data Rate	10-100 kbps	100kbps-10Mbps	10 Mbps-1 Gbps
Latency Requirement	Moderate (non-critical, e.g, smart meters)	Medium (e.g., AMI data aggregation)	Low (<50 ms, for SCADA, PMU, Tele protection)

Power Consumption	Very low (battery-operated sensors)	Moderate	High-performance, utility-grade equipment
Technologies Used	ZigBee, Wi-fi, HomePlug	PLC, RF Mesh, LTE, WiMAX	Fiber Optics, 4G/5G, Microwave, Satellite
Typical Applications	Appliance control, Home Energy Management	Smart metering, outage detection	SCADA, Teleprotection, PMU data transmission

The selection of physical mediums (e.g., optical fiber, copper, or microwave), network topology (centralized or localized), and the protocol stack significantly impacts the grid's performance. Centralized systems are considered suitable for automation over utility-wide feeders, while localized systems rely on regional RTUs with integration into SCADA and DMS.

4. Smart Grid Communication Protocols and Standards

Sophisticated standardized communication protocols are the backbone of interoperability among heterogeneous devices and networks in smart grids today. As we move from a centrally managed, traditionally operated infrastructure to a decentralized, automatically managed infrastructure, these standards facilitate seamless integration and coordination. The market has shifted from proprietary architecture to globally accepted protocols since the 1970s, making deployments, upkeep, and multi-vendor interoperability simpler. Secure, dependable information exchange among IEDs, RTUs, metering, and control systems is enabled by these protocols, and easing the process of modular upgrading and dynamic grid configurations. With greater automation and integration of DERs, EVs, and renewables, the communication standards need to offer low-latency performance, scalability, and built-in cybersecurity. Modern smart grid systems employ flexible, extensible protocols that minimize reconfiguration efforts and ensure long-term modernization of the grid [8], [12].

4.1 Modbus: Simplicity in Legacy Communication

Modbus, introduced in 1979, is still widely used due to its simplicity and ease of implementation. Modbus, using a master-slave (request-response) design, fits well for usage in PLC-PLC, PLC-HMI, and field device communication. Modbus provides two formats: Modbus RTU (binary encapsulated in serial links) and Modbus ASCII (text that is readable by

humans). RTU employs CRC, while ASCII employs LRC to check errors. Modern forms include Modbus TCP/IP, which is transported over Ethernet and mapped into the transport and network layers of the OSI stack. Despite its adaptability, Modbus lacks encryption, authentication, and time synchronization, limiting its suitability for smart grid applications requiring secure and time-sensitive data exchange. Due to security and performance issues, Modbus is largely confined to legacy systems or low-risk installations. This underscores the need for more secure, interoperable modes of communication in modern grid configurations [18].

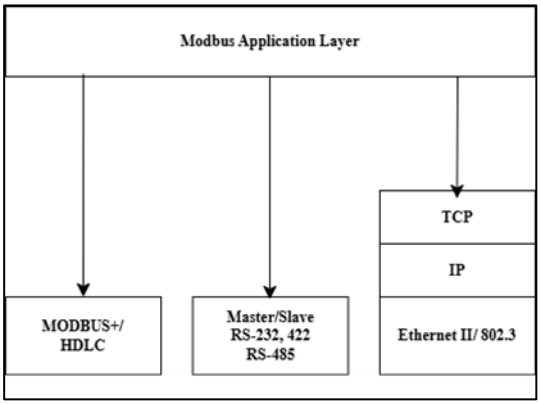

Figure 2. Mapping Modbus onto the OSI Model

Figure 2 illustrates how Modbus variants align with OSI layers, with RTU/ASCII mapping to physical and data link layers (e.g., RS-232/RS-485), and Modbus TCP/IP to TCP/IP and Ethernet infrastructure.

4.2 DNP3: Robustness in SCADA Communication

The Distributed Network Protocol (DNP3) emerged in the early 1990s as an expansion of legacy serial protocols like Modbus. It is adapted to low-bandwidth, noisy channels, polling, and/or event-oriented, being utilized over serial (RS-232/RS-485) or TCP/IP links. DNP3 accommodates time-stamped event reporting, unsolicited messages, and reliable delivery mechanisms. DNP3 defines structured data objects (e.g., Binary Input, Analog Input, Control Output) grouped by object types and accessed with function codes like Read, Write, Select, and Operate. It also includes error detection, time synchronization, and Secure DNP3 extensions for authentication and integrity protection [19]. Despite its widespread adoption and robustness, especially in SCADA systems across North America, DNP3 lacks native support for real-time, object-oriented communication and GOOSE-type messaging, as provided by IEC

61850. Additionally, it often requires intermediary components such as VPNs or protocol-aware firewalls to meet modern cybersecurity requirements.

4.3 IEC 60870-5-101/104: Telecontrol for European Grids

European and Asian countries utilized the IEC 60870-5 protocol family for telecontrol and substation automation. IEC 60870-5-101 operates over serial links, while 60870-5-104 extends the same application layer to TCP/IP over Ethernet, which enables greater flexibility and performance [20]. These protocols support structured framing, balanced and unbalanced transmission, time-tagging, file transfers, and redundancy, making them suitable for long-distance, event-driven monitoring in multi-utility operated environments. IEC 60870 accommodates millions of information objects and is known for its interoperability. However, unlike IEC 61850, this protocol lacks object-oriented modeling, multicast messaging, and peer-to-peer communication. Security must also be implemented externally, as native cybersecurity features are limited. This paper contrasts IEC 60870's layered design with more integrated protocols like IEC 61850 to assess its role in future cyber-resilient smart grid architectures.

4.4 IEC 61850: Object-Oriented Smart Grid Communication

IEC 61850 is a leading standard for smart grid and substation automation, offering object-oriented data modeling that represents physical devices as Logical Devices (LDs) and Logical Nodes (LNs). Each LN comprises Common Data Classes (CDCs), including data objects and attributes that define the functionality and state of devices such as circuit breakers, meters, and switches. This structured design enables vendor-independent interoperability and semantic clarity [6]. IEC 61850 supports a layered communication architecture designed for substation automation, enabling real-time data exchange and control. It includes GOOSE (Generic Object-Oriented Substation Event) for ultra-fast protection signaling with latencies under 4 milliseconds, SMV (Sampled Measured Values) for transmitting high-speed digitized analog measurements essential for synchronization, and MMS (Manufacturing Message Specification) for supervisory tasks such as data access, control commands, and logging operations. These services operate over Ethernet using VLAN tagging, multicast addressing, and QoS mechanisms for traffic prioritization. System configuration is managed through the Substation Configuration Language (SCL), an XML-based schema that defines topology, IED functions, and logical mappings streamlining integration and lifecycle upgrades. While IEC 61850 excels in real-time performance, interoperability, and future-proof scalability, it also

introduces implementation complexity. Adoption has been uneven, with DNP3 still prevalent in North America [9]. This paper highlights IEC 61850's value for scalable, semantically clear automation, but emphasizes the need for standardized engineering practices to ensure full interoperability across vendors.

Engineers and utilities have shifted from Modbus and DNP3 to IEC 61850 to meet the growing need for IP-based, vendor-neutral communication that supports real-time and scalable grid operations. Unlike Modbus, which uses static data registers and fixed message formats, IEC 61850 introduces self-describing, object-oriented data models and enables peer-to-peer messaging with sub-4 ms latency through GOOSE and SMV. Although DNP3 and IEC 60870-5 allow timestamped event reporting and work well over long distances, they don't offer built-in support for hierarchical modeling or fast automation. With its flexible design and support for technologies like HTTP and cloud integration, IEC 61850 stands out as a future-ready standard for digital substations and smart, resilient power systems.

4.5 Other Protocols Supporting Grid Communication

Several communication protocols beyond the substation level play a key role in enabling smart grid operations across home, neighborhood, and wide-area networks. IEEE 802.15.4 (ZigBee) supports low-power, short-range communication in Home Area Networks (HANs), commonly connecting smart meters with household appliances. Its mesh networking capability makes it well-suited for advanced metering infrastructure (AMI) and home energy management. IEEE 802.11 (Wi-Fi) and IEEE 802.16 (WiMAX) extend connectivity in Neighborhood Area Networks (NANs) and Wide Area Networks (WANs), linking field devices, substations, and control centers through medium- to long-range wireless channels. ICCP/TASE.2, built on MMS, enables real-time and secure data exchange between SCADA systems in different locations, supporting coordination across multiple control centers.

Despite these protocols being widely utilized within various layers of the grid, few studies assess how effectively they can coexist when faced with realistic cybersecurity threats. For example, ZigBee's lightweight nature may not be compatible with Multiprotocol Label Switching (MPLS) based WANs if the proper Quality of Service (QoS) mechanisms and protocol mapping are not implemented by engineers. This research gap indicates the need for more investigation intocross-layer interoperability and secure integration within smart grid networks at large scales.

5. Smart Grid Networking Infrastructure

Smart grid networking has progressed from static, manual systems to dynamic, intelligent infrastructures that facilitate real-time monitoring, protection, and control. This section delineates both legacy and contemporary communication architectures within power systems [6], [12].

5.1 Legacy SCADA Infrastructure

Traditional SCADA systems relied on Remote Terminal Units (RTUs) connected through point-to-point serial links such as RS-232 or RS-485. Copper wiring mesh is used in substation equipment, interconnecting current transformers (CTs), voltage transformers (VTs), relays, and bay controllers.

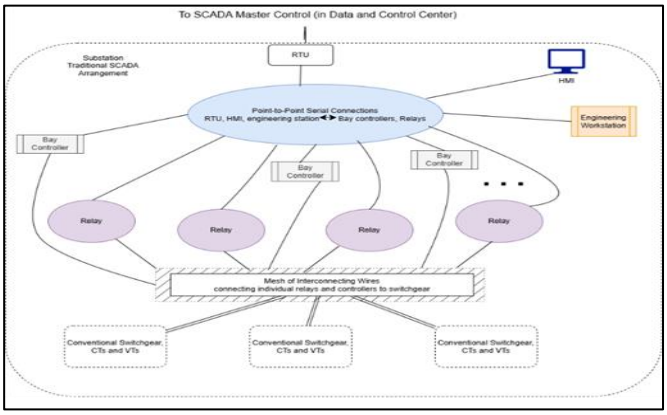

Figure 3. Traditional SCADA Schematics

Traditional SCADA systems operated on a master-slave polling model, where the SCADA Master at the Data and Control Center (DCC) periodically polled Remote Terminal Units (RTUs) for data and issued control commands. Main components included RTUs, electromechanical relays, bay controllers, and Human–Machine Interfaces (HMIs). Early systems employed protocols such as Modbus, Landis & Gyr 8979, and GETAC; later, these were supplemented by DNP3 to support event-driven communication and time-tagged data. These architectures faced limitations, as we discussed already in section 2, including complex wiring, poor scalability, and interoperability issues, with real-time responsiveness hindered by polling delays of 2–5 seconds [21].

5.2 Modern SCADA and IEC 61850-Based Architectures

Modern SCADA systems have evolved from centralized architectures to distributed, Ethernet-based designs, for which IEC 61850 serves as the foundational standard for substation automation [22].

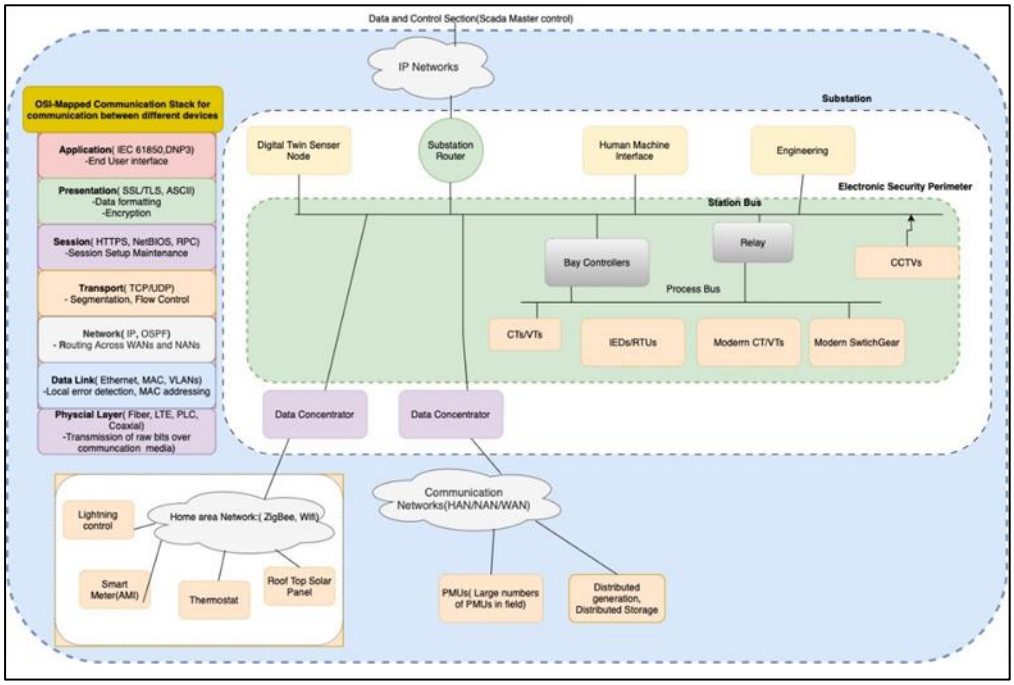

Figure 4. Smart Grid Communication Architecture with Protocol Stack

Intelligent Electronic Devices (IEDs) have replaced legacy RTUs, performing measurement, protection, and control functions directly at the bay and process levels. The communication architecture includes a Process Bus connecting CTs, VTs, and switchgear to IEDs for peer-to-peer communication, and a Station Bus linking IEDs, HMIs, routers, and SCADA masters for broader data exchange. IEC 61850 protocols include MMS for control center interaction, GOOSE for rapid protection messaging under 4 ms, and SMV for synchronized analog measurements. Multifunction IED networks are utilized in modern substations, which are networked through Ethernet switches and IP routers, and VLANs are used for prioritization of information and security. IEC 61850 implementation reduces wiring complexity, enhances interoperability using object-oriented models for information and XML-based SCL, and enables rapid, flexible integration of the grid with DERs, PMUs, and demand-side assets.

5.3 Integrated Infrastructure Components

Modern smart grids rely on an end-to-end network infrastructure through Home Area Networks (HAN), Neighborhood/Field Area Networks (NAN/FAN), and Wide Area Networks (WAN) to facilitate scalable, real-time coordination and control [23]. IP-based SCADA systems currently have IEC 61850 interoperability and facilitate seamless connectivity from the substation to utility control centers. Critical nodes such as Phasor Measurement Units (PMUs) deliver time-synchronized voltage and current data at rates of 30–60 samples per second, transmitted via low-latency, high-bandwidth links like fiber optics or 4G/5G to Phasor Data Concentrators (PDCs) for real-time grid monitoring.

Advanced Metering Infrastructure (AMI) offers two-way meter-utility communication, remote operation, usage profiles, outage notifications, and demand response. It facilitates the integration of either ZigBee or Wi-Fi in Home Area Networks (HANs), PLC or LTE in Neighborhood Area Networks (NANs), and fiber or microwave in Wide Area Networks (WANs) for large-scale integration. Multi-layered architecture enhances observability, automatability, and grid flexibility and facilitates functions including distributed energy resource (DER) coordination, voltage management, and dynamic load balancing, precursors to a self-healing, intelligent grid.

6. Security Issues in Power Grid and Smart Grid Communications

The shift from a traditional power grid to a digital, cyber-physical system has made communication networks more vulnerable to cybersecurity threats. As utilities adopt more IP-based technologies and continue to rely on older protocols, many operational systems lack built-in security features. This opens the door to risks such as unauthorized access, data tampering, and even large-scale outages. A well-known example is the 2015 cyberattack on the Ukrainian power grid, where attackers used spear-phishing emails and malware to breach SCADA systems, ultimately causing blackouts that affected around 230,000 people.

6.1 Common Cyber Threats and Protocol Vulnerabilities

Smart grids are exposed to multiple vulnerabilities due to their distributed and interconnected architecture. Attackers can inject false data into PMU or smart meter streams, misleading control systems and causing grid instability or financial loss. Denial of Service (DoS) attacks overwhelm networks and disrupt critical operations such as SCADA commands

and PMU synchronization. Without proper encryption and authentication, attackers can launch Man-in-the-Middle (MITM) attacks to intercept and alter communication between substations and control centers [24]. Insiders or intruders can also exploit physical access to relays or IEDs through unsecured RS-232 or RS-485 interfaces, enabling direct equipment manipulation. Many field devices operate without adequate protection from electromagnetic interference (EMI), Ground Potential Rise (GPR), or spoofing attacks, especially in unshielded or remote environments. These risks highlight the need to secure protocols and harden infrastructure across all layers of the smart grid for secure, reliable operations.

6.2 Insecure Legacy Protocols

Many industrial control systems still rely on legacy protocols that were never built with security in mind [25]. Early versions of Modbus, DNP3, and IEC 60870-5-101/104 do not include encryption, authentication, or message integrity. As a result, attackers can spoof commands, inject malicious data, or replay old packets to disrupt operations. Vendors also continue to use proprietary protocols like GETAC and Landis & Gyr, which depend on obscurity rather than solid security practices. These closed systems often block third-party audits and make it harder to spot vulnerabilities. In the field, engineers still use serial lines such as RS-232 and RS-485 for communication, even though these links offer no protection against eavesdropping, signal tampering, or unauthorized control.

7. Security Requirements for Modern Grid Networks

Modern power grids operate as tightly integrated cyber-physical systems, exposing communication networks to growing cybersecurity risks. The convergence of Information Technology (IT) and Operational Technology (OT) continues to use legacy protocols, and weak network segmentation increases the chances of attacks spreading from enterprise systems to SCADA, substation automation, or generation control. A strong grid security solution would offer confidentiality, integrity, and availability. Data in transit over WANs, AMI systems, and in the cloud is safeguarded by cryptographic algorithms such as AES, TLS, and IPSec. Integrity solutions, including SHA-based hash functions, digital signatures, and Message Authentication Codes (MACs), detect unauthorized alterations to control or measurement data. To maintain availability, operators use redundant links, failover routing, and intrusion-tolerant communication, especially for voltage regulation, fault isolation, and protection relays.

Identity and access control are equally important. Public Key Infrastructure (PKI), digital certificates, and multi-factor authentication secure communication between control centers and substations. Role-Based Access Control (RBAC) restricts access based on users' roles, and VLANs, firewalls, and Access Control Lists (ACLs) isolate critical traffic. Secure Boot, hardware authenticity checks, and tamper-resistant IEDs offer physical security. At the protocol level, IEC 62351 offers enhanced security for IEC 61850, DNP3, and MMS with the incorporation of encryption and authentication. Intrusion Detection and Prevention Systems (IDS/IPS) track anomalies in GOOSE, Modbus, and DNP3 streams. Lightweight protocols offer security to resource-limited devices such as smart meters and PMUs through ZigBee and 6LoWPAN [26]. Regulatory standards such as NERC CIP and ISO/IEC 27001 guide compliance throughout the grid [27]. Emerging technologies, including AI, federated learning, blockchain, Software-Defined Security (SDS), and Zero Trust Architecture (ZTA), offer dynamic, active defense by identifying intrusions, containing compromised nodes, and securing distributed systems with minimal loss in performance.

8. Global Smart Grid Implementations and Lessons Learned

The purpose of this section is to give examples of real-world implementations of smart grids and how technology standards such as IEC 61850, DNP3, TLS encryption, and ISO 27001 are applied in the real world, reflecting country-specific agendas about interoperability, scalability, and data security. In the United States, the Pacific Northwest Smart Grid Demonstration project funded by the U.S. Department of Energy united 11 utilities to integrate AMI, DERs, and wide-area control using both fibre-optic and wireless communication. Open standards such as DNP3 and IEC 61850 were used to ensure interoperability across diverse vendor equipment. A major outcome was the successful coordination of legacy and modern infrastructures under a unified, standards-based communication framework. India’s Smart Meter National Programme (SMNP) plans to roll out millions of smart meters using technologies such as GPRS, PLC, ZigBee, and LTE. The program follows Indian Standard IS 16444 and ISO/IEC 27001, targeting energy theft prevention, cost reduction, and reliable operation in areas with limited infrastructure. It places strong emphasis on secure data transmission and flexibility, especially in rural settings. Germany has taken a different but equally rigorous approach with its BSI Smart Meter Gateway (SMGW) architecture, managed by the Federal Office for Information Security (BSI). This model routes all communication through encrypted TLS channels and uses PKI-based authentication to protect data exchange.

By enforcing strict privacy policies and adopting a vendor-neutral framework, the system promotes interoperability and ensures compliance with national data protection laws. It serves as a strong example of privacy-by-design in secure smart metering.

9. Challenges and Open Issues

Smart grid communication still faces significant hurdles in achieving secure, scalable, and interoperable deployment due to many factors. Proprietary protocols and inconsistent use of standards like IEC 61850 limit interoperability across existing multi-vendor systems. Legacy infrastructure forces new technologies to interact with outdated devices that lack standardized interfaces and built-in security. Real-time functions such as fault detection demand sub-50 ms latency, which remains difficult over wide-area, heterogeneous networks. Encryption improves security but adds delay and processing load, especially for low-power field devices

Non-technical factors such as high upgrade costs, limited rural broadband, and delays in policy areas like 5G spectrum allocation create additional barriers to smart grid adoption beyond purely technical challenges. Mixed environments of old and new systems often create security gaps due to uneven protection. The sector still needs better tools for protocol testing, consistent global standards, and more training in cybersecurity and grid networking. Solving these issues will require close coordination among utilities, regulators, security experts, and standards organizations [12].

10. Future work and Conclusion

The future of smart grid communications is oriented towards intelligent, adaptive, and self-healing infrastructures that are resilient to physical and cyber threats. These infrastructures will utilize AI-enhanced situational awareness, decentralized control, and real-time data acquisition for predictive defense and rapid response. Emerging paradigms such as Wide-Area Situational Awareness and Control (WASA&C) will employ Phasor Measurement Units (PMUs) and cloud analytics to proactively anticipate instability and intrusions. To ensure enduring security, utilities are beginning to deploy post-quantum cryptography (PQC), including hybrid cryptographic stacks across Wide Area Networks (WANs), SCADA connectivity, and Distributed Energy Resource (DER) transactions. Protocols such as IEC 61850, DLMS/COSEM, and DNP3 will function over resilient backhaul infrastructures, including LTE, Medium Voltage Power Line Communication (MV-PLC), and optical fiber.

Digital twins and the Internet of Energy (IoE) are transforming grid planning and coordination. Digital twins simulate component behavior for predictive maintenance and cyber-defense validation, while IoE architectures facilitate peer-to-peer energy exchange among DERs, Electric Vehicles (EVs), and smart homes. The success of these technologies hinges on seamless integration across Home Area Networks (HAN), Neighborhood Area Networks (NAN)/Field Area Networks (FAN), and WAN layers, utilizing tiered, Quality of Service (QoS)-enabled routing. Security frameworks will evolve through Electronic Security Perimeters (ESPs), Security Information and Event Management (SIEM) systems, VPN tunnels, and Zero Trust enforcement. Future grid communications will adopt Software-Defined Networking (SDN) overlays, dynamic reconfiguration, and programmable architectures aligned with OSI-layered protocol stacks to enhance reliability, automation, and regulatory compliance.

In summary, this review analyzed the transition from legacy protocols such as Modbus and DNP3 to modern standards like IEC 61850, emphasizing the necessity for secure, scalable, and interoperable communication infrastructures. With the increasing penetration of DERs, real-time analytics, and consumer interactivity, the role of secure networking is central to grid reliability. Achieving this vision requires harmonized global standards, robust cybersecurity frameworks, and sustained investment in edge-to-cloud architectures validated through coordinated pilot deployments

References

[1] Abrahamsen, Fredrik Ege, Yun Ai, and Michael Cheffena. "Communication technologies for smart grid: A comprehensive survey." Sensors 21, no. 23 (2021): 8087.

[2] O'Reilly, Gerard P., Steven H. Richman, and Andjelka Kelic. "Power, telecommunications, and emergency services in a converged network world." In 2007 6th International Workshop on Design and Reliable Communication Networks, IEEE, (2007): 1-6.

[3] X. Yu and Y. Xue, "Smart Grids: A Cyber–Physical Systems Perspective," in Proceedings of the IEEE, vol. 104, no. 5, May (2016): 1058-1070, doi: 10.1109/JPROC.2015.2503119.

[4] Basnet, Biswash, Kishor Sapkota, Rabison Poudel, Sandip Kshetri, and Ram Prasad Pandey. "Dynamic-Static Var Compensation for Improving Power Factor." Journal of Engineering and Sciences 1, no. 1 (2022): 46-49.

[5] Jain, P. C. "Trends in smart power grid communication and networking." In 2015 International Conference on Signal Processing and Communication (ICSC), IEEE, (2015): 374-379.

[6] R. E. Mackiewicz, "Overview of IEC 61850 and Benefits," 2006 IEEE PES Power Systems Conference and Exposition, Atlanta, GA, USA, (2006): 623-630, doi: 10.1109/PSCE.2006.296392.

[7] Gungor, Vehbi C., Dilan Sahin, Taskin Kocak, Salih Ergut, Concettina Buccella, Carlo Cecati, and Gerhard P. Hancke. "Smart grid technologies: Communication technologies and standards." IEEE transactions on Industrial informatics 7, no. 4 (2011): 529-539.

[8] Kuzlu, Murat, Manisa Pipattanasomporn, and Saifur Rahman. "Communication network requirements for major smart grid applications in HAN, NAN and WAN." Computer Networks 67 (2014): 74-88.

[9] Yan, Ye, Yi Qian, Hamid Sharif, and David Tipper. "A survey on cyber security for smart grid communications." IEEE communications surveys & tutorials 14, no. 4 (2012): 998-1010.

[10] Moslehi, Khosrow, and Ranjit Kumar. "Smart grid-a reliability perspective." In 2010 Innovative smart grid technologies (ISGT), pp. 1-8. IEEE, 2010.

[11] Sauter, Thilo, and Maksim Lobashov. "End-to-end communication architecture for smart grids." IEEE Transactions on Industrial Electronics 58, no. 4 (2010): 1218-1228.

[12] Budka, Kenneth C., Jayant G. Deshpande, Marina Thottan, Kenneth C. Budka, Jayant G. Deshpande, and Marina Thottan. "Elements of Communication Networking for Power System Practitioners." Communication Networks for Smart Grids: Making Smart Grid Real (2014): 47-90.

[13] Tan, Song, Debraj De, Wen-Zhan Song, Junjie Yang, and Sajal K. Das. "Survey of security advances in smart grid: A data driven approach." IEEE Communications Surveys & Tutorials 19, no. 1 (2016): 397-422.

[14] Lopez, Gregorio, Javier Matanza, David De La Vega, Marta Castro, Amaia Arrinda, José Ignacio Moreno, and Alberto Sendin. "The role of power line communications in the smart grid revisited: Applications, challenges, and research initiatives." IEEE access 7 (2019): 117346-117368.

[15] McDaniel, Patrick, and Stephen McLaughlin. "Security and privacy challenges in the smart grid." IEEE security & privacy 7, no. 3 (2009): 75-77.

[16] Ayala, Andrés Felipe Rodríguez, Daniela Johanna Rojas Martínez, and Armando Giral-Ramírez. “A REVIEW OF COMMUNICATION PROTOCOLS IN POWER SYSTEMS.”. Vol., no. 20 (2022). https://www.jatit.org/volumes/Vol100No20/24Vol100No20.pdf

[17] A. Albarakati et al., "Security Monitoring of IEC 61850 Substations Using IEC 62351-7 Network and System Management," in IEEE Transactions on Industrial Informatics, vol. 18, no. 3, March (2022): 1641-1653, doi: 10.1109/TII.2021.3082079.

[18] McLaughlin, Kieran, Ivo Friedberg, BooJoong Kang, Peter Maynard, Sakir Sezer, and Gavin McWilliams. "Secure communications in smart grid: Networking and protocols." In Smart Grid Security, Syngress,(2015): 113-148.

[19] Amoah, Raphael, Seyit Camtepe, and Ernest Foo. "Securing DNP3 broadcast communications in SCADA systems." IEEE Transactions on Industrial Informatics 12, no. 4 (2016): 1474-1485.

[20] Fu, Qin-Cui, Jian-Yun Chen, and Zi-Ying Liu. "Implementation of telecontrol protocols in SCADA systems based on FSM." In 2007 International Power Engineering Conference (IPEC 2007), pp. 75-79. IEEE, 2007.

[21] Yadav, Geeta, and Kolin Paul. "Architecture and security of SCADA systems: A review." International Journal of Critical Infrastructure Protection 34 (2021): 100433.

[22] Das, Narottam, Akramul Haque, Hasneen Zaman, Sayidul Morsalin, and Syed Islam. "Exploring the potential application of IEC 61850 to enable energy interconnectivity in smart grid systems." IEEE Access (2024).

[23] Atlagić, Branislav, and Mihalj Šagi. "Proposal of a modern SCADA system architecture." In 2011 19thTelecommunications Forum (TELFOR) Proceedings of Papers, IEEE, (2011): 1430-1433.

[24] Zideh, Mehdi Jabbari, Paroma Chatterjee, and Anurag K. Srivastava. "Physics-informed machine learning for data anomaly detection, classification, localization, and mitigation: A review, challenges, and path forward." IEEE Access 12 (2023): 4597-4617.

[25] Volkova, Anna, Michael Niedermeier, Robert Basmadjian, and Hermann de Meer. "Security challenges in control network protocols: A survey." IEEE Communications Surveys & Tutorials 21, no. 1 (2018): 619-639.

[26] Singh, Mahipal, and Sriram Sankaran. "Lightweight Security Architecture for IoT Edge Devices." In 2022 IEEE International Symposium on Smart Electronic Systems (iSES), IEEE, (2022): 455-458.

[27] Guarino, Alessandro. "Information security standards in critical infrastructure protection." In ISSE 2015: Highlights of the Information Security Solutions Europe 2015 Conference, pp. 263-269. Wiesbaden: Springer Fachmedien Wiesbaden, 2015