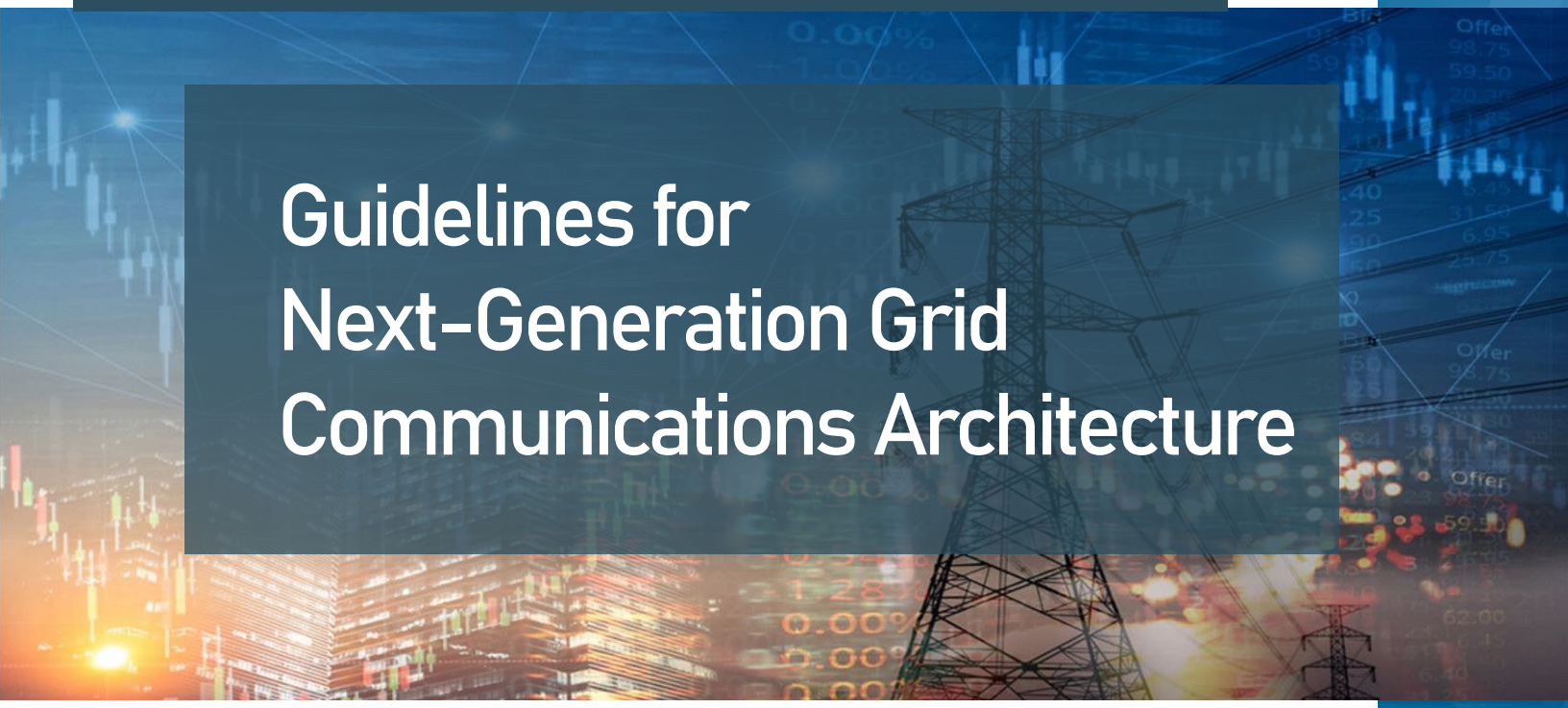

Guidelines for Next-Generation Grid Communications Architecture

October 4, 2024

Prepared by:
U.S. DEPARTMENT OF ENERGY,
OFFICE OF ELECTRICITY

Part of a series of white papers on
Secure Pathways for Resilient Communications.

SPaRC
Secure Pathways for Resilient Communications

U.S. DEPARTMENT OF ENERGY | OFFICE OF ELECTRICITY

Executive Summary

Next-generation grid communications architectures will be expected to meet increasing demands placed on a modern electric grid that will rapidly evolve with the integration of distributed energy resources (DERs), variable renewable energy sources like wind and solar, and advanced automation technologies. The communications architecture to support the evolving grid focuses on reliable, secure two-way communication to deliver timely, accurate data throughout the system for real-time coordination among grid operators, DERs, and regulators. The next-generation communications architecture should be able to provide support for an energy infrastructure that is resilient and can respond dynamically to grid conditions while still meeting operational challenges effectively.

Key attributes of the next-generation architecture are redundancy in the communications paths, adaptive protocols, modular designs, and robust security measures. Redundancy ensures continuity of operations in the event of equipment failure or during adverse conditions; multiple paths can reroute data should disruption occur. The next-generation grid communications architecture uses advanced technologies such as edge computing and distributed intelligence to drive processing and decision-making closer to the source of the data. This greatly reduces latency and increases the speed of response to grid events.

The architecture needs to support the appropriate quality-of-service (QoS) requirements for critical grid functions. In the case of protective relays, low and deterministic latency capabilities are essential. Operation of protective relays within milliseconds is required to isolate faults and prevent cascading failures that can result in widespread outages and equipment damage. This guarantees that the architecture will provide high-speed operations in the grid protection mechanisms, making them effective and responsive. The QoS requirements need to be captured from end-to-end, for all portions of the architecture that support that grid service. Adaptive communication protocols should be employed to handle fluctuating network loads and should prioritize time-critical data traffic to ensure timely delivery of control commands and sensor data essential to maintaining the stability of the grid.

The communications architecture is modular, which allows network upgrading and/or adding feature sets without the need for a complete reconstruction of the system; this extends the life of the infrastructure and makes it compatible with emerging technologies. It is also designed to be scalable and flexible, be an architecture that will grow with the grid, and increase bandwidth and throughput as the number of devices and data points increases. It has flexibility to keep supporting continuous digital transformation of the electric grid, enabling further technologies, applications, and devices to get seamlessly integrated while maintaining similar performance. During outages and disruptions, modularity provides reduced outage durations in network restoral type resolutions.

The next-generation grid communications architecture enables utilities to enhance operational capabilities, reduce outage risks, and generally strengthen grid resilience. The end-to-end architecture presented here provides a holistic framework to build a reliable, flexible, and scalable communication network that meets the critical needs of the modern grid and positions utilities for handling challenges with integrating a range of energy resources and enabling a carbon-free energy future.

1. Introduction

Welcome to the eighth paper in a series of white papers authored by the Secure Pathways for Resilient Communications (SPaRC) program. The first four white papers [1], [2], [3], [4] discussed the challenges facing the evolving electric grid, including the communication sector, grid collaboration, and grid device interoperability. The first deep-dive white paper [5] began a series of deep-dive discussions with a look at latency and its impact on grid communications. The second deep-dive white paper [6] explored a series of attributes and characteristics of a network or communications system that together describe the overall performance of that network or system, called Quality-of-Service (QoS). The third deep-dive white paper [7] explored the various communication technologies available, their advantages and limitations for different grid operational processes, aiming to assist the discussion between communications providers and electric utilities.

This white paper, the fourth deep-dive discussion, presents the main attributes required for the next-generation secure communications' architectures and provides general guidelines for how they can be instantiated on the grid. There are both engineering and policy issues that must be resolved. In this white paper, we define the communication architecture as the protocol, medium, hardware, and software/firmware necessary for a communication system or network to operate.

A secure communication system protects the end-to-end physical pathway that transports data from origin to destination. That pathway may: involve different transmission mediums, such as optical fiber, copper wire, and wireless technologies; transport diverse data including grid state information and control messaging; and use a variety of analog and digital formats (see Figure 1). Securing this end-to-end communications pathway—which is essential for reliable grid operations—involves preventing unauthorized access and monitoring traffic to identify anomalous activity without compromising the confidentiality, integrity, or availability of the data. Communications security methods complement cybersecurity approaches used to protect data at origin and destination. Secure communications are critical for the successful operation of the electric grid [3].

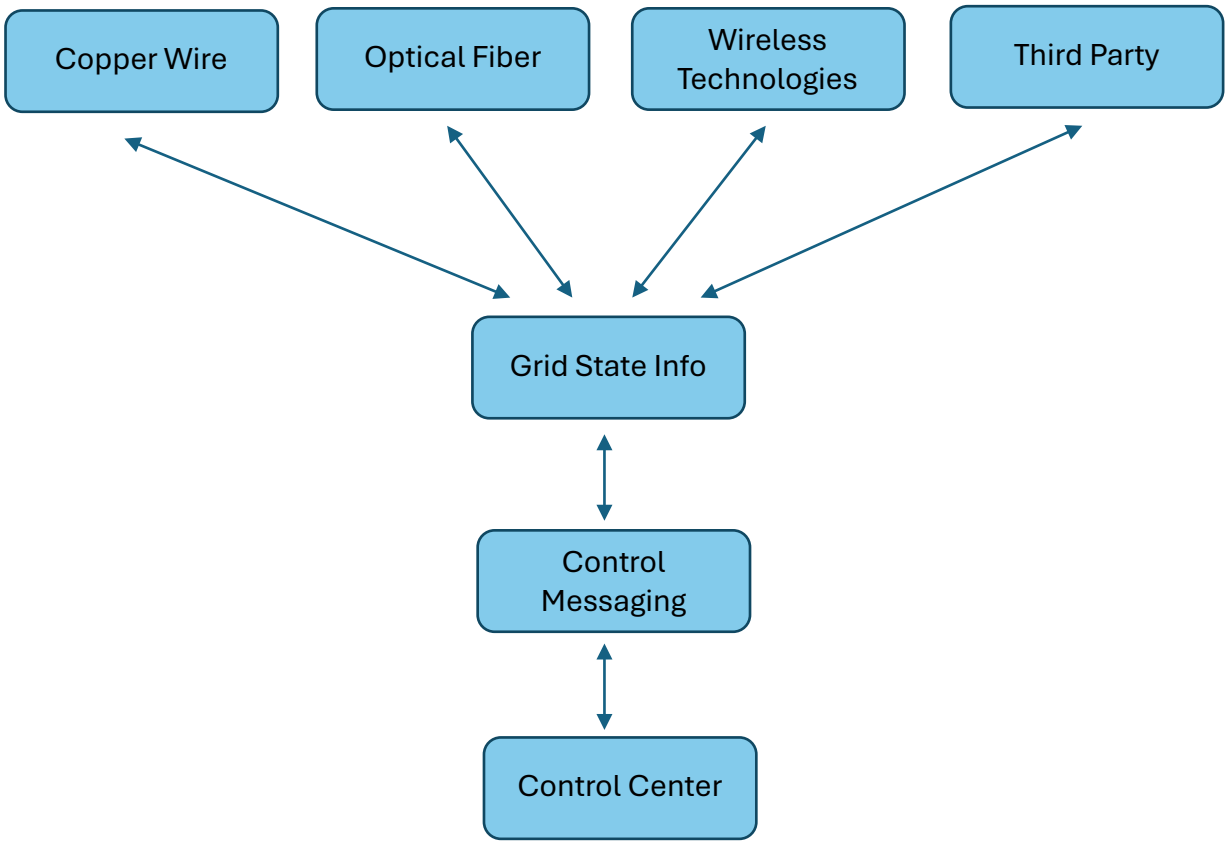

Figure 1. An example of a grid communication pathway.

2. Communications Architecture Attributes

A robust, interoperable communications link with the grid edge allows utilities to bring data driven analysis to decision makers and improve mission success.

Our Nation's electric grid is transitioning from a centralized, producer-controlled network to a distributed, consumer-interactive network. Renewables, primarily driven by variable generation sources such as wind and solar, are expected to be the largest source of generation by 2030 [8]. Simultaneously, there has been a steady growth of installed DERs with capacity closer to the edge of the system. A fully functioning electric grid will feature ubiquitous sensors throughout the transmission and distribution grid. The data from these sensors will be used to balance electric supply (generation) with consumer demand (load) continuously. The communication networks connected to the sensors will need to provide consistent and well-defined latency, higher bandwidth, and two-way communications to transport information between utilities and consumers as needed. Investing in enhanced communications technologies brings about system visibility that—in

addition to the operational and response/recovery improvements described above—enables smarter, more efficient spending better targeted at documented needs. A robust, interoperable communications network with the grid edge allows utilities to bring data-driven analysis to decision makers and improve mission success, suggesting that communications investments should not take a back seat to other priorities.

Existing communication architectures used in the electric grid must evolve to be able to support the requirements of the future grid. The following attributes are required for the next-generation grid communications architecture (see Figure 2):

a. **Reliability and Resilience**: Able to function through natural disasters, power outages, storms, network outages, and cyber-attacks. Degrade gracefully and support traffic prioritization to let the most important traffic go through.
b. **Durability and Flexibility**: The expected lifetime of the communication architecture needs to be larger than (or at least similar to) the expected lifetime of the indoor power grid equipment without requiring significant changes. The architecture should be able to accommodate new devices, new applications, and new requirements without wholesale restructuring that would invalidate existing investments.
c. **Security and Privacy**: Understanding the characteristics of the network, the devices on the network, and the communications paths between those devices so that the network can effectively be monitored for anomalies that might indicate malicious activity. This must be done while still allowing grid functions and processes to perform as designed, without introducing additional operations performance issues.
d. **Interoperability and Standards**: Minimize risk by utilizing standards-based technologies. Avoid vendor lock-in. Easily upgradeable, supports mix-and-match to install best of breed equipment.
e. **Performance and Scalability**: Provide support for applications that demand strict QoS requirements. Use event-based technologies (e.g., Simple Network Management Protocol [SNMP] traps [9]) to avoid constant polling for status. Connect a large number of endpoints and public/private networks together. Distributed technologies such as OpenFMB (pub/sub) [10] are critical for control of tens of thousands of resources in the bulk power grid.

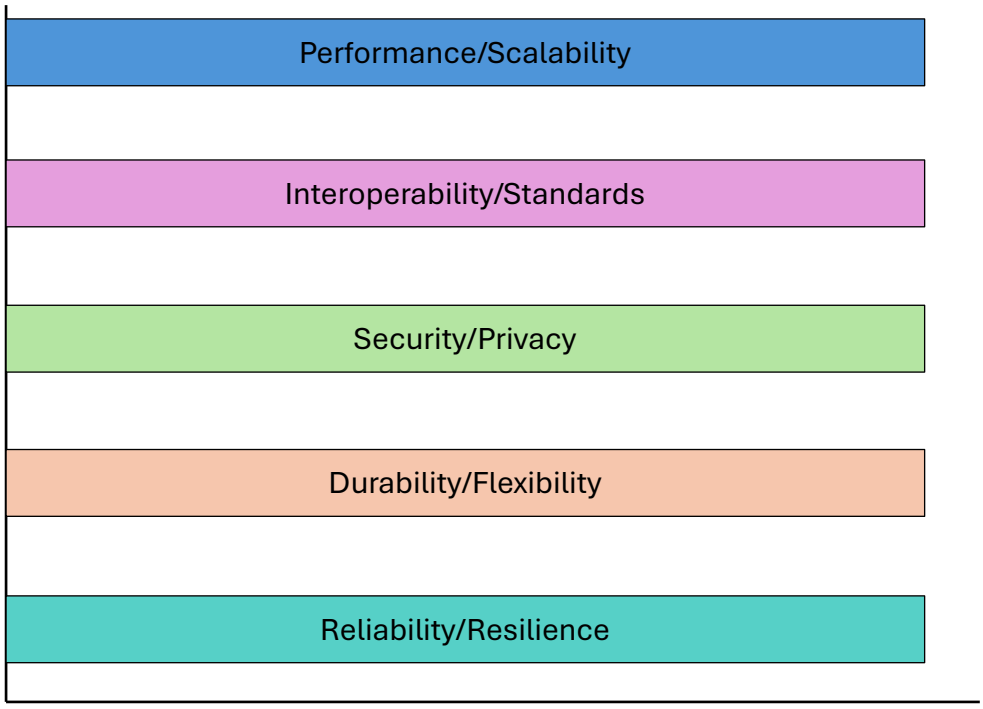

Figure 2. An illustration of the main attributes for next-generation grid communications architecture.

3. Guidelines for the Next-Generation Grid Communications Architecture

Designing a next-generation communications architecture for power systems involves addressing several key design, implementation, and security guidelines to enhance the system efficiency, reliability, and security. Table 1 presents a brief description of the proposed guidelines for each communication architectural attribute.

Table 1. The proposed design, implementation, and security guidelines for each communication architectural attribute

Architectural Guideline / **Architectural Attribute**	**Design**	**Implementation**	**Security**
Reliability and Resilience	Design multiple communication paths to avoid single points of failure	Develop and regularly test a disaster recovery plan to quickly restore communications in case of a major outage or failure	Implement automatic failover mechanisms to maintain service continuity during natural and human-caused hazards

Durability and Flexibility	Design the architecture with modular components that can be upgraded or replaced without overhauling the entire system to accommodate changing requirements	Use industry standards and best practices to ensure compatibility and interoperability with other systems, reducing the risk of obsolescence	Perform regular update/maintenance (e.g., firmware) and implement monitoring tools to ensure all components are functioning correctly
Security and Privacy	Use end-to-end encryption to protect data integrity and confidentiality. Understand what is on the network and control and understand the paths and patterns of communication	Ensure robust authentication and authorization mechanisms throughout the device life cycle	Where possible, use logical and physical separation of networks to enhance security and reduce risk. Monitor for anomalies in your intended communication paths and patterns
Interoperability and Standards	Design the architecture to support various communication protocols used in power systems (e.g., DNP3, Modbus, IEC 61850)	Ensure compatibility with existing legacy systems to facilitate a smooth transition and integration	Choose devices that meet existing security and operational standards rather than outdated or developmental ones
Performance and Scalability	Design the communications architecture to be easily scalable, allowing for the addition of new devices, systems, and technologies as the grid evolves	Utilize edge computing to perform data processing and analysis closer to the source, reducing latency and bandwidth usage	Use distributed intelligence to enable local decision-making and enhance grid responsiveness and security

3.1. Reliability and Resilience

The communication architecture should be resistant to system failures and natural and human made hazards, providing minimal single points of failure.

Smooth operation of the power grid depends on a reliable communication architecture that is also resilient and adapted to the needs of each grid service. An appropriate architecture will need to provide the QoS guarantees required by various grid services [6]. For example, while revenue metering is important, the latency criticality is much lower for it than for other services, such as line protection (see Figure 3). Ensuring that communications related to line protection is resilient and reliable will go a long way to ensure stability and safety of the grid.

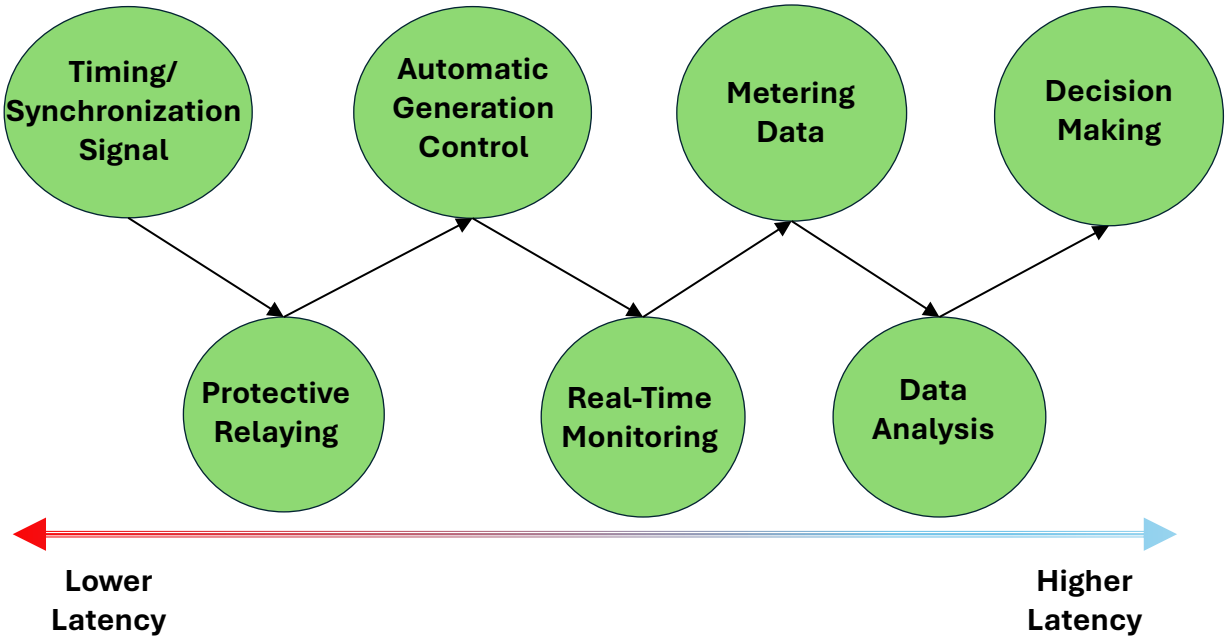

Figure 3. An illustration of utility operational processes with various latency criticalities.

The communication architecture should be resistant to natural and human-caused hazards, providing minimal single points of failure. The degree of resilience must be commensurate with the criticality of the grid service supported, which in turn requires deep knowledge of the operational importance of each service. Not all grid services have similar QoS requirements; some, such as protective relaying and real-time control, require more stringent QoS requirements to prevent safety hazards and equipment damage. Other services, such as metering and demand response can tolerate more relaxed variances in QoS. Effective management of QoS characteristics specific to each service is crucial for reliable grid operations, particularly when using flexible technologies that provide variable latencies, such as IP-based communications networks. With well-set QoS policies, each service gets its due share of the resource thereby retaining the overall performance of the grid. Table 2 presents the latency and reliability requirements (scale 1 to 5 in increasing importance) for key grid services. The requirements for the scalability and security attributes will be discussed later in this document. The requirements for the key grid services presented in Table 2 are visualized in Figure 4.

Table 2. The latency, reliability, scalability, and security requirements (scale 1 to 5) for key grid services.

Service	Latency	Reliability	Scalability	Security
Voltage Regulation	4	5	3	4
Frequency Control	5	5	4	5
Demand Response	3	4	4	3
Energy Storage	2	5	5	4
Load Shedding	5	4	3	4
Black Start Capability	4	5	2	5
Reactive Power Support	3	5	3	3

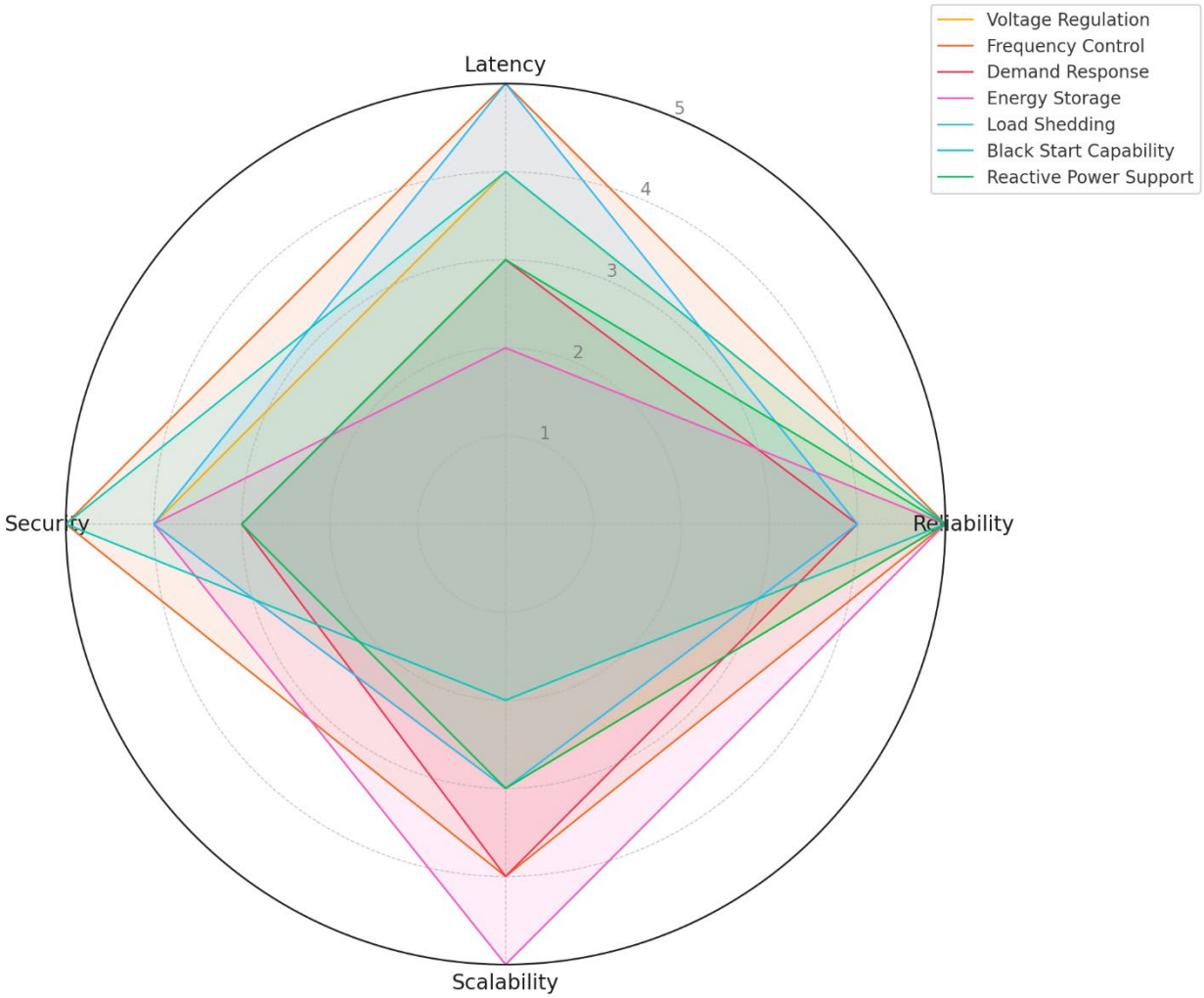

Figure 4. A visualization of the requirements (scale 1 to 5) for some key grid services.

A reliable and resilient communications architecture should match the operational criticality requirements of the grid services it supports.

Like the level of reliability, the level of resiliency in the communication architecture needs to be balanced with the cost and the availability of supporting communications equipment and services. For example, a resilient architecture could include redundant fiber paths that take geographically dispersed routes between two locations, backup power for all devices, and automated failover [11]. However, in a remote location, installing multiple fiber paths (or in fact any fiber path) may be cost prohibitive. While cost and service availability constraints may prevent redundant communication pathways, they should be considered where feasible. Redundancy considerations for critical services include using different providers or technologies for a location (e.g., fiber and cellular or fiber via two different entities) and ensuring the selected technologies do not rely on the same piece of intermediate infrastructure [12]. Cellular may backhaul via a fiber located in the same cable vault as another provider's fiber or possibly even backhaul on an existing provider's fiber if there is only limited fiber availability to a location.

Distinct communications pathways for failover should not stop at the entry to the facility. Backup communications equipment should not be in the same location in a facility nor use the same cable runs to prevent, for example, ceiling flooding on an equipment rack from damaging both sets of equipment. One common redundancy practice is having a backup control center in a different location than the primary control center. Communication facilities and equipment that support critical services should also have backup power available for whatever length of time is warranted for the service. Alternate cooling sources for equipment should be considered where possible, especially if the system relies on a local water supply that could see a service interruption during a power outage.

A resilient architecture should be able to operate through a failure event. Natural disasters like hurricanes, earthquakes, floods, etc. can cause infrastructure damage and can shut down portions of communication networks. In these cases, the system should be able to degrade gracefully by rerouting the data through other paths so that the grid can still be managed. This also involves prioritizing critical data for transmission to let the most important traffic go through and keep up the essential services even in degraded conditions. The ability to operate through an event also includes the ability to recover as quickly as possible from a disaster event. System recovery plans that include the communications architecture and infrastructure should be part of disaster recovery planning. These plans should be periodically reviewed and exercised as well as coordinated with any local supporting response personnel.

In conclusion, the need for uninterrupted secure and accurate flow of data in grid communications comes from the imperatives to handle the complexities of integration of DERs, fending off threats, guaranteeing operational resiliency in the case of natural and human-caused disasters, and assuring aggressive performance needs of modern grid

applications. Without a robust communication architecture, power grid reliability and resilience will be compromised.

3.1.1. Recommendations

A reliable and resilient communications architecture needs to match the operational criticality requirements of the grid service it supports. The reliability and resilience measures listed below should be considered for end-to-end architectures supporting critical services.

- Backup power that allows the communication system to operate even when the grid is de-energized.
- Multiple communication paths that are geographically diverse and meet the necessary QoS requirements. This should include the cable runs through buildings and any associated backup communications equipment.
- Multiple communication providers and media to minimize any specific carrier and or media dependency.
- Communications systems that can prioritize critical grid services in the event of network congestion or failover.
- A disaster recovery plan to quickly restore communications in case of a major outage or failure.

3.2. Durability and Flexibility

A durable communications architecture will have a long lifetime and will be flexible to accommodate changes in technology and requirements over time. A key element for a communications architecture that is durable and flexible is modular componentry. Modular components can easily be upgraded or replaced without overhauling the entire system. New portions of the architecture and new connections should be designed and built with modularity in mind. Existing portions of the architecture can be incrementally moved towards modularity through component replacement as elements either age out or fail over the course of their lifetime. Ensuring interoperability of the old and new systems provides smooth transitions, and hence continuity of operations.

A durable and flexible communications architecture accommodates new devices, new applications, and new requirements without a need for wholesale restructuring or replacing infrastructure investments before end of life. A technology migration roadmap is required to provide a migration path between legacy and future communication technologies.

Selection of technologies and devices that meet current approved standards also allows for a durable architecture with a long life [13]. Components that meet beta standards or standards that are still evolving, may not be compatible with future devices; therefore, are

not good candidates for an architecture with a long life. When replacing legacy equipment, devices should be chosen that are compatible with existing needs but that also will support potential future needs to allow the architecture to transition. A technology roadmap of existing devices and possible replacements and additions that meet the needs of the architecture can assist in planning for this transition. The technology roadmap should consider the evolving needs of the architecture in terms of QoS requirements for grid services and ensure that any replacement or newly added components can support current and future needs. Additionally, procuring longer life cycle equipment should be considered together with longer technical support that includes both hardware, firmware, and software. Longer periods of support reduce the need to replace equipment more frequently; this also extends access to updates to improve performance and patches for security so that the equipment remains reliable and secure longer. Regular maintenance should be conducted that includes hardware, if needed, and firmware/software and security patches. These practices are part of life cycle management, which also includes decisions on extended support contracts, plans for phase-out, and end-of-life transitions.

In addition to maintaining equipment according to manufacturer specifications, equipment should be stored and operated within the manufacturer's environmental specifications for longevity [14]. For instance, network switches and other critical components installed in substations or in a controlled environment must be at proper temperature, humidity, and dust control. Protection against unfavorable conditions allows for a long service life and reduces the risk of premature failure.

3.2.1. Recommendations

- Technology roadmap and migration path: Develop a technology roadmap that provides a clear direction on how to migrate from legacy systems of the past to technologies of the future in a modular fashion as components need to be replaced or new components are acquired.
- Standardization and modularity: Employ standardized protocols for interoperability and to avoid early obsolescence. Modularity within system design allows for incremental upgradeability, enabling easier integration of new technologies without extensive modifications.
- Long life cycle equipment and support: Choose long life cycle equipment, with corresponding technical support, including hardware, firmware, and software.
- Regular maintenance and updates: Follow a preventive maintenance approach, including periodic inspection, updating of firmware, and installation of software patches.
- Environmental protection: Equipment should be stored and operated within the manufacturer's environmental specifications for longevity.
- Extended life cycle management: Determine life cycle management strategies for both aging and newer equipment.

3.3. Security and Privacy

It is essential to monitor and alarm the communications pathways for signs of tampering or unauthorized access, exfiltration of data or files, or injection of false data.

The communications architecture should provide a secure pathway for grid communications. Security and privacy are very sensitive concerns in grid communications systems [15]. To provide the secure pathway, it is essential to understand which devices are part of the communications architecture. A good network inventory and monitoring system can be the foundation of that understanding, provided it is regularly updated as devices are added, replaced, or removed. While it may not be possible to include devices that are not owned by the grid utility, there is still value to having such a system in place. In addition, an understanding of the devices and their expected communication patterns and paths (source/destination) is required for anomaly detection along the path. In many cases, devices or paths can be configured to control possible communication endpoints. A network monitoring system that provides continuous monitoring of the communication path and grid devices enables rapid detection and mitigation against threats. Table 2 and Figure 4 present the security requirement (scale 1 to 5) for key grid services.

There are some caveats to the selection of appropriate network monitoring systems. Those that continuously poll devices may create additional traffic on the network that could cause issues for connections with limited bandwidth. In addition, a monitoring system that can speak to all, or nearly all devices that are part of the communication path may be a challenge because of manufacturer interoperability issues. However, one that can speak to the majority of devices is still valuable to secure the communications pathway.

3.3.1. Recommendations

- Maintain and update an inventory of both grid devices and devices that are part of the communications pathway.
- Monitor and alarm the communications pathways for signs of tampering or unauthorized access, exfiltration of data or files, or injection of false data.
- Where possible, control the ability of various devices to only communicate with other needed devices. This will help keep the communications path secure.

3.4. Interoperability and Standards

An interoperable and standards-based system is a key factor in designing for the future. This interoperable design includes ensuring that older technology using the communications system is not abandoned but maintains support while also selecting new standards-based equipment that is backward-compatible with older, standardized, grid equipment. This includes factors such as open standards for communication as opposed to proprietary vendor protocols.

Within the hybrid communication architecture of a utility in a mixed vendor grid environment, RTUs enable connectivity between devices that are serially connected to the control center over an IP based routable protocol.

There are certain regulatory standards that utilities must adhere to. For example, North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards define security required for equipment within the substations and control centers, but largely exempt the communications pathways between different grid locations [16]. There are different approaches to architecting the communication architecture within a utility. These may include using equipment and applications that involve routable protocols, non-routable protocols, or a hybrid of the two. Different standards of security may apply depending on the approach to communication. Infrastructure with routable protocols tends to have exceptionally stringent requirements for compliance from regulatory bodies. On the other hand, non-routable protocols tend to have fewer compliance standards but may not be as useful for modern applications in the grid. Some utilities have resorted to a hybrid architecture in which intermediary devices such as remote terminal units (RTUs) or port servers are used between a non-routable part of the communication infrastructure and a routable portion to achieve compliance. The routable portion would facilitate communication between the RTU and a control center, although most utilities use additional security measures. The non-routable portion would consist of serial communication between the various devices of the grid, such as meters, and the RTU. Other options used are internal routable connections in substation LANs and serial connections to the communications system.

In terms of interoperability, many devices of different manufacturers can communicate with one another if they use the same communication protocols. However, some manufacturers add additional features to the protocols, meaning that if their devices are on a given network, they would be able to use those features in the communication between their devices. However, if devices of other manufacturers are added, these other devices will not have the benefit of these added features. Therefore, when designing a network with a variety of devices, it is important to have them adhere to the standard protocol for them to be interoperable. Adhering to standard protocols is necessary but not sufficient. Testing and additional configuration work are often needed, especially for communication devices with different manufacturers.

3.4.1. Recommendations

- Adopt open standards and widely accepted communication protocols like DNP3, Modbus, and IEC 61850 to integrate different devices in the grid. This will reduce vendor dependency and make the system more flexible to handle new and legacy technologies.
- Backward compatibility to avoid major overhauling of the system and offer a graceful upgrade path.
- Use hybrid communications architectures with a mixture of both routable and non-routable protocols to balance modern, scalable communication against the continued utilization of existing infrastructures.
- Keep protocol implementations updated for compliance with evolving standards and for compatibility with new devices and applications that may be introduced.

3.5. Performance and Scalability

As mentioned in the second deep-dive white paper [6], matching QoS requirements to grid services and to the grid architecture is critical to maintaining performance and scalability within a network and meeting different application requirements.

Distributed architecture enables local decision making and enhances grid responsiveness and security.

Maintaining performance involves ensuring a reasonable latency, throughput, and minimization of jitter as discussed in the previous white papers. Along with these metrics, we must consider security, which could work against these metrics; for example, if a network monitoring system that does polling overwhelms the throughput of the system. To meet this objective of performance, an appropriate architecture must be selected. Even with fiber connections, adding too many hops or intermediary communications equipment between end points could increase the latency. Furthermore, adopting a Network Management System (NMS) that avoids constant polling for status, such as the SNMP traps [9] is beneficial in reducing traffic and improving throughput. Table 2 and Figure 4 present the scalability requirement (scale 1 to 5) for key grid services.

A scalable communication architecture allows for the addition of new devices, systems, and technologies as the grid evolves [17]. Shifting computing and intelligence near the grid edge helps promote scalable architecture, since data processing and analysis move closer to the source, which significantly reduces the latency and bandwidth usage. Distributed intelligence architecture enables local decision-making and enhances grid responsiveness and security. The Open Field Message Bus (OpenFMB) [10] is a good example for a reference architecture with a common data model that supports distributed intelligence

use cases and grid-edge interoperability. It reduces the need for centralized control and allows management of distributed systems at the circuit level.

3.5.1. Recommendations

- Scalable Architecture: The system architecture should be scalable so that newly added nodes, sensors, and devices do not degrade its performance.
- Distributed Intelligence Architecture: Promote distributed architecture, where feasible, that supports edge-computing and local decision-making.

4. Technology Considerations

Selection of communication technologies in an architecture is governed by several factors, including QoS needs of the grid service, interoperability, and availability along with cost considerations. One technology example is satellite communications.

Technology migration roadmaps for the communications system should be considered, developed, and regularly reviewed and adjusted.

The integration of satellite communications into electric grids is especially useful in remote regions where it could be hard to set up infrastructures for terrestrial communication. Satellite systems can provide large coverage and fast deployment, enhancing grid resilience by serving areas that would otherwise have been unreachable, or too costly to install other communication technologies. This may be a good alternative for metering applications. However, in the case of very low-latency services, such as real-time grid control and protection systems, their higher latency compared to terrestrial systems may preclude the use of satellite communications. This underlines the criticality of latency in these applications; there must be due consideration paid to QoS requirements for the integration of different communications technologies into the grid. The hybrid approaches of satellite (deterministic) and terrestrial (low-latency) networks often satisfy the demanding performance expected by several grid services in operation, which is necessary for a power grid to function effectively.

Communications technologies are evolving in many cases faster than other equipment in the grid is replaced. Over time, communications technologies have moved from time-division multiplexing (TDM) to IP and Ethernet to underlying communications stacks. Equipment manufacturers in both the grid and network communication spaces incorporate these new technologies into their devices and the associated communications stacks. In our prior white paper, “Grid Communications Technologies” [7], we discussed how to balance many of these considerations when procuring new grid equipment, new communications equipment, or new services from communications providers.

Technology migration roadmaps for the communications system should be considered, developed, and regularly reviewed and adjusted with the aim to have an orderly transition from legacy equipment in a current state to the desired future state. Current and future standards for both equipment requiring communications and the associated protocols used are important to consider in developing this roadmap. Choosing the right communications architecture and technologies can make a significant difference in the transition from current grid services to future services and help control associated costs. This includes seeking technologies that can carry legacy traffic while conforming with future standards and delivering future services, while reducing the need for concurrent wholesale replacement of end equipment such as relays and meters. One example of a transitional technology used for transitioning transport is Multiprotocol Label Switching (MPLS) [18]. It is packet-based but supports legacy TDM traffic until all the end devices transition to packet-based or Ethernet-based technology.

Developing this migration path in advance can also assist in building a case for future upgrade and replacement projects for a utility, because it allows consideration of the asset life cycles of both the end equipment and the communications equipment. This can be leveraged to select the optimal replacement window for both assets and ensure that upgraded communications are in place prior to the equipment that will require those capabilities.

Forward-looking practices can also provide time to develop relationships with third party service providers or with adjacent utilities that are willing to trade facilities to increase the redundancy and resilience of their grid communications systems. In either case, this allows time to vet route redundancy and diversity to find the right balance of resiliency and cost.

5. Hybrid Architectures and Migration to a Future State

Hybrid architectures are interim platforms that provide for the integration of new technologies within the existing infrastructure.

Hybrid architectures are interim platforms that provide for the integration of new technologies within the existing infrastructure. Gradual transition is an approach that serves as a steppingstone toward amassing maximum life and value from current investments. A simple example is the RTU, whose ability to convert from one protocol to another is extremely useful (see Figure 5). While more recent equipment communicates with routable protocols, older equipment often does so via serial communication or other legacy protocols. RTUs can provide a bridge, allowing older equipment to communicate with new Supervisory Control and Data Acquisition (SCADA) masters. This is just one reason why RTUs play such an important role, not only in today's grids but also in tomorrow’s grids. Another example is the MPLS [18], which is a networking technology that uses labels to route traffic over a wide area network (WAN). It supports packets of various network protocols and supports a range of access

technologies, including T1/E1, ATM (Asynchronous Transfer Mode), Frame Relay, and DSL (Digital Subscriber Line).

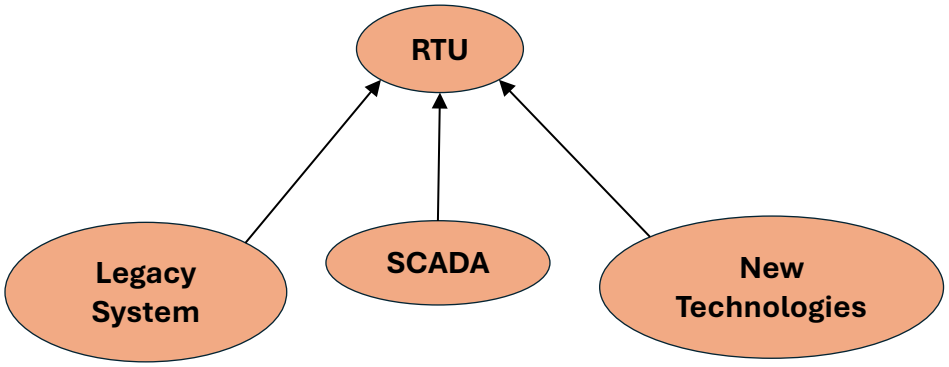

Figure 5. An example of a hybrid communication architecture using an RTU.

6. Progress Toward Objectives—What Can Be Done Today

Inventory and Assessment: A detailed inventory of all installed equipment should be developed, including communication protocols, capabilities, and integration points within the grid. The inventory system should be updated automatically or systematically when a device is added/removed or upgraded/modified. This inventory should be the basis of any future upgrades so that new technologies are integrated with existing systems. Also, the current devices of the inventory should be assessed to determine if they are functioning as intended.

Interoperability First: Add new devices to the system that utilize protocols that are well-established and widely supported. With these, integration will be attainable, long-term support assured, and the guarantee of interoperability available. An RTU should be added to act as the protocol translator to ensure interoperability, if a need arises to introduce a device with an uncommon or proprietary protocol.

Future-Ready: The designed architecture should consider future scalability. New technologies and communication protocols should not only be accommodated to existing systems, but also easily expandable to future technologies and protocols, introducing the least amount of disturbance in the grid infrastructure.

Training and Documentation: Adequate training of operators and engineers according to the limitations and capabilities of present and future systems is necessary. Documentation should include updating maintenance manuals such that each team member should be able to manage and troubleshoot the architecture with confidence.

7. Automatic Underfrequency Load Shedding Use Case

Automatic Underfrequency Load Shedding (UFLS) is one of many tools available to the electric utility responsible for balancing power in an area. UFLS provides a "backstop" to the grid under stressed conditions. It is used as a tool to help avoid complete system failure by reducing load during events when the grid is out of balance or has a shortage of generation [19]. The frequency of the US grid is normally 60 Hz; when there is a shortage of generation the system slows down, and the frequency begins to drop. Similarly, if there is too much generation, the frequency of the system will increase. Traditionally, with large fossil fuel generation, controlling generation was relatively easier due to having fuel available and having fewer utility owned larger systems. In a renewable inverter-based resource (IBR) generation environment this becomes more challenging as the number of generators increases considerably, ownership changes, and the wind and sun are less consistent than stored fuel. Hence, balancing a system is more challenging and previous methodologies may not be sufficient to meet today's inputs and requirements. UFLS is traditionally designed to quickly bring a system back into a stable region by dropping load. UFLS is usually accomplished by relays that will open breakers to reduce identified load, typically at the feeder level, during under frequency events. IBR generation is distributed throughout the system, and dropping feeders to reduce load may inadvertently drop critical generation as well. Hence, ULSF programs must shift from a static off-line analysis based upon load data and generation scenarios to more real-time operational process based upon more information and inputs.

We call the latter a dynamic UFLS solution, in which an appropriate communication architecture enables the use of real-time measurement data into the UFLS solution. The communication architecture needs to provide redundant paths, so even in the event of a system fault, essential system measurements, including those from IBR, are still received. Different service providers will provide a different QoS. Third party vendors can provide part of this architecture, which can generate stochastic real-time data delivery time, if no QoS guarantees are provided. This can have drastic consequences due to the delayed system measurement data from IBRs, and therefore widespread system outage.

Grid-level storage provides damping power in under and over frequency events in the dynamic UFLS solution. Power is provided to the system when underfrequency and absorbed when over frequency. Adaptive communication protocols are required in this case as well, so that critical data traffic is prioritized ensuring that control commands arrive in appropriate time to grid-level storage. Communication protocols that are not adaptive, and not able to handle fluctuating network loads may not be able to provide this QoS guarantee.

The dynamic UFLS can block breaker operation when the distribution feeder is injecting power into the grid. This prevents the disconnection of feeders that are net-generation during the underfrequency event, which would amplify the power imbalance. The architecture must be modular, so that it allows scalability and flexibility with the increasing number of IBRs and data points, guaranteeing that the control command arrives in time at the circuit breaker.

The dynamic UFLS will receive real-time measurements, process them, and send control commands. Communication architecture must be secure and robust to natural hazards, cyber and physical threats, while guaranteeing privacy of information. Real-time monitoring processes used for real-time monitoring must not introduce additional operation time; grid-edge devices with embedded data analytics can be used. Privacy of information is obtained by the architecture with end-to-end encryption. Natural hazard impacts are mitigated through separation of logical and physical networks, such as through software defined networks.

8. Conclusion

A new generation of grid communications architecture affords a structured means by which the evolving complexities of the modern electric grid can be managed. Grid utilities implementing the guidelines provided, now have a much needed resilient, secure, adaptive architecture on their side in support of grid stability and reliability; moreover, are guaranteed a footing on which they can meet these increasing demands within operations without any sacrifices in performance. Examples include features such as redundant paths of communication, modular designs, distributed intelligence, and advanced security measures.

The advanced communication architecture is, however, faced with many challenges related to implementation costs, compatibility with the existing legacy systems, and evolving natural disasters and cyber threats. These types of challenges can be resolved only through cooperation between grid utilities, communication technology providers, and regulatory bodies with an intent to develop standardized communication protocols, cost-effective products, and observing compliance with new and emerging security standards. The proposed architecture can be further refined. Tests for vulnerability can be performed

through continuous testing-validation-pilot field deployments that would build stakeholder confidence in the architecture.

Further work needs to be directed at increasing functionalities of the communication system to cater to growth in volume, hardening against natural disasters and cyber threats, and supporting more advanced applications in grid management. This work should include the potential of emerging technologies, such as artificial intelligence and machine learning, to optimize network performance and enhance predictive maintenance capability. As those areas continue to evolve, this next architecture of communication will incorporate enhancements to present grid operations and lay the foundation for innovative solutions that ensure the future of energy supply is reliable, resilient, and sustainable.

An architecture strategically implemented by communication providers and utilities will better accommodate challenges derived from the diverse mix of integrating energy resources, managing increased grid complexity, and responding to the emerging demands of a modern grid. It's also important in developing a robust energy infrastructure that can handle the next wave of technological advancements without compromising the operational integrity of the electric grid.

To assist with this effort, the SPaRC program is building a tool that will allow grid utilities to walk through some of these considerations and provide guidelines that balance the grid service with the QoS concerns and potentially available technologies.

References

[1] U.S. Department of Energy, “Communications in the Electric Grid: An Evolving Interdependent Ecosystem between the Grid and Communications Utilities,” 2023.
[2] U.S. Department of Energy, “Communications with the Grid Edge - Unlocking Options for Power System Coordination and Reliability,” 2023.
[3] U.S. Department of Energy, “Electric Power Telecommunications Interdependencies,” 2023.
[4] U.S. Department of Energy, “Secure Communications Interoperability Challenges in the Power Grid,” 2023.
[5] U.S. Department of Energy, “Latency Implications for Grid Communications,” 2024.
[6] U.S. Department of Energy, “Understanding and Managing Quality-of-Service in Grid Communications,” 2024.
[7] U.S. Department of Energy, “Grid Communications Technologies,” 2024.
[8] The White House, “Fact Sheet: President Biden Sets 2030 Greenhouse Gas Pollution Reduction Target Aimed at Creating Good-Paying Union Jobs and Securing U.S. Leadership on Clean Energy Technologies,” 2021.
[9] DSP Telecom, “The Basics of SNMP Trap Messages,” 2024. Available at: https://www.dpstele.com/snmp/trap-basics.php

[10] UCA International Users Group, “The Open Field Message Bus (OpenFMB),” Available at: https://openfmb.net/
[11] G. Gür, M. A. Bayir, and C. Ersoy, “Redundancy in Communication Networks for Smart Grids,” Journal of Network and Systems Management, vol. 24, no. 3, pp. 714-742, July 2016.
[12] F. Tariq and L. S. Dooley, “Smart Grid Communication and Networking Technologies: Recent Developments and Future Challenges,” In: Ali, A. (eds) Smart Grids. Green Energy and Technology. Springer, London, 2013. https://doi.org/10.1007/978-1-4471-5210-1_9
[13] IEEE Standards Association, IEEE 802.3-2022 Standard for Ethernet, 2022.
[14] L. Jorguseski, H. Zhang, S. Dijkstra-Soudarissanane, et al., “LTE Delay Assessment for Real-Time Management of Future Smart Grids,” Mobile Networks and Applications, vol. 24, no. 5, pp. 1742–1749, 2019.
[15] T. Chen, X. Yin, and G. Wang, “Securing Communications between Smart Grids and Real Users: Providing a Methodology Based on User Authentication,” Energy Reports, vol. 7, pp. 8042-8050, 2021.
[16] NERC CIP-002-5.1a, section 4.2.3.2 “Exemptions: The Following are Exempt from Standard CIP-002-5.1a: Cyber Assets Associated with Communication Networks and Data Communication Links between Discrete Electronic Security Perimeters.”
[17] S. Potenciano Menci, J. Le Baut, J. Matanza Domingo, G. López López, R. Cossent Arín, and M. Pio Silva, “A Novel Methodology for the Scalability Analysis of ICT Systems for Smart Grids Based on SGAM: The InteGrid Project Approach,” Energies, vol. 13, no. 15, Article 3818, 2020.
[18] Palo Alto Networks, “MPLS: What is Multiprotocol Label Switching,” 2024. Available at: https://www.paloaltonetworks.com/cyberpedia/mpls-what-is-multiprotocol-label-switching
[19] North American Electric Reliability Corporation (NERC), “Lesson Learned: Managing Underfrequency Load Shed Obligations and Service to Critical Loads during an Energy Emergency,” 2024. Available at: https://www.nerc.com/pa/rrm/ea/Lessons%20Learned%20Document%20Library/LL20220301_Managing_UFLS_Obligations_Service_Critical_Loads_during_Energy_Emergency.pdf