Functional and Architectural Considerations in Selecting DER Gateways for Secure and Scalable DER Integration

Yashar Kenarangui
Xcel Energy

Brian Waldron
Schweitzer Engineering Laboratories, Inc.

Presented at the
62nd Annual Midwest Power Systems Conference
Saint Paul, Minnesota
November 10–12, 2026

Functional and Architectural Considerations in Selecting DER Gateways for Secure and Scalable DER Integration

Yashar Kenarangui, *Xcel Energy*
Brian Waldron, *Schweitzer Engineering Laboratories, Inc.*

***Abstract*—With the install base of distributed energy resources (DERs) in the electric power grid increasing, utilities are recognizing the importance of having standardized and secure mechanisms to integrate DER sites into grid operations to achieve a wide variety of benefits and functionality. DER gateways are becoming a key component of the overall distributed energy resources management system (DERMS) architecture, enabling secure and resilient integration of DERs into utility operations. When utilities and DER site owners look for a DER gateway for a site or as a standard for their fleet, they encounter a wide range of technologies, protocols, hardware, and architectures to choose from. It can be difficult for the stakeholders to identify all the decisions necessary and the tradeoffs between the various options. This paper will identify the necessary decisions and discuss the various characteristics of each option to help inform utilities and DER site owners in their effort to execute accurate and efficient deployments. The paper focuses on three important areas utilities should consider before and during deployment to maximize efficiency: interoperability, cybersecurity, and resilient architectures.**

Ultimately, this paper shows how well-informed selections of DER gateways and aggregators—and their grid integration—empower utilities to create resilient, secure, adaptable, and future-ready DER ecosystems. By applying a systems-engineering and grid-architecture-based evaluation framework, which includes understanding the implications of each decision area, stakeholders can reduce integration risks, improve grid reliability and resilience, and confidently support the efficient deployment of DER gateways.

***Keywords*—Distributed Energy Resource, Distributed Energy Resource Gateway, Distributed Energy Resource Management System, Interoperability**

I. Introduction

The selection of a DER gateway involves more than simply choosing a protocol converter. Utilities and system operators must evaluate communications standards, cybersecurity requirements, deployment architectures, maintenance considerations, scalability needs across regions, use cases, and operational resiliency. Decisions regarding protocols—such as IEEE 1815.2-2025 *Standard Profile for Communications with Distributed Energy Resources (DERs) Using IEEE 1815 [Distributed Network Protocol (DNP3)]* and IEEE 2030.5-2018 *Standard for Smart Energy Profile Application Protocol*—influence interoperability and future expansion, while deployment choices between edge and server-based implementations affect system performance, bandwidth utilization, and operational continuity. At the same time, evolving cybersecurity threats require organizations to carefully assess authentication and authorization methods, patch-management practices, and device hardening strategies.

This paper examines the functional and architectural considerations involved in selecting DER gateways for modern grid applications, with a focus on communications protocols, cybersecurity practices, and deployment architectures. The paper argues that successful DER integration requires a balanced evaluation of scalability, security, operational resiliency, and organizational capabilities, rather than reliance on any single technology or deployment model.

II. DER Gateway Protocols

When discussing DERMS and edge devices for DER applications, several protocols are commonly considered for integration with centralized systems. The protocols most frequently discussed are IEEE 1815-2012 *Standard for Electric Power Systems Communications-Distributed Network Protocol (DNP3)* with the IEEE 1815.2 extension, IEEE 2030.5 Smart Energy Profile 2.0, and Open Automated Demand Response (OpenADR). Depending on the gateway application, one or more of these protocols may be considered. No protocol is covered in depth in this paper. The purpose of this paper is to provide a high-level introduction to these protocols, highlight their primary feature sets, and help system implementers identify which options best align with their requirements.

A. IEEE 1815

The IEEE 1815 DNP3 was originally developed in the early 1990s to address several industry challenges at that time [1]:

- Interoperability between utility devices from different vendors
- Increased reliability over low-bandwidth and noisy communications channels
- Support for both simple and complex device data models
- Improved alarm reporting

The protocol successfully addressed these challenges and became the de facto standard for centralized utility SCADA systems. In 2010, it became an IEEE standard. Today, DNP3 serves as a common method of transporting information over serial and Ethernet-based networks, across a wide range of applications. For intelligent electronic devices deployed in electric utility systems, DNP3 is a commonly supported

protocol, making integration with field devices and utility SCADA systems relatively straightforward.

Released in 2026, IEEE 1815.2 does not change the DNP3 protocol. Rather, it overlays a data model and set of functional concepts transported through DNP3 for DER integration. It focuses on the following:

- A standardized data model that enables a consistent data map across DER from multiple vendors [2]
- Interoperability protocol supported using IEEE 1547-2018 Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces [2]
- Mapping of the IEC 61850-7-420 DER data model into the DNP3 data model [2]
- A standard format for communicating schedules to devices [2]
- A standard format for distributing grid-support curves to the DER [2]
- Mechanisms for extending the data model to support manufacturer-specific information [2]

Using DNP3 provides the benefit of integration with existing SCADA systems while also supporting schedules for DER management, demand-response applications, and standardized data models that help scale deployments across multiple vendors. These capabilities align with the requirements of modern control systems supporting large-scale DER integration.

B. IEEE 2030.5 Smart Energy Profile Application Protocol

IEEE 2030.5 was specifically designed to integrate DER into a control system. Its primary features include:

- Built-in encryption and device identification with access control lists based on certificate verification [3]
- REST APIs and data-transfer mechanisms optimized for low-bandwidth applications [3]
- Device discovery and real-time device registration
- Scheduling of DER actions [3]
- A standardized data model with support for manufacturer-specific extensions [3]
- Maintenance of device and site identification through multiple layers of aggregation [3]

Although the first revision of IEEE 2030.5 was published in 2013, it has not yet achieved widespread adoption in production utility systems. It is deployed in some utility DERMS applications but represents a relatively small share of edge-to-centralized-system communications compared to DNP3. The flexibility of IEEE 2030.5 makes it well suited for utility-scale DER deployments (sites or inverters greater than 1 MW), commercial-scale systems (50 kW to 1 MW), and residential-scale systems (less than 50 kW). Although individual residential devices are relatively small, these devices are deployed in aggregation, with counts reaching hundreds of thousands or even millions of devices. Built-in support for identification, access control, cybersecurity, runtime registration, and scalability makes large-scale integration significantly more manageable.

C. Other Protocols

Several other protocols are discussed in relation to DER integration. SunSpec Modbus is a common example and is typically focused on communications between inverters and gateways or power plant controllers rather than communications with centralized systems. As such, it is not discussed in this paper. OpenADR is another protocol commonly considered for centralized communications with DERs and gateways. However, OpenADR use cases are primarily focused on commercial and residential devices that are unlikely to be directly managed and controlled with utility-scale DERMS or distribution management systems [4]. This paper does not cover these options in detail, nor does it cover specialized protocols, such as the Open Charge Point Protocol for electric vehicle charging.

D. Considerations in Picking a Protocol for DER Gateways

There are two primary protocol options for integrating DER gateways, whether operating as a single DER or as an aggregator: IEEE 1815.2 (DNP3) and IEEE 2030.5. Both protocols attempt to achieve similar goals through substantially different mechanisms. When selecting between the two protocols, organizations should consider the following factors and their impact on operational requirements.

1) System Integration and Industry Maturity

IEEE 1815.2 does not introduce new DNP3 objects or message types [2], meaning that existing gateway products may be adapted through firmware or software updates. Existing devices may require only firmware or software updates to become compatible. Adding additional devices to a system introduces costs to the organization associated with evaluation, maintenance, and personnel training. IEEE 1815.2 is likely to have a shorter adoption timeline and lower integration cost than IEEE 2030.5, which may require entirely new gateway products and additional staff training. While IEEE 2030.5 offers significant flexibility, that flexibility may also create additional interoperability challenges between products, potentially increasing deployment efforts and cost.

2) Data Model

The way information is organized within a communications model can affect how external applications interact with data, how communications issues are diagnosed and troubleshot, and how information is exchanged between systems. IEEE 2030.5 offers both a standardized and extensible data model, allowing implementers flexibility in defining their approach. Implementers also have the ability to create descriptive names for data objects [3]. IEEE 1815.2 uses index-based representations, and some structured information may be distributed across multiple indexes [2], making the organization less intuitive than the IEEE 2030.5 model.

3) Scale of Deployment

IEEE 2030.5 includes features that support large-scale deployments more effectively than IEEE 1815.2. For organizations managing tens or hundreds of devices, these capabilities may provide limited additional value. However, as deployments expand into the thousands, features such as

persistent unique identifiers, support for multiple levels of aggregation, and protocol-level access control mechanisms simplify the management of large systems and improve scalability.

III. Cybersecurity

A. Operating System and Patch Management

Evaluating the operating system and its patch-management approach has a direct impact on maintaining a DER gateway. Some DER gateways are made of entirely manufacturer-managed software (operating system plus DER gateway), while others require the implementer to provide and maintain the operating system, with the manufacturer only supplying the DER gateway application. While a DER gateway that can be installed on a general-purpose operating system offers additional flexibility, it also creates significantly more maintenance effort and risk for the operating organization, which becomes responsible for maintaining current security patches. If a DER gateway manufacturer provides all software updates, it is important that clear revision notes accompany each release. Organizations should recognize vendors that responsibly disclose cybersecurity issues in their release notes. Vendors that report no cybersecurity-related fixes over multiple releases may not be fully disclosing all security-related changes.

B. Authorized Access and Permissions

A DER gateway is likely to be used by multiple organizations. A utility, a DER site owner, and an operations organization may all require access to the DER gateway for monitoring and information retrieval. Personnel and needs within these organizations are likely to change over time, making individual local accounts for all potential users an impractical approach. The organization that owns and manages the DER gateway configuration should use a centralized authentication system to manage user access and permissions. Common centralized authentication technologies include Lightweight Directory Access Protocol, RADIUS, and single sign-in.

DER gateways should support customizable role-based access controls that allow organizations to tailor access to various system resources. Organizations can benefit from more granular permissions than simple read/write access. For example, a user may be permitted to view system logs and real-time protocol data while being restricted from viewing network interface configurations or authentication settings. Selecting a DER gateway with strong authentication capabilities can reduce maintenance by enabling centralized management across many devices. In addition, a flexible permissions model improves security by limiting access to need-to-know information and reducing exposure of unintended information.

In addition to controlling user access, a DER gateway should be capable of securely establishing its identity with other systems and verifying the identities of devices with which it communicates. A common approach is to use a Public Key Infrastructure. This paper does not discuss the technical details of certificates or how they provide unique identification, but DER gateways will increasingly require these capabilities. It is important that DER gateways provide flexibility in certificate lifecycle management, including configurable certificate lifespans and the ability to generate certificates locally so that private keys never leave the device. Some organizations may prefer to generate their own public and private key pairs and upload them to the device. Industry trends continue toward shorter certificate lifespans, and DER gateways that support automated certificate renewal can improve security while reducing manual maintenance effort.

C. Cybersecurity Hardening

The industry term device hardening, at its basic principle, refers to the process of disabling unused features and services. This commonly includes disabling unused ports, closing network services with listening ports, and turning off unnecessary functionality. For example, a device may enable Network Time Protocol (NTP) time synchronization by default, which listens on UDP port 123, while the DER gateway may instead use IEEE 1815 or IRIG-B time synchronization. In that case, the NTP service may represent an unnecessary open network port.

Although many hardening guides and checklists are available, it is generally preferable for DER gateways to follow a whitelisting approach rather than a blacklisting approach. A product that requires features to be explicitly enabled before use is typically more secure than one that enables numerous features by default and relies on implementers to disable unused functionality. Implementers may be experts in power-system technologies but may not fully understand every network service or communications port that should be reviewed as part of the hardening process.

Selecting a DER gateway that clearly documents its recommended hardening process and requires individual features to be explicitly enabled demonstrates a strong focus on secure deployment from the outset.

IV. DER Gateway Architectures

A. Edge Deployments

DER gateways can be deployed as small physical computing devices at the DER site, e.g., located within a DER cabinet or near the physical point of common coupling to the grid. Edge deployments provide maximum flexibility for individual site behavior when interfacing with centralized systems, e.g., utility DERMS [5]. In addition to protocol-conversion capabilities, an edge deployment can continue to provide functionality when communications with the DER site are lost. Most commonly, this includes the following:

1) Buffered Data

An edge gateway can continue collecting measurements from the DER site and buffer this information with accurate timestamps. When communications are restored, the gateway can transmit the buffered data to the server with the appropriate timestamps. This prevents gaps in the historical records of the centralized system. IEEE 1547 does not require DERs to buffer data, so this capability is dependent on manufacturer

implementation. Protocol gateways have long served as an industry-standard solution for data buffering [5].

2) Default Controls and Fail-Safe

An edge gateway can modify DER dispatch when communications with the centralized system are lost. Depending on the operational context, organizations may require different DER behaviors during communications outages. For example, organizations may choose to revert to no import or export, continue operating at the last received dispatch value based on time of day, or modify dispatch only if communications are not restored within a configurable period. Gateway products commonly include logic engines capable of processing multiple state machines based on operating conditions. This flexibility during communications outages is a unique capability enabled by edge-deployed hardware.

3) Reduce Communications Bandwidth

Many DERs do not support protocols that optimize bandwidth efficiently. For example, many devices use Modbus, which returns current status information during every polling cycle. An edge gateway can use available bandwidth over a local network or direct communications link and transmit only the required changes to the centralized system. This reduces bandwidth consumption between the gateway and the central system. Because many DERs are not connected through organization-owned wide-area networks, reducing bandwidth usage can lower overall operating costs [5].

4) Enforcement of Adherence to Management System Commands and Operational Curves

The DER gateway continuously monitors DER performance at the point of common coupling and verifies compliance with all active management system commands, dispatch instructions, and prescribed operational curves, including active power, reactive power, power factor, volt-var, volt-watt, frequency-watt, and other grid-support functions. Measured DER response is continuously compared against commanded operating setpoints and expected response characteristics to ensure execution within the required accuracy, magnitude, and response-time tolerances defined by applicable interconnection agreements, utility operating requirements, or regulatory standards.

The DER gateway maintains a compliance monitoring and event logging function that records command issuance, DER response, deviations, and communications anomalies. When non-compliance, command execution errors, or performance deviations exceed established thresholds, the gateway generates alarms, logs the event for auditability, and, where authorized, initiates corrective actions to restore compliance. Corrective actions may include retransmitting commands, adjusting control signals, transitioning the DER to an approved fallback operating mode, disconnecting DER from the grid or notifying the management system and utility operator of the observed violation.

This functionality ensures reliable execution of utility dispatch instructions, adherence to required operating envelopes, and continuous verification that DER is operating in accordance with grid reliability, safety, and interconnection requirements.

V. Server Deployment

DER gateways can be virtualized and deployed on server hardware using a wide range of segmentation and aggregation strategies. This paper does not evaluate or consider design choices regarding how many DERs are placed within a single virtualized gateway application. Instead, it examines the options, benefits, and challenges associated with deploying DER gateway applications on centralized hardware, including both on-premises and cloud environments. It is important to note that the characterizations about on-premises and cloud environments are generalizations taken from a wide range of application deployments in both IT and OT applications. These characteristics will not necessarily be true in all cases.

While cloud-based application deployments are not an emerging solution, the use of cloud deployments to assist with monitoring and data aggregation into SCADA and DERMS type applications is a new emerging solution in the electric utility industry that some utilities are starting to deploy or consider more frequently in their system architectures. The use of cloud deployment for any type of control is out of scope of this paper, as the considerations of this paper are focused on the monitoring and data aggregation architectures that cloud infrastructure may apply.

A. Virtual Application Considerations

Virtualized DER gateway applications may take several forms compared to hardware-based edge DER gateways. Edge gateways are typically delivered as embedded firmware, where the application and operating system are managed through a single image with documentation associated with each release. Virtualized DER gateways may be provided as applications installed on an operating system that the organization deploys and maintains—as containers deployed on platforms, such as Kubernetes, or as virtual machines deployed on a hypervisor [6]. In these scenarios, system maintenance is unlikely to be as straightforward as with an edge DER gateway product, where upgrades may involve a single file and well-defined instructions. Organizations may need to evaluate operating system patches and updates for compatibility with the DER gateway application or maintain staff with expertise in container deployment and administration [6].

Regardless of whether server-based or edge-hardware deployments are selected, organizations should expect to perform software updates over time. Server-based deployments may require less organizational logistic effort, because they eliminate physical travel and are often supported by automated infrastructure for updating virtual machines and containers [7]. Manufacturers of edge devices may or may not provide infrastructure and software tools for remotely updating large numbers of field devices. Depending on the DER gateway manufacturer and the internal engineering expertise of the organization, either deployment model may offer advantages in maintenance effort and operational efficiency.

Server-based deployments provide substantial flexibility in how DER gateways are deployed and what resources are allocated to them. Configurations can dynamically scale to meet changing processing demands and may include redundancy and other availability features. However, these benefits come with increased configuration and operational complexity [7]. The required skill set differs from that of most power-system engineers. Many large organizations employ personnel with this expertise and can manage these complexities effectively. Organizations without this expertise may face increased risk of poor design and implementation decisions or may need to outsource the work to consultants who may not fully understand the DER gateway requirements of the organization [8].

B. On-Premises Deployment

1) Economics

On-premises deployments require organizations to purchase and maintain storage, server, networking, and security infrastructure. The initial capital investment will generally exceed the upfront cost of cloud deployment. However, depending on resource consumption, on-premises infrastructure may be more economical over the long term [8]. Calculating this comparison can be difficult because on-premises costs include hardware acquisition, engineering and configuration, and ongoing maintenance of operating systems, hypervisors, and security controls. Long-term operating costs are also generally more predictable than cloud deployments, where organizations are dependent on service pricing that may fluctuate over time [8].

2) Performance and Latency

On-premises deployments typically co-locate communicating systems within a local area network, reducing latency because communications remain within a private network infrastructure and avoid additional public-network traversal and security layers. When equipment is distributed across multiple locations, organizations have greater flexibility and autonomy in determining performance characteristics. The latency associated with communications with individual DERs should be evaluated as part of the deployment design [7].

3) Sovereignty and Security

Using an on-premises deployment does not inherently make DER gateway applications more secure than cloud-based deployments. However, specific design and implementation choices can result in significantly higher security. For example, communications among DERs, gateway applications, and centralized systems can be isolated from other data exchanges and public internet connectivity. This paper does not evaluate all cybersecurity options available for cloud and on-premises deployments, but it recognizes that some on-premises architectures may provide fundamentally stronger security boundaries [7].

An on-premises deployment provides organizations with complete control over hardware selection, network architecture, firewall configuration, hypervisor technologies, and related infrastructure decisions. Depending on the expertise of the organization, this flexibility may be either an advantage or a disadvantage compared to cloud deployments, where many infrastructure decisions and maintenance activities are managed by the service provider. This paper does not discuss in detail the division of responsibilities between cloud and on-premises deployment models [7].

While the most common DER gateway use cases do not call for direct control algorithms, if an organization wanted to implement a control algorithm, the additional data access management and security design would be simpler to implement in an on-premises deployment. Any type of control algorithm deployment on-cloud should undergo additional evaluation and consideration [7].

C. Cloud

1) Deployment Speed and Scalability

Cloud-based deployments can significantly accelerate implementation of DER gateway applications [7], depending on the existing infrastructure of the organization. Most cloud providers offer near-real-time provisioning of new resources [7], whereas on-premises deployments may require ordering, receiving, and installing new equipment. Many cloud services also provide elastic resource allocation [7]. For example, a DER gateway application may consume a baseline level of resources during normal operation. During a system event that significantly increases communications or processing requirements, cloud infrastructure can automatically expand available resources and later reduce them when demand returns to normal [8].

Another significant advantage of cloud-based deployments is the ability to streamline software version management [8] and accelerate the delivery of new DER gateway capabilities. As DER technologies, interoperability standards, utility operating practices, and regulatory requirements continue to evolve, cloud-hosted platforms provide an efficient mechanism for deploying feature enhancements, protocol support, analytics capabilities, control functions, cybersecurity improvements, and other software updates across the entire deployment fleet. Centralized version control helps maintain software consistency, reduces operational overhead associated with update distribution, and enables organizations to rapidly adopt new functionality while ensuring deployed systems remain aligned with current business and operational needs [6].

While similar capabilities are possible with on-premises deployments, they typically require additional configuration and operational complexity.

2) Economic Considerations

Cloud deployments use a substantially different cost model than on-premises deployments. Most cloud expenses are operational expenditures that recur over time. This often reduces initial deployment costs. However, depending on resource consumption and service pricing, operational costs may eventually exceed the capital and operational costs associated with an on-premises solution. On-premises deployments generally include both capital and operational expenditures [9].

While cloud costs are frequently viewed as operating expenses, the distinction is not always absolute. Depending on applicable accounting guidance, regulatory treatment, and organizational capitalization policies, certain implementation, configuration, integration, software development, or migration activities may be eligible for capitalization. In some cases, cloud-based solutions may also be incorporated into broader capital projects, enabling a portion of the overall investment to be treated as a capital expenditure. As a result, the financial treatment of cloud deployments should be evaluated on a case-by-case basis [9].

3) Infrastructure Management

Cloud deployments eliminate many of the hardware management responsibilities associated with on-premises infrastructure. This includes physical facilities, power, cooling, wiring, cabling, and server hardware management. Cloud providers also commonly offer deployment options across multiple geographic regions, automated hardware redundancy, and resilient computing resources, often with minimal configuration effort required from the end user [7].

While cloud eliminates many hardware infrastructure management concerns, it adds some additional complexity in the networking and cybersecurity engineering that is necessary to incorporate the aggregated data at the cloud deployment back to a centralized system that is unlikely to be deployed in the same cloud environment. The centralized system is likely to be an on-premises solution that will require additional engineering to securely move the data between the two different deployments [7].

VI. Decision Considerations for Cloud vs. On-Premise Deployment

Reasons for choosing an on-premises deployment often include the following priorities:

- Security and data access are high priorities [7]
- Internal applications require low latency (for example, a DERMS accessing information from a DER gateway) [6]
- The organization has staff with the skills required to operate a data center
- Computational requirements are known and predictable over an extended period [7]
- Independence and autonomy in system design and implementation are high priorities [7]

Reasons for choosing a cloud deployment often include the following considerations:

- Capital budget is limited [9]
- Computational resources are required across several geographic locations [8]
- Rapid deployment expansion is a priority [8]
- The organization has limited staff available to operate a data center

If an organization decides to deploy DER gateways on servers, the optimal approach will vary based on staff expertise, service territory size, and the types of DERs being aggregated. For example, a DER gateway that aggregates one hundred battery energy storage systems, ranging from 2 MW to 20 MW, may be better suited to an on-premise deployment. These assets typically require greater data accessibility, enhanced security, and closer integration with utility distribution management systems and DERMS platforms. In contrast, DER gateways that aggregate tens of thousands of thermostats, water heaters, and electric vehicle chargers may be better suited to cloud deployment, because these assets are distributed across broad geographic areas and can benefit from geographically distributed communications infrastructures. These residential and consumer devices may also experience greater variability in availability, causing computational and communications requirements to fluctuate over time. Cloud deployments are often better suited to accommodate these changing workloads. [8] If a DER gateway application has any consideration of control algorithms, then additional caution should be taken when evaluating data access, authentication, and cybersecurity posture with cloud solutions. This paper does not explore the additional evaluations for cloud deployments that may be involved with control algorithms. Depending on DER type, location, and security or data-access requirements, either cloud or on-premises deployments may be the preferred solution.

VII. Edge vs. Server Deployment

When considering the decision of edge or server deployment here are some common reasons to select edge deployments seen as advantages across the general industry. It is important to remember that these characterizations may not be true in all scenarios but are generally typical industry experiences:

- Continued operation and design flexibility during communications outages [5]
- Reduced bandwidth costs [5]
- Simpler software management (the DER gateway may require only a single embedded firmware image)

Common challenges with edge deployments:

- Logistical challenges associated with software updates, which may require physical site visits or non-automated update processes
- Asset Management challenges associated with keeping track of hundreds or thousands of devices organized with separate settings, serial numbers, and software versions

Common reasons to select server deployments:

- Simplified software-update logistics through automated data-center management tools [7]
- Greater flexibility in deploying applications for redundancy and resource allocation [7]

Common challenges with server deployments:

- Requires personnel with expertise in virtualization platforms, software maintenance, and cybersecurity
- Increased bandwidth consumption at remote sites [5]
- Reduced DER site control and coordination during communications outages

The selection of edge versus server deployment for DER gateways will generally depend on organizational expertise and

site requirements. A smaller organization without a large IT staff experienced in virtualized environments may choose edge DER gateways, because of their relative simplicity, even if logistical maintenance costs are higher. An organization may also choose edge gateways for DER sites larger than 500 kW, where site-level operational impacts on the grid are more significant. In these cases, local gateway logic that can continue operating during communications outages may be more important than other considerations. For smaller DER sites, server-based deployments may provide advantages by eliminating the need for individual hardware installations and reducing the associated long-term maintenance challenges.

VIII. Selection Criteria for DER Gateway Considerations

This paper covered high-level considerations for DER gateways across three primary categories:

- Protocol integration
- Cybersecurity
- Deployment architecture

Across these categories, several key aspects of DER integration were identified to help power-system engineers make informed tradeoffs and decisions when selecting DER gateways.

A. Scalability

If an organization needs to incorporate thousands or tens of thousands of DERs, certain technologies within these categories offer clear advantages. IEEE 2030.5 provides strong [3] mechanisms for identity management and scalable integration. Server-based deployments will likely be more efficient for initial deployment and may reduce long-term maintenance costs. [5] However, if an organization prioritizes security, data access, and control resiliency, because of the scale and impact of DERs, edge DER gateways may be a better choice. In those cases, both IEEE 1815/1815.2 and IEEE 2030.5 can be appropriate options, depending on the centralized systems with which the assets primarily interact.

B. Security and Sovereignty

The electric grid is critical infrastructure and often justifies additional security measures and independent communications systems to improve control-system reliability. Identifying the required level of security and sovereignty for the DERs under consideration will help determine the most suitable attributes within each category. When security and sovereignty are high priorities, either edge-hardware deployments or on-premises deployments are likely to be preferred. Selecting a manufacturer that emphasizes security features and maintains a strong cybersecurity posture may justify additional expense for the DER gateway solution.

C. Communications Network Infrastructure

If an organization pays for bandwidth provided by a telecommunications service provider, optimizing data transmission between DERs and a DER gateway may become a higher priority. This may lead to the selection of an edge DER gateway, depending on the natively supported DER protocols, to better manage data-transfer volumes and make more intelligent decisions regarding when data should be transmitted.

IX. Conclusion

DER gateways play a foundational role in enabling secure, reliable, and scalable integration of distributed energy resources into grid operations. As discussed throughout this paper, protocol selection, cybersecurity posture, and deployment architecture each present distinct advantages and tradeoffs that must be evaluated within the context of the operational objectives of the communications infrastructure and the workforce expertise of an organization. No single gateway approach is universally optimal; instead, the most effective solution is one that aligns technical capabilities with the specific requirements of the DER portfolio being managed.

As DER adoption continues to accelerate, future developments will likely place greater emphasis on standardized interoperability, automated cybersecurity management, and highly scalable architectures capable of supporting millions of connected utility-owned and end-user devices. Organizations that establish thoughtful DER gateway selection criteria today will be better positioned to leverage emerging grid services, enable flexible interconnections, improve operational efficiencies, and support the reliable transition to a more distributed, resilient, and dynamic power system.

X. References

[1] IEEE 1815-2012, *IEEE Standard for Electric Power Systems Communications-Distributed Network Protocol (DNP3)*.

[2] IEEE 1815.2-2025, *IEEE Standard Profile for Communications with Distributed Energy Resources (DERs) Using IEEE Std 1815(TM) [Distributed Network Protocol (DNP3)].*

[3] IEEE 2030.5–2025, *IEEE Standard for Smart Energy Profile Application Protocol.*

[4] 4I. G. Damousis, E. Bazouki, D. Agtzidis, D. Tzovaras, P. Barrachina, and R. Perez de Zabalza, "Openadr-based information and communication infrastructure for implicit demand response scenarios," proceedings of The 12th Mediterranean Conference on Power Generation, Transmission, Distribution, and Energy Conversion, Online Conference, November 2020, pp. 276-282.

[5] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge Computing: Vision and Challenges," *IEEE Internet of Things Journal*, Vol. 3, No. 5, 2016.

[6] M. Souppaya, and K. Scarfone, *Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology*, NIST SP 800-40 Rev. 4, National Institute of Standards and Technology, 2022.

[7] S. Zhang,, A. Pandey, X. Luo, M. Powell, R. Banerji, A, Parchure, L. Fan, and E. Luzcando, "Practical Adoption of Cloud Computing in Power Systems: Drivers, Challenges, Guidance, and Real-world Use Cases," IEEE Transactions on Smart Grid, 2022.

[8] X. Luo, S. Zhang, and E. Litvinov, "Practical Design and Implementation of Cloud Computing for Power System Planning Studies," IEEE Transactions on Smart Grid, 2018.

[9] E. Walker, "The Real Cost of a CPU Hour," *Computer*, vol. 42, no. 4, pp. 35-41, April 2009.

XI. Biographies

Yashar Kenarangui is a Senior Principal Engineer at Xcel Energy and a technical leader in grid modernization efforts. With more than 15 years of experience in power systems engineering and grid architecture, he has led the design and deployment of mission-critical microgrids, DERMS, and other advanced grid technologies that enable the reliable and resilient integration of

distributed energy resources into utility operations. His work focuses on grid modernization strategy, mission-critical microgrids, and the development of next-generation utility architectures. Yashar holds a BS and MS in Electrical Engineering from the University of Texas at Arlington and the University of Wisconsin-Madison, respectively.

Brian Waldron is a senior automation engineer with Schweitzer Engineering Laboratories, Inc. (SEL). He has over a decade of experience in designing and troubleshooting automation systems, communications networks, and distributed energy resources (DERs) control systems. He has authored several technical papers, application guides, and teaching presentations focused on integrating automation products. Brian graduated from Gonzaga University with a BS degree in electrical engineering.

© 2026 by Xcel Energy and
Schweitzer Engineering Laboratories, Inc.
All rights reserved.
20261021 • TP7285-01