EPRI ELECTRIC POWER RESEARCH INSTITUTE

SYSTEMS INTEROPERABILITY AND CYBER SECURITY

An EPRI FO-2222 Phase 1 Collaborative Report

- Wholesale Market Operations & Design
- Distribution Reliability & Safety
- Transmission Operations & Planning
- Transmission, Distribution & Aggregator Coordination
- Information, Communication, Cyber Security
- Customer Technologies & Retail Programs

Bringing together key stakeholders to ensure the reliable and economic participation of distributed energy resources in wholesale electricity markets and establishing a research and development roadmap

July 2021

Introduction and Background

The Federal Energy Regulatory Commission's (FERC's) Order No. 2222 (FO2222) is an important step to enable the participation of distributed energy resources (DER) in the wholesale electricity markets.[1] The Order 2222 facilitates the participation of DERs in the energy, capacity, and ancillary service markets that are managed by the regional transmission operators organizations (RTOs) and independent system operators (ISOs). Through Order 2222 and the efforts across ISOs/RTOs, distribution utilities, and others; there is a need to ensure grid reliability and resiliency while providing additional value streams to DERs and customers through their participation in the wholesale markets. FERC defines DERs,[2] as the following:

> *Any resource located on the distribution system, any subsystem thereof or behind a customer meter. This includes resources that are in front or behind the customer meter, energy storage resources, intermittent generation, distributed generation, demand response, energy efficiency, thermal storage, electric vehicle, and their supply equipment as long as such a resource is located on the distribution system, any subsystem thereof or behind a customer meter.*

With emphasis on DER technologies that include demand response (DR) of manageable loads, distributed generation (DG) including both small thermal resources and variable renewables, energy storage, and electric vehicles (EVs), the purpose of this study is to highlight the role of a crosscutting topic – secure and interoperable data communications and information management. The study reviews and provides high-level recommendations for metering, data management, telemetry, interoperability and cybersecurity requirements, and how associated challenges and solutions may present themselves from active DER participation in wholesale markets. The primary audience for the study is (ISOs/RTOs), transmission utilities, distribution utilities, and DER aggregators. In addition, the study recommendations could be relevant for state and federal regulators and customers (including owners and operators of DERs).

The scope of the study is limited to DER interactions between the smart grid domains, actors and information exchanges pertinent to Order 2222. These interactions are shown in Figure 1, Reference communications architecture. The interactions show the information and data communication pathways between the key actors within the five smart grid domains—DERs, ISO/RTO, DERA, and Market Operations. Considering that the distribution utilities play a key role in overall DER customer relationships and distribution system reliability, they're included in the study analyses. The domain, Market Operations, is included separately (and not under each RTO, TSO and DSO domains) to align with the United States' national Smart Grid Framework developed by the National Institute of Technology (NIST).[3] The focus is on the data and information exchange among the domains and actors, as emphasized by the NIST Smart Grid Framework, and not on the power flow across all the smart grid domains and actors. It should be noted that the reference architecture does not consider specific regional implementations that may have a unique actor interfacing between ISO and market participant such as

Table of Contents

[1] Federal Energy Regulatory Commission, "Participation of Distributed Energy Resource Aggregations in Markets Operated by Regional Transmission Organizations and Independent System Operators," Order No. 2222, issued September 17, 2020. https://www.ferc.gov/sites/default/files/2020-09/E-1_0.pdf.

[2] *Distributed Energy Resource Aggregation Participation in Organized Markets: Federal Energy Regulatory Commission Order 2222 Summary, Current State-of-the-Art, and Further Research Needs*. EPRI, Palo Alto, CA: 2021. 3002020586.

[3] Gopstein A, Nguyen G, O'Fallon C, Hastings N, and Wollman D; NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 4.0, NIST Special Publication 1108r4, National Institute of Standards and Technology (NIST), February 2021. https://www.nist.gov/el/smart-grid/smart-grid-framework.

a scheduling coordinator in the California independent system operator (CAISO) territory to coordinate operations.[4] The CAISO requires DERAs retain the services of a certified scheduling coordinator (SC) to participate in the ISO electricity markets. The role of SCs is to directly bid or self-schedule DER aggregation participation in the wholesale markets and manage the settlement process. In the reference architecture, such a role is part of the Market Operations domain.

In Figure 1, the Market Operations domain is indicative of the retail and wholesale electricity markets. The smart grid architecture represents DER participation in retail and/or wholesale markets in reference to a "total TSO" or a "hybrid DSO" conceptual model.[5] Under a total TSO model, a TSO "optimizes the entire electric power system including the distribution system and dispatch coordination of all DER services and schedules." Under the hybrid DSO model, the TSO "optimizes the bulk power system, including dispatch of all wholesale DER services, but has no visibility to the distribution system." The DSO "optimizes the distribution system, including dispatch of all distribution DER services and coordinates with TSO on all DER dispatch." The focus of metering and telemetry in Order 2222 is between the ISO/RTO, and Aggregator of DER (red arrows in Figure 1). The reference communications architecture includes the domain for regions with DSO-managed DER markets with participation by the underlying DER customers (black arrows in Figure 1).

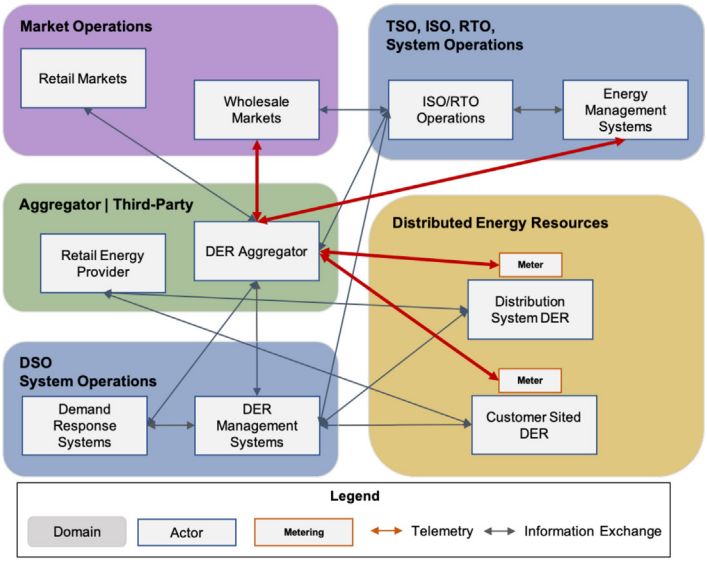

Figure 1. Reference communications architecture

It is important to highlight that outside the information and communication requirements, the coordination of ISO/RTO, DER aggregators and distribution utilities (DUs) is an important topic. Reviewing the challenges or proposing solutions for coordination between the DU and the Order 2222 domains is covered in a separate workstream of the project. While Figure 2 shows the reference communications architecture relevant to the Order 2222 scope, a high-level Smart Grid Architecture Model (SGAM) shows the different layers that are necessary for full interoperability of communications. Highlighting the scope, the coordination framework focuses on the business and function layers, while this study focuses on the information and communication layers (information model and protocol), including the cyber security concerns, specifically confidentiality, integrity, and availability issues, associated with both. It's the combination of these layers, taken as a whole, that will lead to interoperability across the domains and the actors.

The recommendations relevant to aggregator requirements from Order 2222 are provided. The specific rules from O2222 must require that:

- Each DERA provide "a list of the distributed energy resources" used in the aggregation with information related to individual DERs, its resource capacity, location, and operating limits.
- DERAs maintain aggregate settlement data for the DER.
- DERAs maintain data of each resource in the DER aggregation for a duration, as required by the ISOs/RTOs for the purpose of auditing.

[4] California Independent System Operator (CAISO). "Becoming a Scheduling Coordinator." http://www.caiso.com/participate/Pages/BecomeSchedulingCoordinator/Default.aspx. Accessed May 2021.

[5] Newport Consortium; Coordination of Distributed Energy Resources; International System Architecture Insights for Future Market Design. May 2018.

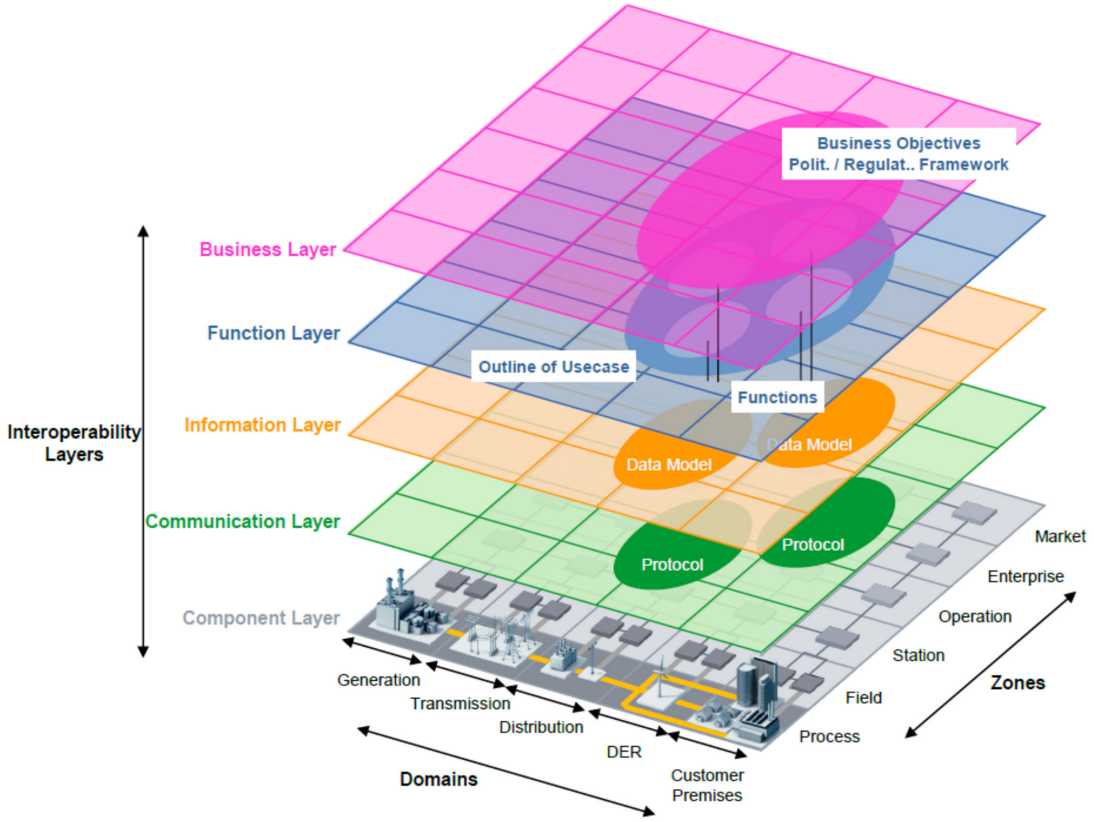

Figure 2. Smart Grid Architecture Model

The Order 2222 recommends that the DERAs must submit to the ISO/RTO the physical parameters that are *"not already represented in general registration requirements or bidding parameters applicable to DER aggregations"* and that the DERAs must provide *"a list of the individual DERs participating in their aggregations."*

Additional informational requirements beyond those listed can be identified and explained by ISO/RTO in its compliance filings. An important note in Section IV.F is the requirement for ISO/RTO to propose the information-sharing requirements with the affected distribution utilities; and in Section IV.I, requiring the DERA to keep a list of individual DERs and information that has changed.

Without the knowledge of ISO/RTO market rules and varied monitoring and verification (M&V) methods used for settlements, it is not possible to make explicit recommendations for information and data requirements. Instead, generic recommendations are made. The ISOs/RTOs can use these generic recommendations for potential revisions to its tariff.

With explicit metering and telemetry requirements listed in the Order 2222, specific recommendations are made for these areas.

Report Organization

The methodology used for the study analyses is shown in Figure 3.

The definitions of these five core areas discussed in this guide are, as follows:

- ***Metering*** – Measurement of energy, either consumed or produced, used for settlements.
- ***Telemetry*** – The RTO process(es) for direct measurement and communication of requisite physical, operational, and performance characteristics of a DER.
- ***Data*** – Data and information related to DERs, actors, settlements, and performance monitoring of individual DERs.
- ***Interoperability*** – Ability of the DER systems among the relevant smart grid domains and actors, markets, and networks to exchange requisite data and information.
- ***Cyber security*** – Maintaining the integrity, confidentiality, and availability of both requisite data and DER systems.

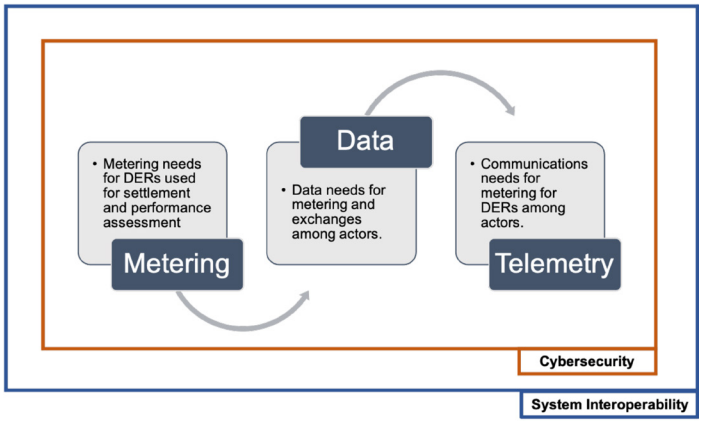

Figure 3. Topics and methodology used for the study analyses

This report focuses on the cross-cutting interoperability and cybersecurity. Metering, data, and telemetry are covered in a parallel report.[6]

Systems Interoperability

Systems interoperability in the context of the Order 2222 is in reference to the ability of the systems among the relevant domains and actors, markets, and networks to exchange requisite data and information. The exchange of data and information is considerate of the cyber security and privacy requirements.

One of the critical needs for heterogeneous DER interactions across the systems or devices for ISOs/RTOs, market operations, DERAs, and customer DERs is addressing the vendor lock-ins through proprietary technologies. Interoperability protocols and standards are proven mechanisms to do so. According to the Energy Independence and Securities Act of 2007, interoperability:

> *Protocols and standards shall further align policy, business, and technology approaches in a manner that would enable all electric resources, including demand-side resources, to contribute to an efficient, reliable electricity network.*[7]

The study leverages the NIST's definition[8] of interoperability in the context of the Order 2222:

> *Interoperability as the capability of two or more networks, systems, devices, applications, or components to work together, and to exchange and readily use information—securely, effectively, and with little or no inconvenience to the user.*

As a result, the study focuses on data, information, and communication interoperability. Interconnection standards that focus on the electrical interfaces are out of scope. The Order 2222 requires interactions among networks, systems, devices, applications, or components across the ISO/RTO, Market Operations, DERA, and customer DERs. Interoperability across a diversity of operational and economic systems has to be a key consideration to enable integration across increasingly complex and sophisticated technology and information landscape.[9] In reference to the SGAM from the Introduction and Background section, interoperability has to exist across all layers—component, communications, information, function, and business—to support the Order 2222 information and data requirements. As a reference, the Protocols Reference Guidebook Edition 4.0 from EPRI, provides a guide to the relevant stakeholders engaged in the DER programs with in-depth analysis and deployment options for protocols and standards across the component, communications, and information layers.[10]

Key Considerations and Gaps

The value of interoperability is enhanced when heterogeneous DER devices and systems must connect and communicate with one or more DU or DERA systems. Interoperability across DERA systems can foster market-competitiveness that benefits RTOs/ TSOs and DER customers. Earlier EPRI research has concluded that understanding traditional deployment methods (for example, non-interoperable systems) is required to assess the value of integrated

[6] *Metering, Data and Information, and Telemetry: An EPRI FO2222 Phase 1 Collaborative Report*. EPRI, Palo Alto, CA: 2020. 3002020596.

[7] Energy Independence and Security Act of 2007. §1301 and §1305, 42 USC §17381 and §17385. 110th Cong, 1st sess, 19 December 2007.

[8] NIST Smart Grid Framework 4.0.

[9] U.S. Department of Energy. The National Opportunity for Interoperability and its Benefits for a Reliable, Robust, and Future Grid Realized Through Buildings. DOE/EE-1341. https://doi.org/10.2172/1420233.

[10] *DER Protocol Reference Guidebook – 4th Edition: Understanding the Characteristics of Communications with Distributed Energy Resource (DER) and Demand Response Technologies*. EPRI, Palo Alto, CA: 2020. 3002018544.

DER deployments.[11] Nonetheless, research has shown, and is highlighted in this study, that interoperability provides numerous intangible benefits.

In addition to the extant complexity, the evolving cloud-architecture for DERAs and third parties further increases the complexity and underscores the interoperability and cyber security considerations. EPRI's guide for interoperability among DR systems defines the cloud-based architecture as the following:

> *A customer DR system or DR device interactions (customer interface) with a) cloud service provider (aggregator); b) aggregator standards-based endpoint; and c) aggregator optimization of DR resources.*[12]

EPRI's DR interoperability guide lists the following features from the use of cloud-based architecture for interoperability across the ISO/RTO, DU, DERA, and customer DERs and their systems:

- Provides DERA value-added services for customer DERs.
- Enables DERA integration of standardized DR signals from a diversity of DU DR programs.
- Supports the use of DERA systems for participation in the DU DR programs or ISO/RTO markets.
- The ISOs/RTOs and DUs rely on DERAs for customer participation and performance validation.

As an example of CAISO's process to dispatch a proxy DR (PDR) to the customer DERs via DERAs is a good example where interoperability considerations with the extant resources must be considered. Figure 4 shows the CAISO PDR dispatch process.

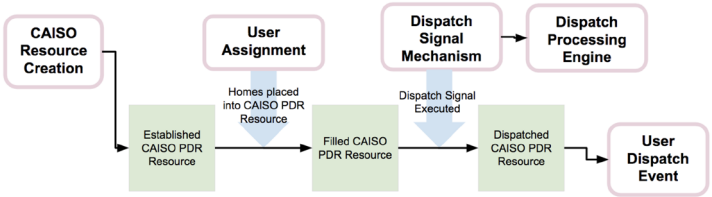

Figure 4. CAISO process to dispatch PDR event

The update to the Order 2222 (2222-A) allows the DERs participating in the retail markets to participate in the ISO/RTO markets. TSO/DSO coordination needs to account for DERs participating in multiple markets. (Figure 5, red dot- ted arrows).

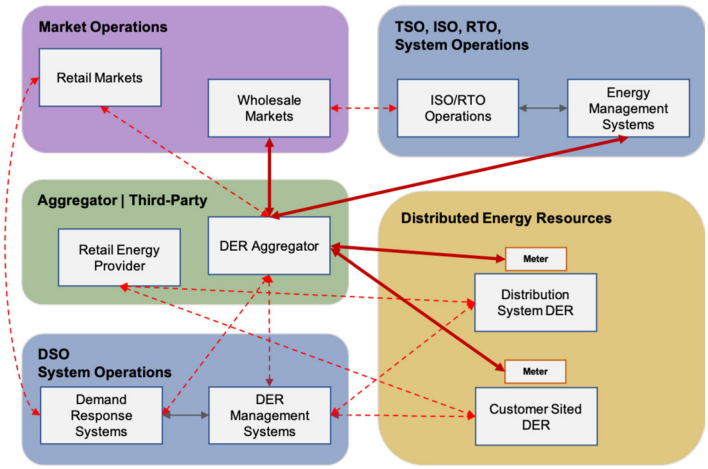

Figure 5. DSO systems interoperability considerations relative to ISO/RTO

With the Orders 2222 and 2222-A, the integration of customer DERs into disparate systems and networks, actors and smart grid domains, electricity markets, etc., makes interoperability a critical need to consider. While DERAs may leverage interoperability standards and protocols for efficient integration of customer DERs into ISO/RTO markets and coordination with DUs, the proliferation of cloud-based architecture requires further review to enable interoperability and cyber security of customer and DER data.

[11] *The Economics of Customer and Grid Connectivity and Grid Interoperability: Evaluation of the Potential Impacts of Interoperability in Utility Economic Analyses and Program Design*. EPRI, Palo Alto, CA: 2018. 3002013624.

[12] *Demand Response Interoperability Guidebook: a Repository of Information to Support Utilities in Achieving Interoperability in Demand Response Technologies*. EPRI, Palo Alto, CA: 2020. 3002018543.

Key Recommendations

The following are some high-level recommendations based on the interviews and presentation by a small subset of technology vendors and potential DERAs (EPRI Order 2222 Webcasts for members):

- ISO/RTO dispatches for market participation of DERs must identify and use interoperable and secure data and communication standards and protocols (e.g. IEC 62325)
- Where applicable, the system architecture must support interoperability standards and protocols and DU market participation rules for DERs to ensure scalability and market competitiveness.
- ISOs/RTOs must work with research organizations and DUs to recommend a common set of standards and protocols for data and information exchange among smart grid domains and actors.
- The interoperability considerations must be reviewed across all SGAM layers and domains and during the establishment of information and data requirements for the physical and operational characteristics of DERA.

Cyber Security

Cyber security is the protection of systems and data from cyber threats. Three key objectives of cyber security include the maintaining of:

1. Data confidentiality to prevent the unauthorized disclosure of data
2. Integrity of systems and data from misuse or modification
3. Availability to ensure that critical systems and data are readily accessible to authorized users

Failure of one or more of these three can lead to a loss-of-control event, where a cyber threat manipulates a system or makes it unavailable to fulfill key operational objectives, or a data-loss event where sensitive personal or company data are made available to unauthorizes parties. Consideration for these objectives and these events must be inherently included in the design of electricity markets and operations; otherwise, significant risk to grid reliability and safety can occur.

The cyber security threat landscape continues to advance and impact critical industrial control systems, as exhibited by the 2021 Oldsmar Water Facility Attack and the 2015 cyber attack against Ukraine's power grid.[13] Order 2222 introduces a major paradigm shift that now involves expanded use of public networks and third-party DER systems located in private aggregator networks and customer home area networks. These factors can significantly expand attack surfaces against the grid, and the industry should now also consider a new set of attack vectors that occur outside the scope of utility responsibility, which is often regulated through industry compliance standards, including NERC-CIP.

Key Considerations and Gaps

It should be noted that Order 2222 does not specify a requirement for cyber security and data privacy. Rather, the Order recommends that ISOs/RTOs *"coordinate with distribution utilities and relevant electric retail regulatory authorities to establish protocols for sharing metering and telemetry data, and that such protocols minimize costs and other burdens and address concerns raised with respect to privacy and cyber security."* Key risk considerations include 1) data privacy, including both personal and market data, 2) data integrity both at-rest and in-transit among electric market entities, and 3) data availability.

Customer and Market Data Privacy

Per FERC Order 2222, ISO/RTO must revise their tariffs such that DERAs provide *"a list of the individual resources in its aggregation, necessary information that must be submitted for individual DERS, and retain performance data for individual DERs."* This need for detailed DER data may raise concerns over customer data privacy as the sources of data can come from customer-owned devices and the data are expected to leave the premises of home area networks.

Customer Data Privacy – Data exchanges between market entities may entail identifiable information associated with customer energy use and production. For example, registration processes with DER aggregators may require customers to validate their identities using their social security or driver's license numbers.

[13] SANS, E-ISAC, "Analysis of the Cyber Attack on the Ukrainian Power Grid," 18 March 2016. https://media.kasperskycontenthub.com/wp-content/uploads/sites/58/2016/12/21181126/E-ISAC_SANS_Ukraine_DUC_5.pdf. Accessed 20 April 2021.

These data, known as personally identifiable information (PII), may lead to large-scale identity theft events if exfiltrated by adversaries due to poorly implemented security measures. Further, energy and device data may also have significant privacy issues if associated with PII. Considering that DERAs interface directly with customers, these entities have an emphasized responsibility to ensure the safe custody, transport, and storage of customer data.

Market Data Privacy – Generation information, including capacity and scheduling, may be considered to have critical confidentiality requirements, as exposure of this information to an unauthorized party may use these data to establish an unfair advantage over competitors in the electricity market.

Data Integrity

Telemetry is important to establish situational awareness, effective management of DERs, and performance of market settlements. Manipulation of data from revenue and settlement meters can have a direct financial impact on all stakeholders of the DER ecosystem. Telemetry data that are manipulated in transit or in flight may lead to incorrect responsive actions for market settlement and dispatch, leading to disturbances in grid reliability. More direct grid reliability consequences can result from either manipulation or spoofing of dispatch signals from an unauthorized source. With acknowledgement to the inherent use of untrusted public networks and home area networks to communicate telemetry and dispatch across multiple parties, large attack surfaces provide several opportunities to realize the aforementioned scenarios. Further, use of proprietary protocols and the lack of an end-to-end technology standard to provide protection assurances for data in flight may lead to incon- sistencies, and weak points, where data may be manipulated for adversarial purposes.

Data Availability

Higher penetration of IP-enabled DER devices and the use of public networks increase attack exposures against critical systems, increasing inherent likelihoods of denial-of-service attacks. DERAs can potentially provide an abstraction layer between critical ISO/RTO systems and DER devices by preventing the need for a direct interface to untrusted, exposed customer systems. Despite this, considerations of risks pertaining to large DERAs with high generation and load-shedding capacities should be considered.

In the event of widespread communication disruption, a DERA may not be able to provide critical grid support services, which emphasizes the need to include cyber security controls and design principle to maintain availability of data in flight. Data availability at rest is also an important consideration per the Order 2222, which requires that DERAs *"retain performance data for individual DERs in DER aggregation for auditing purposes."*

Key Recommendations

In alignment with the considerations and gaps that must be addressed relative to the Order 2222, specific recommendations are made for data privacy, integrity, and availability areas.

Data Privacy Recommendations

Entities participating in energy markets must be aware of data privacy regulations, understand the potential impact to customer privacy in the event of data-loss events, and ensure both technical and procedural controls are implemented to ensure both transparencies in how data are used and adequate protections for consumer data. These recommendations include:

- Reviewing and complying with data privacy such as those specified by EU General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), and New York SHIELD, and establish both technical and procedural controls to comply with current and emerging privacy legislation.
- Conducting privacy impact assessments (PIAs) to understand the degree of privacy risk that may be incurred through the collection of energy use and energy production data from behind-the-meter devices.
- Designing for a privacy-by-design data architecture and governance framework aligned to Fair Information Practice Principles (FIPPs).
- Aggregators and other entities should acquire customer consent to store and share data with market operators and other entities that have a relevant business need for customer data.
- Entities that handle customer data should provide transparency in how customer data are consumed and shared with other parties.
- Entities should ensure that explicit permission is provided by the customer prior to sharing of data with third parties.

- Where applicable, customer data should be aggregated across multiple customers to obfuscate the identity of information.
- Industry-accepted encryption standards should be employed for data in transit and at rest. Specifically:
  - Registration information stored in databases must be encrypted and accessed only through authorized personnel.
  - Transport mechanisms to share registration information, specifically across public networks, should be capable of handling industry-accepted encryption standards.

Data Integrity Recommendations

- Perform data integrity checks upon receipt and before transmittal of data.
- Leverage NIST-accepted cryptographic standards to protect data in flight from manipulation.
- Consider testing standards for both open-source and proprietary protocols and for systems to ensure adequacy of security control implementations.
- Perform logging and non-repudiation checks of data changes within entity databases.

Data Availability Recommendations

- DERAs should perform a risk assessment to evaluate their role in the electric sector to determine the appropriate availability and redundancy measures commensurate to their risk tolerance thresholds.
- Business-to-business (B2B) contracts should specify availability and service levels for negotiated grid and data-sharing services.
- Cloud-based services and critical systems should include upfront resiliency and redundancy design capabilities to ensure persistent availability of critical data and services.

Conclusions and Next Steps

Systems Interoperability – While metering and telemetry are leveraged to provide visibility into customer DER systems and DER performance settlement, interoperability can future-proof scalable data and information exchange among ISO/RTO-chosen systems and actors and any changes to market rules or cloud-architectural practices. The ISOs/RTOs must work with respective DUs and DERAs to review electricity market rules and how customer DERs can provide services across the electricity system in a scalable manner. Without system interoperability considerations, the costs to enable customer DER participation may not be efficient and cost-effective.

Cyber Security – Cyber security is vital to maintain integrity of electric markets and to provide assurances for customer privacy. Each entity in the DU market must review their roles and the pertinent cyber risks they must address to maintain confidentiality, integrity, and availability across the metering, telemetry, and system operability domains. ISOs/RTOs must coordinate with DUs and DERAs to determine expected cyber security responsibilities and needed technical controls, specifically those that are co-dependent.

Note

For further information about EPRI, call the EPRI Customer Assistance Center at 800.313.3774 Or e-mail askepri@epri.com.

EPRI RESOURCES

Sean Crimmins, *Principal Project Manager*
650.855.7901, scrimmins@epri.com

Girish Ghatikar, *Senior Program Manager*
650.855.8749, gghatikar@epri.com

Xavier Francia, *Senior Technical Leader*
650.855.2883, xfrancia@epri.com

Transmission Operations

The Electric Power Research Institute, Inc. (EPRI, www.epri.com) conducts research and development relating to the generation, delivery and use of electricity for the benefit of the public. An independent, nonprofit organization, EPRI brings together its scientists and engineers as well as experts from academia and industry to help address challenges in electricity, including reliability, efficiency, affordability, health, safety and the environment. EPRI also provides technology, policy and economic analyses to drive long-range research and development planning, and supports research in emerging technologies. EPRI members represent 90% of the electricity generated and delivered in the United States with international participation extending to nearly 40 countries. EPRI's principal offices and laboratories are located in Palo Alto, Calif.; Charlotte, N.C.; Knoxville, Tenn.; Dallas, Texas; Lenox, Mass.; and Washington, D.C.

Together…Shaping the Future of Electricity

Export Control Restrictions

Access to and use of this EPRI product is granted with the specific understanding and requirement that responsibility for ensuring full compliance with all applicable U.S. and foreign export laws and regulations is being undertaken by you and your company. This includes an obligation to ensure that any individual receiving access hereunder who is not a U.S. citizen or U.S. permanent resident is permitted access under applicable U.S. and foreign export laws and regulations.

In the event you are uncertain whether you or your company may lawfully obtain access to this EPRI product, you acknowledge that it is your obligation to consult with your company's legal counsel to determine whether this access is lawful. Although EPRI may make available on a case by case basis an informal assessment of the applicable U.S. export classification for specific EPRI products, you and your company acknowledge that this assessment is solely for informational purposes and not for reliance purposes.

Your obligations regarding U.S. export control requirements apply during and after you and your company's engagement with EPRI. To be clear, the obligations continue after your retirement or other departure from your company, and include any knowledge retained after gaining access to EPRI products.

You and your company understand and acknowledge your obligations to make a prompt report to EPRI and the appropriate authorities regarding any access to or use of this EPRI product hereunder that may be in violation of applicable U.S. or foreign export laws or regulations.

3002020597 July 2021

Electric Power Research Institute
3420 Hillview Avenue, Palo Alto, California 94304-1338 • PO Box 10412, Palo Alto, California 94303-0813 USA
800.313.3774 • 650.855.2121 • *askepri@epri.com* • *www.epri.com*