EPRI | ELECTRIC POWER RESEARCH INSTITUTE

Cybersecurity Interoperability Specifications for End-to-end DER Architecture

Enable BTM DER-provided Grid Services that Maximize Customer Grid Benefits (ENGAGE)

3002022403

Cybersecurity Interoperability Specifications for End-to-end DER Architecture

Enable BTM DER-provided Grid Services that Maximize Customer Grid Benefits (ENGAGE)

3002022403

Technical Update, July 2021

EPRI Project Manager

A. Huque

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

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

NOTE

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

ACKNOWLEDGMENTS

The Electric Power Research Institute (EPRI) prepared this report.

Principal Investigators
X. Francia
S.R. Ganti

This report describes research sponsored by EPRI.

This material is based upon work supported by the U.S. Department of Energy's Office of Energy Efficiency and Renewable Energy (EERE) under the Solar Energy Technologies Office Award Number DE-EE0009021.

This publication is a corporate document that should be cited in the literature in the following manner:

Cybersecurity Interoperability Specifications for End-to-end DER Architecture: Enable BTM DER-provided Grid Services that Maximize Customer Grid Benefits (ENGAGE). EPRI, Palo Alto, CA: 2021. 3002022403.

ABSTRACT

A secured aggregation platform supporting interoperability is critical for system operators to procure grid services from behind-the-meter distributed energy resources (DERs). Several cybersecurity aspects must be considered, including ensuring the authentication and integrity of exchanged data and controls among entities, coordination and clarification of cybersecurity responsibilities among all participating parties, assurances in personal privacy of customer information and energy use data, and other relevant concerns that must be addressed to ensure a secure-by-design DER integration architecture. This report provides a summary of the risk methodology used to determine cybersecurity specifications, attributes and vulnerabilities inherent in communication interfaces, and impact and likelihood ratings associated with high consequence scenarios related to the identified communication interfaces. It leverages the risk assessment to determine what security specifications are required for each aspect of the end-to-end DER integration architecture. This report also discusses why certain specifications are required based on the inherent attributes identified within the architecture's interfaces.

Keywords

Cybersecurity Risks
Cybersecurity Risk Assessment
Distributed Energy Resource (DER)
Grid Services
Behind-the-meter (BTM)

CONTENTS

LIST OF FIGURES

LIST OF TABLES

1
INTRODUCTION

A secured aggregation platform supporting interoperability is critical for system operators to procure grid services from behind-the-meter DERs. Several cybersecurity aspects must be considered, including ensuring the authentication and integrity of exchanged data and controls among entities, coordination and clarification of cybersecurity responsibilities among all participating parties, assurances in personal privacy of customer information and energy use data, and other relevant concerns that must be addressed to ensure a secure-by-design DER integration architecture.

The development of this cybersecurity architecture is attributed to a 3-year project titled *"Enable Behind-the-meter DER-provided Grid Services that Maximize Customer and Grid Benefits (ENGAGE)"*. This EPRI-led collaborative research project is funded in part by the U.S. Department of Energy (DOE) through the Solar Energy Technologies Office (SETO). The EPRI Project Team brings together utilities, academia and industry partners.

The developed architecture will include a cyber security and interoperability specification plan to evaluate end-to-end functional and communication requirements within the architecture, inclusive of both on-premise and aggregation considerations.

Report Organization

This report summarizing results of this research is organized as follows:

Section 2 provides a summary of the risk methodology used to determine cybersecurity specifications, attributes, and vulnerabilities inherent in communication interfaces, and impact and likelihood ratings associated with high consequence scenarios related to the identified communication interfaces.

Section 3 leverages the risk assessment to determine what security specifications are required for each aspect of the end-to-end-architecture. This section discusses why certain specifications are required based on the inherent attributes identified within the architecture's interfaces.

2
CYBERSECURITY RISKS

This section evaluates cybersecurity risks pertaining to the functional and communication interoperability requirements to enable grid services by behind-the-meter DERs. In this paper, cybersecurity risk is defined as a loss of confidentiality, integrity, or availability (i.e., the CIA triad) of a system or logical interface. Degradation in one or more aspects of the CIA triad can lead to negative consequences related to grid reliability, personal safety, or data privacy. Thus, a risk and consequence-based approach is important to identify the necessary security specifications for the architecture. In this section, the methodology with which risk is evaluated is discussed, followed by discussion of components within the end-to-end architecture, interface attributes and their associated vulnerability considerations, and finally, likelihood and impact ratings for identified interfaces.

Risk Assessment Methodology

An asset/impact-oriented approach was used to assess risk against the components in the end-to-end DER architecture. The steps in this risk analysis approach include 1) identification of logical interfaces and device components in the DER integration architecture, 2) identification and analysis of attributes inherent within interfaces and device components, 3) qualitative impact and likelihood analysis of likely attack vectors, and 4) specification of cybersecurity requirements appropriately commensurate to identified vulnerabilities. These steps and their contributions towards understanding risks are described further below:

1. **Identification of Architectural Components –** Two sets of components were identified within the end-to-end DER architecture. These include 1) the logical interfaces which enable communications between the systems and subsystems of the DER integration architecture, and 2) the devices and systems necessary to enable communication among the architecture's components. The role each of these components have in the overall architecture was first characterized to inform how a loss-of-control or data-loss event among these components can impact reliability, safety, and privacy as discussed in Step 3 of the methodology. In the context of this research, loss-of-control and data-loss scenarios are defined as follows:

   Loss-of-control Event – A scenario where a system or its data is manipulated, either through internal or external means, to disrupt its operational objectives.

   Data-loss Event – A scenario where data is exfiltrated and disclosed to unauthorized parties.

2. **Identify Interface and Component Attributes and Vulnerabilities –** Potential attributes, such as patch management constraints, use of proprietary protocols, etc. were identified among the architecture's components. Identification of these potential attributes is important because it helps to identify what cybersecurity vulnerabilities and constraints must be considered for specification development. For example, logical interfaces which use wireless media may be subject to higher exposures to wardriving attacks or unauthorized network access, and requirements, such as VPNs or protocol encryption, become critical to adequately secure these interfaces.

3. **Likelihood and Impact Analysis of Possible Attack Vectors –** The identified attributes in Step 2 were used to perform qualitative analysis of likelihood and impact ratings attributed to possible attack vectors against the architecture's components. Likelihood defines the occurrence in which a threat event occurs and certain criteria, such as attack sophistication, skill required, and logical or physical access needs were considered to help identify likelihood ratings. Impact ratings qualify the consequence that may result from a cyber event, and safety, grid reliability, and privacy considerations are included in these ratings.

4. **Identify Cybersecurity Requirements and Specifications –** Finally, Step 4 of the risk approach identifies the cybersecurity requirement specifications among each of the components depending on the attributes, likelihood, and attack vectors identified in Step 2 and Step 3.

End-to-end System Architecture, Interoperability, and Component Requirements

To consider the cybersecurity and interoperability requirements for end-to-end aggregation and control architecture, a high-level communication architecture that can support end-to-end aggregation and control was developed as shown in Figure 2-1.

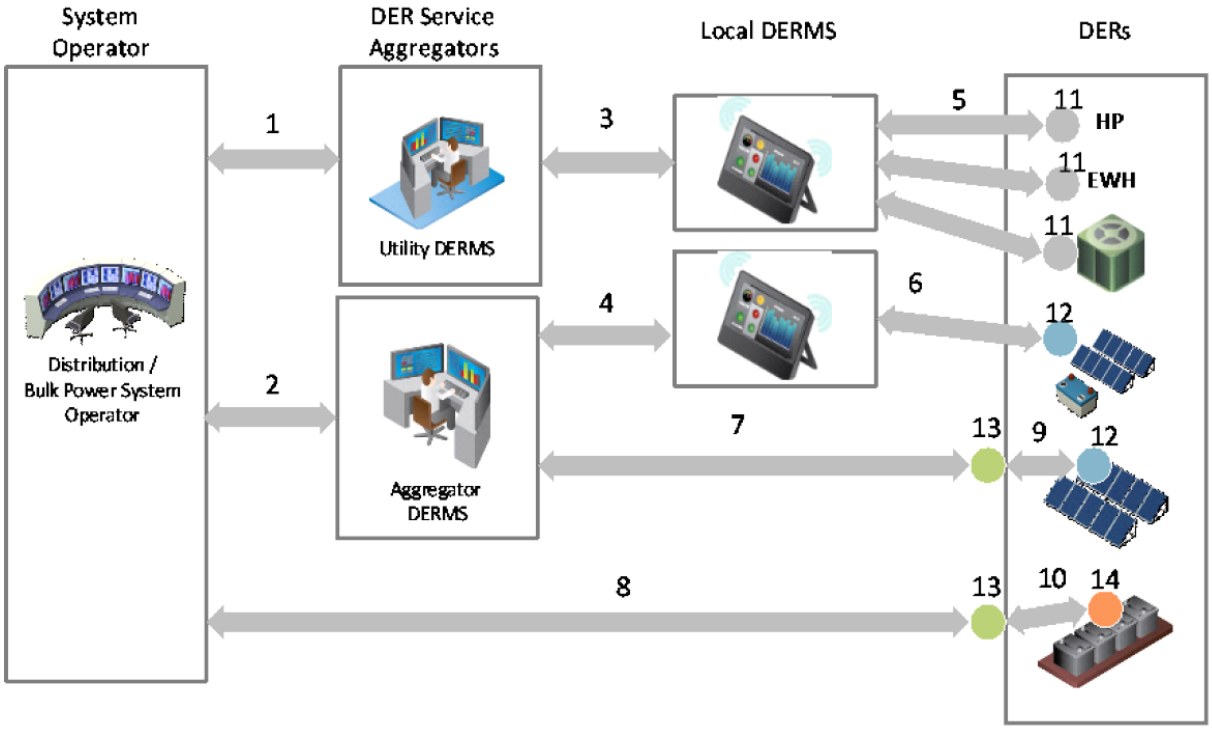

Figure 2-1
Connectivity Requirements

At minimum, ten different types of communication interfaces should be considered to achieve the desired cybersecurity and interoperability requirements of the end-to-end architecture. Additionally, the architecture also considers four different types of communication-enabled devices which play important functions in end-to-end connectivity and interoperability. These communication interfaces and communication-enabled devices are discussed in Table 2-1.

Table 2-1
Logical Interfaces of End-to-end DER Interoperability Architecture

Communication Interface	Description
1. Utility System Operator – Utility DERMS	These two interfaces describe communications between control systems owned by a distribution or bulk power system operator, acting as a managing entity, and a utility or aggregator Distributed Energy Resource Management System (DERMS).
2. Utility System Operator – Aggregator DERMS	
3. Utility DERMS – Local DERMS	These two interfaces describe communications between a utility or aggregator DERMS system and another DERMS system at the local DER site (L-DERMS).
4. Aggregator DERMS – Local DERMS	
5. Local DERMS – CTA-2045 Adaptor	Communication between the DER site's L-DERMS system and various CTA-2045 adaptors on load systems, such as heat pumps, electric water heaters, or HVAC systems.
6. Local DERMS – Smart Inverter	Communications between a site's L-DERMS and a smart inverter
7. Aggregator DERMS – Aggregator Gateway	Communications between an aggregator's DERMS (A-DERMS) and a site's smart inverter.
8. Utility System Operator – Utility DER Gateway	Communications between a distribution or bulk power system operator and a utility-owned DER gateway.
9. Aggregator DER Gateway – Smart Inverter	Communications between a DER site's smart inverter and the utility-owned DER gateway.
10. Utility DER Gateway – Local Energy Management System (EMS)	Communications between a DER gateway and a local site's energy management system (EMS).

Table 2-2
Key Communication Devices of End-to-end DER Interoperability Architecture

Communication Device	Description
11. CTA-2045 Adaptor	The ANSI/CTA-2045 universal communication module is a modular communication port that provides a standard on how information is exchanged between the module and DER. These devices typically support Wi-Fi, and some protypes are in development to support 4G TLE and Low Power Wide Area Network (LPWAN). [1]
12. Smart Inverter	An inverter which is capable of grid-reliability supporting functions, including bulk system support, including voltage and frequency ride-through and frequency-watt control, and voltage management, including volt-watt/volt-VAR control and fixed power factor. It is assumed in this architecture that these smart inverters are also capable of communication & interactivity, such as remote configuration and coordination.
13. Utility or Aggregator DER Gateway	A utility-deployed and managed network gateway which connects to utility networks to monitor and control interconnections with DER sites. In this architecture, it is assumed that sites which host a utility gateway have a local nameplate capacity greater than 1 MW.
14. Local Energy Management System (EMS)	A computer system used to optimize the performance and use of the DER site's generation and load-shedding capabilities. In this architecture, it is assumed that the EMS is used to manage energy resources within a microgrid, commercial facility, or industrial facility.

Interface and Device Attribute and Vulnerability Considerations

The communication interfaces and devices identified in the end-to-end DER hierarchical architecture may involve a variety of inherent attributes, which determine certain vulnerabilities that must be considered for cybersecurity specification, and constraints which limit or complicate the use of certain cybersecurity controls. Attributes, adapted from *NISTIR 7628 Revision 1: Guidelines for Smart Grid Cybersecurity,* for each interface and communication device is described in Table 2-3. These attributes, and their associated vulnerabilities include:

ATR-1a and ATR-1b Confidentiality/Privacy Requirements – The component stores or transmits sensitive data, that if exposed to unauthorized parties, may lead to breach of personal privacy or exposure of confidential business data. Interfaces which host L-DERMS or gateways are subject to customer privacy considerations as these systems are expected to have full observability of local DER systems. In comparison to other interfaces, it is assumed that confidentiality requirements are expected to be relatively low or non-existent for interfaces which only have partial observability of DER systems, as is the case with utility or aggregator DERMS.

Associated Vulnerabilities and Constraints – Inadequate data governance and privacy policies which should define expected data handling requirements can lead to overly permissive access to customer data, possibly from unauthorized parties. Inadequate network segmentation, which logically and physically separates networks from unauthorized

systems, and inadequate encryption of customer data at-rest and in-transit can both lead to unauthorized monitoring and or exfiltration.

ATR-2: Data Integrity/Accuracy Requirements – The component requires that data has not been modified in-transit or at-rest or requires highly accurate data to make correct logical or operational decisions. Although data integrity is attributed for all interfaces in the architecture, implications to safety and reliability will vary in degree. For example, attacks against data integrity among communications between a CTA-2045 adaptor is only expected to impact the local customer, but manipulation of control communications between an operator and aggregator may result in broader consequences.

Associated Vulnerabilities and Constraints – Absence of encryption and integrity checks for data at-rest or data-in transit may expose metering and telemetry data to unauthorized manipulation. This can occur as a result of immature security design of protocols, as discussed in ATR-7, or through overly permissive data write or delete access for data-at-rest.

ATR-3: System or Data Availability Requirements – Certain components may have a high reliance on data or commands from another system in order to accurately execute the operational objectives. If an interface or system is rendered unavailable, this may lead to operational disruptions. For example, in consideration of the DERMS control and monitoring hierarchy, a utility DERMS may be dependent on aggregator DERMS (A-DERMS) systems to execute needed schedules for a group of DERs. This requirement is particularly relevant for systems which have a real-time component for observability and control, as discussed in ATR-9, depending on the expected system objectives and negotiated contract between entities.

Associated Vulnerabilities and Constraints – Attack vectors, such as denial-of-service (DoS) attacks, which render a system unavailable for control or observation, should be considered particularly for systems which must interface with other systems through public networks. These attack vectors can include bad-packet inject against systems, which lack data-input validation or invalid parameter checks, loss-of-power to the system, ransomware attacks, etc.

ATR-4: Low bandwidth of communications channels – The communication interface may involve limited bandwidth that prevents certain technologies, such as intrusion detection and prevention technologies, from being used because of their impact to network performance. Unexpected, high utilization of these channels may lead to data loss and unavailability of upstream or downstream communications. This attribute is likely the case for interfaces which host local, private networks which are owned and maintained by a customer.

Associated Vulnerabilities and Constraints – Low-bandwidth networks can be particularly prone to denial-of-service (DoS) attacks which can flood systems, such as routers, firewalls, and switches, with network traffic such that local networks become unavailable. Networks which have low-bandwidth characteristics can place limitations in the deployment of network-based security monitoring or cryptographic controls due to their impacts on network performance.

ATR-5: Microprocessor constraints on memory and compute capabilities – Components prevent the use of endpoint detection and response (EDR) technologies due to limitations in the system's computation and memory resources. Unexpected, high utilization of computational and memory resources can lead to unavailability of a component. This attribute may be the case for local systems, such as gateways, smart inverters, CTA-2045 adaptors, etc.

> **Associated Vulnerabilities and Constraints –** These systems can be prone to denial-of-service (DoS) attacks which overutilize memory or computing resources. Additionally, microprocessor constraints can result in the inability to leverage endpoint detection and response (EDR) and cryptographic controls, which are responsible for the monitoring and prevention of malware and to protect communications or data-at-rest, respectively.

ATR-6: Wireless media – Certain networks may leverage wireless-based technologies, such as Wi-fi or Bluetooth, to communicate to other components. Although wireless-based vulnerabilities may be relevant for all interfaces in the architecture, threat likelihood ratings are driven higher for local networks that host customer networks, which may not be equipped with the same protections as commercial or industrial technologies networks.

> **Associated Vulnerabilities and Constraints –** Wireless networks may contain vulnerabilities subject to certain attack techniques which allow for reconnaissance or unauthorized access, such as piggybacking, wardriving, evil-twin attacks, wireless sniffing, or unauthorized access [2].

ATR-7: Immature or proprietary protocols – Immature protocols or proprietary protocols that lack transparency in cybersecurity features may not have undergone adequate testing and review, or may lack necessary cryptographic features for authentication and confidentiality. This attribute may be particularly relevant for local or aggregator systems where the manufacturer elects to use its own proprietary protocols for more flexibility and reliability in device interoperability and management.

> **Associated Vulnerabilities and Constraints –** Protocols which have inadequate cryptographic features to fulfill data integrity checks, authentication, and confidentiality, can expose interfaces to man-in-the-middle and device spoofing attacks. Even if these features are present within proprietary protocols, they may be subject to undiscovered vulnerabilities, due to lack of transparency in design or implementation.

ATR-8/16: Inter-organizational interactions and Access Constraints – Communication interfaces among the architecture can involve interactions with different organizations which have incompatible cybersecurity policies or limitations in fulfilling the interfacing third-party's security requirements. These interactions may often involve communications over public networks such as the Internet. These complexities introduce challenges to establish cybersecurity trust in inter-organizational interactions.

> **Associated Vulnerabilities and Constraints –** Systems involved in inter-organization interactions have a higher exposure to third-party risks. Some entities, particularly aggregators or customers, are not subject to certain industry compliance standards, such as NERC-CIP, and may lack security maturity or capabilities to adequately meet interacting organizations' security policies. Lack of monitoring or inability to introduce security

controls to third-party systems or networks can present trust issues in system and data availability among interacting parties.

ATR-9: Real-time operational requirements – This characteristic describes interfaces which have a low threshold for tolerating network latencies and relies on timely receipt of data to execute operational decisions. In consideration of the Utility-DERMS, A-DERMS, and L-DERMS hierarchy, this attribute is relevant mainly for interfaces which have a negotiated contract for real-time observability or real-time control requirements. In comparison, this attribute may not be the case for interfaces which only utilize "booking" or "scheduling" types of controllability.

Associated Vulnerabilities and Constraints – Interfaces with this attribute can be particularly sensitive to denial-of-service attacks against these networks or systems. Additionally, these real-time constraints can place limitations in introducing security monitoring and prevention technologies due to their impacts on performance thresholds.

ATR-12: Insecure, untrusted locations – The communication interface or device resides in a location that lacks proper physical security controls or is outside the domain of the interfacing entity's physical and cyber security policy enforcement. In consideration of the proposed DERMS control and monitoring hierarchy, this presents a challenge for entities which must interface with another party's DERMS who may not be able to establish full trust in the data integrity of received controls, data, metering, and telemetry.

Associated Vulnerabilities and Constraints – Similar to the vulnerabilities discussed in ATR-8/16, entities interfacing with systems and networks with this attribute are subject to third-party risk exposures.

ATR-13: Key management for large numbers of devices – A well-managed public key infrastructure (PKI) system involves the provisioning, deprovisioning, revocation, and renewal of certificates and associated public and private keys. This management becomes increasingly complex for many devices, especially if they do not have access to centralized certificate management systems. This challenge is expected to be encountered for large-scale deployments of L-DERMS, gateway, smart inverter, and DER systems.

Associated Vulnerabilities and Constraints – Lack of a renewal processes for expired certificates can lead to unavailability of systems. Systems whose private keys were compromised can be exposed to spoofing types of attacks, and lack of processes or inability to update certificates of these devices can prolong these exposures. Constraints for PKI management can be expected for systems which do not have access to centralized certificate management systems.

ATR-14: Patch and update management constraints – Patch management requires adequate testing of updates, especially for operational technology environments, before they are provisioned to systems. Systems which do not have access to update management servers may be subject to prolonged exposure to security vulnerabilities.

Associated Vulnerabilities and Constraints – The variety and large number of different systems requiring patches may introduce delays in security patch frequency. Interfaces

between different systems and different owners of these systems can introduce complexities in performing adequate patch testing.

ATR-15: Interaction unpredictability and variability – Communication interfaces with this attribute involve unpredictable and variable interactions. This variability can make baselining of communications difficult or impossible.

Associated Vulnerabilities and Constraints – Communication interfaces with high variability and unpredictability can introduce difficulties in establishing security monitoring and anomaly detection capabilities due to the indeterministic characteristics of interactions.

ATR-18: Autonomous control – Systems which autonomously issue controls to end devices are not monitored by centralized control systems. This attribute is likely to be the case for interfaces involving L-DERMS, which may execute actions to DER to meet local operational objectives.

Associated Vulnerabilities and Constraints – Autonomy of systems can introduce limitations for centralized systems to verify control actions before they are executed.

Table 2-3
Communication Interface/Device Attributes

Communication Interface:	Interface Attributes													
	ATR-1a/b: Confidentiality/Privacy Requirements	ATR-2: Data Integrity/Accuracy Requirements	ATR-3: System or Data Availability Requirements	ATR-4: Low bandwidth of communications	ATR-5: Microprocessor/memory constraints	ATR-6: Wireless media	ATR-7: Immature or proprietary protocols	ATR-8/16: Inter-organizational interactions	ATR-9: Real-time operational requirements	ATR-12: Insecure, untrusted locations	ATR-13: Key management for large no. of devices	ATR-14: Patch and update management constraints	ATR-15: Interaction unpredictability & variability	ATR-18: Autonomous control
1. Utility System Operator – Utility DERMS		X	X						X			X		X
2. Utility System Operator – Aggregator DERMS		X	X					X	X			X		
3. Utility DERMS – Local DERMS	X	X	X					X	X	X	X	X		
4. Aggregator DERMS – Local DERMS	X	X	X				X	X	X	X	X	X		
5. Local DERMS – CTA-2045 Adaptor	X	X		X	X	X				X	X	X	X	X
6. Local DERMS – Smart Inverter		X	X	X	X	X	X			X	X	X	X	X
7. Aggregator DERMS – Aggregator Gateway		X	X		X		X		X	X	X	X		
8. Utility System Operator – Utility DER Gateway	X	X	X		X				X	X	X	X		
9. Aggregator DER Gateway – Smart Inverter		X	X	X	X	X	X	X	X	X	X	X	X	X
10. Utility DER Gateway – Local Energy Management System (EMS)	X	X	X	X		X		X	X	X	X	X	X	X

Likelihood and Impact Analysis of Possible Attack Vectors

Impacts to grid reliability, safety, and privacy were evaluated for each of the ten communication interfaces identified in the architecture. Financial impacts, including criteria for restoration costs, disturbances in energy markets, utility revenue, economic damages, etc., are another common factor used to evaluate risk. This work omitted evaluation of financial issues in its risk ratings as energy market interfaces were not evaluated in the architecture, and financial measurements vary depending on the scale of utilities and aggregators. Adopted from *National Electric Sector Cybersecurity Organization Resource (NESCOR) Electric Sector Failure Scenarios & Impact Analysis – Version 3.0* [3], the following sections describe criteria considered to evaluate impact ratings among the architecture's interfaces.

Reliability Risks Qualitative Ratings

Table 2-4
Reliability Risk Criteria

Reliability Impact Ratings	
Criteria	**Levels**
System Scale	Low: single utility customer Medium: town or city High: potentially full utility service area and beyond
Negative impact on generation capacity	Low: No effect Medium: More than 10% loss of generation capacity for 8 hours or less High: More than 10% loss of generation capacity for more than 8 hours
Negative impact on the bulk transmission system	Low: None Medium: Major transmission system interruption High: Complete operational failure or shut-down of the transmission system

Safety Risks Qualitative Ratings

Table 2-5
Safety Risk Criteria

Safety Impact Ratings	
Criteria	**Levels**
Workforce safety concern	Low: none, Medium: any possible injury High: any possible death
Public safety concern	Low: none Medium: 100 injured possible High: one death possible

Privacy Risks Qualitative Ratings

Table 2-6
Privacy Risk Criteria

Privacy Impact Ratings	
Criteria	**Levels**
Causes a loss of privacy for a significant number of stakeholders	Low: none Medium: greater than 1000's of individuals High: millions of individuals

Risk Likelihood Qualitative Ratings

Along with impact ratings, likelihood ratings were also rated based on criteria defined in Table 2-7. Likelihood is defined by the opportunity with which an adversary can realize attack objectives and is based on possible attack vectors skill requirements, required accessibility, and complexity.

Table 2-7
Likelihood Risk Criteria

Likelihood Ratings	
Criteria	**Levels**
Skill Required	Low: deep domain/insider knowledge and ability to build custom attack tools Medium: Domain or special insider knowledge needed High: Basic domain understanding and computer skills
Physical Accessibility	Low: Inaccessible Medium: Fence, standard locks High: Publicly accessible or physical access not required
Logical Accessibility	Low: High expertise to gain access Medium: Publicly accessible but not common knowledge High: Common knowledge or none needed
Attack Vector	Low: Theoretical Medium: Similar attack has occurred High: Straightforward; script or tools available, or simple once access is obtained

Risk and Likelihood Ratings of DER Communication Interfaces

The following table provides reliability, safety, and privacy impact ratings. Several of the described scenarios are adopted from the *National Electric Sector Cybersecurity Organization Resource (NESCOR) Electric Sector Failure Scenarios & Impact Analysis – Version 3.0* [3].

A set of risk ratings were assigned for each of the ten different types of connectivity. These risk ratings are based on an evaluation of inherent risks, which represents the amount of risk present in the architecture without accounting for implemented security controls or measures. Evaluation of inherent risks is a useful first measure to assist in determining what security controls and strategies would be appropriately commensurate towards desired risk reductions for the

architecture. The inherent risk ratings were derived by identification of high consequence attack scenario narratives, based on potential vulnerabilities related to interface attributes.

Table 2-8
Risk and Likelihood Ratings of DER Communication Interfaces[1]

Communication Link	High Consequence Attack Scenarios	Reliability Impact	Safety Impact	Privacy Impact	Potential Likelihood
1. Utility System Operator – Utility DERMS	Compromise of intra-utility communications via man-in-the-middle or denial-of-service attacks between ADMS and Utility DERMS can impact several DERs or control centers, causing widespread grid disturbances. This poses risks to public safety if the cyber event causes a shutdown of the transmission system and loss of customer power for an extended period of time.	High	High	Low	Low-Medium
2. Utility System Operator – Aggregator DERMS	Compromise of communications over public networks between Utility EMS/ADMS and Aggregator DERMS allows for man-in-the-middle or denial-of-service attacks that can impact several DERs. Grid effects may range from single town/city disturbances, if only aggregator DERMS is compromised, or widespread grid effects if utility control systems are also affected.	Medium-High	High	Low	High
3. Utility DERMS – Local DERMS	Communications out to hundreds of local DERMS may go through a combination of public and private networks, providing more exposure to remote-based attacks. These communications are susceptible to man-in-the-middle attacks, which can lead to a large-scale compromise of multiple communications, and communications interception, which can lead to exfiltration of customer energy data sourced from local DERMS systems.	Medium-High	High	Medium	High

[1] The risk ratings identified in this work describe risks relative to other interfaces in the architecture. For example, a cybersecurity event involving the interface between utility operators and DERMS (Interface 1) is expected to have a higher reliability risk than a cyber threat event occurring between a L-DERMS and CTA-2045 Adaptor (Interface 5). These ratings were developed to determine where emphasis of security controls should be considered in a generic architecture. In real-life applications, these risk ratings are expected to vary for each entity in the architecture, and a variety of considerations should be considered that can influence reliability, safety, privacy, and financial risks. Considerations can include, but are not limited to, system protection schemes, DER grouping, aggregated nameplates, DER tripping capabilities, etc.

Table 2-8 (continued)
Risk and Likelihood Ratings of DER Communication Interfaces

Communication Link	High Consequence Attack Scenarios	Reliability Impact	Safety Impact	Privacy Impact	Potential Likelihood
4. Aggregator DERMS – Local DERMS	Similar to Communication Link 3, this interface involved communication out to several hundred local DERMS over a mixture of public and private networks and is subject to the same data integrity and privacy attacks. Reliability impact ranges to isolated disturbances within a local facility or several hundred DER systems managed by the aggregator.	Low-Medium	High	Medium	High
5. Local DERMS – CTA-2045 Adaptor	Communications between local DERMS and CTA-2045 adaptor are susceptible to private network vulnerabilities, but reliability impact may be limited to only the local facility DERMS and BTM devices. Lack of encryption for exchanged data may lead to interception of BTM device data, but is expected to be isolated to a single or small group of customers.	Low	Low	Low	Medium
6. Local DERMS – Smart Inverter	Smart inverters on a consumer's local network can be exploited due to vulnerabilities such as weak network passwords. Placing an inverter with lack of physical access security can allow hardware level attacks or unauthorized modifications, leading to either localized or neighborhood-level grid reliability effects, depending on the scale of DERs served by the smart inverter.	Low-Medium	Low	Low	Medium
7. Aggregator DERMS – Aggregator DER Gateway	Communications out to hundreds of DER gateways may go through a combination of public and private networks. Lack of authentication and encryption features in proprietary protocol make them susceptible to man-in-the-middle attacks which can lead to a large-scale compromise of multiple communications.	Medium-High	Medium	Low	High
8. Utility System Operator – Utility DER Gateway	Supply chain-based attacks effect several hundred utility DER gateways and are compromised to launch a distributed denial-of-service attack against utility ADMS or EMS systems.	High	High	Low	High

Table 2-8 (continued)
Risk and Likelihood Ratings of DER Communication Interfaces

Communication Link	High Consequence Attack Scenarios	Reliability Impact	Safety Impact	Privacy Impact	Potential Likelihood
9. Aggregator DER Gateway – Smart Inverter	A smart inverter can be impersonated with moderately high effort and similarly a gateway can be spoofed. This may lead to control commands from unauthorized sources to the smart inverter.	Medium-High	High	Low	Low
10. Utility DER Gateway – Local Energy Management System (EMS)	Local EMS could be managing utility scale battery energy storage or a microgrid. This adds an inherent risk of having potentially high grid impact, depending on the generation and load scale of the facility. Compromise of the EMS system may allow for extraction of customer energy use and production data.	High	Medium	High	Medium

3
CYBERSECURITY SPECIFICATIONS

This section provides cybersecurity specifications for the DER end-to-end architecture. These specifications were guided by the NIST Cybersecurity Framework (NIST-CSF) Identify, Protect, Detect, Respond, and Recover Domains, and addresses the following categories of security controls [4]:

- Risk Assessment and Management Across Inter-Organization Integrations
- Communication Network Security
- Access Control
- Patch Management
- Security Event Monitoring

The following specifications were selected based on evaluation of identified vulnerabilities and risk ratings among the DER interfaces.

Risk Assessment and Management (RAM) for Inter-organizational Integrations

The risks described in Table 2-8 were evaluated against a generic DER control and monitoring hierarchical architecture, but it is expected that entities involved in DER management perform a similar risk assessment to evaluate their organization's unique role in maintaining safety, reliability, privacy and customer privacy. Per NIST-CSF, the following risk assessment and management controls should be applied by all entities involved in the DER architecture. As discussed in control ID.RM-2 and ID.RM-2, risk assessment and management processes can aid in identifying the appropriate investment in cybersecurity controls. In consideration of the complexities in establishing trust among inter-organizational interactions, each entity should be responsible for understanding the risk of third-party relationships, as discussed in RAM-1 set of controls, and should specify within negotiated contracts the expected controls and responsibilities that must be fulfilled to help establish trust within interactions.

- ID.RA-3: Threats, both internal and external, are identified and documented
- ID.RA-4: Potential business impacts and likelihoods are identified
- ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk
- ID.RA-6: Risk responses are identified and prioritized
- ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders
- ID.RM-2: Organizational risk tolerance is determined and clearly expressed
- ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector-specific risk analysis

RAM-1 – Risk Assessment Specifications of Third-party Relationships

Minimum requirement for communication interface 2, 3, 4, 9, and 10.

RAM-1.1 – System operators should identify their role and third-party roles in maintaining grid safety and reliability to inform their determination of risk tolerance for these business relationships.

RAM-1.2 – System operators and aggregators should develop and enforce third-party security reviews and audits to ensure that business partners have implemented and are maintaining the necessary security controls deemed required to adequately meet risk tolerances.

RAM-2 – Inter-Organizational Contract Specifications

Minimum requirement for communication interface 2, 3, 4, 9, and 10.

RAM-2.1 – Inter-organizational contracts should specify criteria to meet security policies and should include details which may include, but not be limited to:

- Organization risk assessment methodology which include processes to identify threats, their impacts, and timelines/plans to mitigate vulnerabilities.
- Identification and assignment of cybersecurity responsibilities.
- Implementation and continuous improvement of a vulnerability management program.
- Processes and timelines to provide notification of vulnerabilities or cyber events that impact other parties.
- For any proprietary protocols used by the third-party, the owner of the protocol provides attestation that the protocol has been security tested and contains cryptographic mechanisms for authentication, authorization, encryption, and data integrity checks.

Communication Network Security (CNS) Specifications

Three key factors drive higher likelihood and higher impact ratings in the architecture. These include:

- Expected use of public networks, particularly for inter-organization interactions, which increases the likelihood of man-in-the-middle and spoofing attacks.
- Expected use of private networks which may be immature in cybersecurity controls and processes, particularly for customer-owned local area networks.
- Large-scale deployment of DER devices which participate in the control and monitoring architecture increases attack surfaces to the entire system.

In consideration of these issues, the following communication and network security specifications are identified for the architecture. These include network threat monitoring, data

leak prevention, network segmentation, documented network baselines, network availability, and communication protocol requirements.

CNS-1 – Network Threat Monitoring and Data

Relevant NIST CSF Control: DE.CM-1: The network is monitored to detect potential cybersecurity events.

Minimum requirement for communication interface 1, 2, 3, 4, 7, and 8.

Recommended requirement for communication interface 5, 6, 9, and 10.

CNS-1.1 – Communication interfaces employ deep-packet inspection, intrusion prevention and detection, and application firewall technologies to detect for anomalies and threats in the network.

CNS-1.2 – Network security perimeters have capabilities to perform TLS/SSL interception to detect threats within encrypted traffic.

CNS-2 – Data Leak Prevention

Relevant NIST CSF Control: PR.DS-5: Protections against data leaks are implemented

Minimum requirement for communication interface 3, 4, 7, and 8.

Recommended requirement for communication interface 5, and 6.

CNS-2.1 – Data leak/loss detection and prevention systems are implemented on network perimeters to search for customer-related data and prevent their exfiltration to unauthorized parties.

CNS-3 – Network Segmentation

Relevant NIST CSF Controls:

- PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate

Minimum requirement for communication interface 1, 2, 3, 4, 7, 8, 9, and 10.

CNS-3.1 – Network boundaries, and the security controls used to protect these boundaries, are based on trust levels and relationships between networks. For example, higher trust integrations may leverage VPNs between networks, but lower trust integrations may require more stringent security controls, such as secure protocols and intrusion detection and prevention systems.

CNS-3.2 – Demilitarized zones are used to aggregate third-party communications for network threat monitoring and inspection.

CNS-3.3 – Inbound and outbound traffic is restricted through security policies configured in firewalls or gateway devices located on network perimeters.

CNS-4 – Network Availability

Relevant NIST CSF Controls:

- PR.DS-4: Adequate capacity to ensure availability is maintained.

Minimum requirement for communication interface 1, 2, 3, 4, 7, 8.

CNS-4.1 – Critical aggregator and system operator systems, including DERMS, and the networks which serve these systems contain design redundancies to ensure availability during system or network failures.

CNS-5 – Documented Network Baselines

Relevant NIST CSF Controls:

- ID.AM-3: Organizational communication and data flows are mapped.
- DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed.

Minimum requirement for communication interface 1, 2, 3, 4, 7, 8.

CNS-5.1 – Communication, data flows, and network topologies are mapped and documented to inform necessary network-based security requirements.

CNS-5.2 – Ingress and egress data and protocols between systems and networks are identified and documented as part of network baselines.

CNS-6 – Communication Protocol Requirements

Relevant NIST CSF Controls:

- PR.DS-2: Data-in-transit is protected.

Minimum requirement for communication interface 1, 2, 3, 4, 7, and 8.

Recommended requirement for communication interface 5, 6, 9, and 10.

CNS-6.1 – Communications are authenticated, encrypted, authorized, and verified through industry-accepted cryptographic mechanisms and digital certificates.

CNS-6.2 – Communication protocols use the latest state-of-the-art cypher suites and have capabilities to update to network cryptographic standards as older versions become obsolete.

CNS-6.3 – Certificates have expiration date and entities have programs and processes to update certificates as they expire or become revoked.

CNS-6.4 – Systems have the capability to check the status of presented certificates either through communications of online-certificate status protocol (OCSP) to a trusted certificate authority or through OCSP stapling prior to presentation of the certificate.

CNS-6.5 – Entities involved in the public key infrastructure (PKI) ecosystem, including system operators, aggregators, certificate authorities, and DER owners, all have procedures and processes to protect private keys and have incident response procedures in the event a private key becomes compromised.

User and System Access Control (USAC) Specifications

The monitoring and control hierarchy is expected to require access to data and functions hosted by utility DERMS, L-DERMS, A-DERMS, and individual DER. Access to a particular system may be required by multiple organizations, including aggregators, utilities, device manufacturers, customers, etc. Ultimately it is the owner or maintainer of a system that is responsible for the provisioning and deprovisioning of access, the assignment of the appropriate role for users and systems, the maintenance of access control lists (ACLs), and monitoring of user activity.

As discussed in the ENGAGE control and monitoring hierarchy architecture, certain systems, such as L-DERMS and A-DERMS, are expected to only require limited control and monitoring to upstream entities. Permissions within these systems must be carefully configured to ensure that data and control privileges are reflective of B2B contracts. Excessive access to controls beyond what is required by contracts, for example, can expose A-DERMS, L-DERMS, and downstream DER systems to system manipulation. Likewise, excessive access to data increases opportunity for exfiltration of sensitive customer energy use and production data.

USAC-1 – User and System Access Requirements

Relevant NIST-CSF Controls:

PR.AC-1: Identities and credentials are managed for authorized devices and users

PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties

PR.MA-1: Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools

PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality

Minimum requirement for systems within all interfaces (1-10):

USAC-1.1 – All electronic access to the system required authentication where users identify themselves through a username and password.

USAC-1.2 – User-created passwords should be at least eight characters in length and should be case sensitive. It should not use common dictionary words and/or consecutive and repeatable characters. Password characters should contain the following:

- At least one uppercase and one lower case letter
- At least one number
- At least one non-alphanumeric character (e.g., @, %, &, *)

USAC-1.3 – Default passwords and accounts should be changed or removed upon installation of the system.

USAC-1.4 – For system-to-system access, authentication should be achieved through device certificates or tokens.

USAC-1.5 – All electronic access to the system requires authorization where the system determines the appropriate system rights and privileges to the system's data and functions.

USAC-1.6 – All user activity to the system and changes to accounts and their permissions are logged to allow for traceability and audit.

Additional requirements for Utility-DERMS and A-DERMS within all interfaces (1,2,3,4,7, and 8):

USAC-1.7 – Electronic access to the system requires authentication where administrative or higher-privilege users identify themselves with additional factors (multi-factor authentication) in addition to passwords. These can include biometrics, hardware or software-based tokens, access cards, etc.

USAC-1.8 – The principle of least-privilege is used for the design of access control lists, such that users are only provisioned access to system data and functions that reflect their expected job duties and functions.

USAC-1.9 – User activity is logged, aggregated, and correlated within a centralized monitoring system, such as a Security Information and Event Management (SIEM) system.

USAC-1.10 – Users are automatically logged out of the system after a period of user inactivity.

USAC-1.11 – Systems authenticate upstream and downstream systems through the use of certificate whitelists.

Patch and Vulnerability Management (PVM) Specifications

New security vulnerabilities are expected to be discovered throughout the lifetime of devices. Each entity within the DER architecture should be expected to have their devices enrolled in a patch management program. As discussed in earlier chapters, two challenges are expected to be encountered: 1) scaling patches across numerous DER devices geographically and logically dispersed across multiple networks and 2) coordination of patch updates across systems participating in inter-organizational transactions.

Relevant NIST-CSF Controls:

DE.CM-8: Vulnerability scans are performed.

PR.IP-12: A vulnerability management plan is developed and implemented.

PVM-1 – Vulnerability Scanning

Minimum requirement for systems within interfaces (1, 2 , 3, 4, 7, 8):

PVM-1.1 – Entities perform periodic vulnerability scans against systems which they are responsible for maintaining to identify open ports, unpatched operating systems, software, and firmware.

PVM-1.2 – Entities test vulnerability scans within a reference test environment to ensure that scans do not incidentally cause denial-of-service of networks and systems and degradation on needed performance.

PVM-2 – Patch Management

Minimum requirement for systems within interfaces (1, 2, 3, 4, 7, 8):

PVM-2.1 – Each entity monitors for disclosure of new security vulnerabilities for systems which they are responsible for maintaining.

PVM-2.2 – Patches are authenticated through the use of digital signatures before they are applied to systems.

PVM-2.3– Patches are tested within a safe environment before they are deployed for production.

Recommended requirements for systems within interfaces (1, 2, 3, 4, 7, 8):

PVM-2.3– Entities involved in inter-organizational interactions provide a reference system implantation for the interfacing third-party to ensure continuity of system interoperability after the application of patches, system updates, or configuration updates.

Security Logging and Monitoring (SLM) Specifications

Systems are expected to perform security logging to ensure detection of threat indicators of compromise (IoC). Monitoring of IoC enables execution of the appropriate incident response courses-of-action for any attempted or successful cyber-attacks. DER interoperability architectures are expected to present a challenge where no single entity will have full security monitoring end-to-end due to differing ownership of interfacing systems. For example, utility security operations will likely only able to collect security log information from their own DERMS, but they will not have purview over security events related to A-DERMS, L-DERMS, and other behind-the-meter DER systems. Thus, each entity within the architecture must be held responsible for monitoring security events of systems which they own and maintain.

Relevant NIST-CSF Controls:

DE.AE-2: Detected events are analyzed to understand attack targets and methods

DE.AE-3: Event data are collected and correlated from multiple sources and sensors

DE.AE-4: Impact of events is determined

DE.AE-5: Incident alert thresholds are established

DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events

SLM-1 – Security Logging

Minimum requirements for systems within all interfaces (1-10):

SLM-1.1 – Each system should be capable of logging security related events. These logs should include, but not be limited to:

- Successful and unsuccessful login attempts
- Detection of malicious code
- Software/firmware installation events
- Configuration changes
- Malicious code detection
- User activities

Minimum requirement for systems within interfaces (1, 2, 3, 4, 7, 8):

SLM-1.2 – Each system sends security related logs to a centralized Security Information and Event Management (SIEM) for aggregation. The SIEM determines the criticality of potential events relative to potential impact against grid reliability, safety, privacy, and financial consequences.

SLM-1.3 – Each entity reports security related events to interfacing third-parties if it is regarded that the event has a potential impact to peer systems.

4
CONCLUSIONS

In this work, communication interfaces were identified for the DERMS hierarchical architecture. Individual qualitative risk ratings and attack vectors were discussed for each of these interfaces and helped inform the necessary cybersecurity controls specifications to ensure confidentiality of private data, integrity of interactions, and availability of systems and communications. These specifications help to address some of the challenges expected to be encountered for a multi-party architecture where inter-organization interactions are expected to be inherently required for interoperability. The specifications help to ensure a defense-in-depth approach to help lower the likelihood and impact of cyber-attacks against power systems involved in DER architectures.

5
REFERENCES

1. EPRI. *Demand Response Interoperability Guidebook A Repository of Information to Support Utilities in Achieving Interoperability in Demand Response Technologies*. https://www.epri.com/research/products/000000003002018543
2. Cybersecurity & Infrastructure Security Agency. *Security Tip (ST05-003): Securing Wireless Networks*. March 11, 2020 https://us-cert.cisa.gov/ncas/tips/ST05-003
3. *National Electric Sector Cybersecurity Organization Resource (NESCOR) Electric Sector Failure Scenarios & Impact Analysis – Version 3.0*. EPRI. https://smartgrid.epri.com/NESCOR.aspx
4. *Framework for Improving Critical Infrastructure Cybersecurity – Version 1.1*. NIST. April 16, 2018 https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

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

3002022403

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