October, 2015

Cyber Security Requirements and Recommendations for CSI RD&D Solicitation #4 Distributed Energy Resource Communications

Jordan Henry, Rick Ramirez, Sandia National Laboratories

Frances Cleveland, Xanthus Consulting International

Annabelle Lee, Brian Seal, Electric Power Research Institute

Tom Tansy, Bob Fox, Anil Pochiraju, SunSpec Alliance

Cyber Security Requirements and Recommendations for CSI RD&D Solicitation #4 Distributed Energy Resource Communications

Jordan Henry, Frances Cleveland, Annabelle Lee, Rick Ramirez, Brian Seal, Tom Tansy, Bob Fox, Anil Pochiraju

Abstract

This California Solar Initiative (CSI) RD&D Solicitation #4 Distributed Energy Resource (DER) cyber security document provides cyber security recommendations for residential inverter-based DER assets that use a removable communications module. The communications module is a CEA-2045 snap-in module that is responsible for translating wide area network (WAN) communications, such as OpenADR 2.0b and IEEE 2030.5 (SEP2), into SunSpec Modbus messages which are supported by most residential DER systems. Specific communications addressed in the scope include communications between a utility or aggregator/vendor and the inverter via the CEA-2045 communication module. This includes the local interface between the module and the DER system itself. The cyber security recommendations are based on impact levels of low, moderate, and high for the various security requirements and security objectives. Threat analysis, functional scoring, best practices, and practical considerations were all considered during the development of the recommendations.

Table of Contents

1 EXECUTIVE SUMMARY 1-1
2 BACKGROUND 2-1

2.1 Scope 2-1
2.2 Objectives 2-3
2.3 Utility DER Communication Architecture 2-4

3 INCORPORATION OF INDUSTRY STANDARDS 3-1

3.1 Cyber Security High Level Guidance 3-1
3.2 Communication Application Layer Cyber Security Standards and Guidelines 3-2
3.3 Transport Layer Cyber Security Standards 3-2
3.4 Wireless Cryptography 3-3
3.5 Some Additional Cyber Security Techniques 3-4

4 THREATS, VULNERABILITIES, AND IMPACTS ON POWER SYSTEM RESILIENCE WITH DER SYSTEMS 4-1

4.1 Resilience and Cyber Security 4-1
4.2 Threats – Engineering and Cyber 4-2
4.2.1 Physical and Electrical Threats – Mostly but Not Entirely Inadvertent 4-2
4.2.2 Cyber Threats – Inadvertent and Deliberate 4-3

4.3 Vulnerabilities – Engineering and Cyber Vulnerabilities 4-6
4.3.1 Power System Vulnerabilities and Attacks 4-7
4.3.2 Cyber Security Vulnerabilities and Attacks 4-9

4.4 Risk Management and Mitigation Techniques 4-11
4.4.1 Risk Handling 4-11
4.4.2 Risk Mitigation Categories 4-12

5 CYBER SECURITY RECOMMENDATIONS METHODOLOGY 5-1

5.1 Methodology Overview 5-1
5.2 Inverter Functions 5-2
5.3 Security Assessment 5-6
5.4 Inclusion of Threat 5-8
5.5 Analysis 5-8

6 CYBER SECURITY RECOMMENDATIONS FOR CSI RD&D SOLICITATION #4 DER COMMUNICATION MODULES 6-1

6.1 Cyber Security Recommendation Categories 6-1
6.2 Interface A: CSI RD&D Solicitation #4 DER Cyber Security Recommendations 6-1
6.3 Interface B: CSI RD&D Solicitation #4 DER Cyber Security Recommendations 6-4

6.4 Cyber Security for Communication Protocols 6-6
6.4.1 IEEE 2030.5 (SEP2) Cyber Security 6-6
6.4.2 IEEE 1815 (DNP3) Cyber Security 6-8

7 SUMMARY 7-1
APPENDIX A – CYBER SECURITY SCORING OF DER FUNCTIONS FOR RESIDENTIAL DER SYSTEM A-1

List of Figures

Figure 1: CSI RD & D Solicitation #4 DER Cyber Security Scope 2-1
Figure 2: Communications between Utilities and individual DER systems, FDEMS, and REPS ... 2-2
Figure 3: Scope of EPRI CSI RD&D Solicitation #4 Interactions with DER Systems within Residential Sites 2-3
Figure 4: Five-Level Hierarchical DER System Architecture 2-4
Figure 5: Security Requirements, Threats, and Possible Attacks 4-11

List of Tables

Table 1: Mitigation Categories for Cyber-Physical Systems 4-14
Table 2: DER Inverter Function List 5-2
Table 3: Cyber Security Recommendations for CSI RD&D Solicitation #4 DER Communication: Interface A 6-2
Table 4: Cyber Security Recommendations for CSI RD&D Solicitation #4 DER Communication: Interface B 6-4
Table 5: IEEE 2030.5 Security Measures 6-7
Table A1: Cyber Security Scoring of DER Functions: Communication Module to Utility A-1
Table A2: Cyber Security Scoring of DER Functions: Communication Module to Aggregator/Vendor A-9
Table A3: Cyber Security Scoring of DER Functions: Communication Module to DER A-17

Nomenclature

ACL: Access Control List.
AES: Advanced Encryption Standard.
BITW: Bump In The Wire.
CA: Certificate Authority.
CIM: Common Information Model.
CRL: Certificate Revocation List.
CSI4: California Solar Initiative 4.
DER: Distributed Energy Resource.
DERMS: DER Database and Management Systems.
DMS: Distribution Management Systems.
DNP3: Distributed Network Protocol 3.0.
DR: Demand Response.
DSO: Distribution System Operators.
EAP: Extensible Authentication Protocol.
ECP: Electrical Connection Points.
FDEMS: Facility DER Energy Management System.
FIPS: Federal Information Processing Standards.
GIS: Geographical Information System.
HEMS: Home Energy Management System.
HTTPS: Hyper-Text Transfer Protocol.
ICCP: Inter-Control Center Protocol.
ICS: Industrial Control System.
IDS: Intrusion Detection System.
IEC: International Electromechanical Commission.
IED: Intelligent Electronic Device.
IEEE: Institute of Electrical and Electronics Engineers.
IP: Internet Protocol.
IPS: Intrusion Prevention System.
IPsec: Internet Protocol Security.
ISO: Independent System Operators.
MMS: Manufacturing Message Specification.
NAT: Network Address Translation.
NERC: North American Electric Reliability Council.
NIST: National Institute of Standards and Technology.
OCSP: Online Certificate Status Protocol.
OMS: Outage Management System.
PCC: Point of Common Coupling.
PKI: Public Key Infrastructure.
REP: Retail Energy Provider.
RFC: Request For Comment.
RTO: Regional Transmission Operators.

SCADA: Supervisory Control and Data Acquisition.
SEP2: Smart Energy Profile 2.0.
SGIP: Smart Grid Interoperability Panel.
SIWG: Smart Inverter Working Group.
TBLM: Transmission Bus Load Model.
TCP: Transmission Control Protocol.
TLS: Transport Layer Security.
TSO: Transmission System Operators.
VPN: Virtual Private Network.
WAN: Wide Area Network.
XML: Extensible Markup Language.

1 EXECUTIVE SUMMARY

This CSI RD & D Solicitation #4 Distributed Energy Resource (DER) cyber security document provides cyber security recommendations for smart residential inverter-based DER assets that use the SunSpec Modbus protocol and CEA-2045 communications module as well as for wide-area communication systems that use protocols such as OpenADR 2.0b and IEEE 2030.5. The Consumer Electronics Association CEA-2045 communications module is a plug-in device, responsible for translating wide area network (WAN) communications into SunSpec Modbus messages which are supported by most residential DER systems. Specific communications addressed in the scope include communications between:

- A utility and the communication module
- An aggregator/vendor and the communication module
- The communication module and the DER system itself

The cyber security recommendations in this document are based on impact levels of low, moderate, and high assigned to the security requirements. Threat analysis, functional scoring, best practices, and practical considerations were all considered during the development of the recommendations.

This project formed a cybersecurity working group that developed this report. The cybersecurity working group scoring results for all three residential DER communication interfaces can be found in Appendix A. The scores generally indicate that:

- Authentication and integrity of data are the most important cyber security requirements, and were assessed to be critical for all types of interactions, including monitoring and control commands, to ensure that the data exchanged comes from known sources and has not been modified in transit.
- Authorization and non-repudiation are important to ensure that commands are authorized, executed as specified, and reported back accurately.
- Availability is less critical since DER systems usually operate autonomously and can be preset to perform the DER functions.

Confidentiality is only important for select DER functions where either privacy or sensitive data is being exchanged, such as personal information or contractual data. For residential DER systems, it is not expected that much confidential data will be exchanged.

Cyber security recommendations are then enumerated in Sections 6.2 and 6.3. The recommendations are meant to work in tandem with applicable industry standard best practices (Section 3), not replace them.

2 BACKGROUND

2.1 Scope

The scope of this California Solar Initiative 4 (CSI RD&D Solicitation #4) Distributed Energy Resource (DER) cyber security document covers cyber security for the communications of residential inverter-based DER assets using the CEA-2045 format communications module.

The communications module is a plug-in device in the Consumer Electronics Association's CEA-2045 format, responsible for translating wide area network (WAN) communications, such as IEEE 2030.5 (SEP2), into SunSpec Modbus messages which are supported by most residential DER systems. Specific communications addressed in the scope include communications between:

- A utility and the communication module
- An aggregator/vendor and the communication module
- The communication module and the DER system

Outside the scope of this document are interfaces that do not use the communications module. For instance, the following are excluded: communication interfaces for commercial, industrial, and utility owned DERs, communication interfaces for non-inverter-based DERs, and utility-to-aggregator communication interfaces. Additionally, this document does not address communication interfaces from utilities or aggregators to home energy management systems (HEMS), to facility DER energy management systems (FDEMS), or to other DER proxies such as data concentrators/gateways.

The scope is illustrated most succinctly in Figure 1. As depicted in the figure, the scope includes DER communication interfaces "A" and "B", where interface "A" represents the first two scope bullets above and interface "B" represents the third scope bullet above. Communication interface "A" is the network interface that connects from the utility or aggregator/vendor to the communications module, while communication interface "B" is local between the communications module and the DER system.

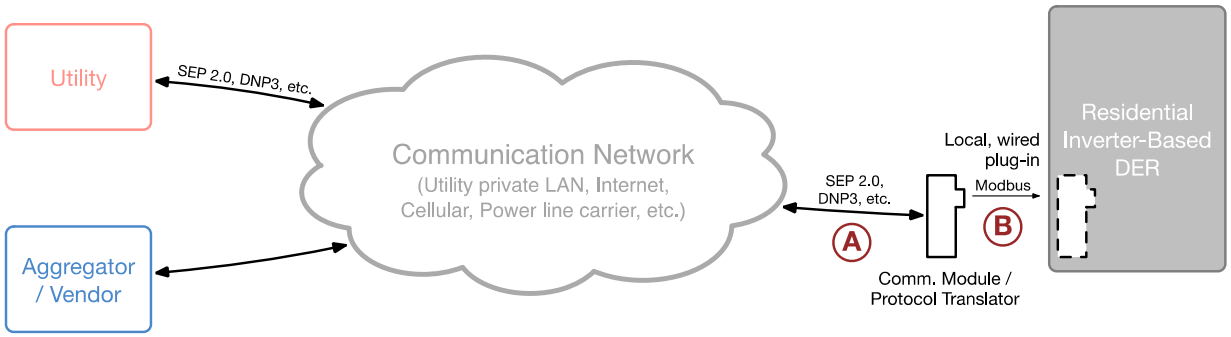

Figure 1: CSI RD & D Solicitation #4 DER Cyber Security Scope

One of the motivators of the CSI RD&D Solicitation #4 project was California's Smart Inverter Working Group (SIWG) effort to define the functional and communications requirements for inverter-based DER systems within California. The SIWG Phase 2 communications scope is illustrated in Figure 2 and comprises the communications requirements between (see red lightning bolts indicating Wide Area Networks):

1. Utilities and individual DER Systems
2. Utilities and Facility DER Energy Management Systems (FDEMS) which manage DER systems within a facility, plant, and/or microgrid
3. Utilities and Retail Energy Providers (REP) / Aggregators / Fleet Operators which manage and operate DER systems at various facilities

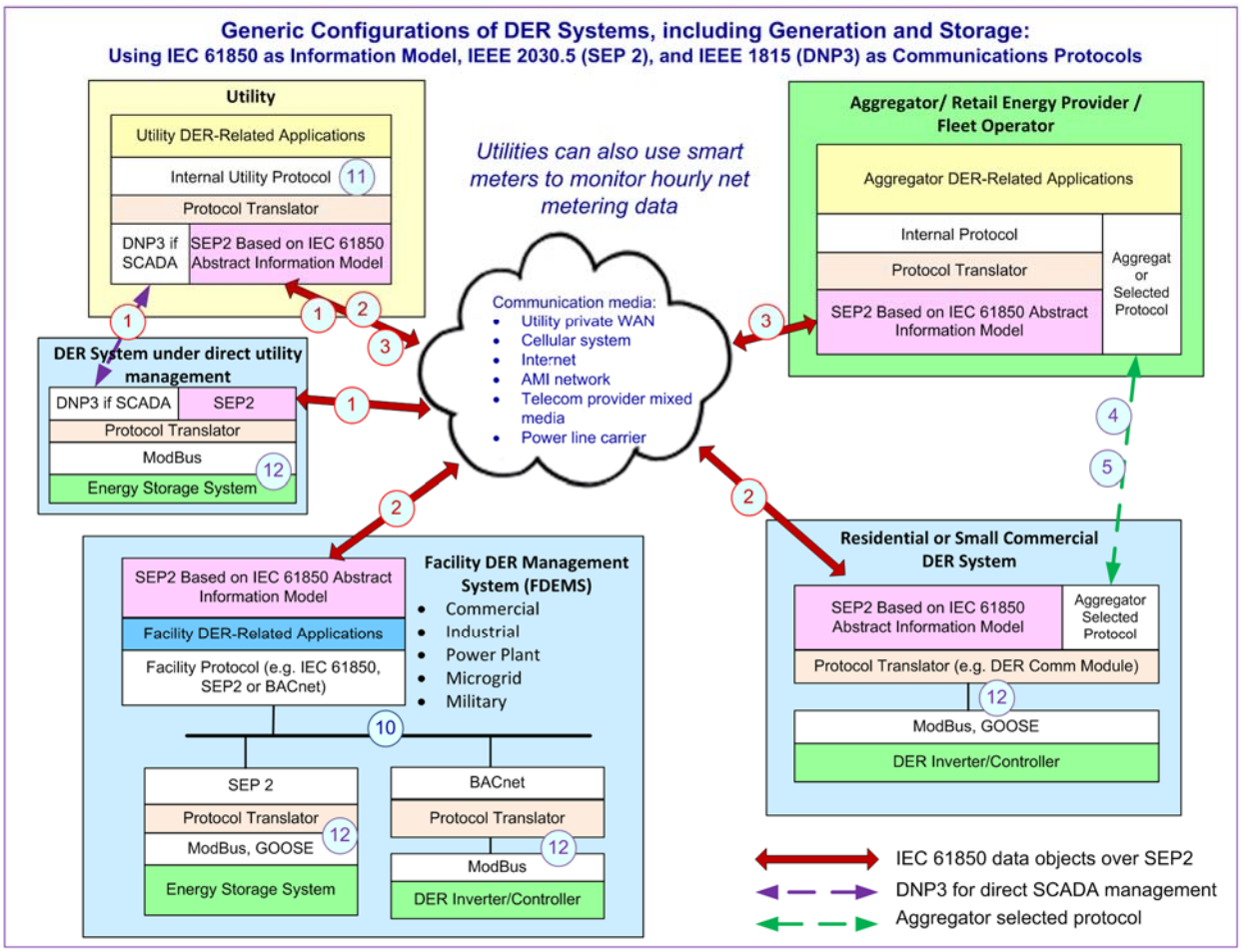

Figure 2: Communications between Utilities and individual DER systems, FDEMS, and REPS

The circled numbers #2, #5, and #12 within the residential box at the lower right side of the figure illustrate the project's scope as it relates to the Smart Inverter Working Group (SIWG), assuming that the interfaces #2 and #5 are with the DER system and not a home energy management system. Notice that the project effort's scope is significantly narrower and fundamentally different from that of the SIWG. The SIWG Phase 2 recommendations for updates to Rule 21 only focus on the

communications interfaces at the utilities and leave the broader scope of exactly what is recommended at the DER facilities to other efforts, such as the CSI RD & D Solicitation #4 project.

Another diagram Figure 3 can be used to illustrate the scope of the CSI RD&D Solicitation #4 project, which addresses the cyber security requirements at the communication module.

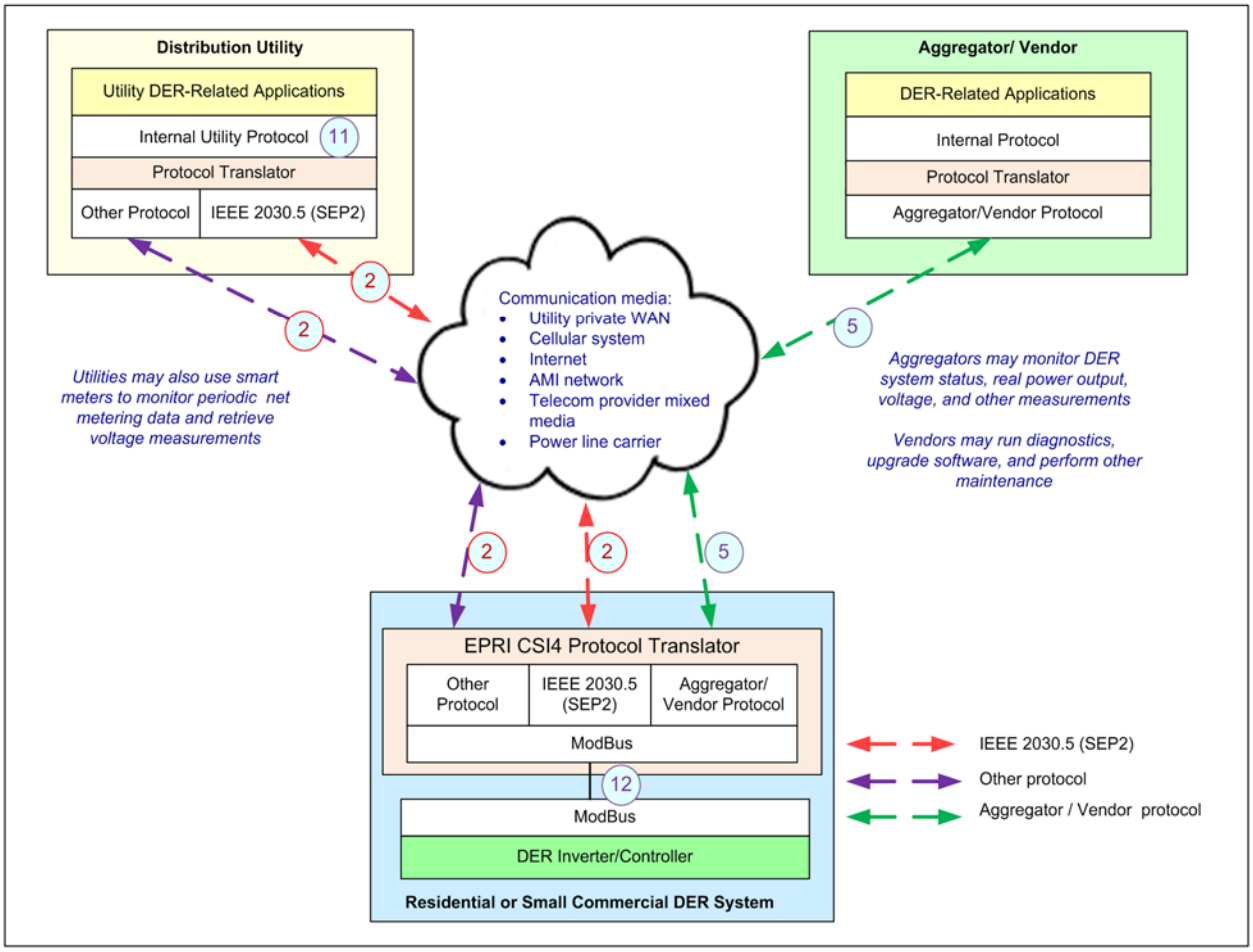

Figure 3: Scope of EPRI CSI RD&D Solicitation #4 Interactions with DER Systems within Residential Sites

2.2 Objectives

The objectives of this document are first, to provide general information on cyber security concerns related to residential inverter-based DER communications, covering cyber security policies, procedures, and technologies that can be used to mitigate these cyber security concerns, and secondly, to recommend specific cyber security solutions for the communications interfaces with CSI RD&D Solicitation #4 DER communications modules.

In particular, this document will present general recommendations – using a logical taxonomy that mimics the National Institute of Standards and Technology Interagency Report (NISTIR) 7628 and NIST Special Publication (SP) 800-53, rev 4 control classes – that address cyber security for any size residential inverter-based DER communications interfaces in a holistic fashion. This document also

provides cyber security implementation guidance for IEEE 2030.5 (SEP2), IEEE 1815 (DNP3), and Modbus.

2.3 Utility DER Communication Architecture

In the SIWG, in the Smart Grid Interoperability Panel (SGIP), and in other forums, the hierarchical architecture of DER systems has been developed and illustrated as in Figure 4.

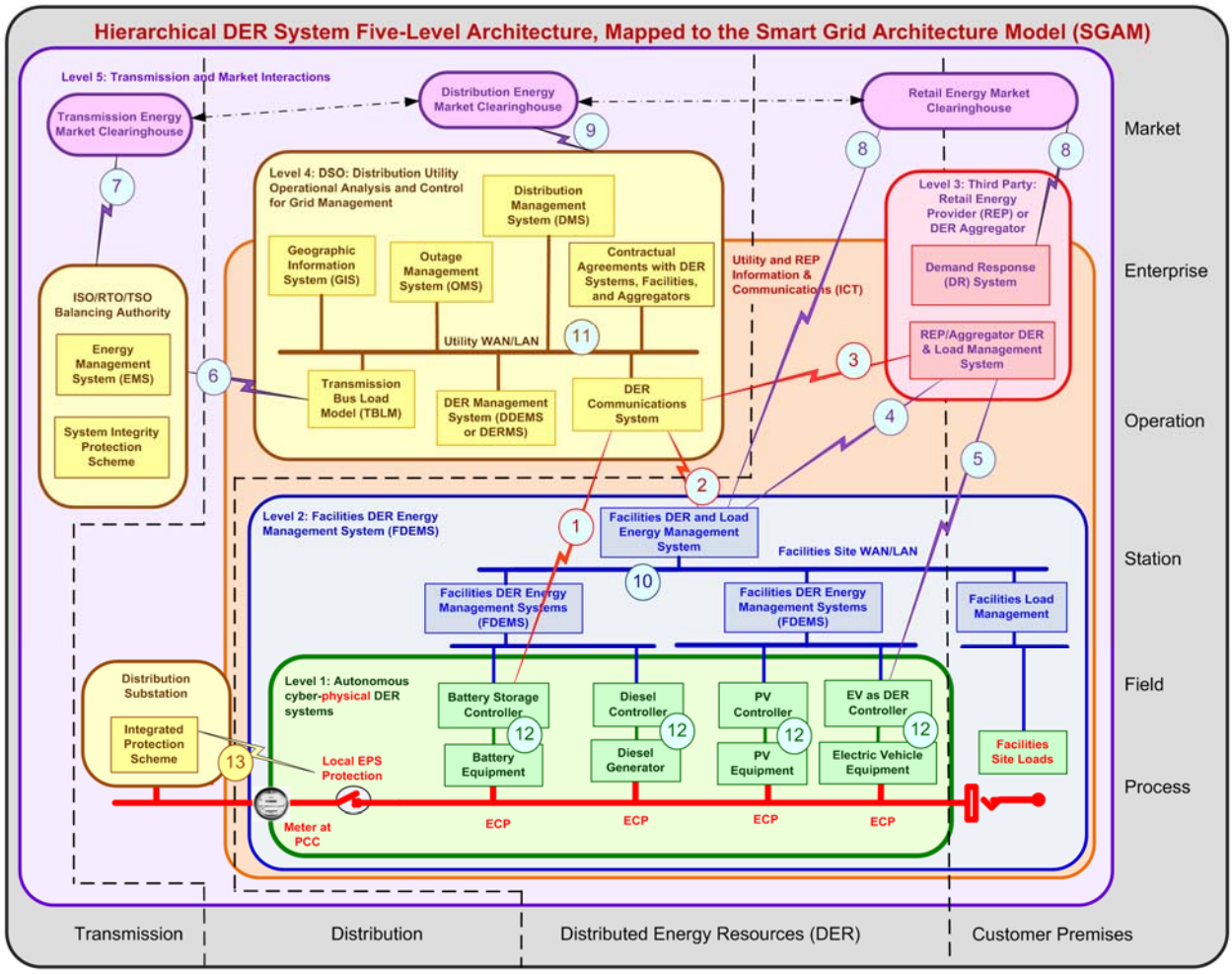

Figure 4: Five-Level Hierarchical DER System Architecture

The five different levels are described as:

1. **Level 1 DER Systems** (green in the Figure) is the lowest level and includes the cyber-physical DER systems. These DER systems are interconnected to local grids at Electrical Connection Points (ECPs) and to the utility grid through the Point of Common Coupling (PCC) (the ECP and the PCC may be the same if the DER is directly grid-connected). These DER systems will usually be operated autonomously. In other words, these DER systems will be running based on local conditions, such as photovoltaic systems operating when the sun is shining, wind turbines operating when the wind is blowing, electric vehicles charging when plugged in by the owner, and diesel generators

operating when started up by the customer. This autonomous operation can be modified by DER owner preferences, pre-set parameter, and commands issued by utilities and aggregators.

2. **Level 2 Facility DER Management** (blue in the Figure) is the next higher level in which a facility DER management system (FDEMS) manages the operation of the Level 1 DER systems. This FDEMS may be managing one or two DER systems in a residential home, but more likely will be managing multiple DER systems in commercial and industrial sites, such as university campuses and shopping malls. Utilities may also use a FDEMS to handle DER systems located at utility sites such as substations or power plant sites.
3. **Level 3 Third Parties: Retail Energy Provider or Aggregators** (red in the Figure) shows market-based aggregators and retail energy providers (REP) who request or even command DER systems (either through the facility's FDEMS or via aggregator-provided direct communication links) to take specific actions, such as turning on or off, setting or limiting output, providing ancillary services (e.g. volt-var control), and other grid management functions. Aggregator DER commands would likely be price-based either to minimize customer costs or in response to utility requirements for safety and reliability purposes. The combination of this level and level 2 may have varying scenarios, while still fundamentally providing the same services.
4. **Level 4 Distribution Utility Operational Grid Management** (yellow in the Figure) applies to utility applications that are needed to determine what requests or commands should be issued to which DER systems. Distribution System Operators (DSOs) will monitor the power system and assess if efficiency or reliability of the power system can be improved by having DER systems modify their operation. This utility assessment involves many utility control center systems, orchestrated by the Distribution Management System (DMS) and including the DER database and management systems (DERMS), Geographical Information Systems (GIS), Transmission Bus Load Model (TBLM), Outage Management Systems (OMS), and Demand Response (DR) systems. Once the utility has determined that modified requests or commands should be issued, it will send these either directly to a DER system, indirectly through the FDEMS, or indirectly through the REP/Aggregator.
5. **Level 5 Transmission and Market Operations** (purple in the Figure) is the highest level, and involves the larger utility environment where Transmission System Operators (TSOs), regional transmission operators (RTOs), or independent system operators (ISOs) may need information about DER capabilities or operations and/or may request aggregated services for the bulk power system from DER systems through the distribution utility or through the REP/Aggregators. These aggregated services may be established through contracts, tariffs, or market operations.

Although in general DER systems will be part of a hierarchy, different scenarios will consist of different hierarchical levels and variations even within the same hierarchical level. For instance, small residential PV systems may not include sophisticated Facilities DER Energy Management Systems (FDEMS), while large industrial and commercial sites could include multiple FDEMS and even multiple levels of FDEMS. Some DER systems will be managed by aggregators through

demand response programs, while others may be managed (not necessarily directly controlled) by utilities through financial and operational contracts or tariffs with DER owners.

3 INCORPORATION OF INDUSTRY STANDARDS

Smart Grid cyber security industry standards are procedural and technical rules generally accepted (if not widely implemented) by the industry as critical to improve the safety, reliability, security, sustainability, and cost effectiveness of grid operations. Following these industry standards can save time and money, and offer benefits of increased security to both utilities and consumers alike. Some Smart Grid cyber security industry standards even offer guidelines that have been tested and proven to enable higher levels of reliability and security for DER communications. Applicability of relevant standards from different industries should also never go overlooked and incorporated where possible.

3.1 Cyber Security High Level Guidance

Some applicable Smart Grid cyber security guidelines, industrial standards, and technical specifications are:

- **NISTIR 7628 Guidelines for Smart Grid Cybersecurity, rev 1**; the Smart Grid Interoperability Panel Cyber Security Working Group, September 2014. This is a 3 volume report including Smart Grid Cybersecurity Strategy, Architecture, and High Level Requirements, Privacy and the Smart Grid, and Supportive Analyses and References.
- **North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Cyber Security Standards 002-009;** this is a series of standards including Critical Cyber Asset Identifications, Security Management Controls, Personnel and Training, Electronic Security Parameters, Physical Security of Critical Cyber assets, Systems Security Management, Incident Reporting and Response a Planning, Recovery Plans for Critical Cyber Assets.
- **IEC/ISO 27001, 27002, and 27019:** Information Security Standards, with 27019 focused on electric power industry.
- **NIST SP 800-53 Security and Privacy Controls for Federal Information Systems and Organizations, Rev 4**; This publication covers the steps in the Risk Management Framework that address security control selection for federal information systems in accordance with the security requirements in Federal Information Processing Standard (FIPS) 200.
- **NIST SP 800-82 Guide to Industrial Control Systems (ICS) Security, rev 2**: this is a guide for securing ICS including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control systems used in electric, water and wastewater, oil and natural gas, chemical, pharmaceutical, pulp and paper, food and beverage, and discrete manufacturing industries.
- **IEC 62351 Parts 8-13, Information Security for Power System Control Operations**: defines high level security requirements for power system management and information exchange, including role-based access control, key management, security architecture, XML security, DER resilience, and cyber security requirements in standards.

- **IEC 62443 Series on Security for Industrial Processes:** measurement and control *(work in process)*
- **IEEE 1686 Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities** *(being updated)*
- **CIGRE B5/D2.46:** Application and management of cyber security measures for Protection & Control systems
- **CIGRE D2.31 Security architecture principles** for digital systems in Electric Power Utilities EPUs
- **DOE / DHS Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)**
- **DOE/NIST/NERC Electricity Subsector Cybersecurity Risk Management Process Guideline**

3.2 Communication Application Layer Cyber Security Standards and Guidelines

Communications have very specific cyber security requirements

- **IEC 62351 Parts 1-7, Information Security for Power System Control Operations**: defines security requirements for power system management and information exchange, including security for TCP/IP and MMS profiles, security for IEC 61850, DNP3, ICCP, and communications network management.
- **IEEE 2030.5 (SEP2):** defines cyber security requirements for the SEP2 protocol.
- **IEEE 1815 (DNP3)**: defines cyber security requirements for DNP3.

3.3 Transport Layer Cyber Security Standards

Some applicable Transport Layer security requirements include:

- **IETF RFC 6272 Internet Protocols for the Smart Grid** (identifies RFCs used in the Smart Grid)
- **Transport Layer Security (TLS)** was derived from Secure Sockets Layer (SSL) and specifies asymmetric cryptography for authentication of key exchanges via a Public Key Infrastructure (PKI), symmetric encryption for confidentiality, and message authentication codes for message integrity. As indicated by the name, TLS provides security for the transport layer. Although the most commonly implemented version is still TLS 1.0, the newest version TLS v 1.2, defined in RFC 5246, should be specified for new implementations. TLS includes many alternative cipher suites – these could or should be pared down to a few in specifications to ensure that implementations provide adequate security and interoperability. IEC 62351-3 Ed 2 provides such a specification.

- **Hypertext Transfer Protocol Security (HTTPS)** is a combining of HTTP over TLS, and is formalized in RFC 2818.
- **Internet Protocol Security (IPsec)** authenticates and encrypts each IP packet as well as providing mutual authentication at the start of a session, thus providing security at the Network Layer rather than at the Transport Layer. IPsec is covered in RFCs 4101, RFC 4102, RFC 4103 Base standards for IP Security.
- **Virtual Private Network (VPN)** creates a "tunnel" through the Internet (or other network) in which the entire IP packet is encrypted and then encapsulated into another IP packet. IPsec is often used to create the secure tunnel, although TLS and other security protocols can also be used.
- **The Group Domain Of Interpretation (GDOI) method** defined in RFC 6407 supports the distribution of a symmetric group key to all pre-configured or otherwise enrolled entities, typically devices.
- **RFC 6347 Datagram Transport Layer Security (DTLS)**
- **RFC 3711 Secure Real-time Transport Protocol (SRTP)**
- **RFC 4962 Authentication, Authorization, and Accounting**
- **RFC 5247 Extensible Authentication Protocol (EAP)** Key Management Framework
- **RFC 5746 Transport Layer Security (TLS) Renegotiation Indication Extension**
- **RFC 2712:1999**, Addition of Kerberos Cipher Suites to Transport Later Security (TLS)
- **RFC 3268**, 2002, Advanced Encryption Standard (AES) Cipher suites for Transport Layer Security (TLS)
- **FIPS 186-2**, Digital Signature Standard (DSS)
- **RFC 3447**, Public-Key Cryptography Standards (PKCS) #1; RSA Cryptography Specifications, Version 2.1

3.4 Wireless Cryptography

Wireless cryptography systems use the security provided by **IEEE 802.11i WPA2**, which establishes a Robust Security Network (RSN) that uses the Advanced Encryption Standard (AES) block cipher (as do most cipher suites at this time), requires the Counter with Cipher Block Chaining Message Authentication Code (CCM) Protocol (CCMP) for a 4-way handshake between two stations, and the includes a Group Key Handshake. Some suggestions for managing WiFi could include:

- Using centrally managed WiFi infrastructures and the authentication
- Adopting the IEEE 801.1x authentication infrastructure
- Adopting a rogue AP detection mechanism

The **Extensible Authentication Protocol (EAP)** is an authentication framework frequently used in wireless networks and point-to-point connections. It is defined in RFC 3748 and was updated by

RFC 5247. EAP is one of the possible authentication schema of the more general IEEE 801.1x standard that is the de-facto mandatory standard for WiFi enterprise deployment, and it is also applicable to wired LANs. When applied to wired LANs, 802.1x can allow a logical segregation of VLAN inside the same physical infrastructure. 802.1x is a role based Network Access Control mechanism and brings the RBAC model to LAN access control.

3.5 Some Additional Cyber Security Techniques

Some additional cyber security techniques include the following:

- **Network Address Translation (NAT)** functions isolate systems from direct access by external systems. They are often included in WiFi network routers, in which a single Internet IP is provided to a site, and is shared by all networked devices at that site. The NAT handles all interactions with the Internet and passes only authorized messages to the systems behind the NAT router, thus providing security against unauthorized traffic.
- **Access Control Lists (ACL)** are used in routers to limit which ports and/or IP addresses are permitted to be accessed by which entities.
- **Intrusion Detection and Prevention systems (IDS and IPS)** monitor networks for malicious or impermissible traffic. The IDS can detect such malicious traffic and notify users, while an IPS can actually block malicious traffic and support prevention of addition traffic from a suspect IP address.

4 THREATS, VULNERABILITIES, AND IMPACTS ON POWER SYSTEM RESILIENCE WITH DER SYSTEMS

4.1 Resilience and Cyber Security

In the energy sector, two key phrases are becoming the focus of international and national policies: "grid resilience" and "cyber security of the cyber-physical grid". Grid resilience responds to the overarching concern: *"The critical infrastructure, the Smart Electric Grid, must be resilient - to be protected against both physical and cyber problems when possible, but also to cope with and recover from the inevitable disruptive event, no matter what the cause of that problem is - cyber, physical, malicious, or inadvertent."*

"Grid resilience … includes hardening, advanced capabilities, and recovery/reconstitution. Although most attention is placed on best practices for hardening, resilience strategies must also consider options to improve grid flexibility and control."[1] Resilience of the grid is often associated with making the grid able to withstand and recover from severe weather and other physical events, but resilience should also include the ability of the cyber-physical grid to withstand and recover from malicious and inadvertent cyber events.

Resilience, sometimes defined as "*the fast recovery with continued operations from any type of disruption*" can be applied to the power system critical infrastructure. A resilient power system is designed and operated not only to prevent and withstand malicious attacks and inadvertent failures, but also to detect, assess, cope with, recover from, and eventually analyze such attacks and failures in a timely manner while continuing to respond to any additional threats.

The "cyber-physical grid" implies that the power system consists of both cyber and physical assets that are tightly intertwined. Both the cyber assets and the physical assets must be protected in order for the grid to be resilient. But protection of these assets is not enough: these cyber and physical assets must also be used in combination to cope with and recover from both cyber and physical attacks into order to truly improve the Resilience of the power system infrastructure.

All too often, cyber security experts concentrate only on traditional "IT cyber security" for protecting the cyber assets, without focusing on the overall resilience of the physical systems. At the same time, power system experts concentrate only on traditional "power system security" based on the engineering design and operational strategies that keep the physical and electrical assets safe and functioning correctly, without focusing on the security of the cyber assets. However, the two must be combined: resilience of the overall cyber-physical system must include tightly entwined cyber security technologies and physical asset engineering and operations, combined with risk management to ensure appropriate levels of mitigation strategies.

[1] "*Economic Benefits of Increasing Electric Grid Resilience to Weather Outages*," Executive Office of the President, August 2013. See http://www.smartgrid.gov/sites/default/files/doc/files/Grid%20Resilience%20Report_FINAL.pdf

As an example, distributed energy resources (DER) systems are cyber-physical systems that are increasingly being interconnected to the distribution power system to provide energy and ancillary services. However, distribution power systems were not originally designed to handle these dispersed sources of generation, while DER systems are generally not under direct utility management or under the security policies and procedures of the utilities. Many DER systems provide energy from renewable sources, which are not reliably available at all times. Therefore, the Resilience of power systems to even typical disruptions is increasingly at risk as more of these DER systems are interconnected.

4.2 Threats – Engineering and Cyber

4.2.1 Physical and Electrical Threats – Mostly but Not Entirely Inadvertent

Utilities are accustomed to worrying about physical threats, such as equipment failures and safety-impacting carelessness. Transformers can overheat and explode. Power lines can sag into trees, trip circuit breakers, and cause cascading power failures. Squirrels can chew through cables and cause local outages. Natural disasters are getting increased attention, particularly for utilities that commonly experience hurricanes, earthquakes, cyclones, ice storms, etc., even though these are looked upon as beyond the control of the utility. In fact, severe weather events seem to becoming more common, so that utilities are trying to increase the resilience of their power systems in general through disaster planning and disaster recovery strategies.

Electrical threats include inadequate generation to meet the load causing brownout or outages, over-generation, and frequency fluctuations that can cause cascading power failures. Utilities are continually trying to improve their management of these factors through forecasting generation and load, monitoring current power system status, and analyzing power system conditions for possible contingencies.

Some threats can be deliberate, such as a person shooting a transformer so that the oil drains out or stealing copper grounding wires out of substations.

A new type of electrical “threat” is beginning to be realized, namely the impact of DER systems that are not under the direct control of utilities. DER systems can now impact normal power system operations if they are large enough or if they consist of a large enough group of smaller DER systems. Such electrical threats could include deliberate rapid fluctuations of real power by large (or large groups of) DER systems to cause power system instability, or the unauthorized export of excess generation to overload a circuit. These impacts include the following:

- **Anti-islanding failures**. Under certain circumstances DER systems may not properly disconnect when the grid does experience an outage, thus failing to detect an electrical “island”. This situation can be a serious safety hazard.
- **Power system instability**. Variations in DER generation due to unmanaged and unmonitored DER systems can cause power system instability and possibly widespread power outages.

- **Fluctuating energy output**. Fluctuations in DER energy output due to variable renewable energy sources or responses to local loads can cause changes in voltage and frequency which may cause them to exceed their normal ranges.
- **Unnecessary DER disconnections**. If voltage and/or frequency exceed their normal ranges, DER systems will cease energizing the grid and disconnect, thus worsening a situation that might otherwise have been recovered from.
- **Reverse power flows**. Unmonitored DER output can cause back-feeding in substations that are not designed for reverse power flows.

4.2.2 Cyber Threats – Inadvertent and Deliberate

Utilities are increasingly recognizing the importance of protecting cyber assets and cyber information, which are becoming critical aspects of safe, reliable, and efficient power system operations. Cyber assets now are used to operate circuit breakers, monitor power system equipment, and manage energy markets. Cyber information that is inadvertently or deliberately compromised could cause major outages, destroy equipment, and trigger financial disruptions.

Threats are generally viewed as the potential for attacks against assets. These assets can be physical equipment, computer hardware, buildings, and even people. In the cyber world, however, assets also include information, databases, firmware, and software. Countermeasures to these security threats must include protection against both physical attacks as well as cyber-attacks.

Threats to assets can result from inadvertent events as well as deliberate attacks. In fact, often damage can result from safety breakdowns, equipment failures, carelessness, and natural disasters than from deliberate attacks. However, the reactions to successful deliberate attacks can have tremendous legal, social, and financial consequences that could far exceed the physical damage.

Security risk assessment and management is vital in determining exactly what needs to be secured against what threats and to what degree of security. The key is determining the cost-benefit ratio, where the likelihood and magnitude of an impact are greater than the cost to mitigate that impact. There is no silver bullet: just encrypting data or just requiring usernames and passwords do not by themselves provide adequate security. For both power system engineering and for cyber security, layers of defensive mechanisms are better than a single solution. That is why redundant protective relays are used in a substation, and why even authorized input data should be checked for validity and reasonability. Ultimately no protection against attacks, failures, mistakes, or natural disasters can ever be completely absolute. Therefore the planning of coping mechanisms during emergency situations and recovery procedures from those emergency situations must also be part of a complete Resilience strategy.

Threat agents can be defined as one of the following:

- **Malicious person *[malicious]*** who is deliberately attacking systems for financial, power, revenge, or other gain
- **Inadvertent mistake *[error]*** caused by a person who either failed to pay attention or did not recognize the consequences of their action. Computer applications can also have

"bugs" or other flaws that cause them to misoperate. Poorly designed systems and inadequate operating procedures also fall in this category.

- **Equipment failure** [***failure***] that was not any person's fault, but reflects the fact that electronic and mechanical devices can fail. Equipment that responds in unexpected ways to normal conditions can also be placed in this category.
- **Natural disasters *[disaster]*** caused by events completely outside the control of humans.

The following sections discuss some of the most common threats which can have significant impacts. Understanding these threats can help in the development of the best mitigation strategies.

4.2.2.1 Inadvertent Threats

Inadvertent threats are more common that deliberate attacks, while the impacts of these inadvertent actions are not focused on any specific purpose. This makes these threats both less easy to prevent but more amenable to layers of security and to resilience designs and operations. Utilities have a lot of experience in designing systems to resist and cope with these types of threats. However, often other DER stakeholders do not have this extensive experience, since integration of DER systems is still a new and evolving area.

- **Safety Failures:** Safety has always been a primary concern for any power system facilities, and must be part of DER implementation and operation. In the power industry, meticulous procedures have been developed and refined to improve safety, but not all of these have yet been fully developed for DER systems. Autonomous safety measures such as protective relaying, are a primary defense, but monitoring of the status of key equipment and the logging/alarming of compliance to safety procedures can enhance safety to a significant degree.
- **Equipment Failures:** Equipment failures are the most common and expected threats to the reliable operation of the power system. Often the monitoring of the physical status of DER equipment can also benefit maintenance efficiency, possible prevention of certain types of equipment failures, real-time detection of failures not previously monitored, and forensic analysis of equipment failure processes and impacts. '
- **Software/Firmware Malfunctions:** Software and firmware malfunctions (e.g. bugs, crashes, and incorrect results) can still occur even if systems are thoroughly tested, often due to the complexity of the software and how it interacts with the operating system or other software applications. Newly implemented or upgraded software applications are particularly vulnerable to malfunctions, while patches and upgrades to reliable software can sometimes cause malfunctions.
- **Mistakes, Carelessness, or Lack of Knowledge:** Mistakes caused by carelessness or just a lack of knowledge is one of the "threats" to protecting DER systems, whether it is not locking doors or inadvertently allowing unauthorized personnel to access passwords, keys, and other security safeguards. Often this carelessness is due to complacency ("no one has ever harmed this DER system yet") or inexperience ("I didn't realize that the email

did not come from the DER manufacturer, and so I provided the attacker with my password into the DER system").

- **Natural Disasters:** Natural disasters, such as storms, hurricanes, and earthquakes, can lead to widespread power system failures, safety breaches, and opportunities for theft, vandalism, and terrorism. Monitoring of the physical and cyber status of DER systems in real-time can provide the "eyes and ears" to understand what is taking place and to take ameliorating actions with respect to the utilization of DER to minimize the impact of these natural disasters on power system operations.

4.2.2.2 Deliberate Threats

Deliberate threats can cause more focused damage to facilities and equipment in substations than the inadvertent threats. The incentives for these deliberate threats are increasing as the results from successful attacks can have increasingly economic and/or "socio/political" benefits to the attackers. Sophisticated monitoring of facilities and equipment can help detect and prevent some of these threats, while ameliorating the impact of successful attacks through real-time notifications and forensic trails. This is a new area for most DER stakeholders, including utilities, where the threats are less well understood. Engineers understand Resilience requirements against inadvertent threats to their power systems but are still developing their understanding of how deliberate cyber threats can impact this Resilience.

- **Disgruntled Employee**: Disgruntled employees are an important threat for attacks on power system assets, including DER systems. Unhappy employees who have the detailed knowledge to do harm can cause significantly more damage than a non-employee, particularly in the power system industry where the DER equipment and supporting systems are unique to the industry.

- **Industrial Espionage:** Industrial espionage in the power system industry is becoming more of a threat as deregulation and competition involving millions of dollars provide growing incentives for unauthorized access to information – and the possible damaging of equipment for nefarious purposes. DER systems are particularly vulnerable since they are usually located in relatively unprotected environments on customer property. In addition to financial gains, some attackers could gain "socio/political" benefits through "showing up" the incompetence or unreliability of competitors.

- **Vandalism:** Vandalism can damage facilities and equipment with no specific gain to the attackers other than the act of doing it, and the proof to themselves and others that they can do it. Often, the vandals are unaware of or do not care about the possible consequences of their actions. Again, DER systems may be particularly vulnerable to vandalism, partly because of their unprotected environments, but also because their generation capabilities can directly affect the power grid, including causing outages.

- **Cyber Hackers:** Cyber hackers are people who seek to breach cyber security for gain. This gain may be directly monetary, industrial knowledge, political, social, or just individual challenge to see if the hacker can gain access. Most hackers use the Internet as their primary gateway to entry, and therefore firewalls, isolation techniques, and other

countermeasures can be used to separate DER systems from the Internet. However, hackers may initiate multi-stage attacks that use the internet just to set up an attack, while the actual attack occurs on a DER system that is not connected to the internet. DER systems may use the Internet for software updates, thus opening up a channel for cyber hackers. Individual DER systems are unlikely to be targeted by sophisticated Cyber adversaries (nation-states), however when networked into microgrids and at places where DER data is aggregated they could become such targets.

- **Viruses and Worms:** Like hackers, viruses and worms typically attack via the Internet. However, some viruses and worms can be embedded in software that is loaded into systems that have been isolated from the Internet, or could possibly be transmitted over secure communications from some insecure laptop or other system. They could include man-in-the-middle viruses, spyware for capturing power system data, and other Trojan horses. A famous (or infamous) example is the Stuxnet worm, which successfully attacked the Iranian uranium centrifuges. DER systems are equally vulnerable to such attacks.
- **Theft:** Theft has a straightforward purpose – the attackers take something (equipment, data, or knowledge) that they are not authorized to take. Generally, the purpose has financial gain as the motive, although other motives are possible as well. Monitoring access to locked facilities and alarming anomalies in the physical status and health of equipment (e.g. not responding or disconnected) are the primary methods for alerting personnel that theft is possibly being committed.
- **Terrorism:** Terrorism is the least likely threat but the one with possibly the largest consequences since the primary purpose of terrorism is to inflict the greatest degree of physical, financial, and socio/political damage. Monitoring and alarming anomalies to access (including physical proximity) to substation facilities is possibly the most effective means to alert personnel to potential terrorist acts, such as physically blowing up a substation or other facility. However, terrorists could become more sophisticated in their actions, and seek to damage specific equipment or render critical equipment inoperative in ways that could potentially do more harm to the power system at large than just blowing up one substation. Therefore, additional types of monitoring are critical, including the status and health of equipment. That being said, the Resilience benefits of distributed generation – which presents many small dispersed targets to the adversary – should not be overlooked.

4.3 Vulnerabilities – Engineering and Cyber Vulnerabilities

All systems have vulnerabilities. The key requirement is to develop cyber techniques, engineering strategies, and operational strategies to minimize the likelihood of an attack/failure or to mitigate the impact of an attack/failure. There is generally not a one-to-one correspondence between a vulnerability and a mitigation technique; often multiple mitigation techniques can be used in combination to address multiple vulnerabilities. Layers of mitigations can provide defense-in-depth combinations that increase the strength of these mitigations. For instance, cyber security techniques can help decrease the likelihood of a particular attack/failure, while engineering coping strategies can mitigate the impact of a successful attack or system failure.

4.3.1 Power System Vulnerabilities and Attacks

Power systems have been vulnerable to equipment failures, operational mistakes, and natural disasters since they were first invented. Some of the vulnerabilities are related to the software and hardware that is used in the power system equipment controllers and analysis systems.

Different vulnerabilities can be present in equipment at different stages of its life. Some vulnerabilities affect newly developed systems, such as a software bug causing incorrect results. Some vulnerabilities become more critical over time, for instance when a system that had been working correctly with small numbers of alarms, is required to handle large volumes of alarms and now fails to process them. Particularly critical are the times when systems are patched or updated, since new vulnerabilities can cause a previously reliable system to fail or to be open to cyber attackers.

Some of the causes of these types of vulnerabilities include:

- **Equipment vulnerabilities**: Equipment failures cause improper operations. For instance, a circuit breaker fails to trip during a short circuit event, causing power equipment to overload and burn, and personnel to be electrocuted.
- **Complexity of analysis**: Complexity of analysis of large numbers of DERs provides incorrect results. For example, engineers who set protective relay parameters have not taken into account certain types of contingencies, so that one event causes a second event, and causes a cascading failure of the power system, resulting in major outages.
- **Lack of standardized operating procedures:** Lack of standardized operating procedures causes misunderstandings and results in incorrect actions, incorrect responses to situations, and confusion during emergencies.
- **Incorrect settings**: Incorrect settings cause incorrect responses to power system situations. For instance, DER systems have not included appropriate voltage and frequency ride-through settings, which results in numerous outages whenever voltage and frequency fluctuations occur due to storms or rapid changes in sunlight or wind.
- **Inability to detect loss of grid power**: The inability of DER systems to detect the loss of grid power causes safety concerns as well as uncertainty and delay in addressing emergency situations. For example, DER systems which are supposed to disconnect upon the loss of the grid power, do not disconnect because their traditional anti-islanding methods fail to detect the loss of power due to masking by other DER systems or their own smart DER volt-var functions, causing safety problems and equipment damage.
- **Inadequate analysis capabilities**: Inadequate analysis capabilities of software applications results in sending invalid pricing signals, control settings, and control commands to DER systems. For instance, inadequate analysis of the location and amount of DER generation causes over or under voltage or frequency events and results in large scale outages.
- **Inadequate personnel training**: Inadequate personnel training results in poor judgment on actions. For example, inadequately trained crews fail to disconnect DER systems during

system maintenance activities, or inadequately trained fire and police on how to cope with DER systems, leading to safety problems and outages.

- **Manipulated or mistaken market prices**: Manipulated or mistaken market prices result in uneconomical or unfair actions. For instance, market pricing signals call for decreased generation when actually more generation is needed, leading to higher prices for spot generation or even outages.
- **Inadequately structured authority hierarchy**: Inadequately structured authority or contractual hierarchy causes confusion during emergencies. For example, a DER operator ignores utility-set limits and generates more than the utility circuit can handle, damaging substation equipment and causing outages.
- **Degradation in analysis accuracy**: Degradation over time in analysis accuracy due to the rapid growth and resulting increasingly complex interactions between DER systems, causes increasing reliability and power quality problems. For instance, DER systems are expanding rapidly in their number and types of deployments, resulting in increasingly complex interactions between them and also between these DER systems and other grid equipment, leading to incorrect settings and non-optimal actions by operators.
- **Incomplete testing of complex intelligent DER systems:** Multiple DER systems, each with complex intelligent behavior, cause unsafe or unexpected actions because their complexity inhibits the testing of all possible combinations of situations. For instance, intelligent DER systems capable of undertaking many new functionalities, tend to have more design and operational errors because development is more complex and testing just cannot cover all possible types of interactions. Often there are unintended consequences to actions in complex environments that may not be evident in simpler environments.
- **Inadequately specified requirements:** Inadequately specified requirements for DER systems cause unsafe or unexpected actions, because the systems that are not well understood can lead to errors in development and performance. For instance, the requirements for managing high penetrations of DER systems in coordination with existing distribution equipment are still under extensive study.
- **Mismatched assumptions between organizations**: Mismatched assumptions between organizations result in confused or incorrect actions. For instance, if one organization uses encryption techniques or some settings not supported by another organization, then the expected interactions will not take place.
- **Lack of confidence in analysis results:** Lack of confidence in analysis results in slow responses to problems. For example, some power flow studies or DER generation forecasts or other complex analyses may not be trusted by operators, possibly due to previous failures or inexperience with the type of analysis, leading to personnel responding slowly or taking incorrect actions.
- **Inadequate change management procedures:** Inadequate change management causes decisions to be made on inaccurate data. For example, inadequate management of

changes to systems, which should include pre-testing of the changes and the ability to restore a previous version if the changed system fails to operate correctly, could cause failures and incorrect results.

Power systems are now vulnerable to problems actually caused by cyber security technologies. These include:

- **Denial of Service**: DER systems lose access to third party cryptographic key authentication and update servers, causing communications with the utility to be denied. Or encrypted messages increase the traffic on a communications channel to the point where a high priority message cannot get through in a timely manner, causing an outage.
- **Inadequately protected backdoor access**: A vendor of a DER system performs maintenance using a "back door" port, then leaves this port open. An attacker uses this port which has complete access to the DER software since it is assumed that no unauthorized access could be possible through this normally deactivated port.
- **Poor management of passwords**: A power system event occurs but the utility operator does not have (remember) the right password to undertake a critical DER operation to prevent a cascading failure.
- **Poor security maintenance**: A certificate or secret key expires before a new one is activated, causing equipment to shut down or cease to respond to communication commands.
- **Inadequate security training**: Frustrated maintenance personnel who cannot remember large numbers of passwords, use the same password for all equipment. When their password is compromised by an attacker, that attacker can now access all of that equipment which was assumed to be cyber secure.
- **Inadequate re-testing procedures:** Security personnel maintain secure access to some critical equipment, but misunderstand or do not properly test a request to update the security of the software and cause the equipment to lock-out.
- **Security management failures:** Inadequate security management may allow unauthorized personnel to learn passwords or other sensitive material.

4.3.2 Cyber Security Vulnerabilities and Attacks

The threats can be realized by many different types of attacks, some of which are illustrated in Figure 5. Often an attack takes advantage of a vulnerability, which may be due to human carelessness, an inadequately designed system, or circumstances such as a major storm. As can be seen, the same type of attack can often be involved in different security threats. This web of potential attacks means that there is not just one method of meeting a particular security requirement: each of the types of attacks that present a specific threat needs to be countered.

Although importance of specific cyber threats can vary greatly depending upon the assets being secured, some of the more common human and system vulnerabilities that enable attacks are:

- **Lack of security**: Security, even if it exists, is never "turned on".

- **Indiscretions by personnel:** Employees write down their username and passwords and place them in their desk drawer.
- **Simple or easy-to-guess passwords**: Employees use short alpha-only passwords or use their dog's name and/or their birthday as their password.
- **Social engineering**: An attacker uses personal information or subterfuge to learn a user's password, such as pretending to be from a bank or leaning over someone's shoulder as they type their password.
- **Bypass controls**: Employees turn off security measures, do not change default passwords, or everyone uses the same password to access all substation equipment. Or a software application is assumed to be in a secure environment, so does not authenticate its actions.
- **Integrity violation**: Data is modified without adequate validation, such that the modified data causes equipment to malfunction or allows access to unauthorized users or applications.
- **Software updates and patches**: The software is updated without adequate testing or validation such that worms, viruses, and Trojan Horses are allowed into otherwise secure systems. Alternatively, security patches needed to fix vulnerabilities are not applied.
- **Lack of trust**: Different organizations have different security requirements and use different cyber security standards.

Some common types of attacks include:

- **Eavesdropping**: a hacker "listens" to confidential or private data as it is transmitted, thus stealing the information. This is typically used to access intellectual property, market and financial data, personnel data, and other sensitive information.
- **Masquerade**: a hacker uses someone else's credentials to pretend to be an authorized user, and thus able to steal information, take unauthorized actions, and possibly "plant" malware.
- **Man-in-the-middle**: a gateway, data server, communications channel, or other non-end equipment is compromised, so the data that is supposed to flow through this middle node is read or modified before it is sent on its way.
- **Resource exhaustion**: equipment is inadvertently (or deliberately) overloaded and cannot therefore perform its functions. Or a certificate expires and prevents access to equipment. This denial of service can seriously impact a power system operator trying to control the power system.
- **Replay**: a command being sent from one system to another is copied by an attacker. This command is then used at some other time to further the attacker's purpose, such as tripping a breaker or limiting generation output.
- **Trojan horse**: the attacker adds malware to a system, possibly as part of an innocent-appearing enhancement or application, and possibly during the supply chain (e.g. during component manufacturing or system integration or shipping or during installation). This

malware does nothing until some circumstance locally or remotely triggers it to cause an unauthorized action.

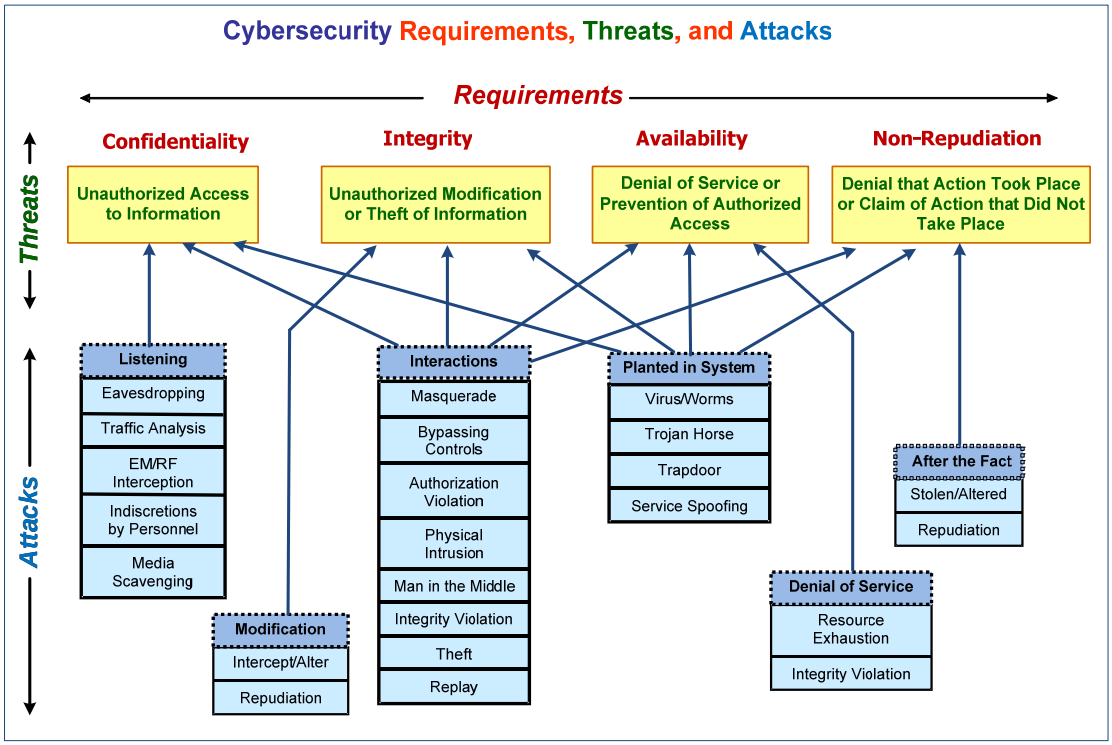

Figure 5: Security Requirements, Threats, and Possible Attacks

4.4 Risk Management and Mitigation Techniques

4.4.1 Risk Handling

The risk associated with an attack or failure is the combination of the likelihood of the event (including the cost to the attacker to undertake the attack) with the probable impact of a successful attack or failure. Risks can be handled in different ways:

- **The risk can be accepted (ignored)** because the expected likelihood and impact of an event does not appear to be worth the cost of implementing mitigation measures. For instance, requiring redundant communications to all DER systems would most likely not be worth the cost of implementing such redundancy.
- **The risk can be shared**, for instance by paying an insurance company to take on the risk. This approach is often used for protection against the loss of physical assets such as buildings and the physical DER equipment.
- **The risk can be transferred**, for instance by contracting a third party to take responsibility for operating and maintaining DER systems.
- **The risk can be mitigated** to different levels. For instance, some DER systems may require only the use of username/password for access control protection, while other DER

systems may require two-party authentication and cryptographic certificate verification for any access.

Risk mitigation usually implies costs. These mitigation costs can range from minimal to totally impractical. Therefore, risk management is the art and science of balancing the likelihood and impact of an event against the mitigation cost. Risk assessment methodologies are covered in detail in NIST Special Publication (SP) 800-30, "*Guide for Conducting Risk Assessments.*"

4.4.2 Risk Mitigation Categories

Mitigations against the effects of attacks and failures are often described as having eight categories. Associated security countermeasures can mitigate one or more of these purposes; these mitigations are illustrated in Table 1:

- **Prevention of attack**, by taking active measures that are in effect at all times and are designed to prevent a failure or attack. These usually are engineering designs and procedures, as well as cyber security design and architecture measures.
- **Deterrence to a failure or attack**, to try to make failures and attacks less likely, or at least delay them long enough for counter actions to be undertaken.
- **Detection of a failure or attack**, to notify the appropriate person or systems that an attack or failure event took place. This notification could also include attempts at attacks or failures that "self-healed". Detection is crucial to any other security measures since if an attack is not recognized, little can be done to prevent it. Monitoring of systems and communications is critical, while intrusion detection capabilities can play a large role in this effort.
- **Assessment of a failure or attack,** to determine the nature and severity of the attack. For instance, is the entry of a number of wrong passwords just someone forgetting or is it a deliberate attempt by an attacker to guess some likely passwords.
- **Response to a failure or attack**, which includes actions by the appropriate authorities and computer systems to stop the spread of the attack or failure in a timely manner. This response can then deter or delay a subsequent attack or failure, or mitigate the impact of cascading failures or attacks.
- **Coping during a failure or attack,** which includes initiating additional activities to mitigate the impacts, such as performing switching operations to improve the Resilience of the power system, sending crews to failure sites, requiring increased authentication measures for any interactions with compromised systems, and gracefully degrading performance as necessary.
- **Resilience during failure or attack,** which involves sustaining minimum essential operations during attack despite system compromise and some operational degradation.
- **Recovery from a failure or attack,** which includes restoration to normal operations after a failure has be corrected, requiring full virus and validation scans of affected systems, or changing passwords for affected systems.

- **Audit and legal reactions to a failure or attack,** which could include analyzing audit logs, assessing the nature and consequences of the event, performing additional risk assessments, and even pursuing litigation against those responsible for the event.

Table 1: Mitigation Categories for Cyber-Physical Systems

	Category	Description	Power Engineering Examples	Cyber Examples
Protection and Deterrence Before Failure or Attack	**Preparation and protection against a failure or attack**	Active measures used in normal circumstances that are designed to prevent an attack	Erect substation fences; Limit access to control center; Specify robust, hardened equipment Design the power system with adequate flexibility to handle anomalous situations; Deploy redundant equipment; Establish default system settings to failures; Establish autonomous modes of operation in case of lack or loss of communications; Perform contingency analysis studies on power system conditions; Design communication networks to be isolated from each other; Train personnel adequately	Design systems and applications to handle anomalous situations; Test all software applications for both normal operations and anomalous situations; Validate data entry; Require message authentication; Require strong passwords; Use role-based access control; Encrypt confidential messages; Disable unneeded ports/services; Require non-repudiation methods; Validate patches before implementing them;
	Deterrence to a failure or attack	Preparing for a possible failure or discouraging someone from engaging in an attack	Develop emergency operations plans and procedures; Test emergency plans periodically; Display signs indicating danger or private property; Warn of legal actions; Deploy CCTV cameras; Change system settings for storms or other natural disasters; Test new software and systems; Assess potential failure impacts of all additions to the power system	Develop emergency plans for network failures; Display warnings when applications or data are modified; Require legal acceptance when installing software

	Category	Description	Power Engineering Examples	Cyber Examples
Detection, Assessment, Response, and Coping During Failure or Attack	**Detection of a failure or attack**	Identifying a failure or attack and notifying appropriate entities	Monitor power system status and measurements; enter events in event log; alarm operators; initiate cellphone call to on-duty person; provide quality flags for monitored data	Detect intrusions; check signatures; scan for viruses; monitor network configurations; alarm security personnel
	Assessment of a failure or attack	Assess and categorize the severity of a failure or attack, using triage concepts	Initiate dynamic response to power system conditions; use power flow contingency analysis to determine changes in power system resilience; run equipment diagnostic tests	Determine the security level of the attack's target; determine the number of simultaneous attacks; determine the type of attack
	Response to a failure or attack	Stopping the spread of the failure or attack by using emergency measures	Initiate emergency functions such as DER ride-through; trip breakers; shed load; increase generation; isolate microgrids; switch to different equipment settings	Shut down network; turn off computer; isolate network
	Coping during a failure or attack	Initiating additional activities to mitigate the impact	Switch to backup systems; reconfigure feeders; start additional generation; manage microgrids	Start manual activities to replace automated activities
	Resilience during a failure or attack	Sustaining minimum essential operations despite the failure or attack, preparing for continuing attacks	Protect against cascading failures, such as short-term voltage anomalies triggering DER systems to disconnect and causing unnecessary outages, degrading performance as necessary	Ensuring that systems providing essential services remain operational so long as they are not directly affected by the failure or attack
Recovery and Analysis After Failure or Attack	**Recovery from a failure or attack**	Restoring to normal operations after a failure has be corrected or an attack has been stopped	Test all failed or compromised power equipment; restore power; switch to primary systems; reestablish normal settings and modes; return to normal operations	Test all systems and networks; reconnect isolated networks and systems;
	Analysis of causes and assessment of coping response	Analysis and assessment of the nature and consequences of a failure or attack	Analyze audit logs and other records; change procedures for handling similar events; provide additional training for such events;	Debrief and post-mortem analysis; system re-configuration; policy changes

5 CYBER SECURITY RECOMMENDATIONS METHODOLOGY

The cyber security recommendations in this document are based on a methodology that combines empirical methods and a numerical scoring-based approach, since neither method alone has been proven to yield completely exhaustive results. Threat analysis, functional scoring, best practices, and practical considerations were all considered during the development of the recommendations.

5.1 Methodology Overview

At its core, the methodology used in the development of the recommendations analyzes DER inverter functions to determine the types of threats, the likelihood (risk) of those threats being realized, and the cost (financial, privacy, and societal) of the possible impact of a successful attack. The risk multiplied by the impact is then weighed against the different types and levels of possible cyber security measures, recognizing that the likelihood of certain attacks is a subjective assessment and some impacts may not be quantifiable.

However, by investigating the functions and capabilities of the Distributed Energy Resource (DER) inverters themselves, the team was able to assess the types of cyber security measures commensurate to the criticality of each function. The methodology followed the following general process:

1. **Perform threat analysis** on residential inverter-based DER systems to identify threats and vulnerabilities.
2. **Enumerate potential inverter-based DER functions**, since attacks on different functions could have different impacts.
3. **Score each DER function** (High, Medium, or Low) on the merits of confidentiality, integrity, availability, authentication, authorization, and accountability.
4. **Combine DER scoring metrics**, threat data, industry standards, and practical requirements to develop general, high-level cyber security recommendations for residential inverter-based DER systems.

DER function scoring was repeated for each of the three DER inverter communication interfaces identified in the scope, including communications between:

- Utility and the communication module
- Aggregator/vendor and the communication module
- The communication module and the DER inverter itself

This separation ensured any variances in requirements due to differences in communication endpoints were identified.

5.2 Inverter Functions

The DER functions used in the scoring were derived from the IEC 61850-90-7 standard and the Smart Inverter Working Group (SIWG) Phase 1 and Phase 3 functions, which were based on and extensions to the IEC 61850-90-7 functions. The list of DER functions is enumerated in Table 2 below.

Table 2: DER Inverter Function List

SIWG/IEC Function	Description
Anti-Islanding Protection (AI)	The DER system trips off if voltage or frequency limits are exceeded over specified time periods. Although default trip-off limits settings would be implemented initially, these settings could be modifiable through agreement between the Area EPS and the DER operator.
Low/High Voltage Ride-through (L/HVRT)	The DER system remains connected during voltage excursions beyond normal limits, based on extended voltage limits during specified time windows. The DER system would disconnect only when the ride-through window has expired. Although default ride-through settings would be implemented initially, these settings could be modifiable through agreement between the Area EPS and the DER operator, based on the technical capabilities of the DER system and used to possibly mitigate abrupt losses of generation.
Low/High Frequency Ride-through (L/HFRT)	The DER system remains connected during frequency excursions beyond normal limits, based on extended frequency limits during specified time windows. The DER system would disconnect only when the ride-through window has expired. Although default ride-through settings would be implemented initially, these settings could be modifiable through agreement between the Area EPS and the DER operator, based on the technical capabilities of the DER system and used to possibly mitigate abrupt losses of generation.
Volt-Var Mode with Watt-Priority	The DER system implements volt/var curves that define the available reactive power required at different voltage levels. Settings are coordinated between the utility and DER operator. Available reactive power is defined as what reactive power is available without decreasing real power output. • DER controller contains pre- established volt/var settings, and/or • Volt/var settings can be updated remotely
Ramp Rates	The default ramp rate is established, contingent upon what the DER can do. Additional emergency ramp rates and high/low ramp rate limits may also be defined.
Fixed Power Factor	The DER system sets the inverter to the specified power factor setting: • DER controller contains pre-established power factor setting, and/or • Power factor setting can be updated remotely
Soft Start	The DER system reconnects to the grid after power is restored using soft- start methods such as ramping up and/or randomly turning on within a time window after grid power is restored, to avoid abrupt increases in generation. The delay time between power restoration and the start of reconnection is preset, as are the ramping rate and the time window.

SIWG/IEC Function	Description
Communication Interface	Standard interfaces can connect to different wired and/or wireless media. These media could include utility wireless systems, cellphone GPRS, customer WiFi network, and the Internet. Utilities would specify which communication interface modules are required for specific implementations.
Transport Protocols	Basic Internet transport layer standards of TCP/IP, in particular an IP address.
Data Model	Abstract information models for DER systems should use the IEC 61850-7-420 and IEC 61850-90-7 for DER systems.
Mapping to Application Protocols	DER systems should support the ability to map the abstract IEC 61850 information model to standard protocols, such as ModBus, DNP3 (IEEE 1815), IEC 61850 (MMS), IEEE 2030.5, etc. The default protocol for communications with a utility is DNP3 (IEEE 1815:2012) although other mutually agreed to protocols could be used. The utility protocol may be used between a facility gateway and the utility, while the communications between the facility gateway and the DER systems may use other protocols. This gateway may be provided by the DER owner or by the utility, reflecting the most economical arrangement.
Transport Cyber Security	Cyber security at the transport layer should be provided, such as Transport Layer Security (TLS) or IEEE 802.11i.
User Cyber Security	Cyber security for user and device identification and authentication should be provided, based on user passwords, device security certificates, and role-based access control. Confidentiality is optional. Public Key Infrastructure (PKI) could be used for key management.
Monitor Alarms	The DER system (and aggregations of DER systems, such as virtual power plants) provides alarms and supporting emergency information via the FDEMS to the utility. This function is feasible only if the ICT infrastructure is available.
Monitor DER Status and Output	The DER system (and aggregations of DER systems, such as virtual power plants) provides current status, power system measurements, and other real- time data (possibly aggregated via the FDEMS) to the utility, in order to support real-time and short-term analysis applications. This function is feasible only if the ICT infrastructure is available. (Revenue metering data is provided via alternate means.)
Limit Maximum Real Power	The utility issues a direct command to limit the maximum real power output at the ECP or PCC. The reason might be that unusual or emergency conditions are causing reverse flow into the feeder's substation or because the total DER real power output on the feeder is greater than some percentage of total load. The command might be an absolute watt value or might be a percentage of I- DER output. This function is feasible only if the ICT infrastructure is available. It might also be used to ensure fairness across many DER systems.
Connect/Disconnect	The DER system performs a disconnect or reconnect at the ECP or PCC. Time windows are established for different DER systems to respond randomly within that window to the disconnect and reconnect commands. This function is feasible only if the ICT infrastructure is available.
Provide DER Information at Interconnection/Startup	The DER system provides operational characteristics after its "discovery" and whenever changes are made to its operational status.
Initiate Periodic Tests of Software and Patches	Initial DER software installations and later updates are tested before deployment for functionality and for meeting regulatory and utility requirements, including

SIWG/IEC Function	Description
	safety. After deployment, testing validates the I- DER systems are operating correctly, safely, and securely.
Schedule Output Limits at PCC	The utility establishes (or pre- establishes) a schedule (e.g. on-peak & off-peak) of actual or maximum real power output levels at the ECP or PCC, possibly combining generation, storage, and load management. The reason might be to minimize output during low load conditions while allowing or requiring higher output during peak load time periods.
Schedule DER Functions	The DER system receives and follows schedules for real power settings, reactive settings, limits, modes (such as autonomous volt/var, frequency- watt), and other operational settings.
Schedule Storage	For a DER system that has storage capabilities, such as battery storage or a combined PV + storage system or a fleet of electric vehicles. Preset time- of-charge values can be established. Settings are coordinated between the utility and DER operator. Different scenarios could include: • Low load conditions at night are causing some renewable energy to be wasted, so charging energy storage DER systems at that time makes power system operations more efficient. • DER controller charges at the specified rate (less than or equal to the maximum charging rate) until the state-of-charge (SOC) reaches a specified level. • DER controller charges at the necessary rate in order to reach the specified SOC within the “charge-by” time.
Frequency-Watt Mode	The DER system reduces real power to counteract frequency excursions beyond normal limits (and vice versa if additional generation or storage is available), particularly for microgrids. Hysteresis can be used as the frequency returns within the normal range to avoid abrupt changes by groups of DER systems.
Voltage-Watt Mode	The DER system monitors the local (or feeder) voltage and modifies real power output in order to damp voltage deviations. Settings are coordinated between the utility and DER operator. Hysteresis and delayed responses could be used to ensure overreactions or hunting do not occur.
Dynamic Current Support	The DER system counteracts voltage anomalies (spikes or sags) through “dynamic current support”. The DER system supports the grid during short periods of abnormally high or low voltage levels by feeding reactive current to the grid until the voltage either returns within its normal range, or the DER system ramps down, or the DER system is required to disconnect.
Limit Maximum Real Power	DER systems are interconnected to the grid with a preset limit of real power output to be measured at the PCC. The reason might be that the I- DER system is sized to handle most of the local load behind an ECP or the PCC, but occasionally that load decreases below a critical level and the increased real power at the ECP or PCC may cause backflow at the substation and be a reliability concern for the utility. Most likely for larger DER systems.
Set Real Power	The utility either presets or issues a direct command to set the actual real power output at the ECP or PCC (constant export/import if load changes; constant watts if no load). The reason might be to establish a base or known generation level without the need for constant monitoring. This is the approach often used today with synchronous generators. This function is feasible only if the ICT

SIWG/IEC Function	Description
	infrastructure is available. Meter reads could provide 15-minute energy by the end of the day could provide production information for operational planning.
Smooth Frequency Deviations	The DER system modifies real power output rapidly to counter minor frequency deviations. The frequency- watt settings define the percentage of real-power output to modify for different degrees of frequency deviations on a second or even sub- second basis
Backup Power	The DER system, including energy storage and electric vehicles, has the ability to provide real power when the site is disconnected from grid power. The reason is for providing backup power to the facility and possibly black start capabilities.
Imitate Capacitor Bank Triggers	Similar to capacitor banks on distribution circuits, the DER system implements temperature-var curves that define the reactive power for different ambient temperatures, similar to use of feeder capacitors for improving the voltage profile. Curves could also be defined for current-var and for time-of-day-var.
Operate within an Islanded Microgrid	After grid power is lost or disconnected, or upon command, the DER system enters into microgrid “mode” as either “leading” or “following” the microgrid frequency and voltage, while acting either as base generation or as load-matching, depending upon preset parameters.
Provide Low Cost Energy	Utility, REP, or FDEMS determines which I- DER systems are to generate how much energy over what time period in order to minimize energy costs. Some DER systems, such as PV systems, would provide low cost energy autonomously, while storage systems would need to be managed.
Provide Low Emissions Energy	Utility, REP, or FDEMS determines which non-renewable DER systems are to generate how much energy in order to minimize emissions. Renewable DER systems would operate autonomously.
Provide Renewable Energy	Utility, REP, or FDEMS selects which non- renewable DER systems are to generate how much energy in order to maximize the use of renewable energy. Renewable DER systems would operate autonomously.
Execute Schedules	The FDEMS provides scheduled, planned, and/or forecast information for available energy and ancillary services over the next hours, days, weeks, etc., for input into planning applications. Separate DER generation from load behind the PCC. This function is feasible only if the ICT infrastructure is available.
Issue Generation and Storage Schedules	The DER system provides schedules of expected generation and storage reflecting customer requirements, maintenance, local weather forecasts, etc. This function is feasible only if the ICT infrastructure is available.
Provide Black Start Capabilities	The DER system operates as a microgrid (possibly just itself) and supports additional loads being added, so long as they are within its generation capabilities. This function is feasible only if the ICT infrastructure is available.
Participate in Automatic Generation Control	The DER system (or aggregations of DER systems) implements modification of real- power output based on AGC signals on a multi-second basis. This function is feasible only if the ICT infrastructure is available.

SIWG/IEC Function	Description
Provide Spinning or Operational Reserve	The DER system provides emergency real power upon command at short notice (seconds or minutes), either through increasing generation or discharging storage devices. This function would be in response to market bids for providing this reserve. This function is feasible only if the ICT infrastructure is available.
Real Power Response to Demand Response Price Signals	The DER system receives a demand response (DR) pricing signal from a utility or retail energy provider (REP) for a time period in the future and determines what real power to output at that time. This function is feasible only if the ICT infrastructure is available.
Manage Ancillary Service Response to Demand Response Signals	The DER system receives a DR pricing signal from a utility or retail energy provider (REP) for a time period in the future and determines what ancillary services to provide at that time. This function is feasible only if the ICT infrastructure is available.
Registration (Automated DER Discovery)	The DER system supports its automated "discovery" as interconnected to a location on the power system and initiates the integration process. This function is feasible only if the ICT infrastructure is available. Otherwise, manual methods must be used.
PV/Storage Functions	Change the signal parameters for the storage system
Volt-Var mode	Provide maximum vars constrained by WMax
Temperature mode behavior	Temperature-based curves
Pricing signal mode behavior	Mode curves based on utility signal (pricing information???double check)
Event/History Logging	Request event logs
Time Synchronization	Set inverter time (manual/automated based on timing signals [GPS or network])

5.3 Security Assessment

Assessing the security of each DER inverter function was based on six different items. The first three items are security objectives and the second three are security requirements:

- **Confidentiality:** Imposing authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
- **Integrity:** Preventing improper information modification, destruction, or theft.
- **Availability:** Ensuring timely and reliable access to inverter-based DERs and ensuring their ability to perform as required.
- **Authentication:** A way of verifying the identity of users and devices to ensure the user or device is who or what it is declared to be.
- **Authorization:** Granting permission for performing specific tasks with a device.
- **Non-Repudiation:** Preventing the denial of an action that took place or the claim of an action that did not take place (note to include auditing in here as well).

The traditional information security objectives of confidentiality, integrity, and availability form the basis of the analysis; however, the additional requirements of authentication, authorization, and non-repudiation were added to enable more granularity and emphasis on specific security issues. Each security objective was given a value of High, Moderate, or Low for every DER inverter function. The values are based on the High, Moderate, and Low definitions are loosely based on the Federal Information Processing Standards (FIPS) Publication 199:

- **Low:** The loss of confidentiality, integrity, availability, authentication, authorization, or non-repudiation could be expected to have a limited adverse effect on organizational operation, organizational assets, or individuals.

  AMPLIFICATION: A limited adverse effect means that, for example, the loss of confidentiality, integrity, availability, authentication, authorization, or non-repudiation might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.

- **Moderate:** The loss of confidentiality, integrity, availability, authentication, authorization, or non-repudiation could be expected to have serious adverse effect on organizational operations, organizational assets, or individuals.

  AMPLIFICATION: A serious adverse effect means that, for example, the loss of confidentiality, integrity, availability, authentication, authorization, or non-repudiation might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.

- **High:** The loss of confidentiality, integrity, availability, authentication, authorization, or non-repudiation could be expected to have catastrophic adverse effect on organizational operations, organizational assets, or individuals.

  AMPLIFICATION: A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, availability, authentication, authorization, or non-repudiation might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

Each DER inverter function value was assigned collectively by the CSI RD & D Solicitation #4 cyber working group.

5.4 Inclusion of Threat

Threat and vulnerability analysis was used as a feedback loop into the DER function scoring. Relevant threats and vulnerabilities were mapped to each function and included in the decision making process of the scoring. Detailed threat analysis can be found in Section 4.

5.5 Analysis

The cybersecurity working group results for all three residential DER communication interfaces can be found in Appendix A. The values generally indicate that:

- Authentication and integrity of data are the most important cyber security requirements, and were assessed to be critical for all types of interactions, including monitoring and control commands, to ensure that the data exchanged comes from known sources and has not been modified in transit.
- Authorization and non-repudiation are important to ensure that commands are authorized, executed as specified, and reported back accurately.
- Availability is less critical since DER systems usually operate autonomously and can be preset to perform the DER functions.
- Confidentiality is only important for select DER functions where either privacy or sensitive data is being exchanged, such as personal information or contractual data. For residential DER systems, it is not expected that much confidential data will be exchanged.

The results of this analysis led to the cyber security recommendations enumerated in Section 6.

6 CYBER SECURITY RECOMMENDATIONS FOR CSI RD&D Solicitation #4 DER COMMUNICATION MODULES

6.1 Cyber Security Recommendation Categories

This section provides the cybersecurity recommendations for residential inverter-based DER communications as suggested by the CSI RD & D Solicitation #4 working group. Recommendations are captured in the sections below. Recommendations are categorized using the following taxonomy:

- Physical Security
- Access Control
  - Authentication
  - Authorization
  - Registration
- Integrity
  - Data Integrity
  - Hardware Integrity
- Confidentiality
- Cryptography/Key Management
- Policy
  - Audit
  - Logging

These general recommendations are intended to address cyber security implications related to DER systems that include a CSI RD&D Solicitation #4 DER communications module. These recommendations are guidelines meant to work in tandem with applicable standards and industry best practices to strengthen security for residential inverter-based DER communications. As illustrated in Figure 1, Section 6.2 outlines recommendations for communication interface "A" and Section 6.3 outlines recommendations for communication interface "B".

It is recognized that DER cyber security can also be enhanced through engineering strategies in the design and implementation of DER systems. Guidelines on these engineering strategies can be found in IEC/TR 62351-12 "*Resilience and Security Recommendations for Power Systems with Distributed Energy Resources (DER) Cyber-Physical Systems*" (to be published soon).

6.2 Interface A: CSI RD&D Solicitation #4 DER Cyber Security Recommendations

Communication interface "A", as depicted in Figure 1, is the outward, wide area network-facing interface of the CSI RD&D Solicitation #4 DER communications module. It is this interface that utility, aggregator, and vendor communications will directly communicate via some routable control protocol, such as IEEE 2030.5 (SEP2), IEEE 1815 (DNP3), OpenADR, etc. Utility, aggregator,

and vendor specific communications to this interface were considered while formulating the recommendations below.

Table 3: Cyber Security Recommendations for CSI RD&D Solicitation #4 DER Communication: Interface A

Category	Description
Physical Security	
Physical Security	The DER and accompanying communication module should be physically secured from direct physical access to prevent tampering and access to the physical communication interface (e.g., module is behind a lock box, located behind locked doors, etc.).
Access Control	
Authentication	Communication modules should individually authenticate with the owner, utility, vendor, and aggregator communication systems with role-based access permissions enforced.
Authentication	Communication protocols used between the communication module and other systems are required to authenticate all messages, including their source and destinations.
Authentication	Role-based access permissions should be established for individual data and DER functions.
Authorization	At minimum, the communication module should have pre-defined roles for DER owner, aggregator, vendor, and utility with default access permissions for each role.
Authorization	The DER system establishes “operating states” that modify what permissions different roles may have in the different operating states (e.g. normal, maintenance, or emergency operating states).
Authorization	The DER system only permits authorized users and systems to access its information and provide settings and commands.
Authorization	A compromised communication module does not permit unauthorized access through the communications network to other DER systems or to other entities, including utility, vendor, and aggregator systems.
Authorization	Communication module configurations are intrinsically designed to ensure they are prohibited from joining unauthorized networks.
Integrity	
Hardware Integrity	The communication modules contain secure firmware that prevents module driver access over network connections.
Hardware Integrity	The communication modules should be factory tested for cyber-physical security issues.
Data Integrity	WAN communication protocols implemented by the communication module to manage DER systems should validate the integrity of the data in transit.

Data Integrity	Communication modules that are accessible through public Internet channels should have additional Internet security.
Data Integrity	The communication module is designed such that only essential software and applications are installed and that unnecessary ports are disabled.
Data Integrity	Communication module should satisfy low latency requirements for control.
Data Integrity	The communication module should be time synchronized to the rest of the system to ensure accurate log and data records.
Confidentiality	
Confidentiality	The DER system contains secure firmware or hardware memory for passwords and other embedded private or confidential information that is encrypted or otherwise secured against unauthorized access.
Confidentiality	Communication protocols used for confidential or private information must ensure confidentiality of this information in transit.
Confidentiality	The confidentiality of information about the DER system, including functionality, ownership, and operational settings should be appropriately preserved.
Confidentiality	Communication modules on shared media use secure technologies such as VPNs or BITW encryption devices to protect confidential DER information.
Cryptography/Key Management	
Cryptography	DER communication modules should use validated and endorsed cryptography, do not use deprecated cryptographic suites, and provide a means of upgrading deprecated cryptographic suites.
Cryptography	Communication modules should leverage PKI for transport layer security (incorporating at least TLS 1.2) of critical DER functions, including re-keying activities, registration, customer privacy information, and pricing information.
Key Management	The key management system ensures that the DER communication modules have valid cyber security certificates before communications are established.
Key Management	The communication module should honor certificate revocation lists and update certificates in a timely fashion.
Policy	
Audit	Communication modules should be certified using penetration testing to ensure the modules are well protected against cyber-attacks.
Logging	Communication module logs should capture all cyber security events, including security parameter changes, changes in certificate status, invalid log-in attempts, suspicious errors, etc.
Logging	Communication module logs should capture all network and system “health” events, including temporary and permanent channel failures, excess latency of message exchanges, lost packets, etc.

6.3 Interface B: CSI RD&D Solicitation #4 DER Cyber Security Recommendations

Communication interface "B", as depicted in Figure 1, is the inward, DER-facing interface of the CSI RD & D Solicitation #4 DER communications module which translates the wide area network (WAN) communication protocols to SunSpec Modbus, which runs over serial link. The Modbus protocol does not support cyber security; so typical cyber security controls are not possible. In fact, the lack of security with Modbus led to the mantra "if you can ping a Modbus device, you own it". As such, physical security of the Modbus channel is an important security measure for interface "B". It is assumed that in the vast majority of cases, the communication module will be co-located with inverter-based DER; however, there may be cases where the communication module is located in another location than the DER, such as the case if WAN communications use wireless technologies that require the communication module and it's antenna to be located in an exterior location. Physical security can be enhanced by locating the communication module within the same locked container or facility as the DER controller, with only a very short serial link between them. This security can be improved, albeit at the cost of increased complexity and decreased practicality for residential systems, by including technology to send alarms whenever the lock is opened or if the normal Modbus traffic pattern is modified or stopped, or if the communication module identifies any other abnormal actions on the Modbus link. In the case when the communication module is not co-located with the DER, bump-in-the-wire (BITW) encryption devices may be used between the communication module and the DER. The Modbus protocol would be transmitted through the BITW devices between the communications module and the DER controller in a secure manner. This approach removes the burden of the communication module or the DER from supporting encryption capabilities.

Additional methods for partially securing the Modbus link at interface B are possible. These recommendations are enumerated in Table 4 below. The recommendations were developed with the mindset that due to the distributed location of the communication modules and the unsecure nature of the Modbus protocol, the Modbus data should never be trusted and always assumed to be malicious. Protocol conversion is also often implemented insecurely using embedded devices where cost dominates design decisions. The CSI RD&D Solicitation #4 communication module should balance cost with security, ensuring embedded devices have the hardware capabilities to implement additional security controls, including controls that conduct extra checks to verify the Modbus communications. Fortunately, Modbus has a narrow scope of functionality and data (especially when limiting data structures to only the SunSpec specification), making data checking and verification easier.

Table 4: Cyber Security Recommendations for CSI RD&D Solicitation #4 DER Communication: Interface B

Category	Description

Physical Security	
Physical Security	CSI RD&D Solicitation #4 DER communications module should be within the same locked container or facility as the DER controller, with only a very short serial link between them. "Bolt-on" or integrated communication modules are preferred.
Physical Security	Security technology should be included to send alarms whenever the lock is opened or if the normal Modbus traffic pattern is modified or stopped, or if the communication module identifies any other abnormal actions on the Modbus link.
Physical Security	Communication module components and serial headers should be potted and encapsulated to make tampering more difficult.
Access Control	
Authorization	The CSI RD&D Solicitation #4 DER communication module should not permit (drop) any unsolicited or anomalous Modbus traffic from Modbus DER slaves
Authorization	The communication module should not permit (drop) any traffic that appears to be traffic from a Modbus master. This is to prevent a rogue Modbus master or masquerading Modbus slave to use the CSI RD&D Solicitation #4 control module as a means of communicating with other DER on the network.
Authentication	Role-based access permissions should be established for individual data and DER functions.
Authorization	At minimum, the DER system should have pre-defined roles for DER owner, aggregator, vendor, and utility with default access permissions for each role.
Authorization	The DER system establishes "operating states" that modify what permissions different roles may have in the different operating states (e.g. normal, maintenance, or emergency operating states).
Authorization	The DER system only permits authorized users and systems to access its information and provide settings and commands.
Authorization	Reconfiguration of the communication module should not be permitted from the Modbus side of the module.
Integrity	
Data Integrity	If CSI RD&D Solicitation #4 DER communication module is not co-located with the inverter-based DER, BITW devices should be used to secure the Modbus channel to the DER.
Data Integrity	The communication module should drop all Modbus communications from unfamiliar Modbus slave IDs.
Data Integrity	The CSI RD&D Solicitation #4 DER communication module should ensure only requested registers are returned from Modbus slaves, no more, no less.
Data integrity	The communication module should drop any non-standard function codes received from DER Modbus slaves.

Data Integrity	The Modbus driver implemented within the communication module should be thoroughly tested and verified for robustness to prevent fuzzing techniques from disabling the Modbus stack or opening access to the WAN side of the module.
Data Integrity	The communication module should have controls in place on the Modbus side that guard against brute force attacks, such as communication throttling and timeouts.
Data Integrity	The communication module should be time synchronized to the rest of the system to ensure accurate log and data records.
Policy	
Logging	The inverter-based DER should log and alert on Modbus write commands that are beyond reasonable bounds. This requires that valid operational limits be configured within the DER.
Logging	The DER should log and alert on Modbus communications for unassigned registers or registers outside the SunSpec/local utility unique specification.
Logging	The communication module should log and alert on responses from unfamiliar traffic from unknown slave IDs or from traffic that appears to be from a Modbus master.
Logging	The communication module should log and alert on any additional or omitted registers received from the DER slave.
Logging	The communication module should log all network and system "health" events, including temporary and permanent channel failures, excess latency of message exchanges, lost packets, tampering with locks, etc.

6.4 Cyber Security for Communication Protocols

6.4.1 IEEE 2030.5 (SEP2) Cyber Security

IEEE 2030.5 (SEP2) is a protocol based on a representational state transfer (REST) architecture that is widely used for web-based services that employ hyper-text transfer protocol (HTTP). This RESTful architecture follows a client-server model where servers expose resources to clients and clients make requests to access these resources using common HTTP methods (i.e., GET, POST, PUT, DELETE, HEAD). The representation of each resource is similar to the IEC Common Information Model (CIM), defined in IEC 61968. The actual DER data objects are based on IEC 61850-7-420.

IEEE 2030.5 specifies TLS 1.2 (although TLS 1.0 is more often implemented) to secure communications between devices, digital certificates for authentication, and native IPv6 addressing. Concisely put, IEEE 2030.5 is an XML-based protocol (leveraging IEC CIM and EXI) developed on a RESTful architecture that uses HTTP over TLS for transport.

Although IEEE 2030.5 can be applied to other environments (e.g., utility to DER communications), the standard is primarily focused on communications of devices within home area networks, where the majority of devices are often compute and bandwidth deficient to minimize costs. The IEEE

2030.5 standard defines the mechanisms for exchanging application level messages, error messages, and the security features used to protect the application messages.

Given its focus on home area networks, the base security outlined in IEEE 2030.5 is designed to accommodate "native SEP2" devices, which are bandwidth and compute constrained devices predominately found in homes. This base security specifies minimal security features based on manufacturer certificates for authentication and the use of TLS 1.2 for transport layer security (when required). The manufacturing PKI infrastructure specified for native SEP2 devices use SEP2-contracted CAs, which necessarily chains back to a root CA.

IEEE 2030.5 also affords additional security features for "non-native SEP2" devices. If a device possesses adequate hardware resources and has a need for greater security, additional security mechanisms may be implemented. Table 5 describes the recommendations for security measures for IEEE 2030.5 when used with CSI RD&D Solicitation #4 DER communication modules.

For more detailed information regarding existing security controls implemented by the IEEE 2030.5 standard, reference the IEEE 2030.5 standard document.

Table 5: IEEE 2030.5 Security Measures

Security Requirement	IEEE 2030.5 Security Measure
User authentication	It is recommended that Role-Based Access Control capability be implemented for user authentication that identifies at least the following types of users: • Residential user • Vendor • Maintenance personnel • Security personnel Users shall be assigned to one or more roles. Passwords or other authentication mechanisms shall be used per individual users, not per role.
Device identification and authentication	All devices shall have certificates that are (or are chained from) their original manufacturer or root certificates to ensure identification for authentication. Separate certificates may be established for testing – these shall not be used for operational purposes. Self-signed certifications shall not be permitted. Each device shall have a globally unique ID.
Device authentication	HTTP over TLS [RFC 2818] (also known as HTTPS) shall use TLS version 1.2 [RFC 5246]. The mandatory-to-implement cipher suite does not permit only authentication without encryption. However, additional cipher suites can be used that would permit authentication without encryption.

Security Requirement	IEEE 2030.5 Security Measure
Access	Access Control Lists (ACLs) are applied to resources, identified by their URI. The ACL shall contains the security requirements for each URI and shall verify these security requirements are met for any message to a specific URI. It is recommended that ACLs be developed to ensure users and devices are permitted only to access their allowed data or allowed services.
PKI	Public Key Infrastructure (PKI) shall be supported as the mechanism to establish certificates, register cryptographic keys, and exchange secret cryptographic keys. PKI may also be used to exchange messages if secret keys are not used for messages.
Certificates	Certificate revocation lists (CRLs) or Online Certificate Status Protocol (OCSP) shall be supported to ensure that revoked certificates are identified by all parties and no further interactions permitted.
Cipher suite	The following cipher suite is mandated: TLS_ECDHE_ECDSA_WITH _AES_128_CCM_8 Other cipher suites are permitted upon mutual agreement. These should be updated if (and when) deprecated or if improved cipher suites are recommended in the future.
Security logs	Security logs shall include events and alarms, such as valid logins by users, invalid attempts to access devices, invalid use of the ports, loss of communications, number of communication failures, near-term certificate expirations, certificate revocations, as well as certain technical logs, such as unintentional DER disconnections.

6.4.2 IEEE 1815 (DNP3) Cyber Security

It is not expected that the CSI RD&D Solicitation #4 DER communication module will need to translate to DNP3, but if so, IEEE 1815 includes all cyber security requirements. The basic requirements are the same as for IEEE 2030.5, with the following additions:

- “Authentication only” is permitted (no encryption of messages, use of secret keys for authentication and digital signatures, and use of PKI to exchange secret keys)
- Modifications to the DNP3 message structure to add security fields

7 SUMMARY

Cyber security is becoming increasingly important and should be part of system designs from the initial stages, including in the CSI RD&D Solicitation #4 project. Without built-in security, DER systems, even at small residential installations, could have major impacts on the grid. Initially these impacts might just be to the residential DER owner, but in aggregate could impact the operation of the grid as increasing numbers of these small DER systems become interconnected. Therefore, implementation of the CSI RD&D Solicitation #4 communication module for residential inverter-based DER communications should comprise inclusion of industry standard best practices and the cyber security recommendations in this document as an integral part of design and development.

Cyber security policies, procedures, and technologies shall ensure, at a minimum, authentication, authorization, accountability, and integrity of the information exchanges. Cyber security technologies shall support end-to-end security of the information across all intermediary systems and networks. Network and system management technologies shall support the security of communications networks.

Privacy and confidentiality shall also be supported through cyber security policies, procedures, and technologies, as mutually agreed between Local and Area EPS operators.

Critical “at rest” DER and security data, such as passwords and cryptographic keys that are stored in DER systems, shall be secured from unauthorized access.

Finally, to foster interoperability, the information models, communication protocols, and cyber security technologies used for the information exchanges shall be international standards.

A. APPENDIX A – Cyber Security Scoring of DER Functions for Residential DER System

Below are the scoring tables used in the DER function analysis. A few notes regarding formatting and nomenclature:

- In the "Communication Requirements" column, "Autonomous" means that the function normally performs autonomously based on local measurements. The "ICT" designation, which stands for "information and communication technologies", means that remote communication technologies can be used to collect data from the device and change configuration settings.
- The "Res/Small Com" column designates the function's applicability to residential inverter-based DER. A "" in this column denotes that this function is likely to be present in a residential inverter-based DER. A "NA" means the function is not likely to be present in a residential inverter-based DER, therefore was not considered in the analysis.
- The "M" and "C" designations under the "IMPACT LEVELS" represent "monitoring" and "control" of each function. Monitoring should infer collecting data from the DER or collecting configuration information, where control should infer sending control commands or modifying configuration settings.

Table A1: Cyber Security Scoring of DER Functions: Communication Module to Utility

Q #	DER Functions	Description	Communication Requirements	Res/ Small Com	Constraints & Comments	IMPACT LEVELS											
						Confidentiality		*Integrity*		*Availability*		*Authentication*		*Authorization*		*Non-Repudiation*	
						M	*C*	*M*	*C*	*M*	*C*	*M*	*C*	*M*	*C*	*M*	*C*
	Monitoring																
1	**Monitor Alarms**: Provide emergency alarms and information	The DER system (and aggregations of DER systems, such as virtual power plants) provides alarms and supporting emergency information via the FDEMS to the utility. This function is feasible only if the ICT infrastructure is available.	*ICT*: DER system provides alarms and emergency information to utility and/or REP	**NA**	Utility does not have need asset management information. Only operational information needed. For material resources, information regarding planned and unplanned outages is needed for operational planning.	L	L	H	H	H	H	M	H	L	H	L	M
2	**Monitor DER Status and Output**: Provide status and measurements on current energy and ancillary services	The DER system (and aggregations of DER systems, such as virtual power plants) provides current status, power system measurements, and other real-time data (possibly aggregated via the FDEMS) to the utility, in order to support real-time and short-term analysis applications. This function is feasible only if the ICT infrastructure is available. (Revenue metering data is provided via alternate means.)	*ICT*: DER system provides status and measurement values to utility and/or REP		Important for understanding system state. The materiality of the resource determines its inclusion. This would include a de-rating of capacity. Status should be limited to those that effect the utility's management and use of the DER.	**M**	**M**	**H**	**H**	**M**	**M**	**H**	**H**	**L**	**H**	**L**	**M**

Q #	DER Functions	Description	Communication Requirements	Res/ Small Com	Constraints & Comments	IMPACT LEVELS											
						Confidentiality		*Integrity*		*Availability*		*Authentication*		*Authorization*		*Non-Repudiation*	
						M	*C*	*M*	*C*	*M*	*C*	*M*	*C*	*M*	*C*	*M*	*C*
	Real Power Functions																
3	**Limit Maximum Real Power:** Limit maximum real power output at an ECP or the PCC upon a direct command from the utility	The utility issues a direct command to limit the maximum real power output at the ECP or PCC. The reason might be that unusual or emergency conditions are causing reverse flow into the feeder's substation or because the total DER real power output on the feeder is greater than some percentage of total load. The command might be an absolute watt value or might be a percentage of DER output. This function is feasible only if the ICT infrastructure is available. It might also be used to ensure fairness across many DER systems.	*Autonomous* *Local: Monitor real power output at PCC* *ICT*: Utility issues a command to limit the real power output at the ECP or PCC		All resources must have the capability of being limited. Material resources have the capability of supporting the system more rapidly and warrant	M	M	H	H	L	M	M	H	L	H	L	M
4	**Set Real Power:** Set actual real power output at the ECP or PCC	The utility either presets or issues a direct command to set the actual real power output at the ECP or PCC (constant export/import if load changes; constant watts if no load). The reason might be to establish a base or known generation level without the need for constant monitoring. This is the approach often used today with synchronous generators. This function is feasible only if the ICT infrastructure is available. Meter reads could provide 15-minute energy by the end of the day could provide production information for operational planning.	*Autonomous* *Local: Monitor real power output at PCC.* *ICT: utility issues a command to modify the real power output at the ECP or PCC including for charging or discharging storage systems*		Larger DERs or multiple DERs within a facility No guarantee for intermittent resources without backup.	M	M	H	H	L	M	M	H	L	H	L	M
5	**Command DER to Connect or Disconnect:** Support direct command to disconnect or reconnect	The DER system performs a disconnect or reconnect at the ECP or PCC. Time windows are established for different DER systems to respond randomly within that window to the disconnect and reconnect commands. This function is feasible only if the ICT infrastructure is available.	*ICT*: Utility or FDEMS issues disconnect or reconnect command		This should largely be supported by the autonomous functions for small systems. For material systems a utility breaker might be used. However, better communications make this a desirable function to minimize cost.	M	M	H	H	L	H	M	H	L	H	L	M
	Autonomous DER Functions																
6	**Frequency-Watt:** Counteract frequency excursions beyond normal limits by decreasing or increasing real power	The DER system reduces real power to counteract frequency excursions beyond normal limits (and vice versa if additional generation or storage is available), particularly for microgrids. Hysteresis can be used as the frequency returns within the normal range to avoid abrupt changes by groups of DER systems.	*Autonomous* *Local: Monitor voltage anomalies* *ICT: Utility updates frequency response settings*		Can't provide up regulation – only down for over frequency conditions.	M	M	H	H	L	M	M	H	L	H	L	M
7	**Voltage-Watt:** Modify real power output autonomously in response to local voltage variations	The DER system monitors the local (or feeder) voltage and modifies real power output in order to damp voltage deviations. Settings are coordinated between the utility and DER operator. Hysteresis and delayed responses could be used to ensure overreactions or hunting does not occur.	*Autonomous* *Local: Monitor voltage* *ICT: Utility modifies the real power output settings*			M	M	H	H	L	M	M	H	L	H	L	M
8	**Dynamic Current Support:** Counteract voltage excursions beyond normal limits by providing dynamic current support	The DER system counteracts voltage anomalies (spikes or sags) through "dynamic current support". The DER system supports the grid during short periods of abnormally high or low voltage levels by feeding reactive current to the grid until the voltage either returns within its normal range, or the DER system ramps down, or the DER system is required to disconnect.	*Autonomous* *Local: Monitor voltage anomalies* *ICT: Utility updates dynamic current settings*		All DER systems but may not always be activated	M	M	H	H	L	M	M	H	L	H	L	M
9	**Watt- Power Factor:** Power factor is shifted based on real power output	The power factor is not fixed but changes with the power level. It might be slightly capacitive at very low output power levels and becoming slightly inductive at high power levels.	*Autonomous* *Local: Monitor real power output* *ICT: Utility updates power factor settings*		Needs to be enabled and controlled from an on-off perspective to ensure it doesn't negatively impact performance.	M	M	H	H	L	M	M	H	L	H	L	M

Q #	DER Functions	Description	Communication Requirements	Res/ Small Com	Constraints & Comments	IMPACT LEVELS											
						Confidentiality		*Integrity*		*Availability*		*Authentication*		*Authorization*		*Non-Repudiation*	
						M	*C*	*M*	*C*	*M*	*C*	*M*	*C*	*M*	*C*	*M*	*C*
10	**Smooth Frequency Deviations:** Smooth minor frequency deviations by rapidly modifying real power output to these deviations	The DER system modifies real power output rapidly to counter minor frequency deviations. The frequency-watt settings define the percentage of real-power output to modify for different degrees of frequency deviations on a second or even sub-second basis	*Autonomous* *Local: Monitor frequency* *ICT: Utility updates the frequency-watt settings*	**NA**	Recommended for all DER systems but may not always be activated. May be a problem for the ISO.	M	M	H	H	L	M	M	H	L	H	L	M
11	**Imitate capacitor bank triggers:** Provide reactive power through autonomous responses to weather, current, or time-of-day	Similar to capacitor banks on distribution circuits, the DER system implements temperature-var curves that define the reactive power for different ambient temperatures, similar to use of feeder capacitors for improving the voltage profile. Curves could also be defined for current-var and for time-of-day-var.	*Autonomous* *Local: Monitor weather conditions* *ICT: Utility updates xx-var curves*		Utilities may optionally identify some DER systems that could provide this functionality, with agreement by DER owner	**M**	**M**	**H**	**H**	**L**	**M**	**M**	**H**	**L**	**H**	**L**	**M**
12	**Short Circuit Current Limit:** DER must have short circuit limits	DER should limit their short circuit current to no more than 1.2 p.u. This is useful for utilities in order to perform short circuit impact studies.	*Autonomous*	**NA**	This is not a smart inverter function, but it is a good idea.	M	M	H	H	L	M	M	H	L	H	L	M
	Ancillary Services																
13	**Provide black start capabilities**	The DER system operates as a microgrid (possibly just itself) and supports additional loads being added, so long as they are within its generation capabilities. This function is feasible only if the ICT infrastructure is available.	*ICT: Utility issues "black start mode" command*		Optional, market driven, and based on capabilities of the DER systems. More of interest to customer microgrids.	**M**	**M**	**H**	**H**	**L**	**M**	**M**	**H**	**L**	**H**	**L**	**M**
14	**Participate in AGC:** Support frequency regulation by automatic generation control (AGC) commands	The DER system (or aggregations of DER systems) implements modification of real-power output based on AGC signals on a multi-second basis. This function is feasible only if the ICT infrastructure is available.	*ICT: Utility issues AGC commands to modify real power output*		Utilities may identify some DER systems to provide this functionality, with agreement by DER owner	**M**	**M**	**H**	**H**	**M**	**H**	**M**	**H**	**L**	**H**	**L**	**M**
15	**Provide "spinning" or operational reserve as bid into market**	The DER system provides emergency real power upon command at short notice (seconds or minutes), either through increasing generation or discharging storage devices. This function would be in response to market bids for providing this reserve. This function is feasible only if the ICT infrastructure is available.	*ICT: Utility issues command for emergency reserve*	**NA**	Optional, market driven, and based on capabilities of the DER systems. Interaction with the ISO and may need refinement coordination via a DSO in the future.	M	M	H	H	L	M	M	H	L	H	L	M
16	**Reactive Power Support during non-generating times:** Support the grid with reactive power during non-generating times	DERs support the grid with reactive power (VARs) when there is no primary energy (i.e. solar irradiance). This can be used by utilities to reduce the stress in the system in areas with high motor load (A/C) during peak times	*ICT: Utility or REP*		Depending on circumstances of the utility it may be used or not.	**M**	**M**	**H**	**H**	**L**	**L**	**M**	**H**	**L**	**H**	**L**	**M**

Q #	DER Functions	Description	Communication Requirements	Res/ Small Com	Constraints & Comments	IMPACT LEVELS											
						Confidentiality		*Integrity*		*Availability*		*Authentication*		*Authorization*		*Non-Repudiation*	
						M	*C*	*M*	*C*	*M*	*C*	*M*	*C*	*M*	*C*	*M*	*C*
17	**Single phase power control on multi-phase units:** Control power output independently in each phase	Multi-phase DER inverters/converters can have ability to control phase independently. This will be useful to balanced distribution circuits.	*ICT: Utility or REP*	**NA**		M	M	H	H	L	M	M	H	L	H	L	M
18	**Fast VAR Support for voltage mitigations:** DER fast VAR support 0.7PF to mitigate voltage deviations	DER can provide VAR support when the voltage goes out of normal range. Provide 0.7PF leading when voltage is between 88% and 50%. Provide 0.7 PF when the voltage is between 105% and 110%. This will provide grid support during voltage events (such as FIDVR events)	*Autonomous*		This function may have different values to different utilities based on their system characteristics.	**M**	**M**	**H**	**H**	**L**	**M**	**M**	**H**	**L**	**H**	**L**	**M**
19	**Backup Power :** Provide backup power after disconnecting from grid	The DER system, including energy storage and electric vehicles, has the ability to provide real power when the site is disconnected from grid power. The reason is for providing backup power to the facility and possibly black start capabilities.	*Autonomous* *Local: Monitor voltage, frequency, and connected load*		Decision by the DER owner/manager to provide their own microgrid capability. The customer decided to purchase this capability for their own needs.	**M**	**M**	**H**	**H**	**L**	**M**	**M**	**H**	**L**	**H**	**L**	**M**
	Storage-specific Functions																
20	**Set Charge Rate:** Storage converters should have the ability to set a charge rate	DER storage converters should have the ability to have charge rates (e.g., 30% / hour)	*Autonomous*		Importance depends on operating agreement for FDEMS Ramp rate and charge rate need to both be managed.	**M**	**M**	**H**	**H**	**L**	**L**	**M**	**H**	**L**	**H**	**L**	**M**
21	**Set Ramp Rate**	DER storage converters should have the ability to have ramp rates (e.g., default 10% / minute) so that they do not provoke inrush in local utilities				**M**	**M**	**H**	**H**	**L**	**L**	**M**	**H**	**L**	**H**	**L**	**M**
22	**Storage Frequency-Watt:** Ability to vary active power during frequency changes	Storage facilities can charge during over frequency and discharge during under frequency events. This can support the grid and support grid stabilization.	*Autonomous* *ICT: Utility or REP*		Scoring based of frequency watt above although the costs to implement are much higher to get more capability.	**M**	**M**	**H**	**H**	**L**	**L**	**M**	**H**	**L**	**H**	**L**	**M**
23	**Schedule Storage**: Set or schedule the storage of energy for later delivery, indicating time to start charging, charging rate and/or "charge-by" time	For a DER system that has storage capabilities, such as battery storage or a combined PV + storage system or a fleet of electric vehicles. Preset time-of-charge values can be established. Settings are coordinated between the utility and DER operator. Different scenarios could include: · Low load conditions at night are causing some renewable energy to be wasted, so charging energy storage DER systems at that time makes power system operations more efficient. · DER controller charges at the specified rate (less than or equal to the maximum charging rate) until the state-of-charge (SOC) reaches a specified level. · DER controller charges at the necessary rate in order to reach the specified SOC within the "charge-by" time.	*Autonomous* *ICT: Utility updates the storage settings and/or schedule*		Recommended for DER systems with storage capabilities	**M**	**M**	**H**	**H**	**L**	**L**	**M**	**H**	**L**	**H**	**L**	**M**

Q #	DER Functions	Description	Communication Requirements	Res/ Small Com	Constraints & Comments	IMPACT LEVELS											
						Confidentiality		*Integrity*		*Availability*		*Authentication*		*Authorization*		*Non-Repudiation*	
						M	*C*	*M*	*C*	*M*	*C*	*M*	*C*	*M*	*C*	*M*	*C*
24	**Flow Reservation :** Storage DER requests either charge or discharge	Storage DER requests either charge or discharge of defined amount of energy (kWh) starting at a defined time and completing by a defined time at a rate not exceeding a defined charge or discharge power level. Utility responds with an authorized energy transfer, start time, and maximum power level. The utility can update the response periodically to modulate the power flow during transfer, but cannot change from discharging to charging, or the reverse, without a new flow reservation request by the storage unit.	*ICT: Utility or REP*		Flow Reservation is initiated by the Storage DER. Other immediate charge/discharge functions based on IEC 61850 INV4 are initiated by Utility. **(IEEE 2030.5 SEP2)**	**M**	**M**	**H**	**H**	**L**	**L**	**M**	**H**	**L**	**H**	**L**	**M**
	Scheduling and Forecasts																
25	**Schedule output at PCC**: Schedule actual or maximum real power output at specific times	The utility establishes (or pre-establishes) a schedule (e.g. on-peak & off-peak) of actual or maximum real power output levels at the ECP or PCC, possibly combining generation, storage, and load management. The reason might be to minimize output during low load conditions while allowing or requiring higher output during peak load time periods.	*Autonomous* *Local: Monitor real power output at ECP or PCC.* *ICT: Utility updates the schedule of actual or maximum real power values*		Larger DERs or multiple DERs within a facility	**M**	**M**	**H**	**H**	**L**	**L**	**M**	**H**	**L**	**H**	**L**	**M**
26	**Schedule DER Functions:** Schedule real power and ancillary service outputs	The DER system receives and follows schedules for real power settings, reactive settings, limits, modes (such as autonomous volt/var, frequency-watt), and other operational settings.	*Autonomous* *ICT: Utility, REP, or FDEMS issues schedules to DER system*		Recommended for all DER systems but may not always be activated	**M**	**M**	**H**	**H**	**L**	**L**	**M**	**H**	**L**	**H**	**L**	**M**
27	**FDEMS or Aggregator provides generation and storage schedules:** Provide schedules to utilities or others	The FDEMS or Aggregator provides schedules of expected generation and storage reflecting customer requirements, maintenance, local weather forecasts, etc. This function is feasible only if the ICT infrastructure is available.	*ICT: Provide scheduling information to Utility, REP, or FDEMS*	**NA**	Only relevant for FDEMS and Aggregator. Aggregators report back based on the shared group identity. Note – this is highly related to 26.	M	M	H	H	L	L	M	H	L	H	L	M
28	**FDEMS or Aggregator provides forecasts of available energy or ancillary services:** Scheduled, planned, or forecast of available energy and ancillary services	The FDEMS or Aggregator provides scheduled, planned, and/or forecast information for available energy and ancillary services over the next hours, days, weeks, etc., for input into planning applications. Separate DER generation from load behind the PCC. This function is feasible only if the ICT infrastructure is available.	*ICT: FDEMS provides information to utility and/or REP*	**NA**	Optional, market driven, and based on capabilities of the DER systems	M	M	H	H	L	L	M	H	L	H	L	M
29	**FDEMS or Aggregator provides micro-locational weather forecasts:** Provide real-time and forecast weather forecasts	The FDEMS or Aggregator provides micro-locational weather forecasts, such as: Ambient temperature, Wet bulb temperature, Cloud cover level, Humidity, Dew point, Micro-location diffuse insolation, Micro-location direct normal insolation, Daylight duration (time elapsed between sunrise and sunset), Micro-location total horizontal insolation, Micro-location horizontal wind direction, Micro-location horizontal wind speed, Micro-location vertical wind direction, Vertical wind speed, Micro-location wind gust speed, Barometric pressure, Rainfall, Micro-location density of snowfall, Micro-location temperature of snowfall, Micro-location snow cover, Micro-location snowfall, Water equivalent of snowfall	*ICT: FDEMS provides information to utility and/or REP*	**NA**	Not planning on relying on external systems for weather forecast.	M	M	H	H	L	L	M	H	L	H	L	M

Q #	DER Functions	Description	Communication Requirements	Res/ Small Com	Constraints & Comments	IMPACT LEVELS											
						Confidentiality		*Integrity*		*Availability*		*Authentication*		*Authorization*		*Non-Repudiation*	
						M	*C*	*M*	*C*	*M*	*C*	*M*	*C*	*M*	*C*	*M*	*C*
	Registration, Maintenance, and Update																
30	**Provide DER Nameplate or As-Built information:** Provide operational characteristics at initial interconnection and upon changes	The DER system provides operational characteristics during initial Rule 21 screening, during implementation, or after its "discovery" and whenever changes are made to its operational status.	*Off-line or ICT*: (may be prior to installation) Provide DER characteristics information to utility		Can be provided via out of band registration and management processes. Can be automated for volume interactions as part of handbook.	**M**	**M**	**H**	**H**	**L**	**L**	**H**	**H**	**L**	**H**	**L**	**H**
31	**Registration:** Initiate automated "discovery" of DER systems	The DER system supports its automated "discovery" as interconnected to a location on the power system and initiates the integration process. This function is feasible only if the ICT infrastructure is available. Otherwise, manual methods must be used.	*Off-line or ICT: Utility, REP, or FDEMS "discovers" a new or moved DER system*		Registration should be a controlled process. More value for smaller systems to support better provisioning processes	**H**	**H**	**H**	**H**	**H**	**H**	**H**	**H**	**H**	**H**	**H**	**H**
32	**Initiate Periodic Tests:** Test DER functionality, performance, software patching and updates	Initial DER software installations and later updates are tested before deployment for functionality and for meeting regulatory and utility requirements, including safety. After deployment, testing validates the DER systems are operating correctly, safely, and securely.	*Off-line, local, or ICT*: (may be prior to installation or handled locally) Test DER software	**NA**	Recommended for all DER systems, using appropriate types of testing. However, the testing is managed outside of the utility and thus optional from a rule 21 perspective.	M	M	H	H	H	H	H	H	M	H	M	H
33	**DC Fault Test during startup:** Test the DC circuitry for fault conditions	DER tests its primary energy mover (DC solar PV modules) for fault conditions. This feature will try to alarm plant operators, owners, public that the DC side has a potential short that could lead to a fire hazard.	*Autonomous*	**NA**	A protective function of the DER itself. Not relevant from a rule 21 communications perspective. Already incorporated in codes (NEC 690.11) for DER continuous fault testing.	M	M	H	H	H	M	H	H	L	H	L	H
34	**DER Configuration Assessment:** the DER determines if the feeder's configuration has changed	The DER does an assessment of whether it is on a weak or strong feeder, and learns whether its configuration has changed	*Autonomous*		*How does this relate to rule 21 usage?* *Would need to report back its changed settings to the utility for its modelling and operational needs.*	**M**	**M**	**H**	**H**	**H**	**M**	**H**	**H**	**L**	**H**	**L**	**H**
	Scenarios for Decision-Making																
35	**Operate within an islanded microgrid:** Operate within an islanded microgrid	After grid power is lost or disconnected, or upon command, the DER system enters into microgrid "mode" as either "leading" or "following" the microgrid frequency and voltage, while acting either as base generation or as load-matching, depending upon preset parameters.	*Autonomous* *ICT: Utility or FDEMS issues "microgrid mode" command*	**NA**	Optional decision by DER owners/ managers if the DER systems have been designed to support microgrid operations	M	M	H	H	M	H	M	H	L	H	L	H
36	**Provide low cost energy**	Utility, REP, or FDEMS determines which DER systems are to generate how much energy over what time period in order to minimize energy costs. Some DER systems, such as PV	*Autonomous for renewables*	**NA**	Optional, market driven, and based on capabilities of the DER systems	M	M	H	H	M	H	M	H	L	H	L	M

Q #	DER Functions	Description	Communication Requirements	Res/ Small Com	Constraints & Comments	IMPACT LEVELS											
						Confidentiality		*Integrity*		*Availability*		*Authentication*		*Authorization*		*Non-Repudiation*	
						M	*C*	*M*	*C*	*M*	*C*	*M*	*C*	*M*	*C*	*M*	*C*
		systems, would provide low cost energy autonomously, while storage systems would need to be managed.	*ICT: Utility or REP issues real power output requirement to other DER systems*														
37	**Provide low emissions energy**	Utility, REP, or FDEMS determines which non-renewable DER systems are to generate how much energy in order to minimize emissions. Renewable DER systems would operate autonomously.	*Autonomous for renewables* *ICT: Utility or REP issues real power output level to other DER systems*	**NA**	Optional, market driven, and based on capabilities of the DER systems	M	M	H	H	M	H	M	H	L	H	L	M
38	**Provide renewable energy**	Utility, REP, or FDEMS selects which non-renewable DER systems are to generate how much energy in order to maximize the use of renewable energy. Renewable DER systems would operate autonomously.	*Autonomous for renewables* *ICT: Utility or REP issues real power output level to other DER systems*	**NA**	Optional, market driven, and based on capabilities of the DER systems	M	M	H	H	M	H	M	H	L	H	L	M
	Market Interactions																
39	**Respond to Real Power Pricing Signals:** Manage real power output based on demand response (DR) pricing signals	The DER system receives a demand response (DR) pricing signal from a utility or retail energy provider (REP) for a time period in the future and determines what real power to output at that time. This function is feasible only if the ICT infrastructure is available.	*ICT: Utility or REP issues DR pricing signal*		Optional, market driven, and based on capabilities of the DER systems. Possibly more important in a DSO future state.	**M**	**M**	**H**	**H**	**L**	**H**	**M**	**H**	**L**	**H**	**L**	**H**
40	**Respond to Ancillary Services Pricing Signals:** Manage selected ancillary services based on demand response (DR) pricing signals	The DER system receives a DR pricing signal from a utility or retail energy provider (REP) for a time period in the future and determines what ancillary services to provide at that time. This function is feasible only if the ICT infrastructure is available.	*ICT: Utility or REP issues DR pricing signal*		Optional, market driven, and based on capabilities of the DER systems. Possibly more important in a DSO future state.	**M**	**M**	**H**	**H**	**L**	**H**	**M**	**H**	**L**	**H**	**L**	**H**
	IEC 61850-90-7 (Not covered by functions above)																
41	**PV/Storage Functions**	Change the signal parameters for the storage system	*Autonomous* *ICT*: Utility or REP issues var settings			**M**	**M**	**H**	**H**	**L**	**L**	**M**	**H**	**L**	**H**	**L**	**M**
42	**Volt-Var mode**	Provide maximum vars constrained by Wmax, establish fixed var settings, no var support	*Autonomous* *ICT*: Utility or REP issues var settings			**M**	**M**	**H**	**H**	**L**	**M**	**M**	**H**	**L**	**H**	**L**	**M**
43	**Power factor settings**	Set power factor in response to feed-in power	*Autonomous* *ICT*: Utility or REP issues real power output level to other I- DER systems			**M**	**M**	**H**	**H**	**L**	**M**	**M**	**H**	**L**	**H**	**L**	**M**

Q #	DER Functions	Description	Communication Requirements	Res/ Small Com	Constraints & Comments	IMPACT LEVELS											
						Confidentiality		*Integrity*		*Availability*		*Authentication*		*Authorization*		*Non-Repudiation*	
						M	*C*	*M*	*C*	*M*	*C*	*M*	*C*	*M*	*C*	*M*	*C*
44	**Power factor settings**	Modify power factor-watts curve according to other parameters	*Autonomous* *ICT*: Utility or REP issues curves			**M**	**M**	**H**	**H**	**L**	**M**	**M**	**H**	**L**	**H**	**L**	**M**
45	**Temperature mode behavior**	Temperature-based curves	*Autonomous* *ICT*: Utility or REP issues real power output level to other I- DER systems			**M**	**M**	**H**	**H**	**L**	**L**	**M**	**H**	**L**	**H**	**L**	**M**
46	**Pricing signal mode behavior**	Mode curves based on utility signal	*Autonomous* *ICT*: Utility or REP issues mode curves			**M**	**M**	**H**	**H**	**M**	**M**	**M**	**H**	**L**	**H**	**L**	**M**
47	**Modify DER Inverter Settings**	Set default ramp rate, min. storage level, max. storage charge/discharge rate	*Autonomous* *ICT*: Utility or REP issues settings			**M**	**M**	**H**	**H**	**L**	**M**	**M**	**H**	**L**	**H**	**L**	**M**
48	**Event/History Logging**	Request event logs	*Autonomous* *ICT*: Utility or REP requests event logs			**M**	**M**	**H**	**H**	**L**	**L**	**M**	**H**	**L**	**H**	**L**	**M**
49	**Time Synchronization**	Set inverter time (manual/automated based on timing signals [GPS or network])	*ICT*: Utility or REP issues new time			**M**	**M**	**H**	**H**	**L**	**L**	**L**	**M**	**L**	**H**	**L**	**M**
50	**Connect/disconnect settings**	Set frequency ride-through or disconnect requirements	*Autonomous* *ICT*: Utility or REP issues settings			**M**	**M**	**H**	**H**	**L**	**M**	**M**	**H**	**L**	**H**	**L**	**M**

Table A2: Cyber Security Scoring of DER Functions: Communication Module to Aggregator/Vendor

Q#	DER Functions	Description	Communication Requirements	Res/ Small Com	Constraints & Comments	IMPACT LEVELS											
						Confidentiality		*Integrity*		*Availability*		*Authentication*		*Authorization*		*Non-Repudiation*	
						M	*C*	*M*	*C*	*M*	*C*	*M*	*C*	*M*	*C*	*M*	*C*
	Monitoring																
1	**Monitor Alarms**: Provide emergency alarms and information	The DER system (and aggregations of DER systems, such as virtual power plants) provides alarms and supporting emergency information via the FDEMS to the utility. This function is feasible only if the ICT infrastructure is available.	*ICT*: DER system provides alarms and emergency information to utility and/or REP	**NA**	Utility does not have need asset management information. Only operational information needed. For material resources, information regarding planned and unplanned outages is needed for operational planning.	L	L	H	H	H	H	H	H	L	H	L	H
2	**Monitor DER Status and Output**: Provide status and measurements on current energy and ancillary services	The DER system (and aggregations of DER systems, such as virtual power plants) provides current status, power system measurements, and other real-time data (possibly aggregated via the FDEMS) to the utility, in order to support real-time and short-term analysis applications. This function is feasible only if the ICT infrastructure is available. (Revenue metering data is provided via alternate means.)	*ICT*: DER system provides status and measurement values to utility and/or REP		Important for understanding system state. The materiality of the resource determines its inclusion. This would include a de-rating of capacity. Status should be limited to those that effect the utility's management and use of the DER.	**H**	**M**	**H**	**H**	**M**	**M**	**H**	**H**	**L**	**H**	**L**	**M**
	Real Power Functions																
3	**Limit Maximum Real Power:** Limit maximum real power output at an ECP or the PCC upon a direct command from the utility	The utility issues a direct command to limit the maximum real power output at the ECP or PCC. The reason might be that unusual or emergency conditions are causing reverse flow into the feeder's substation or because the total DER real power output on the feeder is greater than some percentage of total load. The command might be an absolute watt value or might be a percentage of DER output. This function is feasible only if the ICT infrastructure is available. It might also be used to ensure fairness across many DER systems.	*Autonomous* *Local: Monitor real power output at PCC* *ICT*: Utility issues a command to limit the real power output at the ECP or PCC		All resources must have the capability of being limited. Material resources have the capability of supporting the system more rapidly and warrant	**M**	**M**	**H**	**H**	**L**	**M**	**M**	**H**	**L**	**H**	**L**	**M**
4	**Set Real Power:** Set actual real power output at the ECP or PCC	The utility either presets or issues a direct command to set the actual real power output at the ECP or PCC (constant export/import if load changes; constant watts if no load). The reason might be to establish a base or known generation level without the need for constant monitoring. This is the approach often used today with synchronous generators. This function is feasible only if the ICT infrastructure is available. Meter reads could provide 15-minute energy by the end of the day could provide production information for operational planning.	*Autonomous* *Local: Monitor real power output at PCC.* *ICT: utility issues a command to modify the real power output at the ECP or PCC including for charging or discharging storage systems*		Larger DERs or multiple DERs within a facility No guarantee for intermittent resources without backup.	**M**	**M**	**H**	**H**	**L**	**M**	**M**	**H**	**L**	**H**	**L**	**M**
5	**Command DER to Connect or Disconnect:** Support direct command to disconnect or reconnect	The DER system performs a disconnect or reconnect at the ECP or PCC. Time windows are established for different DER systems to respond randomly within that window to the disconnect and reconnect commands. This function is feasible only if the ICT infrastructure is available.	*ICT*: Utility or FDEMS issues disconnect or reconnect command		This should largely be supported by the autonomous functions for small systems. For material systems a utility breaker might be used. However, better communications make this a desirable function to minimize cost.	**M**	**M**	**H**	**H**	**M**	**M**	**M**	**H**	**L**	**H**	**L**	**M**

Q#	DER Functions	Description	Communication Requirements	Res/ Small Com	Constraints & Comments	IMPACT LEVELS											
						Confidentiality		*Integrity*		*Availability*		*Authentication*		*Authorization*		*Non-Repudiation*	
						M	*C*	*M*	*C*	*M*	*C*	*M*	*C*	*M*	*C*	*M*	*C*
	Autonomous DER Functions																
6	**Frequency-Watt:** Counteract frequency excursions beyond normal limits by decreasing or increasing real power	The DER system reduces real power to counteract frequency excursions beyond normal limits (and vice versa if additional generation or storage is available), particularly for microgrids. Hysteresis can be used as the frequency returns within the normal range to avoid abrupt changes by groups of DER systems.	*Autonomous* *Local: Monitor voltage anomalies* *ICT: Utility updates frequency response settings*		Can't provide up regulation – only down for over frequency conditions.	**M**	**M**	**H**	**H**	**L**	**M**	**M**	**H**	**L**	**H**	**L**	**M**
7	**Voltage-Watt:** Modify real power output autonomously in response to local voltage variations	The DER system monitors the local (or feeder) voltage and modifies real power output in order to damp voltage deviations. Settings are coordinated between the utility and DER operator. Hysteresis and delayed responses could be used to ensure overreactions or hunting does not occur.	*Autonomous* *Local: Monitor voltage* *ICT: Utility modifies the real power output settings*			**M**	**M**	**H**	**H**	**L**	**M**	**M**	**H**	**L**	**H**	**L**	**M**
8	**Dynamic Current Support:** Counteract voltage excursions beyond normal limits by providing dynamic current support	The DER system counteracts voltage anomalies (spikes or sags) through "dynamic current support". The DER system supports the grid during short periods of abnormally high or low voltage levels by feeding reactive current to the grid until the voltage either returns within its normal range, or the DER system ramps down, or the DER system is required to disconnect.	*Autonomous* *Local: Monitor voltage anomalies* *ICT: Utility updates dynamic current settings*		All DER systems but may not always be activated	**M**	**M**	**H**	**H**	**L**	**M**	**M**	**H**	**L**	**H**	**L**	**M**
9	**Watt- Power Factor:** Power factor is shifted based on real power output	The power factor is not fixed but changes with the power level. It might be slightly capacitive at very low output power levels and becoming slightly inductive at high power levels.	*Autonomous* *Local: Monitor real power output* *ICT: Utility updates power factor settings*		Needs to be enabled and controlled from an on-off perspective to ensure it doesn't negatively impact performance.	**M**	**M**	**H**	**H**	**L**	**M**	**M**	**H**	**L**	**H**	**L**	**M**
10	**Smooth Frequency Deviations:** Smooth minor frequency deviations by rapidly modifying real power output to these deviations	The DER system modifies real power output rapidly to counter minor frequency deviations. The frequency-watt settings define the percentage of real-power output to modify for different degrees of frequency deviations on a second or even sub-second basis	*Autonomous* *Local: Monitor frequency* *ICT: Utility updates the frequency-watt settings*	**NA**	Recommended for all DER systems but may not always be activated. May be a problem for the ISO.	**M**	**M**	**H**	**H**	**L**	**M**	**M**	**H**	**L**	**H**	**L**	**M**
11	**Imitate capacitor bank triggers:** Provide reactive power through autonomous responses to weather, current, or time-of-day	Similar to capacitor banks on distribution circuits, the DER system implements temperature-var curves that define the reactive power for different ambient temperatures, similar to use of feeder capacitors for improving the voltage profile. Curves could also be defined for current-var and for time-of-day-var.	*Autonomous* *Local: Monitor weather conditions* *ICT: Utility updates xx-var curves*		Utilities may optionally identify some DER systems that could provide this functionality, with agreement by DER owner	**M**	**M**	**H**	**H**	**L**	**M**	**M**	**H**	**L**	**H**	**L**	**M**
12	**Short Circuit Current Limit:** DER must have short circuit limits	DER should limit their short circuit current to no more than 1.2 p.u. This is useful for utilities in order to perform short circuit impact studies.	*Autonomous*	**NA**	This is not a smart inverter function, but it is a good idea.	**M**	**M**	**H**	**H**	**L**	**M**	**M**	**H**	**L**	**H**	**L**	**M**

Q#	DER Functions	Description	Communication Requirements	Res/ Small Com	Constraints & Comments	IMPACT LEVELS											
						Confidentiality		*Integrity*		*Availability*		*Authentication*		*Authorization*		*Non-Repudiation*	
						M	*C*	*M*	*C*	*M*	*C*	*M*	*C*	*M*	*C*	*M*	*C*
	Ancillary Services																
13	**Provide black start capabilities**	The DER system operates as a microgrid (possibly just itself) and supports additional loads being added, so long as they are within its generation capabilities. This function is feasible only if the ICT infrastructure is available.	*ICT: Utility issues "black start mode" command*		Optional, market driven, and based on capabilities of the DER systems. More of interest to customer microgrids.	**M**	**M**	**H**	**H**	**L**	**M**	**M**	**H**	**L**	**H**	**L**	**M**
14	**Participate in AGC:** Support frequency regulation by automatic generation control (AGC) commands	The DER system (or aggregations of DER systems) implements modification of real-power output based on AGC signals on a multi-second basis. This function is feasible only if the ICT infrastructure is available.	*ICT: Utility issues AGC commands to modify real power output*		Utilities may identify some DER systems to provide this functionality, with agreement by DER owner	**M**	**M**	**H**	**H**	**M**	**H**	**M**	**H**	**L**	**H**	**L**	**M**
15	**Provide "spinning" or operational reserve as bid into market**	The DER system provides emergency real power upon command at short notice (seconds or minutes), either through increasing generation or discharging storage devices. This function would be in response to market bids for providing this reserve. This function is feasible only if the ICT infrastructure is available.	*ICT: Utility issues command for emergency reserve*	**NA**	Optional, market driven, and based on capabilities of the DER systems. Interaction with the ISO and may need refinement coordination via a DSO in the future.	**M**	**M**	**H**	**H**	**L**	**M**	**M**	**H**	**L**	**H**	**L**	**M**
16	**Reactive Power Support during non-generating times:** Support the grid with reactive power during non-generating times	DERs support the grid with reactive power (VARs) when there is no primary energy (i.e. solar irradiance). This can be used by utilities to reduce the stress in the system in areas with high motor load (A/C) during peak times	*ICT: Utility or REP*		Depending on circumstances of the utility it may be used or not.	**M**	**M**	**H**	**H**	**L**	**L**	**M**	**H**	**L**	**H**	**L**	**M**
17	**Single phase power control on multi-phase units:** Control power output independently in each phase	Multi-phase DER inverters/converters can have ability to control phase independently. This will be useful to balanced distribution circuits.	*ICT: Utility or REP*	**NA**		**M**	**M**	**H**	**H**	**L**	**M**	**M**	**H**	**L**	**H**	**L**	**M**
18	**Fast VAR Support for voltage mitigations:** DER fast VAR support 0.7PF to mitigate voltage deviations	DER can provide VAR support when the voltage goes out of normal range. Provide 0.7PF leading when voltage is between 88% and 50%. Provide 0.7 PF when the voltage is between 105% and 110%. This will provide grid support during voltage events (such as FIDVR events)	*Autonomous*		This function may have different values to different utilities based on their system characteristics.	**M**	**M**	**H**	**H**	**L**	**M**	**M**	**H**	**L**	**H**	**L**	**M**
19	**Backup Power :** Provide backup power after disconnecting from grid	The DER system, including energy storage and electric vehicles, has the ability to provide real power when the site is disconnected from grid power. The reason is for providing backup power to the facility and possibly black start capabilities.	*Autonomous* *Local: Monitor voltage, frequency, and connected load*		Decision by the DER owner/manager to provide their own microgrid capability. The customer decided to purchase this capability for their own needs.	**M**	**M**	**H**	**H**	**L**	**M**	**M**	**H**	**L**	**H**	**L**	**M**

Q#	DER Functions	Description	Communication Requirements	Res/ Small Com	Constraints & Comments	IMPACT LEVELS											
						Confidentiality		*Integrity*		*Availability*		*Authentication*		*Authorization*		*Non-Repudiation*	
						M	*C*	*M*	*C*	*M*	*C*	*M*	*C*	*M*	*C*	*M*	*C*
	Storage-specific Functions																
20	**Set Charge Rate:** Storage converters should have the ability to set a charge rate	DER storage converters should have the ability to have charge rates (e.g., 30% / hour)	*Autonomous*		Importance depends on operating agreement for FDEMS Ramp rate and charge rate need to both be managed.	**M**	**M**	**H**	**H**	**L**	**L**	**M**	**H**	**L**	**H**	**L**	**M**
21	**Set Ramp Rate**	DER storage converters should have the ability to have ramp rates (e.g., default 10% / minute) so that they do not provoke inrush in local utilities				**M**	**M**	**H**	**H**	**L**	**L**	**M**	**H**	**L**	**H**	**L**	**M**
22	**Storage Frequency-Watt:** Ability to vary active power during frequency changes	Storage facilities can charge during over frequency and discharge during under frequency events. This can support the grid and support grid stabilization.	*Autonomous* *ICT: Utility or REP*		Scoring based of frequency watt above although the costs to implement are much higher to get more capability.	**M**	**M**	**H**	**H**	**L**	**L**	**M**	**H**	**L**	**H**	**L**	**M**
23	**Schedule Storage**: Set or schedule the storage of energy for later delivery, indicating time to start charging, charging rate and/or "charge-by" time	For a DER system that has storage capabilities, such as battery storage or a combined PV + storage system or a fleet of electric vehicles. Preset time-of-charge values can be established. Settings are coordinated between the utility and DER operator. Different scenarios could include: · Low load conditions at night are causing some renewable energy to be wasted, so charging energy storage DER systems at that time makes power system operations more efficient. · DER controller charges at the specified rate (less than or equal to the maximum charging rate) until the state-of-charge (SOC) reaches a specified level. · DER controller charges at the necessary rate in order to reach the specified SOC within the "charge-by" time.	*Autonomous* *ICT: Utility updates the storage settings and/or schedule*		Recommended for DER systems with storage capabilities	**M**	**M**	**H**	**H**	**L**	**L**	**M**	**H**	**L**	**H**	**L**	**M**
24	**Flow Reservation :** Storage DER requests either charge or discharge	Storage DER requests either charge or discharge of defined amount of energy (kWh) starting at a defined time and completing by a defined time at a rate not exceeding a defined charge or discharge power level. Utility responds with an authorized energy transfer, start time, and maximum power level. The utility can update the response periodically to modulate the power flow during transfer, but cannot change from discharging to charging, or the reverse, without a new flow reservation request by the storage unit.	*ICT: Utility or REP*		Flow Reservation is initiated by the Storage DER. Other immediate charge/discharge functions based on IEC 61850 INV4 are initiated by Utility. **(IEEE 2030.5 SEP2)**	**M**	**M**	**H**	**H**	**L**	**L**	**M**	**H**	**L**	**H**	**L**	**M**

Q#	DER Functions	Description	Communication Requirements	Res/ Small Com	Constraints & Comments	IMPACT LEVELS											
						Confidentiality		*Integrity*		*Availability*		*Authentication*		*Authorization*		*Non-Repudiation*	
						M	*C*	*M*	*C*	*M*	*C*	*M*	*C*	*M*	*C*	*M*	*C*
	Scheduling and Forecasts																
25	**Schedule output at PCC**: Schedule actual or maximum real power output at specific times	The utility establishes (or pre-establishes) a schedule (e.g. on-peak & off-peak) of actual or maximum real power output levels at the ECP or PCC, possibly combining generation, storage, and load management. The reason might be to minimize output during low load conditions while allowing or requiring higher output during peak load time periods.	*Autonomous* *Local: Monitor real power output at ECP or PCC.* *ICT: Utility updates the schedule of actual or maximum real power values*		Larger DERs or multiple DERs within a facility	**M**	**M**	**H**	**H**	**L**	**L**	**M**	**H**	**L**	**H**	**L**	**M**
26	**Schedule DER Functions:** Schedule real power and ancillary service outputs	The DER system receives and follows schedules for real power settings, reactive settings, limits, modes (such as autonomous volt/var, frequency-watt), and other operational settings.	*Autonomous* *ICT: Utility, REP, or FDEMS issues schedules to DER system*		Recommended for all DER systems but may not always be activated	**M**	**M**	**H**	**H**	**L**	**L**	**M**	**H**	**L**	**H**	**L**	**M**
27	**FDEMS or Aggregator provides generation and storage schedules:** Provide schedules to utilities or others	The FDEMS or Aggregator provides schedules of expected generation and storage reflecting customer requirements, maintenance, local weather forecasts, etc. This function is feasible only if the ICT infrastructure is available.	*ICT: Provide scheduling information to Utility, REP, or FDEMS*	**NA**	Only relevant for FDEMS and Aggregator. Aggregators report back based on the shared group identity. Note – this is highly related to 26.	M	M	H	H	L	L	M	H	L	H	L	M
28	**FDEMS or Aggregator provides forecasts of available energy or ancillary services:** Scheduled, planned, or forecast of available energy and ancillary services	The FDEMS or Aggregator provides scheduled, planned, and/or forecast information for available energy and ancillary services over the next hours, days, weeks, etc., for input into planning applications. Separate DER generation from load behind the PCC. This function is feasible only if the ICT infrastructure is available.	*ICT: FDEMS provides information to utility and/or REP*	**NA**	Optional, market driven, and based on capabilities of the DER systems	M	M	H	H	L	L	M	H	L	H	L	M
29	**FDEMS or Aggregator provides micro-locational weather forecasts:** Provide real-time and forecast weather forecasts	The FDEMS or Aggregator provides micro-locational weather forecasts, such as: Ambient temperature, Wet bulb temperature, Cloud cover level, Humidity, Dew point, Micro-location diffuse insolation, Micro-location direct normal insolation, Daylight duration (time elapsed between sunrise and sunset), Micro-location total horizontal insolation, Micro-location horizontal wind direction, Micro-location horizontal wind speed, Micro-location vertical wind direction, Vertical wind speed, Micro-location wind gust speed, Barometric pressure, Rainfall, Micro-location density of snowfall, Micro-location temperature of snowfall, Micro-location snow cover, Micro-location snowfall, Water equivalent of snowfall	*ICT: FDEMS provides information to utility and/or REP*	**NA**	Not planning on relying on external systems for weather forecast.	M	M	H	H	L	L	M	H	L	H	L	M

Q#	DER Functions	Description	Communication Requirements	Res/ Small Com	Constraints & Comments	IMPACT LEVELS											
						Confidentiality		*Integrity*		*Availability*		*Authentication*		*Authorization*		*Non-Repudiation*	
						M	*C*	*M*	*C*	*M*	*C*	*M*	*C*	*M*	*C*	*M*	*C*
	Registration, Maintenance, and Update																
30	**Provide DER Nameplate or As-Built information:** Provide operational characteristics at initial interconnection and upon changes	The DER system provides operational characteristics during initial Rule 21 screening, during implementation, or after its "discovery" and whenever changes are made to its operational status.	*Off-line or ICT*: (may be prior to installation) Provide DER characteristics information to utility		Can be provided via out of band registration and management processes. Can be automated for volume interactions as part of handbook.	**M**	**M**	**H**	**H**	**L**	**L**	**H**	**H**	**L**	**H**	**L**	**H**
31	**Registration:** Initiate automated "discovery" of DER systems	The DER system supports its automated "discovery" as interconnected to a location on the power system and initiates the integration process. This function is feasible only if the ICT infrastructure is available. Otherwise, manual methods must be used.	*Off-line or ICT: Utility, REP, or FDEMS "discovers" a new or moved DER system*		Registration should be a controlled process. More value for smaller systems to support better provisioning processes	**H**	**H**	**H**	**H**	**H**	**H**	**H**	**H**	**H**	**H**	**H**	**H**
32	**Initiate Periodic Tests:** Test DER functionality, performance, software patching and updates	Initial DER software installations and later updates are tested before deployment for functionality and for meeting regulatory and utility requirements, including safety. After deployment, testing validates the DER systems are operating correctly, safely, and securely.	*Off-line, local, or ICT*: (may be prior to installation or handled locally) Test DER software	**NA**	Recommended for all DER systems, using appropriate types of testing. However, the testing is managed outside of the utility and thus optional from a rule 21 perspective.	M	M	H	H	H	H	H	H	M	H	M	H
33	**DC Fault Test during startup:** Test the DC circuitry for fault conditions	DER tests its primary energy mover (DC solar PV modules) for fault conditions. This feature will try to alarm plant operators, owners, public that the DC side has a potential short that could lead to a fire hazard.	*Autonomous*	**NA**	A protective function of the DER itself. Not relevant from a rule 21 communications perspective. Already incorporated in codes (NEC 690.11) for DER continuous fault testing.	M	M	H	H	H	M	H	H	L	H	L	H
34	**DER Configuration Assessment:** the DER determines if the feeder's configuration has changed	The DER does an assessment of whether it is on a weak or strong feeder, and learns whether its configuration has changed	*Autonomous*		*How does this relate to rule 21 usage?* *Would need to report back its changed settings to the utility for its modelling and operational needs.*	**M**	**M**	**H**	**H**	**H**	**M**	**H**	**H**	**L**	**H**	**L**	**H**
	Scenarios for Decision-Making																
35	**Operate within an islanded microgrid:** Operate within an islanded microgrid	After grid power is lost or disconnected, or upon command, the DER system enters into microgrid "mode" as either "leading" or "following" the microgrid frequency and voltage, while acting either as base generation or as load-matching, depending upon preset parameters.	*Autonomous* *ICT: Utility or FDEMS issues "microgrid mode" command*	**NA**	Optional decision by DER owners/ managers if the DER systems have been designed to support microgrid operations	M	M	H	H	M	H	M	H	L	H	L	H
36	**Provide low cost energy**	Utility, REP, or FDEMS determines which DER systems are to generate how much energy over what time period in order to minimize energy costs. Some DER systems, such as PV systems, would provide low cost energy autonomously, while storage systems would need to be managed.	*Autonomous for renewables* *ICT: Utility or REP issues real power output requirement to other DER systems*	**NA**	Optional, market driven, and based on capabilities of the DER systems	M	M	H	H	M	H	M	H	L	H	L	M

Q#	DER Functions	Description	Communication Requirements	Res/ Small Com	Constraints & Comments	IMPACT LEVELS											
						Confidentiality		*Integrity*		*Availability*		*Authentication*		*Authorization*		*Non-Repudiation*	
						M	*C*	*M*	*C*	*M*	*C*	*M*	*C*	*M*	*C*	*M*	*C*
37	**Provide low emissions energy**	Utility, REP, or FDEMS determines which non-renewable DER systems are to generate how much energy in order to minimize emissions. Renewable DER systems would operate autonomously.	*Autonomous for renewables* *ICT: Utility or REP issues real power output level to other DER systems*	**NA**	Optional, market driven, and based on capabilities of the DER systems	M	M	H	H	M	H	M	H	L	H	L	M
38	**Provide renewable energy**	Utility, REP, or FDEMS selects which non-renewable DER systems are to generate how much energy in order to maximize the use of renewable energy. Renewable DER systems would operate autonomously.	*Autonomous for renewables* *ICT: Utility or REP issues real power output level to other DER systems*	**NA**	Optional, market driven, and based on capabilities of the DER systems	M	M	H	H	M	H	M	H	L	H	L	M
	Market Interactions																
39	**Respond to Real Power Pricing Signals:** Manage real power output based on demand response (DR) pricing signals	The DER system receives a demand response (DR) pricing signal from a utility or retail energy provider (REP) for a time period in the future and determines what real power to output at that time. This function is feasible only if the ICT infrastructure is available.	*ICT: Utility or REP issues DR pricing signal*		Optional, market driven, and based on capabilities of the DER systems. Possibly more important in a DSO future state.	**M**	**M**	**H**	**H**	**L**	**H**	**M**	**H**	**L**	**H**	**L**	**H**
40	**Respond to Ancillary Services Pricing Signals:** Manage selected ancillary services based on demand response (DR) pricing signals	The DER system receives a DR pricing signal from a utility or retail energy provider (REP) for a time period in the future and determines what ancillary services to provide at that time. This function is feasible only if the ICT infrastructure is available.	*ICT: Utility or REP issues DR pricing signal*		Optional, market driven, and based on capabilities of the DER systems. Possibly more important in a DSO future state.	**M**	**M**	**H**	**H**	**L**	**H**	**M**	**H**	**L**	**H**	**L**	**H**
	IEC 61850-90-7 (Not covered by functions above)																
41	**PV/Storage Functions**	Change the signal parameters for the storage system	*Autonomous* *ICT*: Utility or REP issues var settings			**M**	**M**	**H**	**H**	**L**	**L**	**M**	**H**	**L**	**H**	**L**	**M**
42	**Volt-Var mode**	Provide maximum vars constrained by Wmax, establish fixed var settings, no var support	*Autonomous* *ICT*: Utility or REP issues var settings			**M**	**M**	**H**	**H**	**L**	**M**	**M**	**H**	**L**	**H**	**L**	**M**
43	**Power factor settings**	Set power factor in response to feed-in power	*Autonomous* *ICT*: Utility or REP issues real power output level to other I- DER systems			**M**	**M**	**H**	**H**	**L**	**M**	**M**	**H**	**L**	**H**	**L**	**M**
44	**Power factor settings**	Modify power factor-watts curve according to other parameters	*Autonomous* *ICT*: Utility or REP issues curves			**M**	**M**	**H**	**H**	**L**	**M**	**M**	**H**	**L**	**H**	**L**	**M**

Q#	DER Functions	Description	Communication Requirements	Res/ Small Com	Constraints & Comments	IMPACT LEVELS											
						Confidentiality		*Integrity*		*Availability*		*Authentication*		*Authorization*		*Non-Repudiation*	
						M	*C*	*M*	*C*	*M*	*C*	*M*	*C*	*M*	*C*	*M*	*C*
45	**Temperature mode behavior**	Temperature-based curves	*Autonomous* *ICT*: Utility or REP issues real power output level to other I- DER systems			**M**	**M**	**H**	**H**	**L**	**L**	**M**	**H**	**L**	**H**	**L**	**M**
46	**Pricing signal mode behavior**	Mode curves based on utility signal	*Autonomous* *ICT*: Utility or REP issues mode curves			**M**	**M**	**H**	**H**	**M**	**M**	**M**	**H**	**L**	**H**	**L**	**M**
47	**Modify DER Inverter Settings**	Set default ramp rate, min. storage level, max. storage charge/discharge rate	*Autonomous* *ICT*: Utility or REP issues settings			**M**	**M**	**H**	**H**	**L**	**M**	**M**	**H**	**L**	**H**	**L**	**M**
48	**Event/History Logging**	Request event logs	*Autonomous* *ICT*: Utility or REP requests event logs			**M**	**M**	**H**	**H**	**L**	**L**	**M**	**H**	**L**	**H**	**L**	**M**
49	**Time Synchronization**	Set inverter time (manual/automated based on timing signals [GPS or network])	*ICT*: Utility or REP issues new time			**M**	**M**	**H**	**H**	**L**	**L**	**L**	**M**	**L**	**H**	**L**	**M**
50	**Connect/disconnect settings**	Set frequency ride-through or disconnect requirements	*Autonomous* *ICT*: Utility or REP issues settings			**M**	**M**	**H**	**H**	**L**	**M**	**M**	**H**	**L**	**H**	**L**	**M**

Table A3: Cyber Security Scoring of DER Functions: Communication Module to DER

Q#	DER Functions	Description	Communication Requirements	Res/ Small Com	Constraints & Comments	IMPACT LEVELS											
						Confidentiality		*Integrity*		*Availability*		*Authentication*		*Authorization*		*Non-Repudiation*	
						M	*C*	*M*	*C*	*M*	*C*	*M*	*C*	*M*	*C*	*M*	*C*
	Monitoring																
1	**Monitor Alarms**: Provide emergency alarms and information	The DER system (and aggregations of DER systems, such as virtual power plants) provides alarms and supporting emergency information via the FDEMS to the utility. This function is feasible only if the ICT infrastructure is available.	*ICT*: DER system provides alarms and emergency information to utility and/or REP	**NA**	Utility does not have need asset management information. Only operational information needed. For material resources, information regarding planned and unplanned outages is needed for operational planning.	L	L	H	H	H	H	M	H	L	H	L	M
2	**Monitor DER Status and Output**: Provide status and measurements on current energy and ancillary services	The DER system (and aggregations of DER systems, such as virtual power plants) provides current status, power system measurements, and other real-time data (possibly aggregated via the FDEMS) to the utility, in order to support real-time and short-term analysis applications. This function is feasible only if the ICT infrastructure is available. (Revenue metering data is provided via alternate means.)	*ICT*: DER system provides status and measurement values to utility and/or REP		Important for understanding system state. The materiality of the resource determines its inclusion. This would include a de-rating of capacity. Status should be limited to those that effect the utility's management and use of the DER.	**H**	**M**	**H**	**H**	**M**	**M**	**M**	**H**	**L**	**H**	**L**	**M**
	Real Power Functions																
3	**Limit Maximum Real Power:** Limit maximum real power output at an ECP or the PCC upon a direct command from the utility	The utility issues a direct command to limit the maximum real power output at the ECP or PCC. The reason might be that unusual or emergency conditions are causing reverse flow into the feeder's substation or because the total DER real power output on the feeder is greater than some percentage of total load. The command might be an absolute watt value or might be a percentage of DER output. This function is feasible only if the ICT infrastructure is available. It might also be used to ensure fairness across many DER systems.	*Autonomous* *Local: Monitor real power output at PCC* *ICT*: Utility issues a command to limit the real power output at the ECP or PCC		All resources must have the capability of being limited. Material resources have the capability of supporting the system more rapidly and warrant	**M**	**M**	**H**	**H**	**L**	**M**	**M**	**H**	**L**	**H**	**L**	**M**
4	**Set Real Power:** Set actual real power output at the ECP or PCC	The utility either presets or issues a direct command to set the actual real power output at the ECP or PCC (constant export/import if load changes; constant watts if no load). The reason might be to establish a base or known generation level without the need for constant monitoring. This is the approach often used today with synchronous generators. This function is feasible only if the ICT infrastructure is available. Meter reads could provide 15-minute energy by the end of the day could provide production information for operational planning.	*Autonomous* *Local: Monitor real power output at PCC.* *ICT: utility issues a command to modify the real power output at the ECP or PCC including for charging or discharging storage systems*		Larger DERs or multiple DERs within a facility No guarantee for intermittent resources without backup.	**M**	**M**	**H**	**H**	**L**	**M**	**M**	**H**	**L**	**H**	**L**	**M**
5	**Command DER to Connect or Disconnect:** Support direct command to disconnect or reconnect	The DER system performs a disconnect or reconnect at the ECP or PCC. Time windows are established for different DER systems to respond randomly within that window to the disconnect and reconnect commands. This function is feasible only if the ICT infrastructure is available.	*ICT*: Utility or FDEMS issues disconnect or reconnect command		This should largely be supported by the autonomous functions for small systems. For material systems a utility breaker might be used. However, better communications make this a desirable function to minimize cost.	**M**	**M**	**H**	**H**	**L**	**H**	**M**	**H**	**L**	**H**	**L**	**M**

Q#	DER Functions	Description	Communication Requirements	Res/ Small Com	Constraints & Comments	IMPACT LEVELS											
						Confidentiality		*Integrity*		*Availability*		*Authentication*		*Authorization*		*Non-Repudiation*	
						M	*C*	*M*	*C*	*M*	*C*	*M*	*C*	*M*	*C*	*M*	*C*
	Autonomous DER Functions																
6	**Frequency-Watt:** Counteract frequency excursions beyond normal limits by decreasing or increasing real power	The DER system reduces real power to counteract frequency excursions beyond normal limits (and vice versa if additional generation or storage is available), particularly for microgrids. Hysteresis can be used as the frequency returns within the normal range to avoid abrupt changes by groups of DER systems.	*Autonomous* *Local: Monitor voltage anomalies* *ICT: Utility updates frequency response settings*		Can't provide up regulation – only down for over frequency conditions.	**M**	**M**	**H**	**H**	**L**	**M**	**M**	**H**	**L**	**H**	**L**	**M**
7	**Voltage-Watt:** Modify real power output autonomously in response to local voltage variations	The DER system monitors the local (or feeder) voltage and modifies real power output in order to damp voltage deviations. Settings are coordinated between the utility and DER operator. Hysteresis and delayed responses could be used to ensure overreactions or hunting does not occur.	*Autonomous* *Local: Monitor voltage* *ICT: Utility modifies the real power output settings*			**M**	**M**	**H**	**H**	**L**	**M**	**M**	**H**	**L**	**H**	**L**	**M**
8	**Dynamic Current Support:** Counteract voltage excursions beyond normal limits by providing dynamic current support	The DER system counteracts voltage anomalies (spikes or sags) through "dynamic current support". The DER system supports the grid during short periods of abnormally high or low voltage levels by feeding reactive current to the grid until the voltage either returns within its normal range, or the DER system ramps down, or the DER system is required to disconnect.	*Autonomous* *Local: Monitor voltage anomalies* *ICT: Utility updates dynamic current settings*		All DER systems but may not always be activated	**M**	**M**	**H**	**H**	**L**	**M**	**M**	**H**	**L**	**H**	**L**	**M**
9	**Watt- Power Factor:** Power factor is shifted based on real power output	The power factor is not fixed but changes with the power level. It might be slightly capacitive at very low output power levels and becoming slightly inductive at high power levels.	*Autonomous* *Local: Monitor real power output* *ICT: Utility updates power factor settings*		Needs to be enabled and controlled from an on-off perspective to ensure it doesn't negatively impact performance.	**M**	**M**	**H**	**H**	**L**	**M**	**M**	**H**	**L**	**H**	**L**	**M**
10	**Smooth Frequency Deviations:** Smooth minor frequency deviations by rapidly modifying real power output to these deviations	The DER system modifies real power output rapidly to counter minor frequency deviations. The frequency-watt settings define the percentage of real-power output to modify for different degrees of frequency deviations on a second or even sub-second basis	*Autonomous* *Local: Monitor frequency* *ICT: Utility updates the frequency-watt settings*	**NA**	Recommended for all DER systems but may not always be activated. May be a problem for the ISO.	**M**	**M**	**H**	**H**	**L**	**M**	**M**	**H**	**L**	**H**	**L**	**M**
11	**Imitate capacitor bank triggers:** Provide reactive power through autonomous responses to weather, current, or time-of-day	Similar to capacitor banks on distribution circuits, the DER system implements temperature-var curves that define the reactive power for different ambient temperatures, similar to use of feeder capacitors for improving the voltage profile. Curves could also be defined for current-var and for time-of-day-var.	*Autonomous* *Local: Monitor weather conditions* *ICT: Utility updates xx-var curves*		Utilities may optionally identify some DER systems that could provide this functionality, with agreement by DER owner	**M**	**M**	**H**	**H**	**L**	**M**	**M**	**H**	**L**	**H**	**L**	**M**
12	**Short Circuit Current Limit:** DER must have short circuit limits	DER should limit their short circuit current to no more than 1.2 p.u. This is useful for utilities in order to perform short circuit impact studies.	*Autonomous*	**NA**	This is not a smart inverter function, but it is a good idea.	**M**	**M**	**H**	**H**	**L**	**M**	**M**	**H**	**L**	**H**	**L**	**M**

Q#	DER Functions	Description	Communication Requirements	Res/ Small Com	Constraints & Comments	IMPACT LEVELS											
						Confidentiality		*Integrity*		*Availability*		*Authentication*		*Authorization*		*Non-Repudiation*	
						M	*C*	*M*	*C*	*M*	*C*	*M*	*C*	*M*	*C*	*M*	*C*
	Ancillary Services																
13	**Provide black start capabilities**	The DER system operates as a microgrid (possibly just itself) and supports additional loads being added, so long as they are within its generation capabilities. This function is feasible only if the ICT infrastructure is available.	*ICT: Utility issues "black start mode" command*		Optional, market driven, and based on capabilities of the DER systems. More of interest to customer microgrids.	**M**	**M**	**H**	**H**	**L**	**M**	**M**	**H**	**L**	**H**	**L**	**M**
14	**Participate in AGC:** Support frequency regulation by automatic generation control (AGC) commands	The DER system (or aggregations of DER systems) implements modification of real-power output based on AGC signals on a multi-second basis. This function is feasible only if the ICT infrastructure is available.	*ICT: Utility issues AGC commands to modify real power output*		Utilities may identify some DER systems to provide this functionality, with agreement by DER owner	**M**	**M**	**H**	**H**	**M**	**H**	**M**	**H**	**L**	**H**	**L**	**M**
15	**Provide "spinning" or operational reserve as bid into market**	The DER system provides emergency real power upon command at short notice (seconds or minutes), either through increasing generation or discharging storage devices. This function would be in response to market bids for providing this reserve. This function is feasible only if the ICT infrastructure is available.	*ICT: Utility issues command for emergency reserve*	**NA**	Optional, market driven, and based on capabilities of the DER systems. Interaction with the ISO and may need refinement coordination via a DSO in the future.	**M**	**M**	**H**	**H**	**L**	**M**	**M**	**H**	**L**	**H**	**L**	**M**
16	**Reactive Power Support during non-generating times:** Support the grid with reactive power during non-generating times	DERs support the grid with reactive power (VARs) when there is no primary energy (i.e. solar irradiance). This can be used by utilities to reduce the stress in the system in areas with high motor load (A/C) during peak times	*ICT: Utility or REP*		Depending on circumstances of the utility it may be used or not.	**M**	**M**	**H**	**H**	**L**	**L**	**M**	**H**	**L**	**H**	**L**	**M**
17	**Single phase power control on multi-phase units:** Control power output independently in each phase	Multi-phase DER inverters/converters can have ability to control phase independently. This will be useful to balanced distribution circuits.	*ICT: Utility or REP*	**NA**		**M**	**M**	**H**	**H**	**L**	**M**	**M**	**H**	**L**	**H**	**L**	**M**
18	**Fast VAR Support for voltage mitigations:** DER fast VAR support 0.7PF to mitigate voltage deviations	DER can provide VAR support when the voltage goes out of normal range. Provide 0.7PF leading when voltage is between 88% and 50%. Provide 0.7 PF when the voltage is between 105% and 110%. This will provide grid support during voltage events (such as FIDVR events)	*Autonomous*		This function may have different values to different utilities based on their system characteristics.	**M**	**M**	**H**	**H**	**L**	**M**	**M**	**H**	**L**	**H**	**L**	**M**
19	**Backup Power :** Provide backup power after disconnecting from grid	The DER system, including energy storage and electric vehicles, has the ability to provide real power when the site is disconnected from grid power. The reason is for providing backup power to the facility and possibly black start capabilities.	*Autonomous* *Local: Monitor voltage, frequency, and connected load*		Decision by the DER owner/manager to provide their own microgrid capability. The customer decided to purchase this capability for their own needs.	**M**	**M**	**H**	**H**	**L**	**M**	**M**	**H**	**L**	**H**	**L**	**M**

Q#	DER Functions	Description	Communication Requirements	Res/ Small Com	Constraints & Comments	IMPACT LEVELS											
						Confidentiality		*Integrity*		*Availability*		*Authentication*		*Authorization*		*Non-Repudiation*	
						M	*C*	*M*	*C*	*M*	*C*	*M*	*C*	*M*	*C*	*M*	*C*
	Storage-specific Functions																
20	**Set Charge Rate:** Storage converters should have the ability to set a charge rate	DER storage converters should have the ability to have charge rates (e.g., 30% / hour)	*Autonomous*		Importance depends on operating agreement for FDEMS Ramp rate and charge rate need to both be managed.	**M**	**M**	**H**	**H**	**L**	**L**	**M**	**H**	**L**	**H**	**L**	**M**
21	**Set Ramp Rate**	DER storage converters should have the ability to have ramp rates (e.g., default 10% / minute) so that they do not provoke inrush in local utilities				**M**	**M**	**H**	**H**	**L**	**L**	**M**	**H**	**L**	**H**	**L**	**M**
22	**Storage Frequency-Watt:** Ability to vary active power during frequency changes	Storage facilities can charge during overfrequency and discharge during under frequency events. This can support the grid and support grid stabilization.	*Autonomous* *ICT: Utility or REP*		Scoring based of frequency watt above although the costs to implement are much higher to get more capability.	**M**	**M**	**H**	**H**	**L**	**L**	**M**	**H**	**L**	**H**	**L**	**M**
23	**Schedule Storage**: Set or schedule the storage of energy for later delivery, indicating time to start charging, charging rate and/or "charge-by" time	For a DER system that has storage capabilities, such as battery storage or a combined PV + storage system or a fleet of electric vehicles. Preset time-of-charge values can be established. Settings are coordinated between the utility and DER operator. Different scenarios could include: · Low load conditions at night are causing some renewable energy to be wasted, so charging energy storage DER systems at that time makes power system operations more efficient. · DER controller charges at the specified rate (less than or equal to the maximum charging rate) until the state-of-charge (SOC) reaches a specified level. · DER controller charges at the necessary rate in order to reach the specified SOC within the "charge-by" time.	*Autonomous* *ICT: Utility updates the storage settings and/or schedule*		Recommended for DER systems with storage capabilities	**M**	**M**	**H**	**H**	**L**	**L**	**M**	**H**	**L**	**H**	**L**	**M**
24	**Flow Reservation :** Storage DER requests either charge or discharge	Storage DER requests either charge or discharge of defined amount of energy (kWh) starting at a defined time and completing by a defined time at a rate not exceeding a defined charge or discharge power level. Utility responds with an authorized energy transfer, start time, and maximum power level. The utility can update the response periodically to modulate the power flow during transfer, but cannot change from discharging to charging, or the reverse, without a new flow reservation request by the storage unit.	*ICT: Utility or REP*		Flow Reservation is initiated by the Storage DER. Other immediate charge/discharge functions based on IEC 61850 INV4 are initiated by Utility. **(IEEE 2030.5 SEP2)**	**M**	**M**	**H**	**H**	**L**	**L**	**M**	**H**	**L**	**H**	**L**	**M**

Q#	DER Functions	Description	Communication Requirements	Res/ Small Com	Constraints & Comments	IMPACT LEVELS											
						Confidentiality		*Integrity*		*Availability*		*Authentication*		*Authorization*		*Non-Repudiation*	
						M	*C*	*M*	*C*	*M*	*C*	*M*	*C*	*M*	*C*	*M*	*C*
	Scheduling and Forecasts																
25	**Schedule output at PCC**: Schedule actual or maximum real power output at specific times	The utility establishes (or pre-establishes) a schedule (e.g. on-peak & off-peak) of actual or maximum real power output levels at the ECP or PCC, possibly combining generation, storage, and load management. The reason might be to minimize output during low load conditions while allowing or requiring higher output during peak load time periods.	*Autonomous* *Local: Monitor real power output at ECP or PCC.* *ICT: Utility updates the schedule of actual or maximum real power values*		Larger DERs or multiple DERs within a facility	**M**	**M**	**H**	**H**	**L**	**L**	**M**	**H**	**L**	**H**	**L**	**M**
26	**Schedule DER Functions:** Schedule real power and ancillary service outputs	The DER system receives and follows schedules for real power settings, reactive settings, limits, modes (such as autonomous volt/var, frequency-watt), and other operational settings.	*Autonomous* *ICT: Utility, REP, or FDEMS issues schedules to DER system*		Recommended for all DER systems but may not always be activated	**M**	**M**	**H**	**H**	**L**	**L**	**M**	**H**	**L**	**H**	**L**	**M**
27	**FDEMS or Aggregator provides generation and storage schedules:** Provide schedules to utilities or others	The FDEMS or Aggregator provides schedules of expected generation and storage reflecting customer requirements, maintenance, local weather forecasts, etc. This function is feasible only if the ICT infrastructure is available.	*ICT: Provide scheduling information to Utility, REP, or FDEMS*	**NA**	Only relevant for FDEMS and Aggregator. Aggregators report back based on the shared group identity. Note – this is highly related to 26.	M	M	H	H	L	L	M	H	L	H	L	M
28	**FDEMS or Aggregator provides forecasts of available energy or ancillary services:** Scheduled, planned, or forecast of available energy and ancillary services	The FDEMS or Aggregator provides scheduled, planned, and/or forecast information for available energy and ancillary services over the next hours, days, weeks, etc., for input into planning applications. Separate DER generation from load behind the PCC. This function is feasible only if the ICT infrastructure is available.	*ICT: FDEMS provides information to utility and/or REP*	**NA**	Optional, market driven, and based on capabilities of the DER systems	M	M	H	H	L	L	M	H	L	H	L	M
29	**FDEMS or Aggregator provides micro-locational weather forecasts:** Provide real-time and forecast weather forecasts	The FDEMS or Aggregator provides micro-locational weather forecasts, such as: Ambient temperature, Wet bulb temperature, Cloud cover level, Humidity, Dew point, Micro-location diffuse insolation, Micro-location direct normal insolation, Daylight duration (time elapsed between sunrise and sunset), Micro-location total horizontal insolation, Micro-location horizontal wind direction, Micro-location horizontal wind speed, Micro-location vertical wind direction, Vertical wind speed, Micro-location wind gust speed, Barometric pressure, Rainfall, Micro-location density of snowfall, Micro-location temperature of snowfall, Micro-location snow cover, Micro-location snowfall, Water equivalent of snowfall	*ICT: FDEMS provides information to utility and/or REP*	**NA**	Not planning on relying on external systems for weather forecast.	M	M	H	H	L	L	M	H	L	H	L	M

Q#	DER Functions	Description	Communication Requirements	Res/ Small Com	Constraints & Comments	IMPACT LEVELS											
						Confidentiality		*Integrity*		*Availability*		*Authentication*		*Authorization*		*Non-Repudiation*	
						M	*C*	*M*	*C*	*M*	*C*	*M*	*C*	*M*	*C*	*M*	*C*
	Registration, Maintenance, and Update																
30	**Provide DER Nameplate or As-Built information:** Provide operational characteristics at initial interconnection and upon changes	The DER system provides operational characteristics during initial Rule 21 screening, during implementation, or after its "discovery" and whenever changes are made to its operational status.	*Off-line or ICT*: (may be prior to installation) Provide DER characteristics information to utility		Can be provided via out of band registration and management processes. Can be automated for volume interactions as part of handbook.	**M**	**M**	**H**	**H**	**L**	**L**	**H**	**H**	**L**	**H**	**L**	**H**
31	**Registration:** Initiate automated "discovery" of DER systems	The DER system supports its automated "discovery" as interconnected to a location on the power system and initiates the integration process. This function is feasible only if the ICT infrastructure is available. Otherwise, manual methods must be used.	*Off-line or ICT: Utility, REP, or FDEMS "discovers" a new or moved DER system*		Registration should be a controlled process. More value for smaller systems to support better provisioning processes	**H**	**H**	**H**	**H**	**H**	**H**	**H**	**H**	**H**	**H**	**H**	**H**
32	**Initiate Periodic Tests:** Test DER functionality, performance, software patching and updates	Initial DER software installations and later updates are tested before deployment for functionality and for meeting regulatory and utility requirements, including safety. After deployment, testing validates the DER systems are operating correctly, safely, and securely.	*Off-line, local, or ICT*: (may be prior to installation or handled locally) Test DER software	**NA**	Recommended for all DER systems, using appropriate types of testing. However, the testing is managed outside of the utility and thus optional from a rule 21 perspective.	M	M	H	H	H	H	H	H	M	H	M	H
33	**DC Fault Test during startup:** Test the DC circuitry for fault conditions	DER tests its primary energy mover (DC solar PV modules) for fault conditions. This feature will try to alarm plant operators, owners, public that the DC side has a potential short that could lead to a fire hazard.	*Autonomous*	**NA**	A protective function of the DER itself. Not relevant from a rule 21 communications perspective. Already incorporated in codes (NEC 690.11) for DER continuous fault testing.	M	M	H	H	H	M	H	H	L	H	L	H
34	**DER Configuration Assessment:** the DER determines if the feeder's configuration has changed	The DER does an assessment of whether it is on a weak or strong feeder, and learns whether its configuration has changed	*Autonomous*		*How does this relate to rule 21 usage?* *Would need to report back its changed settings to the utility for its modelling and operational needs.*	**M**	**M**	**H**	**H**	**H**	**M**	**H**	**H**	**L**	**H**	**L**	**H**
	Scenarios for Decision-Making																
35	**Operate within an islanded microgrid:** Operate within an islanded microgrid	After grid power is lost or disconnected, or upon command, the DER system enters into microgrid "mode" as either "leading" or "following" the microgrid frequency and voltage, while acting either as base generation or as load-matching, depending upon preset parameters.	*Autonomous* *ICT: Utility or FDEMS issues "microgrid mode" command*	**NA**	Optional decision by DER owners/ managers if the DER systems have been designed to support microgrid operations	M	M	H	H	M	H	M	H	L	H	L	H
36	**Provide low cost energy**	Utility, REP, or FDEMS determines which DER systems are to generate how much energy over what time period in order to minimize energy costs. Some DER systems, such as PV systems, would provide low cost energy autonomously, while storage systems would need to be managed.	*Autonomous for renewables* *ICT: Utility or REP issues real power output requirement to other DER systems*	**NA**	Optional, market driven, and based on capabilities of the DER systems	M	M	H	H	M	H	M	H	L	H	L	M

Q#	DER Functions	Description	Communication Requirements	Res/ Small Com	Constraints & Comments	IMPACT LEVELS											
						Confidentiality		*Integrity*		*Availability*		*Authentication*		*Authorization*		*Non-Repudiation*	
						M	*C*	*M*	*C*	*M*	*C*	*M*	*C*	*M*	*C*	*M*	*C*
37	**Provide low emissions energy**	Utility, REP, or FDEMS determines which non-renewable DER systems are to generate how much energy in order to minimize emissions. Renewable DER systems would operate autonomously.	*Autonomous for renewables* *ICT: Utility or REP issues real power output level to other DER systems*	**NA**	Optional, market driven, and based on capabilities of the DER systems	M	M	H	H	M	H	M	H	L	H	L	M
38	**Provide renewable energy**	Utility, REP, or FDEMS selects which non-renewable DER systems are to generate how much energy in order to maximize the use of renewable energy. Renewable DER systems would operate autonomously.	*Autonomous for renewables* *ICT: Utility or REP issues real power output level to other DER systems*	**NA**	Optional, market driven, and based on capabilities of the DER systems	M	M	H	H	M	H	M	H	L	H	L	M
	Market Interactions																
39	**Respond to Real Power Pricing Signals:** Manage real power output based on demand response (DR) pricing signals	The DER system receives a demand response (DR) pricing signal from a utility or retail energy provider (REP) for a time period in the future and determines what real power to output at that time. This function is feasible only if the ICT infrastructure is available.	*ICT: Utility or REP issues DR pricing signal*		Optional, market driven, and based on capabilities of the DER systems. Possibly more important in a DSO future state.	**M**	**M**	**H**	**H**	**L**	**H**	**M**	**H**	**L**	**H**	**L**	**H**
40	**Respond to Ancillary Services Pricing Signals:** Manage selected ancillary services based on demand response (DR) pricing signals	The DER system receives a DR pricing signal from a utility or retail energy provider (REP) for a time period in the future and determines what ancillary services to provide at that time. This function is feasible only if the ICT infrastructure is available.	*ICT: Utility or REP issues DR pricing signal*		Optional, market driven, and based on capabilities of the DER systems. Possibly more important in a DSO future state.	**M**	**M**	**H**	**H**	**L**	**H**	**M**	**H**	**L**	**H**	**L**	**H**
	IEC 61850-90-7 (Not covered by functions above)																
41	**PV/Storage Functions**	Change the signal parameters for the storage system	*Autonomous* *ICT*: Utility or REP issues var settings			**M**	**M**	**H**	**H**	**L**	**L**	**M**	**H**	**L**	**H**	**L**	**M**
42	**Volt-Var mode**	Provide maximum vars constrained by Wmax, establish fixed var settings, no var support	*Autonomous* *ICT*: Utility or REP issues var settings			**M**	**M**	**H**	**H**	**L**	**M**	**M**	**H**	**L**	**H**	**L**	**M**
43	**Power factor settings**	Set power factor in response to feed-in power	*Autonomous* *ICT*: Utility or REP issues real power output level to other I- DER systems			**M**	**M**	**H**	**H**	**L**	**M**	**M**	**H**	**L**	**H**	**L**	**M**
44	**Power factor settings**	Modify power factor-watts curve according to other parameters	*Autonomous* *ICT*: Utility or REP issues curves			**M**	**M**	**H**	**H**	**L**	**M**	**M**	**H**	**L**	**H**	**L**	**M**

Q#	DER Functions	Description	Communication Requirements	Res/ Small Com	Constraints & Comments	IMPACT LEVELS											
						Confidentiality		*Integrity*		*Availability*		*Authentication*		*Authorization*		*Non-Repudiation*	
						M	*C*	*M*	*C*	*M*	*C*	*M*	*C*	*M*	*C*	*M*	*C*
45	**Temperature mode behavior**	Temperature-based curves	*Autonomous* *ICT*: Utility or REP issues real power output level to other I- DER systems			**M**	**M**	**H**	**H**	**L**	**L**	**M**	**H**	**L**	**H**	**L**	**M**
46	**Pricing signal mode behavior**	Mode curves based on utility signal	*Autonomous* *ICT*: Utility or REP issues mode curves			**M**	**M**	**H**	**H**	**M**	**M**	**M**	**H**	**L**	**H**	**L**	**M**
47	**Modify DER Inverter Settings**	Set default ramp rate, min. storage level, max. storage charge/discharge rate	*Autonomous* *ICT*: Utility or REP issues settings			**M**	**M**	**H**	**H**	**L**	**M**	**M**	**H**	**L**	**H**	**L**	**M**
48	**Event/History Logging**	Request event logs	*Autonomous* *ICT*: Utility or REP requests event logs			**M**	**M**	**H**	**H**	**L**	**L**	**M**	**H**	**L**	**H**	**L**	**M**
49	**Time Synchronization**	Set inverter time (manual/automated based on timing signals [GPS or network])	*ICT*: Utility or REP issues new time			**M**	**M**	**H**	**H**	**L**	**L**	**L**	**M**	**L**	**H**	**L**	**M**
50	**Connect/disconnect settings**	Set frequency ride-through or disconnect requirements	*Autonomous* *ICT*: Utility or REP issues settings			**M**	**M**	**H**	**H**	**L**	**M**	**M**	**H**	**L**	**H**	**L**	**M**