EPRI | ELECTRIC POWER RESEARCH INSTITUTE

Cyber Security for DER Systems

Version 1.0

July 2013

National Electric Sector Cybersecurity Organization Resource (NESCOR)

Cyber Security for DER Systems

Version 1.0

July 2013

Authors:

Frances Cleveland, Xanthus Consulting International
Annabelle Lee, Electric Power Research Institute (EPRI)

Other contributors:

IEC TC57 Working Groups 15 and 17
Smart Grid Interoperability Panel (SGIP) Distributed Renewable Generation and Storage (DRGS) Domain Expert Working Group

Reviewers:

NESCOR Team 2 Members and Volunteers

Principal Investigator:

Annabelle Lee, EPRI

The research was paid for by the Department of Energy (DOE) under the NESCOR grant DE-OE0000524.

The following organization(s), under contract to EPRI, participated in the preparation of this report:

Xanthus Consulting

THE FOLLOWING ORGANIZATION PREPARED THIS REPORT:

Electric Power Research Institute (EPRI)

TABLE OF CONTENTS

Figures

Tables

1 DER SYSTEMS AND THEIR CYBER SECURITY REQUIREMENTS

1.1 Scope

The scope of this NESCOR report is to describe the cyber security requirements for Distributed Energy Resources (DER), reflecting DER functions in the smart grid and taking into account variations of DER architectures. These DER architectures are mapped to the DER Actors, Logical Interfaces, and Logical Interface Categories (LICs) in the National Institute of Standards and Technology Interagency Report (NISTIR) 7628, *Guidelines for Smart Grid Cyber Security*, August 2010, including proposed updates to the existing actors and logical interfaces. The NISTIR 7628 high-level security requirements that are associated with the LICs are assessed for applicability to these DER architectures. In addition, DER-specific issues are discussed.

The report describes five (5) levels of DER system architectures:

1. Autonomous cyber-physical DER systems
2. Facilities DER Energy Management Systems (FDEMS)
3. Information and Communications Technologies (ICT) for Utility and Retail Energy Providers (REP)
4. Distribution Utility DER Operational Analysis (DERMS)
5. Interactions with Independent System Operators/Regional Transmission Organizations (ISOs/RTOs) and the energy markets.

Using the NISTIR 7628 LICs and their associated high-level security requirements, this report identifies cyber security requirements that could be used at each of the five levels. In addition, this report assesses any gaps or concerns, particularly across domain boundaries and between different information standards. Because there are many factors that impact the selection of cyber security requirements, the information included in this document is recommendations. Each utility should identify its span of control and then review and select the applicable cyber security requirements from this document.

1.2 Utility Management of DER Systems within the Smart Grid

In the cyber security area, there are two key concepts for the smart grid: **resiliency** and **cyber-physical**. Resiliency implies that the power system critical infrastructure is designed not only to prevent malicious cyber attacks and inadvertent failures, but also to cope with and recover from such attacks and failures. Cyber-physical implies that the power system consists of both cyber and physical assets that are tightly intertwined and can be used in combination to improve the resiliency of the power system infrastructure.

DER systems are increasingly impacting the resiliency of the power system. At the same time, the power system cyber-physical capabilities can be used to increase resiliency, but only if appropriate cyber security measures are combined with these capabilities.

1.3 Definition of DER Systems

DER systems include renewable generation and storage systems, including photovoltaic systems, wind turbines, bio-fuel systems, fuel cells, battery storage systems, other electric or thermal storage systems, co-generation systems, small hydro plants, as well as non-renewable generators such as diesel generators and gas turbine generators. Each type of DER system has its own unique characteristics, but in general, each DER system can be treated as a small to medium-sized source of electric power. Electric Vehicles (EVs) can sometimes act as DER systems. Since EVs also have different purposes, they are identified as separate from the other types of DER systems.

DER systems range widely in size from a few kilowatts (kW) to tens of megawatts (MW), while groups of DER systems can be combined into large power plants. There are no universally recognized DER size boundaries, but DER systems are usually defined as being interconnected to the distribution power system or possibly the subtransmission power system.

DER systems are located at residential, commercial, and industrial customer sites and are usually owned and managed by the utility customers located at those sites. Utility-owned DER systems may be located at utility sites, such as substations, or may be located by mutual agreement at customer sites (e.g., rent-a-roof contracts). Retail Energy Providers (REP) may manage some DER systems as “virtual power plants,” while independent power producers may manage the groups of DER systems that form power plants.

DER systems consist of physical/electrical components (e.g., the electric generator and storage components) and cyber components (e.g., DER controllers), thus making them cyber-physical systems. They are generally designed to operate “autonomously” according to settings in the DER controller.

1.3.1 Utility Responsibilities for DER Systems Interconnected to their Smart Grid

Individual DER systems may be implemented at residential homes, at commercial facilities, or industrial sites, and make use of financial contracts such as net metering, feed-in tariffs, or other contractual arrangements with the distribution utilities. Multiple DER systems may be co-located in physical power plants, combined in aggregations as virtual power plants, deployed as utility-owned units for ancillary services support, or included in market-driven microgrids. Renewable DER systems pose challenges due to the variability of wind and solar energy, so additional ancillary services from “smart” DER systems may be necessary for counteracting this variability and ensuring the safety, reliability, and resiliency of the power system.

Utilities do not typically have direct organizational control over these DER systems and often need to operate through the DER owners, commercial Retail Energy Providers, Aggregators, Virtual Power Plant managers, or other third parties. In addition, many DER systems will be located at customer sites that have little or no security and with owners who have minimal or no cyber security expertise. In addition, unlike utility-owned smart meters, the customers must be permitted to interact with the DER systems

that they own, since they often use these systems to meet their specific requirements. These factors may increase the potential cyber security vulnerabilities to the interfaces between DER systems and utilities.

This complex DER domain is still evolving; increasing numbers of DER systems are being interconnected, more stakeholders are managing these interconnected systems, and updates to regulations are being debated. Few of the on-going discussions involve cyber security, since most of the focus is on getting the DER functions understood, the DER systems installed and operational, and the interconnection requirements standardized. In addition, many different communication protocols and standards are currently being used that often have inadequate cyber security capabilities. DER interactions cross many different domains and many different organizations, so that no single entity is in charge. Finally, few experts exist who understand both DER functionality and cyber security.

Consequently, given the basic requirement for power system resiliency, it is important to identify the cyber security requirements that utilities should consider before permitting these potentially vulnerable DER systems to be interconnected with their systems.

1.3.2 DER Systems as Cyber-Physical Systems

Cyber-physical systems (CPS) are engineered systems that depend upon the synergy of computational and physical components. Emerging CPS should be coordinated, distributed, and connected, and must be robust and responsive. New CPS will exceed the simple embedded systems of today in capability, adaptability, resiliency, safety, security, and usability.

Electric sector CPS protect against equipment failures, power anomalies such as voltage spikes, and against certain types of errors. Coping with inadvertent failures or deliberate attacks is also critical, since power system equipment cannot be shut off when an anomalous event occurs. Power system equipment must remain functional as much as possible. Recovery strategies after failures or attacks are also critical, since the power must remain on, as much as feasible, even if equipment is removed for repair.

Traditional analysis tools are unable to cope with the full complexity of CPS or adequately predict system behavior. For example, the current electric power grid may experience blackouts over large regions that are triggered by minor events that may escalate with surprising speed into widespread power failures. In addition, traditional real-time performance guarantees are insufficient for CPS when systems are large, and spatially and temporally distributed in arrangements that may rapidly change. With the greater autonomy and cooperation possible with CPS, greater assurances of safety, security, scalability, and reliability are necessary.

Cyber security for cyber-physical systems includes some additional considerations:

- Physical impacts. Cyber security events (whether deliberate or inadvertent) can cause physical results, such as power outages and damaged equipment. These

events are usually caused by compromising the cyber information and/or control commands. Therefore, successful compromises of data (whether deliberate or inadvertent) may affect the DER system operations and cause some physical impact, including harm and death to people.

- Existing cyber-physical systems protections and mitigations. In general, cyber-physical systems (e.g., DER systems and the power system) are designed for resiliency, to cope with equipment failures and inadvertent cyber security events through fault-tolerant equipment design, redundancy of equipment, and software applications that model the physical systems using the laws of physics (e.g., power flow-based applications). These design protections may counter potential cyber security events. In addition, existing cyber-physical reactions may be invoked to mitigate the impact of an attack. These designs and intrinsic mitigations may be enhanced to address new cyber security events, attacks and threats.
- Impacts from cyber security. Some IT cyber security mitigation procedures and technologies can negatively impact cyber-physical systems. Therefore, the cyber security mitigations must be carefully integrated into cyber-physical systems to ensure that the primary functionality is maintained. For example, availability is the key requirement in most power system operational scenarios, so that a cyber security mitigation that shuts down equipment may not be an acceptable strategy.

DER systems are cyber-physical systems that provide energy and ancillary services to the power grid through interconnections to the distribution system. DER systems can be generators, storage devices, and even electric vehicles if their chargers are capable of managing the charging and discharging processes. Generally these DER systems are small (usually less than 50 MW), but potentially there will be millions of DER systems interconnected with the distribution system.

1.3.3 Utility Management of DER Systems

New methods for handling these dispersed sources of generation and storage are being developed, including both new power system functions and new communication capabilities. In particular, the smart capabilities of DER systems will be utilized to allow power system management to take place locally and within the utility environment.

Increased reliance on communications also creates more potential vulnerabilities to cyber security attacks against these cyber-physical DER systems. Many stakeholders (actors) are involved in DER functions that cannot be covered by single organizational cyber security policies and procedures. DER systems are often located in environments with inadequate cyber security where they are outside the direct security management of utilities and they may be open to physical and Internet access in those environments. Since these cyber-physical DER systems can affect the operation and safety of the power grid, cyber security measures are critical to addressing possible electrical impacts to the grid in addition to securing the information flows.

Cyber security for DER systems requires a different approach than for typical IT systems. As stated in the NISTIR 7628:

> *Traditionally, cyber security for Information Technology (IT) focuses on the protection required to ensure the confidentiality, integrity, and availability of the electronic information communication systems. Cyber security needs to be appropriately applied to the combined power system and IT communication system domains to maintain the reliability of the Smart Grid and privacy of consumer information. Cyber security in the Smart Grid must include a balance of both power and cyber system technologies and processes in IT and power system operations and governance. Poorly applied practices from one domain that are applied into another may degrade reliability.*[1]

1.4 DER Actors in the NISTIR 7628 Logical Reference Model

The NISTIR 7628 (2010) defined a cyber security logical reference model that covered the high level Actors and Logical Interfaces of the Smart Grid. It is affectionately termed the "spaghetti diagram," and is shown in Figure 1-1 below.

[1] NISTIR 7628, *Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements*, Section 1.2, August 2010.

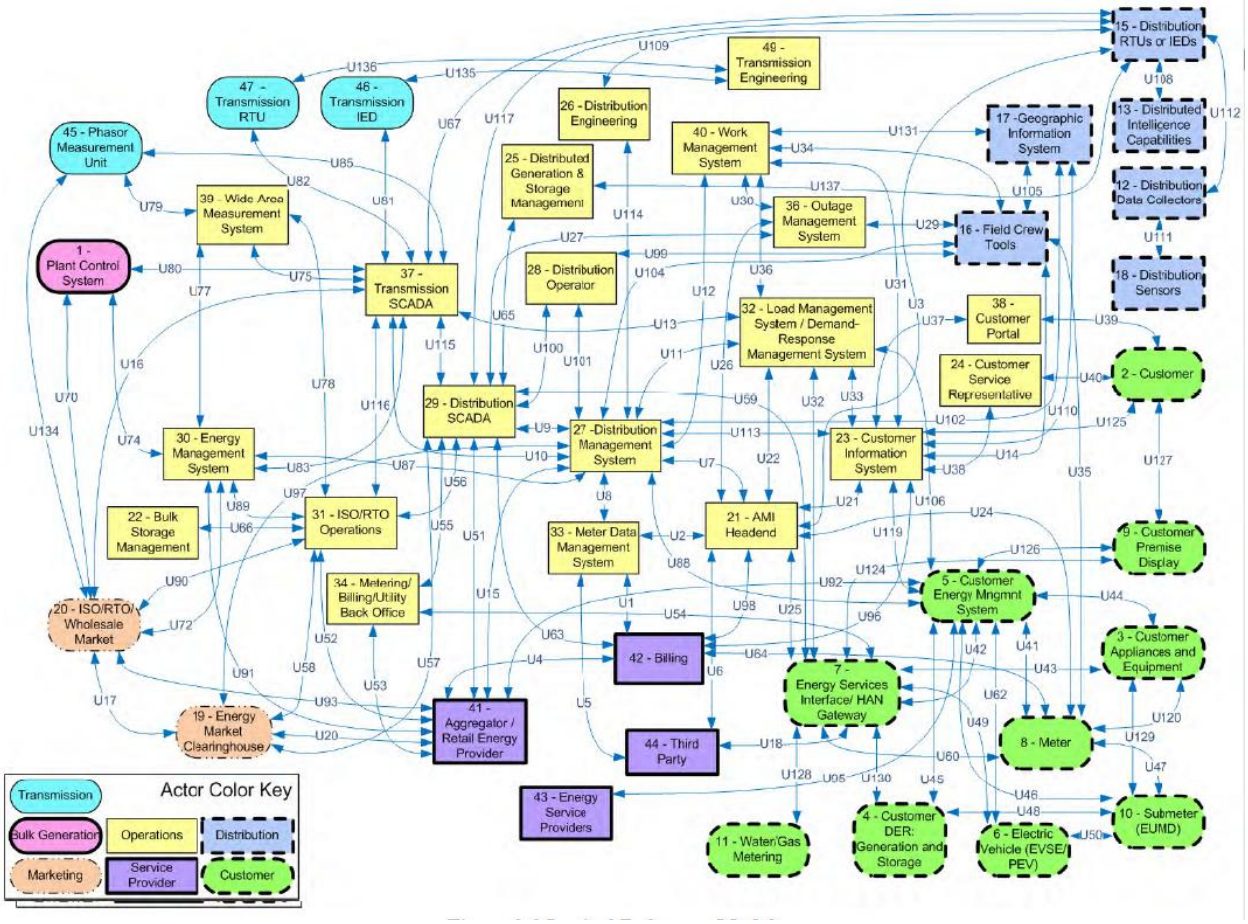

Figure 1-1: NISTIR 7628 – Figure 2.3 Logical Reference Model (“Spaghetti Diagram”)

1.4.1 Extensions and Modifications for DER Systems

Only some of the Actors and Interfaces in the NISTIR 7628 Logical Reference Model are relevant to DER systems. In addition, in some instances, the spaghetti diagram did not provide adequate detail for high-level DER functionality, due in part to the evolving nature of DER system management that was not clear at the time of the NISTIR 7628 publication. This updated DER Logical Reference Model was developed as an extract/expansion of the NISTIR 7628 spaghetti diagram (see Figure 1-2 below).

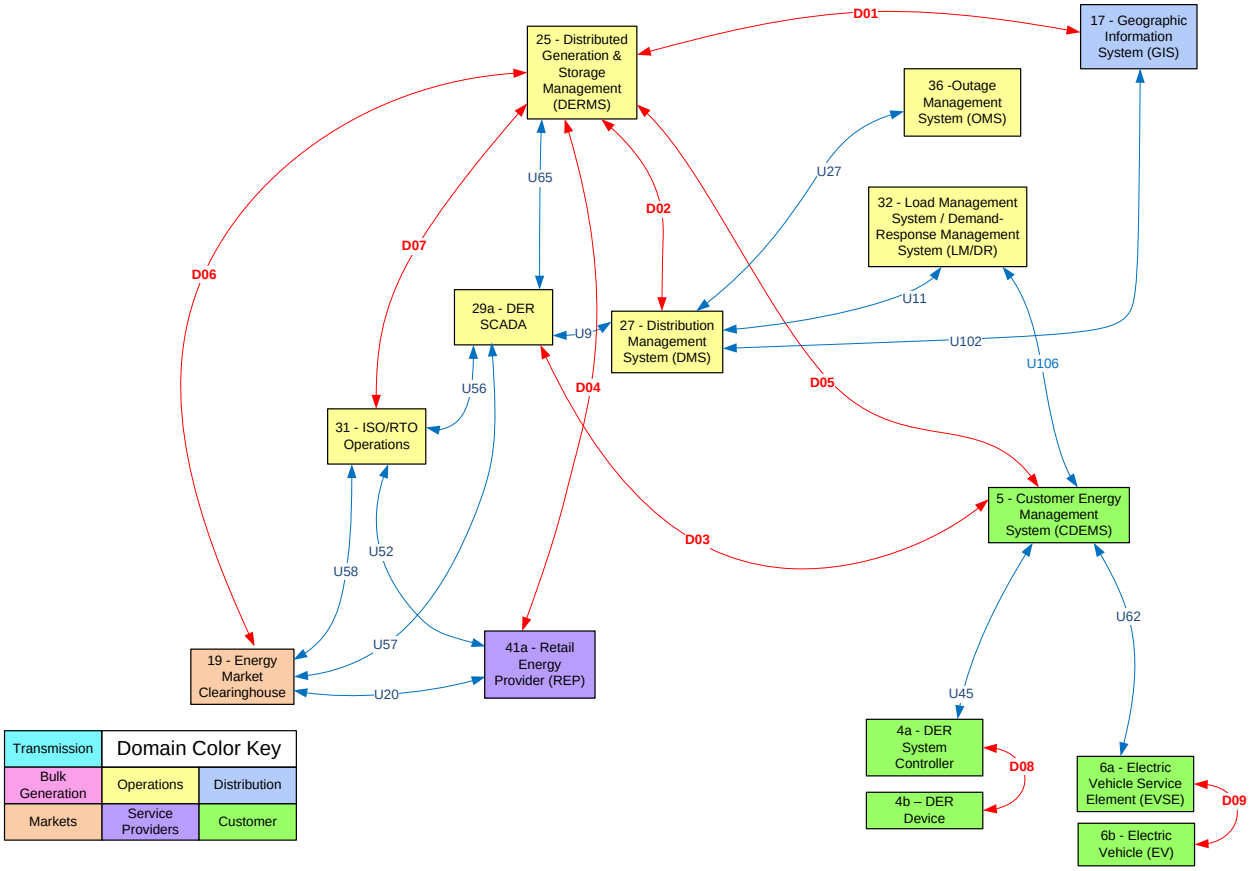

Figure 1-2: DER Logical Reference Model Extended/Modified from the Spaghetti Diagram

In Figure 1-2, the 13 logical interfaces shown in blue (using the designation of Uxx) indicate the original logical interfaces defined in the NISTIR 7628. In assessing DER functional requirements, nine additional logical interfaces (shown in red and using the designation of Dxx) were added to meet all functional requirements. These logical interfaces are discussed in more detail in later sections of this document.

In this DER Logical Reference Model, one Actor was split into two: the combined "Aggregator/Retail Energy Provider" (#41) Actor was separated into the "Retail Energy Provider (REP)" Actor (#41a) and the "Aggregator" (#41b) Actor (not included in the diagram above). These Actors perform different functions and have different scopes in interacting with DER systems. (*The #x numbers refer to the Actors in the spaghetti diagram.)*

In addition, the "Customer DER Generation and Storage" (#4) Actor has been modified to be only "DER generation and storage," since only some of the smaller residential DER systems might be part of a customer Home Area Network (HAN). Most of the larger commercial, industrial, and community DER systems as well as those owned and managed by the utilities will not include an Energy Services Interface (ESI). Therefore, the "Energy Services Gateway/HAN" (#7) Actor was not included. From a cyber security perspective, this means that these DER systems cannot rely on an ESI/HAN firewall and

will require additional security policies, procedures, and technologies that can be provided by the "Customer Energy Management System" (#5) Actor. This Actor's name was also modified to the broader term "Facility Energy Management System (FDEMS)" because not all DER systems are located at customer sites.

The "Distribution SCADA" (#29) Actor was modified to the "DER SCADA" (#29a) Actor, since it is unlikely that the same supervisory control and data acquisition (SCADA) system would be used both for internal utility distribution communications and for communications to customer sites with DER systems. The communication mechanisms that will be used by utilities have not been determined because few utilities currently interact with customer-owned DER systems.

Although DER systems are metered, the metering functions are not specific to DER systems and are therefore outside the scope of this report. Also, the communications systems and protocols used for metering will most likely not be used for DER monitoring and control, although in some cases the same physical media may underlie parts of the different networks (e.g. backhaul WANs). These network configurations are also out-of-scope of this report.

1.4.2 DER Actors in the DER Logical Reference Model

As shown in Figure 1-2, this report only addresses the following DER actors in the DER Logical Reference Model:

- **DER Generation and Storage (*DER systems*) (#4).** DER systems include renewable generation and storage systems; including photovoltaic systems, wind turbines, bio-fuel systems, fuel cells, battery storage systems, other electric or thermal storage systems, co-generation systems, small hydro plants, as well as non-renewable generators such as diesel generators, and gas turbine generators. Each type of DER system has its own characteristics, but in general, each DER system can be treated as a small to medium-sized source of electric power.
- **Electric Vehicles (EVSE/PEV) (EVs) (#6)** are also considered to act as DER systems when they are capable of providing energy storage and/or ancillary services. For this report, only their DER characteristics are considered.
- The **Facilities (DER) Energy Management System *(Facilities EMS)* (#5)** manages combinations of DER generation, DER storage, and customer loads at a residential, commercial, and industrial customer site.
- The **Distribution Utility DER Operational Analysis (DERMS) (#25)** manages the requests and commands to the DER systems. For this architecture, the DERMS is also responsible for the database of interconnection permits and registrations of DER systems.
- The utility **Distribution Management System (*DMS*) (#27)** assesses the short-term forecasts for the distribution system, using power-flow-based applications, geographic information system (GIS) data, load forecasts, DER forecasts,

customer load/generation profiles, and other information to determine the reliability and efficiency of the distribution system over the short term. It can then request modifications to DER system energy and ancillary services through the DERMS.

- The utility **Distribution SCADA system (*Distribution SCADA*) (#29)** monitors and issues controls to power system equipment in real-time, including some individual large DER systems directly, aggregations of smaller DER systems, and combined DER generation and loads generally at substations.
- The utility **Geographic Information System *(GIS)* (#17)** provides geographic and topological information of the power system, including locations of DER systems.
- The utility **Outage Management System *(OMS)* (#36)** monitors and manages power system outages based on SCADA information, trouble call systems, and Advanced Metering Infrastructure (AMI) outage reports.
- The utility **Load Management System/Demand Response Management System *(LM/DR)* (#32)** assess the capabilities of customer loads to respond to direct commands and/or pricing signals from demand response analyses. The LM/DR also issues direct load control commands and/or demand response pricing signals.
- The **Retail Energy Provider/Energy Service Provider (*REP/ESP*) (#41a)** sells and purchases electric energy to/from retail customers and (for the purpose of this architecture) manages the energy and ancillary services provided by groups of DER systems at multiple customer sites. These may be considered as “virtual power plants” that are bid into the electricity market for both energy and ancillary services. The REP/ESP is also responsible for both the electrical and cyber maintenance of these cyber-physical DER systems.
- The **Energy Market Clearinghouse** (***Market***) **(#19)** acts as the market for buying and selling energy and ancillary services.
- The **ISO/RTO Operations (*ISO/RTO)* (#31)** balances the power system to maintain a stable frequency, based on operating reliability regulations and the energy and ancillary services products that were bid into the market.

2 CYBER SECURITY FOR HIERARCHICAL DER ARCHITECTURE LEVELS

2.1 DER System Architectures and Typical Configurations

Direct control by utilities is not feasible for the thousands and potentially millions of DER systems in the field, so a hierarchical approach is necessary for utilities to interact with these widely dispersed cyber-physical systems.

At the local level, DER systems manage their own generation and storage activities autonomously, based on local conditions and DER owner preferences. DER systems are active participants in grid operations and must be coordinated with other DER systems and distribution grid devices. In addition, the distribution utilities must interact with RTOs and/or ISOs for reliability and market purposes. In some regions, REPs or other ESPs are responsible for managing groups of DER systems.

Figure 2-1 below illustrates this hierarchy and the various devices that may be included.

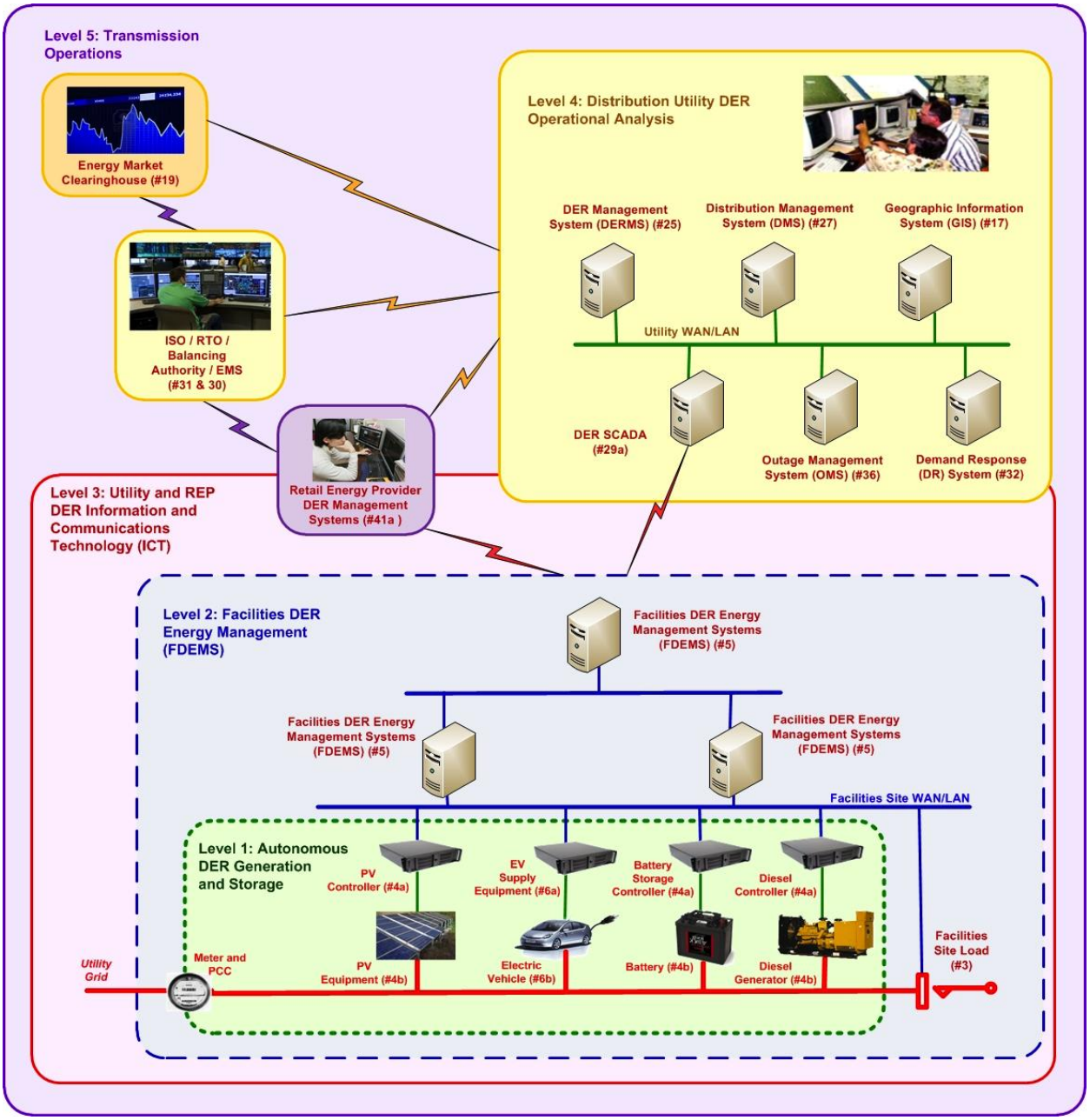

Figure 2-1: Hierarchical DER System Architecture

2.1.1 Logical DER System Architecture

The hierarchy illustrated above is abstracted to the logical architecture shown in Figure 2-2 below. This logical architecture is a hybrid combination of five architectures and is described in the following subsections:

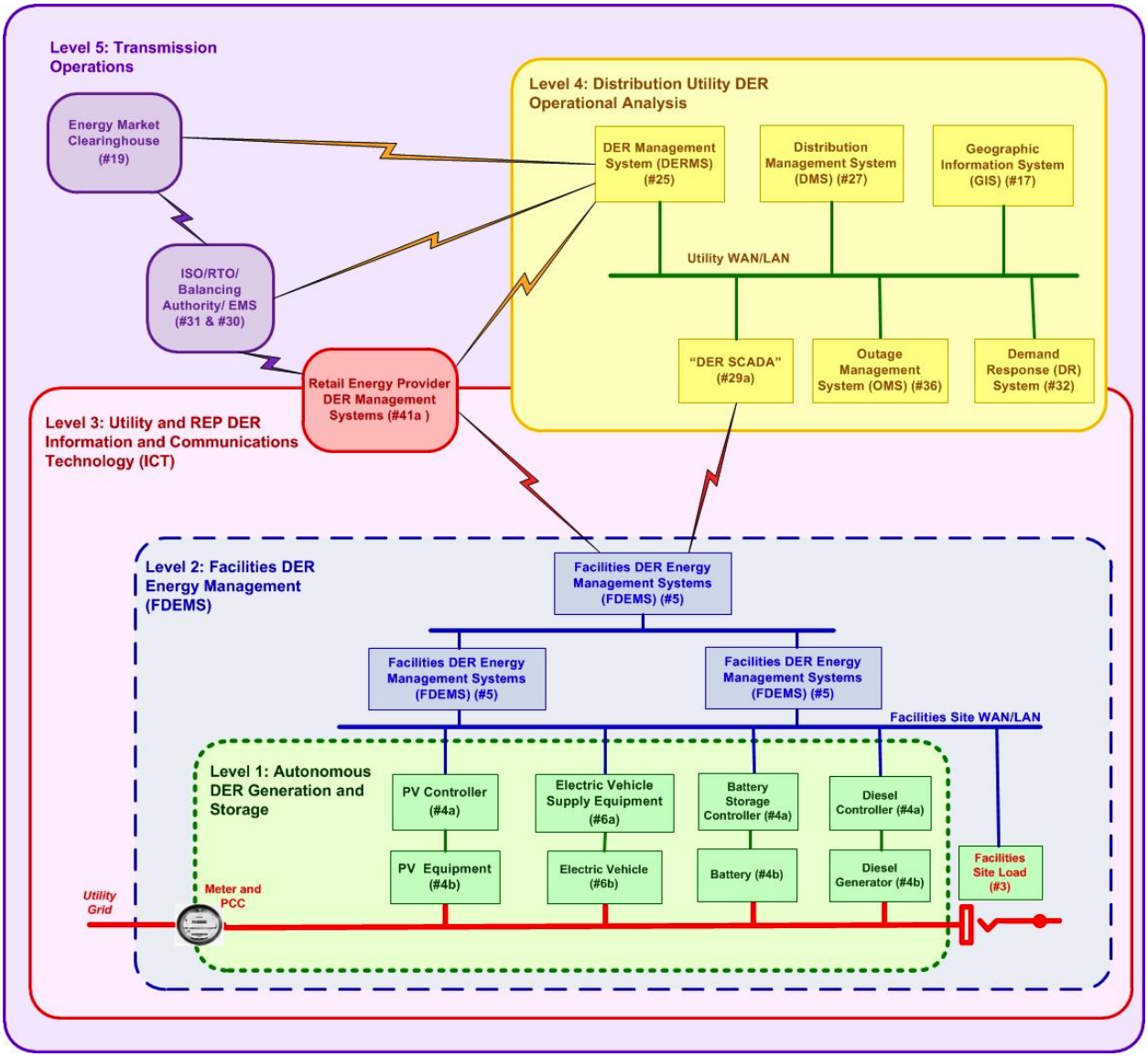

Figure 2-2: Logical Hierarchical DER System Architecture

- **Level 1 Autonomous DER Generation and Storage** (green in the Figure) is the lowest level and includes the cyber-physical DER systems. These DER systems will be interconnected to the utility grid and will usually operate autonomously according to pre-established settings. 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.
- **Level 2 Facilities DER Energy 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 the DER

systems in a residential home, but more likely will be managing DER systems in commercial and industrial sites, such as university campuses, shopping malls, virtual power plants, and industrial combined heat and power (CHP) installations. Utilities may also use a FDEMS to handle DER systems located at utility sites such as substations or physical power plant sites. The settings for autonomous DER operations are modifiable by FDEMS operator preferences in coordination with utilities and REPs.

- **Level 3 Utility and REP Operational Communications** (red in the Figure) extends beyond the local site to allow utilities and possibly REPs to request or require DER systems (typically through a FDEMS) to take specific actions. The settings for autonomous DER operations are modifiable by utilities and REPs. Controls include turning on or off devices, setting or limiting output, providing ancillary services (e.g. volt-var control), and other grid management functions. These requests can be automated and price-based for greater power system efficiency while commands are more likely to be safety or power system reliability related. The combination of this level and level 2 may have varying scenarios, while still fundamentally providing the same services.
- **Level 4 Distribution Utility Operational Analysis** (yellow in the Figure) applies to utility applications that are needed to determine which requests or commands should be issued to specific DER systems. Utilities monitor the power system and assess if efficiency, reliability, or market advantage can be improved by having DER systems modify their operation. This utility assessment involves many utility control center systems, including GIS, DMS, OMS, DR systems, as well as the DERMS. Once the utility has determined that modified requests or commands should be issued, they will be sent as per Level 3.
- **Level 5 Transmission and Market Operations** (purple in the Figure) is the highest level, and involves the larger utility environment. RTOs or ISOs may need to exchange information about the capabilities and operational status of larger DER systems and/or aggregated DER systems.

The description for each level includes the following:

- Description of the components (actors) and the interactions that take place between them.
- The possible vulnerabilities that may be exploited in a cyber security event. This includes both deliberate attacks and inadvertent mistakes.
- Recommended cyber security requirements.

2.1.2 Hierarchical DER Architecture Mapped to NISTIR 7628 Logical Interfaces

The DER actors and logical interfaces can be directly mapped to the NISTIR 7628, as shown in Figure 2-3 below.

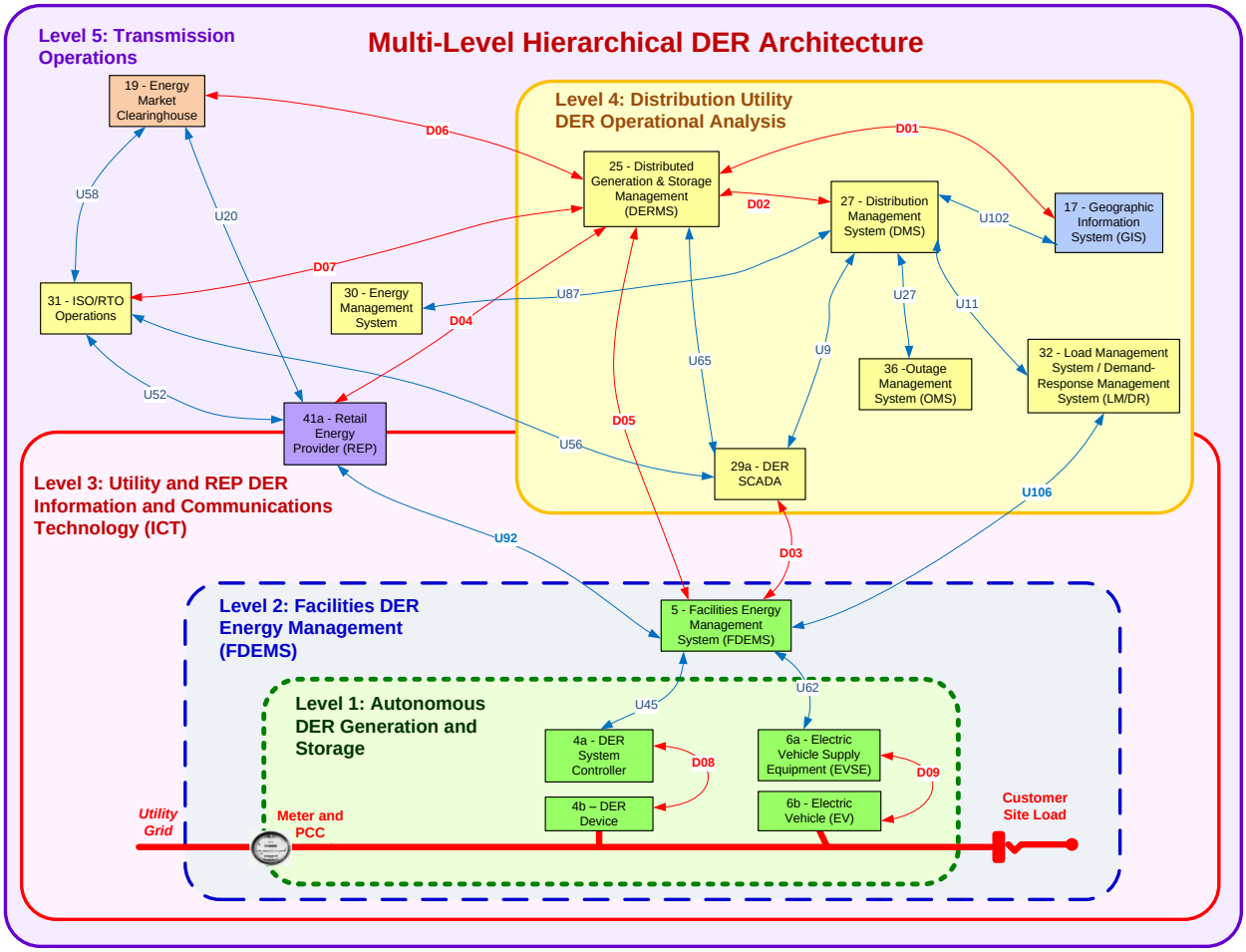

Figure 2-3: Hierarchical DER Architecture Mapped to the NISTIR 7628

3 LEVEL 1: AUTONOMOUS DER CYBER-PHYSICAL SYSTEMS

As seen in Figure 3-1 below, at Level 1, DER generation and storage systems operate autonomously as cyber-physical systems. Each DER system can be viewed as composed of two classes of components: physical hardware/firmware components and cyber controller components that manage the physical components. These components are typically installed at a customer site behind the meter or in some cases within a utility substation. The DER equipment is connected to the Local Electric Power System (EPS) (shown as solid red lines in the diagram) as are customer loads if they exist. This Local EPS is connected to the utility's area EPS through a circuit breaker and meter at the Point of Common Coupling (PCC)[2].

The NISTIR 7628 logical interface D08 supports interactions between DER system controllers and their DER devices, while logical interface D09 supports battery charging/discharging (V2G) interactions between the Electric Vehicle Supply Equipment (EVSE) and the electric vehicle.

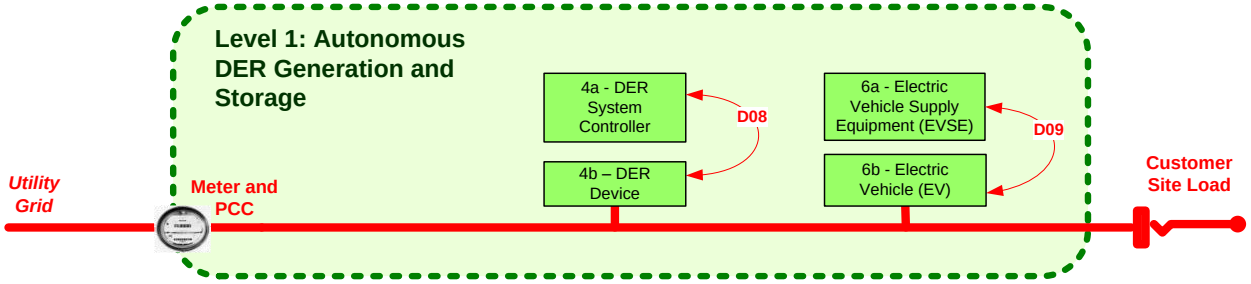

Figure 3-1: Level 1: Autonomous DER systems at smaller customer and utility sites

Most DER systems are supplied as complete units. The controllers are usually located within a short distance of the physical DER devices, with any communications between them limited, point-to-point, and generally using proprietary communication protocols provided by the DER manufacturer. In the diagram, these communication channels are shown as curved red arrows. For example, the controller for a photovoltaic system (PV) or wind turbine may be located at ground level, while the PV panels are located on the roof of the building and the wind blades are high up on a pole. The EVSE charger may be located in a garage or charging station parking spot, only a few feet from the electric vehicle, while the controller for a diesel generator may be directly connected to the physical unit.

Some DER systems include a simple Human-Machine Interface (HMI) (or a port for a laptop HMI). This HMI provides status information and may be used during maintenance.

The only external communications between the utility and these DER systems are the meter readings, typically measured at the PCC between the local EPS and the area EPS.

[2] IEEE 1547:2003 *IEEE Standard for Interconnecting Distributed Resources with Electric Power Systems*

3.1 Level 1 DER Systems: Description

Customers (residential, commercial, or industrial), third parties, or utilities may own DER systems. The owners may directly manage them, or management may be outsourced to REPs or other “virtual power plant (VPP)” companies. Some DER systems may be renting space on customer premises, but owned by other companies.

These individual DER systems operate autonomously most of the time, with the cyber controllers closely monitoring the physical devices and responding to the local electrical conditions by controlling the physical DER systems according to pre-specified settings. The controllers can also respond to customer preferences and to HMI commands to change these settings, or to react to emergency situations. Therefore, the HMI is the local access for viewing the status and measurements of the DER system and for changing the settings of the autonomous actions of the DER system.

3.2 NISTIR 7628 LIC Security Requirements

The NISTIR 7628 identifies logical interfaces between actors, assigns those logical interfaces to one of 22 LICs, and then allocates the high level security requirements to each of those LICs (NISTIR 7628 Vol. 1, Chapter 3). These security requirements are organized into three groups:

- Common Governance, Risk, and Compliance (GRC)
- Common Technical Requirements
- Unique Technical Requirements

The GRC security requirements apply to most of the interfaces since they cover policies and procedures. The common technical requirements address confidentiality, integrity, and availability common to all LICs while the unique technical requirements address specific LICs.

3.3 Level 1 DER Systems: Cyber Security Requirements

3.3.1 Level 1 DER Systems: Potential Cyber Security Vulnerabilities

Level 1 autonomous DER systems do not include wide area communications and the applicable logical interfaces in Figure 3-1 are D08 and D09. Logical interface D08 is the interface between the DER controllers and the physical devices. Logical interface D09 is the interface between the EVSE or charger and the EV. In both cases, these interfaces are used by the controllers to manage the physical devices, including activating protective relaying if the grid experiences extreme voltage or frequency anomalies.

In most Level 1 configurations, the DER systems are not in physically protected environments, and rarely are in locations that are under a utility’s jurisdiction. These autonomous DER systems are therefore vulnerable to local cyber security attacks either through the HMI link to the controller, via the maintenance port, or via direct access to the communications between the controller and the firmware in the physical equipment.

3.3.2 Categorization of Logical Interfaces D08 and D09

The DER controllers to manage the physical DER units and, in emergencies, shut them down for protection use logical interfaces D08 and D09. These logical interfaces do not yet exist in the NISTIR 7628, but they are closest to U108 in functionality and characteristics. U108 is between Distributed Intelligence Capabilities and Distribution RTU or IED. This is similar to the interactions between an intelligent DER controller and a physical DER device, but there are also some differences. U108 belongs to the distribution domain, where the intelligent equipment includes voltage regulators, capacitor bank switches, fault indicators, automated switches, and other distribution line equipment. This intelligent distribution equipment does not explicitly cover generation or storage.

The most relevant description from LIC 3 is: "*Between IEDs (peer-to-peer) for power system protection, including transfer trip signals between equipment in different substations*."

For this reason, D08 and D09 are assigned to LIC 4 for smaller DER systems (the majority) but could also be included in LIC 3 for larger or more critical DER systems.

3.4 Security Requirements for LICs 3 and 4

Residential systems may not require some of the security requirements listed below. As previously stated, these are recommended security requirements. Each utility will need to define their DER systems, perform a risk assessment, and then select and tailor the applicable security requirements.

3.4.1 Unique Technical Security Requirements for LICs 3 and 4

The unique technical security requirements associated with LICs 3 and 4 are shown in Table 3-1: . Two additional unique technical security requirements that are not included in LICs 3 and 4 have been added since they are relevant to DER systems. These additional security requirements are underlined in the table below. Tailoring to autonomous DER systems and the controller-equipment interface are shown in the second column.

Table 3-1: Unique Technical Security Requirements for LICs 3 and 4

NISTIR 7628 Unique Technical Security Requirements	Tailoring for DER Systems
SG.AC-14 Permitted Actions without Identification or Authentication	There should be no permitted actions without identification or authentication.
SG.AU-16 Non-repudiation	All user modifications to security audit logs and security parameters should be associated with a specific identity.

NISTIR 7628 Unique Technical Security Requirements	Tailoring for DER Systems
SG.IA-4 User Identification and Authentication	All user access to the DER system should require identification and authentication. Users include DER manufacturer, vendor/installer, owner, manager, and maintenance personnel. Users should be individually identified and authenticated with access permissions established by their roles.
SG.IA-5 Device Identification and Authentication	Devices should be individually identified and authenticated with access permissions established by their roles. Devices include DER firmware equipment, DER controller, HMI, portable/mobile device connected through a maintenance port.
SG.IA-6 Authenticator Feedback	The authentication mechanism for interactions between a user and the DER controller should obscure passwords and other authentication information.
SG.SC-3 Security Function Isolation	Security functions should be isolated from non-security functions.
SG.SC-7 Boundary Protection	Communication access to DER controllers should be protected, to deter unauthorized connections by external devices.
SG.SC-8 Communication Integrity	Data exchanged between the controller and the device should be protected to detect modifications. These data exchanges are typically point-to-point, multi-drop, and/or local networks.
SG.SC-9 Communication Confidentiality	Most DER information in the controller or provided to the controller through the HMI is not confidential. The exceptions are any security-relevant information (e.g. passwords) and any tariff or pricing information that should be protected for confidentiality when communicated.
SG.SC-26 Confidentiality of Information at Rest	DER passwords and other sensitive and security-relevant information is encrypted and protected against unauthorized access.
SG.SI-7 Software and Information Integrity	The DER software should monitor all modifications to data and applications for tampering.

3.4.2 Common Technical Security Requirements for Autonomous DER Systems (LICs 3 and 4)

For DER systems that are located in insecure environments and have potentially significant impact on the power system, additional technical security requirements are necessary. These include the common technical security requirements identified in Table 3-2 below.

Table 3-2: Common Technical Security Requirements for Autonomous DER Systems

NISTIR 7628 Common Technical Security Requirements	Tailoring for DER Systems
SG.AC-7 Least Privilege	Only the necessary rights and privileges are assigned to each role.
SG.AC-8 Unsuccessful Login Attempts	Since DER systems are generally located in unsecured locations, unsuccessful login attempts should be logged and appropriate users notified.

NISTIR 7628 Common Technical Security Requirements	Tailoring for DER Systems
Session Time-Out[3]	Since DER systems are generally located in unsecured locations where personnel are not experts in cyber security, logins should time out if there is no user activity.
SG.AC-17 Access Control for Portable and Mobile Devices	Access to DER systems via portable or mobile devices should be restricted to authorized personnel.
SG.AU-2 Auditable Events	The DER system should log all compromised data and significant cyber security events, including those that may indicate a cyber security attack. These event logs will permit cyber security assessments to determine if an attack is occurring and the nature of the attacks.
SG.AU-3 Contents of Audit Records	The DER system should include a time stamp, the type of security event, a description of the event, the context of the event, and the status of the system when the event took place.
SG.SA-10 Developer Security Testing	The DER manufacturer and/or system vendor should perform tests for ensuring the security technologies are properly implemented and the security procedures are functional and well defined. The manufacturers of DER systems should use penetration testing to assess for vulnerabilities. The vendor/manufacturer should verify the security and functionality of patches, assess them for malware, and test them on redundant or backup systems first (if possible). The vendor/manufacturer should develop procedures to rollback or de-install the patches.
SG.SC-11 Cryptographic Key Establishment and Management	The DER system operator should establish and manage cryptographic keys.
SG.SC-12 Use of Validated Cryptography	Communication protocols used internally between the DER controller and any separate HMI or portable/mobile maintenance device should: – Use validated cryptography, – Do not use deprecated cryptographic suites in new systems beyond their expiration dates, and – Provide migration paths for older systems using deprecated cryptographic suites. These cryptographic methods should meet national or international standards, such as ISO/IEC 19790:2012, Information technology -- Security techniques -- Security requirements for cryptographic modules.
SG.SC-15 Public Key Infrastructure Certificates	Key management process should ensure that the DER system has valid cyber security certificates before communications are established to any separate HMI or portable/mobile maintenance device.
SG.SC-19 Security Roles	Only authorized users should be allowed to make modifications to the DER system settings and parameters through role-based access control.

[3] There is no comparable NISTIR 7628 security requirement.

NISTIR 7628 Common Technical Security Requirements	Tailoring for DER Systems
SG.SC-20 Message Authenticity	Communication protocols used between DER system components should be required to authenticate all messages, including their source and destination.
SG.SC-22 Fail in Known State	For defined safety and security failures, the DER system should enter a well-defined failure state that may include changing functionality, limiting functionality, restarting, or shutting down. Failure in a known secure state helps prevent a loss of confidentiality, integrity, or availability in the event of a failure of the DER system or a component of the DER system.

3.4.3 Governance, Risk and Compliance (GRC) for D08 Logical Interface

Although GRC security requirements are shown as applicable to all LICs, some are more important to DER systems. These are listed below in Table 3-3.

Table 3-3: Governance, Risk, and Compliance (GRC) Security Requirements for Autonomous DER systems

NISTIR 7628 GRC Security Requirements	Tailoring for DER Systems
SG.AC-4 Access Enforcement	The DER system, as manufactured and installed, should enforce access control for different users and user roles. This is important since many DER systems are located at customer sites where the personnel may not be security experienced.
SG.AT-2 Security Awareness	The DER system should include training for DER owners and/or DER operators on security requirements. This is to reinforce the requirement that security settings are implemented and not bypassed.
SG.AU-5 Response to Audit Processing Failures	The DER system should notify the appropriate user of any failure of the security auditing process.
SG.AU-8 Time Stamps	DER systems should synchronize their time clocks to achieve adequate precision and accuracy to detect any compromise of the timestamps of audit logs. This ensures that a series of events are logged chronologically with the necessary time resolution.
SG.AU-9 Protection of Audit Information	The DER system should detect and log unauthorized modifications to audit logs.
SG.CM-5 Access Restrictions for Configuration Change	Security roles should be restricted in the security settings they may modify or update in the DER system.
SG.CM-10 Factory Default Settings Management	The vendor/installer should have security of the DER system enabled “out of the box,” allowing modifications only by authenticated users. Users should be prevented from using factory-set default access passwords after installation.
SG.IR-7 Incident Reporting	Appropriate entities (people or systems) should be notified if the incident is a cyber attack.
SG.MA-5 Maintenance Personnel	Only authorized maintenance personnel (as specified by the utility and/or DER owner) should permit maintenance.

NISTIR 7628 GRC Security Requirements	Tailoring for DER Systems
SG.SA-9 Developer Configuration Management	The vendor/installer should affirm that they are supplying equipment from manufacturers who provide security-enabled equipment as required by the utility, REP, and/or DER owner.
SG.SI-2 Flaw Remediation	Cyber security patches to DER system software should be applied using strong patch management procedures.
SG.SI-6 Security Functionality Verification	Start-up, restart, and anomalous events should cause the DER system to perform a self-test of the security functionality.

4 LEVEL 2 FACILITIES DER ENERGY MANAGEMENT SYSTEMS (FDEMS)

4.1 Level 2 FDEMS: Customer Management of DER Systems: Description

At Level 2, one or more **Facilities (DER) Energy Management Systems (#5)** (FDEMS) manage multiple DER systems, including combinations of DER generation, DER storage, microgrids, and facility loads. The FDEMS manages a group of DER systems locally, usually within a customer site, substation, or small region such as a subdivision or community.

Multiple FDEMS systems may be involved, with some operating in parallel, while others coordinate multiple smaller FDEMS. For instance, a university campus may include a "building" FDEMS for each campus building that has DER systems, and have one "campus" FDEMS that coordinates the many "building" FDEMS to ensure optimal energy management of the entire campus. A community FDEMS may coordinate the residential FDEMS within a subdivision.

Figure 4-1 illustrates the Level 2 FDEMS management of multiple DER systems. Logical interface U45 supports interactions between the FDEMS and most DER system controllers, and logical interface U62 supports interactions between the FDEMS and the EVSE that manages the charging of electric vehicles.

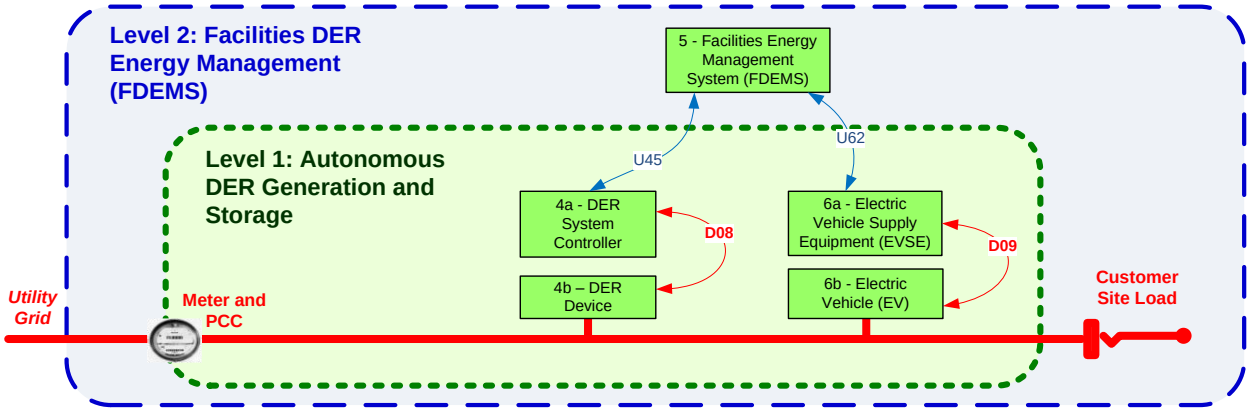

Figure 4-1: Level 2 FDEMS: Facilities DER Energy management systems

The FDEMS may create islanded microgrids if grid power is lost. A campus FDEMS could establish the generation requirements that are needed to meet the load requirement, then take specific actions such as shutting down some loads, starting up additional DER systems such as diesel generators, and issuing the appropriate settings to each DER system so that it will operate in a coordinated manner within this microgrid.

A residential FDEMS manages the equipment connected to a HAN, including PV systems and electric vehicle chargers. Commercial and industrial FDEMS, such as those on university campuses, hospitals, shopping malls, and industrial plants, may allocate DER requirements across multiple DER systems as well as using load management to manage the overall customer energy profile.

A power plant also contains a plant FDEMS to manage the DER systems within the plant. A VPP may contain multiple FDEMSs that manage the DER systems (and often loads) at each location.

Cyber security events (both malicious and non-malicious) on smaller FDEMS systems typically would not significantly affect utility power system operations but could affect public and field crew safety, DER owner financial status, DER vendor finances and reputation, and to a limited degree, utility reputation. Cyber security attacks on larger FDEMS systems could impact utility operations by causing power system instability and potential outages.

4.2 Level 2 FDEMS: Cyber Security Requirements

4.2.1 Level 2 FDEMS: Potential Cyber Security Vulnerabilities

FDEMS are located in facility sites with potentially unknown security policies and security implementations. The FDEMS are typically general-purpose systems whose operating systems, communication networks, and software applications have well-known vulnerabilities. In addition, most FDEMS will connect to external systems, possibly utility systems or market-based ESPs. These connections may be over dedicated networks, general facility networks, public telecommunication systems (e.g. cellular systems), or even the Internet. In any of these network architectures, these connections will transverse the facility site perimeter. Therefore, firewalls should be installed that restrict access to the FDEMS only to authorized users and systems. This makes FDEMS potentially vulnerable to different types of cyber security events.

4.2.2 Level 2 FDEMS: Categorization of Logical Interfaces

The FDEMS interconnects to the DER systems included at Level 1 in Figure 6. The logical interface categories related to these interconnections are:

- FDEMS to DER Systems: U45 is mapped to LIC 15, interface between systems that use customer (residential, commercial, and industrial) site networks that include:
  - Between Customer EMS and Customer Appliances
  - Between Customer EMS and Customer DER
  - Between Energy Service Interface and PEV (EVSE)
- FDEMS to EVSE: U62 is mapped to LIC 15, interface between systems that use customer (residential, commercial, and industrial) site networks which include:

- Between Customer EMS and Customer Appliances
- Between Customer EMS and Customer DER
- Between Energy Service Interface and PEV (EVSE)

4.3 Security Requirements for LIC 15

4.3.1 Unique Technical Security Requirements for LIC 15

The unique technical security requirements associated with U45 and U62 logical interfaces that interconnect the FDEMS to the DER systems in LIC 15 are shown in Table 4-1 below. Some additional unique technical security requirements that are not included in LIC 15 have been added since they are relevant to DER systems. These additional requirements are underlined. Comments on their tailoring to FDEMS-DER system interactions are shown in the second column.

Table 4-1: Unique Technical Security Requirements for LIC 15

NISTIR 7628 Unique Technical Security Requirements	Tailoring for FDEMS Interactions
SG.AC-14 Permitted Actions without Identification or Authentication	There should be no permitted actions without identification or authentication
SG.AU-16 Non-repudiation	All user modifications to FDEMS, security audit logs, and security parameters should be associated with a specific identity.
SG.IA-4 User Identification and Authentication	All user access to the FDEMS system should require authentication. Users include FDEMS manufacturer, vendor/installer, owner, manager, and maintenance personnel. Users should be individually identified and authenticated with access permissions established by their roles.
SG.IA-5 Device Identification and Authentication	Devices and components that should be identified and authenticated in a FDEMS include FDEMS hardware and firmware, FDEMS software applications, HMI, portable/mobile devices connected through a maintenance port.
SG.IA-6 Authenticator Feedback	The authentication mechanism for interactions between a user and the FDEMS should obscure passwords and other authentication information.
SG.SC-3 Security Function Isolation	Security functions in the FDEMS should be isolated from non-security functions.
SG.SC-7 Boundary Protection	Communication access to FDEMS should be protected to permit only authorized connections with DER systems and other customer devices and systems.
SG.SC-8 Communication Integrity	Data exchanged between the FDEMS and DER systems should be protected to detect modifications. These data exchanges are typically point-to-point, multi-drop, and/or local networks.

NISTIR 7628 Unique Technical Security Requirements	Tailoring for FDEMS Interactions
SG.SC-9 Communication Confidentiality	Some DER information in the FDEMS is security-relevant or sensitive. Sensitive information may include intellectual property or financial data such as tariff or pricing information. This information should be protected when communicated.
SG.SC-26 Confidentiality of Information at Rest	The FDEMS passwords and other sensitive and security-relevant information should be encrypted and protected against unauthorized disclosure.
SG.SI-7 Software and Information Integrity	The FDEMS software should monitor all modifications to data and applications for tampering.

4.3.2 Common Technical Security Requirements for FDEMS

For FDEMS systems that are located in insecure environments and have significant impact on the power system, additional technical security requirements are necessary. These include the common technical security requirements identified in Table 4-2.

Table 4-2: Common Technical Security Requirements for FDEMS

NISTIR 7628 Common Technical Security Requirements	Tailoring for FDEMS Systems
SG.AC-7 Least Privilege	Only the necessary rights and privileges should be assigned to each role that will have access to the FDEMS.
Session Time-Out[4]	Since FDEMS are generally located in unsecured locations where personnel are not experts in cyber security, logins should time out if there is no user activity.
SG.AC-17 Access Control for Portable and Mobile Devices	Access to FDEMS via portable or mobile devices should be restricted to authorized personnel.
SG.AU-2 Auditable Events	The FDEMS should log all significant cyber security events, including compromised data that may indicate a cyber security event. These event logs permit cyber security assessments to determine if an attack is occurring and the nature of the attack. Since DER systems are generally located in unsecured locations, unsuccessful login attempts into the FDEMS should be logged.
SG.AU-3 Contents of Audit Records	The FDEMS should include an accurate time stamp, the type of security event, a description of the event, the context of the event, and the status of the system when the event took place.

[4] There is no comparable NISTIR 7628 security requirement.

NISTIR 7628 Common Technical Security Requirements	Tailoring for FDEMS Systems
SG.SA-10 Developer Security Testing	The FDEMS manufacturer and/or system integrator should develop tests for ensuring the security technologies are properly implemented and the security procedures are functional and well defined. The manufacturers of FDEMS should use penetration testing to assess their systems for vulnerabilities. The vendor/manufacturer should verify the security and functionality of patches, should assess for malware, and should test on redundant or backup systems first (if possible), The vendor/manufacturer should develop procedures to rollback or de-install the patches.
SG.SC-11 Cryptographic Key Establishment and Management	The FDEMS system operator should establish and manage cryptographic keys.
SG.SC-12 Use of Validated Cryptography	Communication protocols used internally between the FDEMS and the DER systems should: – Use validated cryptography, – Do not use deprecated cryptographic suites in new systems beyond their expiration dates, and – Provide migration paths for older systems using deprecated cryptographic suites. These cryptographic methods should meet national or international standards, such as ISO/IEC 19790:2012, Information technology -- Security techniques -- Security requirements for cryptographic modules.
SG.SC-15 Public Key Infrastructure Certificates	Key management process should ensure that the FDEMS has valid cyber security certificates before communications are established to any separate HMI or portable/mobile maintenance device.
SG.SC-19 Security Roles	The FDEMS should be designed to enforce role-based permissions and prevent unauthorized access. Only authorized users should be allowed to make modifications to the FDEMS settings and parameters through role-based access control. Devices and other systems connected to a FDEMS should be individually identified and authenticated with access permissions established by their roles. Different FDEMS applications should have their own IDs and authorized roles. Non-DER devices and systems should not have access to DER systems without role-based access authorization. Vendors who maintain access to FDEMS should maintain role-based access control on any open port.
SG.SC-20 Message Authenticity	Communication protocols used between the FDEMS and the DER systems should be required to authenticate all messages, including their source and destination.

NISTIR 7628 Common Technical Security Requirements	Tailoring for FDEMS Systems
SG.SC-22 Fail in Known State	For all safety and security failures, the FDEMS should enter a well-defined failure state that may include changing functionality, limiting functionality, restarting, or shutting down. Failure in a known secure state helps prevent a loss of confidentiality, integrity, or availability in the event of a failure of the FDEMS or a component of the FDEMS.

4.3.3 Governance, Risk and Compliance (GRC) for LIC 15

Although GRC security requirements are shown as applicable to all LICs, some are more important to FDEMS. These are listed below in Table 4-3.

Table 4-3: Governance, Risk, and Compliance (GRC) Security Requirements for FDEMS

NISTIR 7628 GRC Security Requirements	Tailoring for DER Systems
SG.AC-4 Access Enforcement	The FDEMS, as manufactured and installed, should enforce access permissions that are assigned to different users and user roles. This is important since many FDEMS are located at customer sites where the personnel may not be security experienced.
SG.AT-2 Security Awareness	The FDEMS should include training for DER owners and DER operators on security requirements. This is to reinforce the requirement that security settings are implemented and not bypassed.
SG.AU-5 Response to Audit Processing Failures	The FDEMS should notify the appropriate user of any failure of the security auditing process.
SG.AU-6 Audit Monitoring, Analysis, and Reporting	Since DER systems are generally located in unsecured locations, appropriate users should be notified of unsuccessful login attempts into the FDEMS and compromised data.
SG.AU-8 Time Stamps	The FDEMS should synchronize its time clock to achieve adequate precision and accuracy to detect any compromise of the timestamps of security audit logs. This ensures that a series of events are logged chronologically with the necessary time resolution.
SG.AU-9 Protection of Audit Information	The FDEMS should detect and log any unauthorized modifications to audit logs.
SG.CM-5 Access Restrictions for Configuration Change	The FDEMS security roles should be restricted in what security settings they may modify or update.
SG.CM-10 Factory Default Settings Management	The vendor/installer should have security of the FDEMS system enabled “out of the box,” allowing modifications only by authorized users. The FDEMS should prevent the use of factory set default access passwords after installation.

NISTIR 7628 GRC Security Requirements	Tailoring for DER Systems
SG.CP-11 Fail-Safe Response	If communications with one or more DER systems are lost for longer than a set time period, the FDEMS should assume that those DER systems have entered the pre-established operational modes for such a loss of communications.
SG.MA-5 Maintenance Personnel	Maintenance should be permitted only by authorized maintenance personnel (as specified by the utility, FDEMS, and/or DER owner).
SG.RA-4 Risk Assessment	The FDEMS owner should perform a security risk assessment to determine the impact of unauthorized disclosure (confidentiality and privacy), unauthorized modification (integrity) of data in the FDEMS, and inadequate availability when transmitted between the FDEMS and the DER systems.
SG.SA-9 Developer Configuration Management	The vendor/installer should affirm that they are supplying equipment from manufacturers who provide security-enabled equipment as required by the utility, REP, and/or DER owner.
SG.SI-2 Flaw Remediation	Cyber security patches to FDEMS software should be applied using strong patch management procedures.
SG.SI-6 Security Functionality Verification	Start-up, restart, and anomalous events should cause the FDEMS to perform a self-test of the security functionality.

5 LEVEL 3: UTILITY AND REP DER INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT)

5.1 Level 3 DER ICT: Utility and REP Interactions with FDEMS: Description

At Level 3, utilities and/or REPs use ICT to coordinate and manage DER systems from a more global perspective, based on the real-time requirements of the distribution and transmission systems, as well as the demand response pricing signals from market systems.

These DER monitoring and control communications are represented by logical interfaces between utilities/REPs and the FDEMS at facility sites and are shown in Figure 5-1 below.

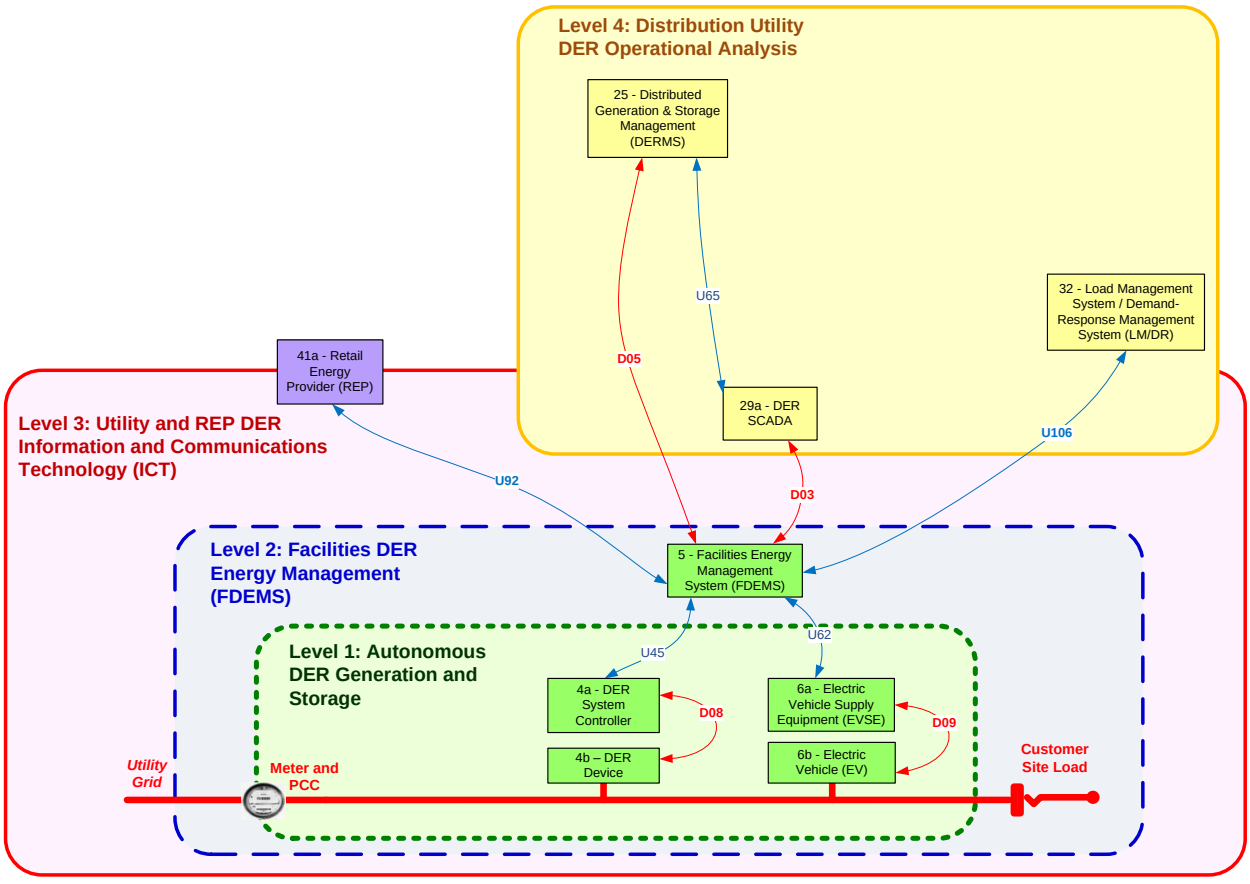

Figure 5-1: Level 3: Utility/REP ICT for Monitoring and Control of FDEMS and DER systems

Since direct real-time communications with thousands of small DER systems is usually not practical, utilities and REPs will typically rely on non-real-time interactions with FDEMS for establishing the settings for autonomous DER actions. Only in some emergency situations will the utility issue control commands such as “shut down

immediately," typically as broadcast or multi-cast commands to groups of FDEMS systems and DER systems.

Information exchanges include interactions between the FDEMS and the utility/REPs, although the types of information exchanged may be different. For instance, communications between the utility's DER SCADA (#29a) and the FDEMS (#5) may include real-time monitoring and emergency control commands, while those with REPs (#41a) and the utility's LM/DR system (#32) are likely to be market-related information. The interactions between the utilities' DERMS systems (#25) and the FDEMS would likely be related to power settings and schedules for future autonomous activities by DER systems.

5.2 Level 3 Utility and REP ICT: Cyber Security Requirements

5.2.1 Level 3 Utility and REP ICT: Potential Cyber Security Vulnerabilities

Level 3 utility and REP ICT involve interactions over wide area networks between different organizations. Most of these interactions are operational, involving the monitoring and control of power system equipment. Control commands from utilities to FDEMS systems are particularly sensitive to cyber security events (including attacks) since these events could cause injury to personnel, damage to equipment, and unstable power system conditions. Cyber security attacks on financially based control commands could cause financial losses as well as legal and regulatory actions.

Utilities typically do not own or manage FDEMS; therefore, there are differences in the cyber security approach to handle these utility-FDEMS interactions, due to:

- *Different ownership*: In general, utilities do not own the FDEMS equipment that they must interact with (the exception is when the FDEMS belongs to the utility and manages a utility-owned DER system in a substation).
- *Unknown trust level*: When utilities monitor and control their own equipment, they manage the cyber security of that equipment and can ensure that adequate protections are in place. Since FDEMS are not owned by utilities, utilities cannot trust the cyber security protections to the same degree as they trust the security protections of their own systems.
- *Different security domains*: Since FDEMS are located in customer facilities, information exchanges between utility systems and FDEMS cross security perimeters. These security perimeters must be protected against unauthorized access and other cyber security attacks.
- *Public communication networks*: Some information exchanges may rely on public telecommunication providers, such as leased communication circuits, General Packet Radio Service (GPRS) cellular systems or the Internet, providing additional attack vectors.

There are two additional factors applicable to FDEMS and utilities.

- *Lack of standards*: The distribution utilities must exchange information between their critical DER applications and large numbers of untrusted FDEMS. Because standards do not yet exist, flexibility in these interfaces must be allowed to permit the many different approaches being used by FDEMS and DER system vendors. Most of these different approaches do not include cyber security.
- *Immature security in communication networks*: Since communication networks for utilities to interact with FDEMS are new, the security approaches are typically immature.

5.2.2 Level 3 Utility and REP ICT: Categorization of Logical Interfaces

An FDEMS interconnects to the utilities and retail energy providers in Level 3. The LICs related to these interconnections are:

- *D03 – between FDEMS and Utility DER SCADA*: This new interface addresses real-time monitoring and control, but does not interact with systems within the same organization. Therefore, D03 should be mapped to LIC 6, Interface between control systems in different organizations, for example:
  - Between an RTO/ISO EMS and a utility energy management system
  - Between a DER SCADA and FDEMS (example added)
- *D06 - between DERMS and FDEMS*: This new interface addresses non-real-time updates to parameters and schedules across different organizations. Therefore D06 should be mapped to LIC 8, Interface between back office systems not under common management authority, for example:
  - Between a third-party billing system and a utility meter data management system
  - Between DERMS and Customer EMS (example added)
- *U106 - between LM/DR and FDEMS*: This interface is currently mapped to LIC 10 but the interface is described in LIC 14. Since the interactions between the LM/DR and the FDEMS is not internal to a utility (and therefore not part of LIC 10) and will most likely not use the AMI system[5] (and therefore not part of LIC 14), U106 should be mapped to LIC 8, which is the interface between back office systems not under common management authority (i.e. not under the same security policy), for example:
  - Between a third-party billing system and a utility meter data management system
  - Between LM/DR and Customer EMS (example moved from LIC 14)

[5] This is still being explored and discussed in the utility industry: may use broadcast media such as the Internet or cell phone system, or may utilize the AMI backbone WAN but then use separate wireless media that does not go through the meter.

- *U92 - between REP and FDEMS*: This interface is mapped to LIC 16, Interface between external systems and the customer site, for example:
  - Between Third Party and HAN Gateway
  - Between ESP and DER
  - Between Customer and CIS Web site
  - Between Retail Energy Provider and FDEMS (example added)

5.3 Security Requirements for LIC 6 and 8: Between Utility and FDEMS

The security requirements for LIC 6 and LIC 8 are similar enough to be combined. These DER LICs include power management interactions between the utility and the FDEMS. The only difference is that under LIC 6, *direct* control commands to power system equipment can be issued, whereas under LIC 8, only *indirect* control commands are issued by changing prices and/or other settings. The results from interactions are quite similar; the DER systems change their output and thus directly affect power operations.

The following subsections identify the security requirements for the interfaces associated with LIC 6 and 8:

- D03: between Utility DER SCADA and FDEMS
- D06: between DERMS and FDEMS
- U106: between LM/DR and FDEMS

5.3.1 Unique Technical Security Requirements for LIC 6 and 8: Between Utility and FDEMS

The unique technical security requirements associated with LIC 6 and LIC 8: interactions between the utility and the FDEMS are shown in Table 5-1. The first column notes where a security requirement was only associated with one or the other LIC. Some additional unique technical security requirements that are not included in LICs 6 and 8 have been added since they are relevant to DER systems. These are underlined in the table below. Comments on their tailoring to Utility-FDEMS interactions are shown in the second column. For convenience, the utility system is referred to as the utility DER SCADA because this system will not only issue its own commands but will probably serve as the gateway between the other utility systems and the FDEMS.

Table 5-1: Unique Technical Security Requirements for LIC 6 and LIC 8

NISTIR 7628 Unique Technical Security Requirements	Tailoring for Interactions Between Utility and FDEMS
SG.AC-13 Remote Session Termination (for LIC 6 only)	Since FDEMS are generally located in unsecured locations where personnel are not experts in cyber security, remote connections should time out if there is no activity, including application-to-application interactions between the utility DER SCADA and the FDEMS.

NISTIR 7628 Unique Technical Security Requirements	Tailoring for Interactions Between Utility and FDEMS
Session Time-Out[6]	FDEMS are generally located in unsecured locations where personnel are not experts in cyber security. Local logins should time out if there is no activity, including application-to-application interactions between the utility DER SCADA and the FDEMS.
SG.AC-14 Permitted Actions without Identification or Authentication	No actions should be permitted without identification and authentication.
SG.AU-16 Non-repudiation *(shown for LIC 8 only, but should also apply to LIC 6)*	All modifications to the messaging and security logs of interactions between the utility DER SCADA and the FDEMS should be associated with a specific user and/or application identity.
SG.IA-4 User Identification and Authentication	Users should be individually identified and authenticated with access permissions established by their roles.
SG.IA-5 Device Identification and Authentication *(shown for LIC 8 only but should also apply to LIC 6)*	All interactions between the FDEMS system and the utility DER SCADA system should require identification and authentication. FDEMS hardware, firmware, and software applications should be identified and authenticated for system security monitoring and control. All FDEMS and their associated DER systems should be registered and authenticated with the utility before any operational interactions are permitted.
SG.IA-6 Authenticator Feedback	The authentication mechanism for interactions between the utility DER SCADA system and the FDEMS should obscure passwords and other authentication information.
SG.SC-3 Security Function Isolation *(shown for LIC 8 only but should also apply to LIC 6)*	Interactions involving the establishment and updating of security should be isolated from non-security interactions, including those between the utility DER SCADA and the FDEMS.
SG.SC-4 Information Remnants	Privacy and confidentiality of FDEMS information are important. Therefore, sensitive data that is not authorized for DER management should not be available on a shared system resource.
SG.SC-5 Denial-of-Service Protection *(shown for LIC 6 only but should also apply to LIC 8)*	Communication paths between the utility DER SCADA and the FDEMS may be redundant for increased protection against DoS attacks, particularly if different media can be used. IDS and/or NSM capabilities should monitor these communication paths, identify unusually high traffic or low throughput levels, and initiate failover to the redundant path if necessary.

[6] There is no comparable NISTIR 7628 security requirement.

NISTIR 7628 Unique Technical Security Requirements	Tailoring for Interactions Between Utility and FDEMS
SG.SC-7 Boundary Protection	A security boundary should be established between the utility DER SCADA and the FDEMS. This security boundary should be protected to permit only authorized interactions. Examples include firewalls, limiting open ports, limiting functions that interact across the boundary, use of utility-managed networks, use of VPNs, and IDS and NSM capabilities to monitor for anomalous behavior. If the FDEMS is interfaced to the Internet, additional boundary protections should be required between functions that use the Internet and those that interface with the utility DER SCADA.
SG.SC-8 Communication Integrity	Data exchanged between the utility DER SCADA and the FDEMS should be protected to detect unauthorized modifications. Integrity checking may be done at all communication "nodes," particularly those in the "last mile" between a backhaul communication network and the FDEMS.
SG.SC-9 Communication Confidentiality *(not shown for either LIC, but relevant for both)*	All communications between the utility DER SCADA and the FDEMS that include sensitive or security-relevant data should apply security techniques to ensure their confidentiality, particularly since these interactions are across organizational boundaries. Sensitive data would include, for example, private or confidential financial information, intellectual property, and personal data.
SG.SC-26 Confidentiality of Information at Rest *(shown for LIC 8 only but should also apply to LIC 6)*	Password and other sensitive and security-relevant information should be encrypted and protected against unauthorized disclosure.
SG.SI-7 Software and Information Integrity	The Utility DER SCADA and the FDEMS software should monitor all modifications to data and applications for tampering.

5.3.2 Common Technical Security Requirements for LIC 6 and 8 between Utility and FDEMS

The interface between the protected utility control systems and the FDEMS systems with unknown levels of protection must be secure. FDEMS are located in environments that the utility has little control over, and yet the DER systems that they manage could have significant impacts on the power system. Therefore, technical security requirements are necessary. These include the common technical security requirements identified in Table 5-2. Some additional common technical security requirements that are not included in LICs 6 and 8 have been added since they are relevant to DER systems. These additional security requirements are underlined in the table below.

Table 5-2: Common Technical Security Requirements for LIC 6 and 8

NISTIR 7628 Common Technical Security Requirements	Tailoring for Interactions Between Utility and FDEMS
SG.AC-7 Least Privilege	For both the utility DER SCADA and the FDEMS, only the necessary rights and privileges should be assigned to each role, particularly for those involving access between the systems.

NISTIR 7628 Common Technical Security Requirements	Tailoring for Interactions Between Utility and FDEMS
SG.AC-17 Access Control for Portable and Mobile Devices	Access to the network that connects the utility DER SCADA and the FDEMS via portable or mobile devices should be restricted to authorized personnel.
SG.AU-2 Auditable Events	In addition to the functional logging requirements, the utility DER SCADA and the FDEMS should log all significant cyber security events that may indicate a cyber security attack. This will permit cyber security assessments to determine if an attack is occurring and the nature of the attack, as well as provide forensic data for after-the-fact evaluations and possible legal actions. Any attempts to access audit data by unauthorized users or software applications should be logged and notifications sent to security personnel. All changes and revocations to user and to role permissions should be logged by both the utility DER SCADA and the FDEMS. Appropriate users should be notified of unsuccessful login attempts, particularly if these login attempts utilize the network between the DER SCADA and the FDEMS. All interactions on the network that connects the utility DER SCADA and the FDEMS via portable or mobile devices should be monitored for unauthorized access. This monitoring may be more critical if public or open networks are used. Unsuccessful login attempts into the utility DER SCADA and the FDEMS should be logged.
SG.AU-3 Contents of Audit Records	The audit records of the utility DER SCADA and the FDEMS should include an accurate time stamp, the type of security event, a description of the event, the context of the event, and the status of the system when the event took place.
SG.CM-7 Configuration for Least Functionality	Both the utility DER SCADA and the FDEMS should be configured to provide only essential access. Specifically, unused ports should be closed and only authenticated software functions should be permitted to execute.
SG.SA-10 Developer Security Testing	The network between the utility DER SCADA and the FDEMS should be tested by the vendor and/or system integrator to ensure that the security technologies are properly implemented and the security procedures are functioning properly. The vendor/manufacturer should verify the security and functionality of patches, should assess for malware, and should test on redundant or backup systems first (if possible), The vendor/manufacturer should develop procedures to rollback or de-install the patches.
SG.SA-11 Supply Chain Protection	As per the contract and/or SLA between the utility and the FDEMS owner, the vendor/installer of the FDEMS should perform due diligence to ensure that they are supplying equipment from manufacturers who provide security-enabled equipment as required by the utility, FDEMS, and/or DER owner/operator.

NISTIR 7628 Common Technical Security Requirements	Tailoring for Interactions Between Utility and FDEMS
SG.SC-11 Cryptographic Key Establishment and Management	The utility DER SCADA and the FDEMS operator should establish and manage cryptographic keys. This includes updating and revoking the keys. Separate keys should be used for different functions, such as operational controls versus maintenance activities.
SG.SC-12 Use of Validated Cryptography	Interactions between the utility DER SCADA and the FDEMS should: – Use validated cryptography, – Avoid implementing deprecated cryptographic suites in new systems beyond their expiration dates, and – Provide migration paths for older systems that still use deprecated cryptographic suites. These cryptographic methods should meet national or international standards, such as ISO/IEC 19790:2012, Information technology -- Security techniques -- Security requirements for cryptographic modules.
SG.SC-15 Public Key Infrastructure Certificates	Since key management of the utility DER SCADA and the FDEMS are most likely to be handled separately by their separate organizations, the network and communications protocols used between them should use valid cyber security certificates that are updated as necessary and revoked in a timely manner.
SG.SC-19 Security Roles	The utility and FDEMS should establish standard roles for different types of access to each other's systems. Special security roles should be established that are permitted to make modifications to the security procedures and protection of the information flows between the utility DER SCADA and the FDEMS. These security roles could require two-factor authentication and other stricter security measures. Role-based permissions should be established for different utility interactions, including FDEMS discovery, connection establishment, monitoring operations, DER settings updates, control operations, security monitoring, software updates and patching, and deregistration. Role-based permissions should be established for different FDEMS interactions, including security establishment, security key management, discovery, response to utility monitoring requests, response to utility updates to DER settings, response to utility control commands, management of software updates and patching, and deregistration. The FDEMS should be designed to enforce role-based permissions and prevent unauthorized access. Upon the removal of a FDEMS, all roles and permissions associated with that FDEMS should be revoked.

NISTIR 7628 Common Technical Security Requirements	Tailoring for Interactions Between Utility and FDEMS
SG.SC-20 Message Authenticity	Communication protocols used between the utility DER SCADA and the FDEMS should authenticate all messages, including their source and destination. IDS and NSM capabilities should be used to detect possible integrity violations of the communication protocols, such as invalid message formats and suspicious protocol interaction patterns. This detection should take place on the communications media (layers 1-2), transport (layers 3-4), and application (layers 5-7). Data received at the utility DER SCADA and at the FDEMS should be validated as authorized.
SG.SC-22 Fail in Known State	For safety and security failures, the utility DER SCADA should cause the applications and network associated with the FDEMS to enter a well-defined failure state that may include changing functionality, limiting functionality, shutting down the network connection, resetting the FDEMS, or other default actions. Failure in a known secure state helps prevent a loss of confidentiality, integrity, or availability in the event of a failure of the FDEMS.
SG.SI-8 Information Input Validation	Since much of the information exchanged between the utility DER SCADA and the FDEMS involves either direct commands to DER systems or indirect settings that can affect the operation of the DER systems when they are connected to the power grid, the information being exchanged should be validated for accuracy, completeness, validity and authenticity.
SG.SI-9 Error Handling	Since the utility DER SCADA and the FDEMS are owned and operated by different organizations, error handling should include the ability to notify the other organizations of security compromises without revealing potentially private or confidential information. Error messages should contain only the minimal information necessary and should not contain sensitive or private information.

5.3.3 Governance, Risk and Compliance (GRC) for LIC 6 and 8: Between Utility and FDEMS

Although GRC security requirements are applicable across all LICs, some are more important to the interface between the utility DER SCADA and the FDEMS. Since the LICs 6 and 8 interfaces cross-organizational boundaries, each organization's security policies may be different and administered separately. The utility will have minimal control over the security of the thousands of FDEMS in its territory. However, the utility needs to rely on the FDEMS that provide crucial power system generation and energy storage. The utility and the FDEMS may have limited mutual trust, but must work together in a timely and secure manner. Sharing mutual security issues, such as intrusions, confidentiality breaches, deregistered systems, changes in personnel, and revoked certificates can be an important part of this interaction, so that potential security events and attacks can be mitigated.

The more important GRCs are listed below in Table 5-3.

Table 5-3: Governance, Risk, and Compliance (GRC) Security Requirements for Utility DER SCADA to FDEMS Interactions

NISTIR 7628 GRC Security Requirements	Tailoring for Interactions Between Utility and FDEMS
SG.AC-4 Access Enforcement	The utility should enforce the access permissions that are assigned to different users and user roles involving interactions with the FDEMS.
SG.AC-18 Use of External Information Control Systems	The utility should establish the business justifications, rules, and conditions for FDEMS to access information from the utility systems. Conversely, the FDEMS should be designed to ensure that the terms and conditions are met for utility access to its information. The utility should establish and enforce the security requirements for FDEMS and DER systems to interface with the DER SCADA system. These security requirements could be part of an interconnection agreement, a service level agreement, a customer tariff, or other type of contractual agreement between the parties.
SG.AC-20 Publicly Accessible Content	The utility should ensure that personnel who may be primarily responsible for grid operations are aware of the privacy requirements related to DER information. DER information that is made public should not be private information. Alternatively, the data should be aggregated in such a way that no private information can be derived.
SG.AT-2 Security Awareness	The utility should support the FDEMS owners in security awareness and training.
SG.AU-5 Response to Audit Processing Failures	The FDEMS should notify the utility DER SCADA of any failure of the security auditing process, and vice versa.
SG.AU-6 Audit Monitoring, Analysis, and Reporting	Since the utility and FDEMS do not have a single security management structure, regulators or other law enforcement may be required to ensure the audit reporting addresses all relevant events. Appropriate personnel should be alerted to any unauthorized or anomalous events. Audit information at the utility DER SCADA and the FDEMS should be synchronized, in standardized formats and/or easily converted from one form to another without loss of information. Time synchronization will permit the audit logs to be correlated even though they belong to different organizations. Audit records related to utility/FDEMS interactions should be transmittable to each other. To minimize false positives and unwarranted security notifications, security events should be validated from multiple sources and the IDS/NSM functions should be designed to ensure that normal traffic spikes do not cause security notifications.
SG.AU-8 Time Stamps	The utility DER SCADA and the FDEMS should synchronize their time clocks to achieve adequate precision and accuracy to detect any compromise of the timestamps of audit logs. This ensures that a series of events are logged chronologically with the necessary time resolution.

NISTIR 7628 GRC Security Requirements	Tailoring for Interactions Between Utility and FDEMS
SG.AU-9 Protection of Audit Information	The utility DER SCADA and the FDEMS should detect unauthorized modifications to audit logs, and should notify each other if unauthorized modifications have been made.
SG.AU-10 Audit Record Retention	Since the utility DER SCADA and the FDEMS belong to different organizations, the utility should determine the minimum retention time for audit logs that relate to utility-FDEMS interactions.
SG.CM-3 Configuration Change Control	Since uncoordinated changes can allow threat agents to take advantage of potential vulnerabilities, all configuration changes that affect the interactions between the DER SCADA and the FDEMS should be planned, documented, and implemented in a coordinated manner.
SG.CM-4 Monitoring Configuration Changes	Changes in network configurations should be monitored for potential security impact and alarmed if unexpected and/or unauthorized.
SG.CM-5 Access Restrictions for Configuration Change	Security roles should be restricted in modifying or updating security updates and patches to the utility DER SCADA and the FDEMS systems. All configuration changes that affect each other should be provided to the other organization.
SG.CM-9 Addition, Removal, and Disposal of Equipment	If a FDEMS is removed from operation, the utility should ensure that all sensitive and security-relevant utility information is removed.
SG.CM-10 Factory Default Settings Management	The vendor/installer should have security of the FDEMS system enabled “out of the box”, allowing modifications only by authorized users, since many sites that will implement FDEMS systems will not have adequate security expertise.
SG.CP-8 Alternate Telecommunication Services	FDEMS and their associated DER systems can affect the power grid; particularly if the FDEMS manages many MW of DER. The utility should identify alternate telecommunications capabilities if the primary telecommunications are lost for longer than a pre-specified critical time period.
SG.IA-3 Authenticator Management	The identification and authentication process of FDEMS and their associated DER systems should include validation of FDEMS security credentials.
SG.ID-4 Information Exchange	The utility should include security requirements in the interconnection contracts and Service Level Agreements with the FDEMS owners and/or operators.
SG.IR-5 Incident Handling	The utility DER SCADA and the FDEMS should reject any compromised data.
SG.IR-7 Incident Reporting	Since cyber incidents could affect both the utility and the FDEMS, cyber incident information should be shared between the utility and the FDEMS owners/operators. In particular, any cyber incidents that could affect the resilience of power grid operations should be reported immediately to permit mitigating actions to be taken.
SG.IR-11 Coordination of Emergency Response	Since cyber incidents at either the utility or the FDEMS could affect the safety of the public, the security policies of both the utility and FDEMS owner should include plans and procedures for working together and with law enforcement during emergencies.

NISTIR 7628 GRC Security Requirements	Tailoring for Interactions Between Utility and FDEMS
SG.MA-5 Maintenance Personnel	Maintenance of FDEMS and the interface to the utility DER SCADA should be permitted only by authorized maintenance personnel (as specified by the utility, FDEMS, and/or DER owner).
SG.PM-1 Security Policy and Procedures	The utility should develop the security policies for handling interfaces with FDEMS and DER systems that are not under utility jurisdiction, may have minimal security policies, but need to interface with the utility's operational control systems.
SG.PM-5 Risk Management Strategy	The utility should develop a risk management strategy for interfaces with untrusted FDEMS and DER systems. This risk management strategy should address protecting the utility computer systems.
SG.PS-6 Access Agreements	The REP and the FDEMS should have contractual service level agreements that include security requirements.
SG.RA-4 Risk Assessment	The utility should perform a security risk assessment to determine the impact of unauthorized disclosure (confidentiality) and unauthorized modification (integrity) of data when transmitted between the utility DER SCADA and the FDEMS.
SG.SI-2 Flaw Remediation	Cyber security patches to network interface software, communication protocols, and software applications used by both the DER SCADA and the FDEMS should be applied using strong patch management procedures.
SG.SI-6 Security Functionality Verification	Start-up, restart, and anomalous events should cause the utility DER SCADA and the FDEMS to perform a self-test of the security functionality.

5.4 Security Requirements for LIC 16: Between REP and FDEMS

The security requirements for LIC 16 address the interactions on U92 between a REP and those FDEMS that have agreed contractually to be managed by the REP. The REP only manages a subset of FDEMS and exchanges information with the utility (Level 5) to coordinate this management.

These security requirements are similar to those for LIC 6 and 8, since they involve the interactions between the FDEMS and another organization that is providing information to the FDEMS on the DER actions that could or should be taken. However, the REP does not have direct control over the power grid. The REP is more focused on DER management for financial benefits rather than for power system reliability. This difference in focus changes the scope of the commands that a REP can initiate, and the probable effect of these commands on the power grid.

5.4.1 Unique Technical Security Requirements for LIC 16: Between REP and FDEMS

The unique technical security requirements associated with LIC 16 interactions between the REP and the FDEMS are shown in Table 5-4. There is one unique technical security requirements that is not included in LIC 16 that has been added since it is relevant to

DER systems. This requirement is underlined in the table below. Comments on their tailoring to REP-FDEMS interactions are shown in the second column.

Table 5-4: Unique Technical Security Requirements for LIC 16

NISTIR 7628 Unique Technical Security Requirements	Tailoring for Interactions Between REP and FDEMS
Session Time-Out[7]	Since FDEMS are generally located in unsecured locations where personnel are not experts in cyber security, logins or connections should time out if there is no activity, including application-to-application interactions between the REP and the FDEMS.
SG.AC-14 Permitted Actions without Identification or Authentication	No actions should be permitted without identification and authentication.
SG.AU-16 Non-repudiation	All modifications to the messaging and security logs of interactions between the REP and the FDEMS should be associated with a specific user and/or application identity.
SG.IA-3 Authenticator Management	The FDEMS authentication process with the REP should include validation of FDEMS security credentials and should include security credentials updating procedures.
SG.IA-4 User Identification and Authentication	Users should be individually identified and authenticated with access permissions established by their roles. The FDEMS should be authenticated with the REP before any interactions are permitted.
SG.IA-5 Device Identification and Authentication	All interactions between the FDEMS system and the REP system should require authentication. FDEMS hardware, firmware, and software applications should be identified and authenticated for system security monitoring and control.
SG.SC-3 Security Function Isolation	Interactions involving the establishment and updating of security should be isolated from non-security interactions.
SG.SC-5 Denial-of-Service Protection	Communication paths between the REP and the FDEMS may be redundant for increased protection against DoS attacks, particularly if different media can be used.
SG.SC-7 Boundary Protection	A security boundary should be established between the REP and the FDEMS. This security boundary should be protected to permit only authorized interactions. Examples include firewalls, limiting open ports, REP-managed networks, VPNs, IDS/IPS, and one-way “diode” communications to permit only one-way traffic between certain applications.
SG.SC-8 Communication Integrity	Data exchanged between the REP and the FDEMS should detect unauthorized modifications. Integrity checking may be done at all communication “nodes,” particularly those in the “last mile” between a backhaul communication network and the FDEMS.

[7] There is no comparable NISTIR 7628 security requirement.

NISTIR 7628 Unique Technical Security Requirements	Tailoring for Interactions Between REP and FDEMS
SG.SC-9 Communication Confidentiality	All communications between the REP and the FDEMS that include sensitive or security-relevant data should apply security techniques to ensure their confidentiality, particularly since these interactions are across organizational boundaries. Sensitive data would include, for example, security updates, private financial information, intellectual property, and personal data.
SG.SC-26 Confidentiality of Information at Rest	The FDEMS passwords and other sensitive and security-relevant information should be encrypted and protected against unauthorized disclosure when stored in the FDEMS.
SG.SI-7 Software and Information Integrity	The REP and the FDEMS software should monitor all modifications to data and applications for tampering.

5.4.2 Common Technical Security Requirements for LIC 16 between REP and FDEMS

The interface between REP systems and the FDEMS systems with unknown levels of protection must be secure. FDEMS are located in environments that the REP has little control over, and the DER systems that they manage could have significant impacts on the power system. Therefore, additional technical security requirements are necessary. These include the common technical security requirements identified in Table 5-5.

Table 5-5: Common Technical Security Requirements for LIC 16 Interfaces

NISTIR 7628 Common Technical Security Requirements	Tailoring for Interactions Between REP and FDEMS
SG.AC-7 Least Privilege	For both the REP and the FDEMS, only the necessary rights and privileges should be assigned to each role, particularly for those involving access between the systems.
SG.AC-17 Access Control for Portable and Mobile Devices	Access to the network that connects the REP and the FDEMS via portable or mobile devices should be restricted to authorized personnel.

NISTIR 7628 Common Technical Security Requirements	Tailoring for Interactions Between REP and FDEMS
SG.AU-2 Auditable Events	In addition to the functional logging requirements, the REP and the FDEMS should log all significant cyber security events that may indicate a cyber security attack. This will permit cyber security assessments to determine if an attack is occurring and the nature of the attack, as well as provide forensic data for after-the-fact evaluations and possible legal actions. Any attempts to access audit data by unauthorized users or software applications should be logged and notifications sent to security personnel All changes and revocations to user and to role permissions should be provided to and logged by both the REP and the FDEMS. All interactions on the network that connects the REP and the FDEMS via portable or mobile devices should be monitored for unauthorized access. This monitoring may be more critical if public or open networks are used. Unsuccessful login attempts into the REP and FDEMS systems should be logged and appropriate users notified, particularly if these login attempts utilize the network between the REP and the FDEMS. Network management functions should monitor the network for intrusions and log anomalous events.
SG.AU-3 Contents of Audit Records	The audit records of the REP and the FDEMS should include an accurate time stamp, the type of security event, a description of the event, the context of the event, and the status of the system when the event took place.
SG.CM-7 Configuration for Least Functionality	Both the REP and the FDEMS should be configured to provide only essential access. Specifically, unused ports should be closed and only authenticated software functions should be permitted to execute.
SG.SA-10 Developer Security Testing	The network between the REP and the FDEMS should be tested by the system developer or integrator to ensure that the security technologies are properly implemented and the security procedures are functioning properly. The vendor/manufacturer should verify the security and functionality of patches, should assess for malware, and should test on redundant or backup systems first (if possible), The vendor/manufacturer should develop procedures to rollback or de-install the patches.
SG.SA-11 Supply Chain Protection	As per the contract and/or SLA between the REP and the FDEMS owner, the vendor/installer of the FDEMS should be required to perform due diligence that they are supplying equipment from manufacturers who provide authenticated security-enabled equipment as required by the REP and/or FDEMS.
SG.SC-11 Cryptographic Key Establishment and Management	The REP and FDEMS system operators establish and manage cryptographic keys, including key updates and revocations.

NISTIR 7628 Common Technical Security Requirements	Tailoring for Interactions Between REP and FDEMS
SG.SC-12 Use of Validated Cryptography	Interactions between the REP and the FDEMS should: – Use validated cryptography, – Avoid implementing deprecated cryptographic suites in new systems beyond their expiration dates, and – Provide migration paths for older systems that still use deprecated cryptographic suites. These cryptographic methods should meet national or international standards, such as ISO/IEC 19790:2012, Information technology -- Security techniques -- Security requirements for cryptographic modules.
SG.SC-15 Public Key Infrastructure Certificates	Although key management of the REP and the FDEMS are most likely to be handled separately by their separate organizations, the network and communications protocols used between them should use valid cyber security certificates that are updated as necessary and revoked in a timely manner.
SG.SC-19 Security Roles	The REP and FDEMS should establish standard roles for different types of access to each other's systems. Special security roles should be established that are permitted to make modifications to the security procedures and protection of the information flows between the REP and the FDEMS. These security roles could require two-factor authentication and other stricter security measures. Role-based permissions should be established for different REP interactions, including security monitoring, software updates and patching, and deregistration. Role-based permissions should be established for different FDEMS interactions, including security establishment, security key management, management of software updates and patching, and deregistration. The FDEMS should be designed to enforce role-based permissions and prevent unauthorized access. Upon the removal of a FDEMS, all roles and permissions associated with that FDEMS should be revoked.
SG.SC-20 Message Authenticity	Communication protocols used between the REP and the FDEMS should authenticate all messages, including their source and destination. IDS and NSM capabilities should be used to detect possible integrity violations of the communication protocols, such as invalid message formats and suspicious protocol interaction patterns. This detection should take place on the communications media (layers 1-2), transport (layers 3-4), and application (layers 5-7). Data received at the REP and at the FDEMS should be validated as authorized.

NISTIR 7628 Common Technical Security Requirements	Tailoring for Interactions Between REP and FDEMS
SG.SC-22 Fail in Known State	For all safety and security failures, the REP should cause the applications and network associated with the FDEMS to enter a well-defined failure state that may include changing functionality, limiting functionality, shutting down the network connection, resetting the FDEMS, or other default actions. Failure in a known secure state helps prevent a loss of confidentiality, integrity, or availability in the event of a failure of the FDEMS.
SG.SI-8 Information Input Validation	Since much of the information exchanged between the REP and the FDEMS involves either direct commands to DER systems or indirect settings that can affect the operation of the DER systems when they are connected to the power grid, the information being exchanged should be validated for accuracy, completeness, validity and authenticity.
SG.SI-9 Error Handling	Since the REP and the FDEMS are owned and operated by different organizations, error handling should include the ability to notify the other organization of errors or equipment failure conditions without revealing potentially harmful or confidential information.

5.4.3 Governance, Risk and Compliance (GRC) for LIC 16: Between REP and FDEMS

Although GRC security requirements are applicable across all logical interfaces, some are more important to the interface between the REP and the FDEMS. Since the LIC 16 interfaces go across organizational boundaries, each organization's security policies will usually be different and administered separately. The REP and these FDEMS have minimal mutual trust, but must work together in a timely and secure manner. Sharing mutual security issues, such as intrusions, confidentiality breaches, deregistered systems, changes in personnel, and revoked certificates can be an important part of this interaction, so that security events and attacks can be mitigated. The more important GRC requirements are listed below in Table 5-6.

Table 5-6: Governance, Risk, and Compliance (GRC) Security Requirements for REP to FDEMS Interactions

NISTIR 7628 GRC Security Requirements	Tailoring for Interactions Between REP and FDEMS
SG.AC-4 Access Enforcement	The REP should enforce access permissions that are assigned to different users and user roles involving interactions with the FDEMS. The FDEMS should be designed to enforce role-based permissions and prevent unauthorized access.

NISTIR 7628 GRC Security Requirements	Tailoring for Interactions Between REP and FDEMS
SG.AC-18 Use of External Information Control Systems	The REP should establish the rules and conditions for FDEMS to access information from the REP systems. Conversely, the FDEMS should be designed to ensure that the terms and conditions are met for REP access to its information. The REP should establish and enforce the security requirements for FDEMS and DER systems to interface with its REP system. These security requirements could be part of an interconnection agreement, a service level agreement, a customer tariff, or other type of contractual agreement between the parties.
SG.AT-2 Security Awareness	The REP should support the FDEMS owners in security awareness and training, possibly including security requirements in the interconnection contracts, requiring Service Level Agreements with security provisions, managing the security of network connecting to the FDEMS, and the security of the FDEMS.
SG.AU-5 Response to Audit Processing Failures	The FDEMS should notify the REP of any failure of the security auditing process, and vice versa.
SG.AU-6 Audit Monitoring, Analysis, and Reporting	Audit information at the REP and the FDEMS should be synchronized, in standardized formats and/or easily converted from one form to another without loss of information. Time synchronization will permit the audit logs to be correlated even though they belong to different organizations. Audit records related to utility/FDEMS interactions should be transmittable to each other. To minimize false positives and unwarranted security notifications, security events should be validated from multiple sources and the IDS/NSM functions should be designed to ensure that normal traffic spikes do not cause security notifications. Since the REP and FDEMS do not have a single security management structure, regulators and other law enforcement may be required to ensure the audit reporting addresses all relevant events. Appropriate personnel should be alerted to any unauthorized or anomalous events.
SG.AU-8 Time Stamps	The REP and the FDEMS should synchronize their time clocks to achieve adequate precision and accuracy to detect any compromise of the timestamps of audit logs. This ensures that a series of events are logged chronologically with the necessary time resolution.
SG.AU-9 Protection of Audit Information	The REP and the FDEMS should detect unauthorized modifications to audit logs, and should notify each other if unauthorized modifications have been made.
SG.AU-10 Audit Record Retention	Since the REP and the FDEMS belong to different organizations, the REP should determine the minimum retention time for audit logs that relate to REP-FDEMS interactions. These should be consistent with utility audit log retention time.

NISTIR 7628 GRC Security Requirements	Tailoring for Interactions Between REP and FDEMS
SG.CM-3 Configuration Change Control	Since uncoordinated changes can allow threat agents to take advantage of potential vulnerabilities, all configuration changes that affect the interactions between the REP and the FDEMS should be planned, documented, and implemented in a coordinated manner.
SG.CM-4 Monitoring Configuration Changes	Changes in network configurations should be monitored and alarmed if unexpected and/or unauthorized.
SG.CM-5 Access Restrictions for Configuration Change	The REP and the FDEMS security roles should be restricted in what security settings they may modify or update. All configuration changes that affect each other should be provided to the other organization.
SG.CM-9 Addition, Removal, and Disposal of Equipment	If a FDEMS is removed from operation, the REP should ensure that all sensitive and security-relevant REP information is removed from that FDEMS.
SG.CM-10 Factory Default Settings Management	The REP should be able to verify that the FDEMS security has been enabled “out of the box” by the vendor/installer, since many sites that will implement FDEMS systems will not have adequate security expertise.
SG.CP-8 Alternate Telecommunication Services	Since FDEMS and their associated systems can affect the power grid particularly if the FDEMS manages many MW of DER output, the REP should identify alternate telecommunications capabilities in case of the loss of the primary telecommunications for longer than a critical time period.
SG.IA-3 Authenticator Management	All FDEMS and their associated DER systems should be registered and authenticated with the REP before any operational interactions are permitted. This identification and authentication process should include validation of FDEMS security credentials and security credentials updating procedures. Deregistration of a FDEMS should including revoking all security credentials.
SG.ID-4 Information Exchange	The REP should support the FDEMS owners in security awareness, possibly including security requirements in the interconnection contracts, requiring Service Level Agreements with security provisions, managing the security of network connecting to the FDEMS, and/or actually managing the security of the FDEMS.
SG.IR-5 Incident Handling	The REP and the FDEMS should reject any compromised data.
SG.IR-7 Incident Reporting	Since cyber incidents could affect both the REP and the FDEMS, the cyber incident information should be shared between the REP and the FDEMS owners. In particular, any cyber incidents that could affect the security of power grid operations should be reported immediately to permit mitigating actions to be taken.
SG.MA-5 Maintenance Personnel	Maintenance of FDEMS and the interface to the REP should be permitted only by authorized maintenance personnel (as specified by the REP, FDEMS, and/or DER owner).
SG.PM-1 Security Policy and Procedures	The REP should develop the security policies for handling interfaces with FDEMS and DER systems that are not under utility jurisdiction, that may have minimal security policies, but need to interface with the utility’s operational control systems.

NISTIR 7628 GRC Security Requirements	Tailoring for Interactions Between REP and FDEMS
SG.PM-5 Risk Management Strategy	The REP should develop a risk management strategy for interfaces with untrusted FDEMS and DER systems. This risk management strategy should address protecting the REP computer systems.
SG.RA-4 Risk Assessment	The REP performs a security risk assessment to determine the impact of unauthorized disclosure (confidentiality) and unauthorized modification (integrity) of data when transmitted between the REP and the FDEMS.
SG.SA-9 Developer Configuration Management	As per the contract and/or SLA between the REP and the FDEMS owner, the vendor/installer of the FDEMS should be required to certify that they are supplying equipment from manufacturers who are providing authenticated security-enabled equipment as required by the REP, FDEMS, and/or DER owner.
SG.SI-2 Flaw Remediation	Cyber security patches to network interface software, communication protocols, and software applications used by both the REP and the FDEMS should be applied using strong patch management procedures.
SG.SI-6 Security Functionality Verification	Start-up, restart, and anomalous events should cause the REP and the FDEMS to perform a self-test of the security functionality.

6 LEVEL 4: DISTRIBUTION UTILITY DER OPERATIONAL ANALYSIS

6.1 Level 4: Information Exchange Requirements: Description

At Level 4, distribution utilities implement DER management software applications to analyze and coordinate DER generation and storage as part of the broader DMS functions that manage the safe, efficient, and reliable planning and operation of the power grid.

These DMS and DER-focused applications are responsible for executing power flow-based situational awareness, contingency analysis, generation and load forecasts, planning studies, and other assessment functions to determine DER operational requirements. As part of this analysis, the DER applications handle DER registration, determine the optimal settings for DER autonomous functions, establish pricing signals for DER energy and ancillary services, initiate control commands when necessary, and transmit this information to the appropriate FDEMS within the utility jurisdiction.

These types of interactions are illustrated in Figure 6-1. The six main DER operational analysis systems consist of the:

- Distribution Utility DER Operational Analysis (DERMS) (#25),
- Distribution Management System (DMS) (#27),
- Geographic Information System (#17),
- Load Management and Demand Response System (LM/DR) (#32),
- Outage Management System (OMS) (#36), and
- DER SCADA system (#29a) (logically separate from the distribution SCADA system) that interacts with the DER systems within the utility's territory.

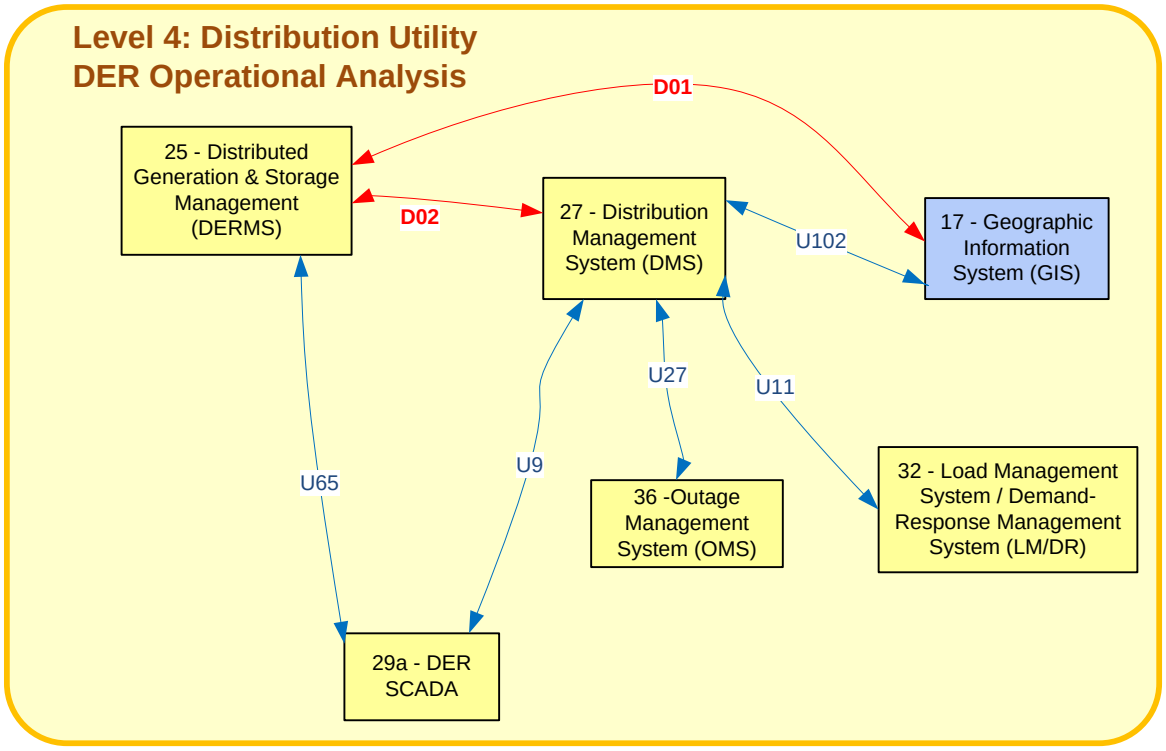

Figure 6-1: Level 4: Distribution Utility DER Operational Analysis (DERMS) for Distribution Operations Architecture

6.2 Level 4 Utility DER Operational Analysis: Cyber Security Requirements

6.2.1 Level 4 Utility DER Operational Analysis: Potential Cyber Security Vulnerabilities

Level 4 utility DER software applications are highly critical to safe and reliable power system operations since their results can affect large numbers of DER systems. Unlike a FDEMS in which a cyber security event (including attacks) might cause a local outage or power quality problems with a few DER systems, cyber events on these utility applications could cause decreased power system resiliency, major outages, and/or widespread equipment damage. In addition, electric power utilities could be the focus of politically motivated cyber attacks, whereas a FDEMS would normally be less politically noticed. At the same time, financially motivated cyber attackers could expect higher payoffs by attacking a utility rather than a customer site.

These DER applications are internal to the distribution utility and are typically covered by a single utility security policy that can be enforced, such as the North American Electric Reliability Corporation Critical Infrastructure Protection standards (NERC CIPs). Distribution utilities can use many of the cyber security concepts in the NERC CIPs to address their cyber security requirements.

The potential cyber security vulnerabilities for utility DER operational analysis are different from those for FDEMS and DER systems, as well as being different from traditional SCADA operations. These vulnerabilities include:

- *Need to interface between trusted utility control systems and untrusted external systems*: Distribution management controls the distribution grid through operational computer systems and communication networks. With the need to interface and exchange data with FDEMS at non-utility-managed sites, cyber security must include protection from these untrusted sites, in particular the verification of the data received.
- *New and evolving DER applications*: Since managing DER systems is new for distribution utilities, few DER software applications exist, leaving their implementation open to the normal set of software bugs, inadequately designed functions, incomplete validation of inputs and outputs, and the increased likelihood of malicious software, as utilities and vendors try to develop these applications.
- *The management of large numbers of DER systems*: This management requires the acquisition, validation, and update of large amounts of data in a timely manner. Out-of-date, incomplete, and invalid data, whether due to inadvertent or malicious actions, could cause incorrect results from the applications that could affect the reliability of the power grid, and that could cause financial harm to the utility as well as to the DER owners.
- *Public communication networks*: The distribution utilities must rely more on public communication networks, although some may deploy their own networks. In many cases, having their own private networks will not be cost-effective for connecting to DER systems. Regardless, the IT infrastructure must reach to customer sites and other non-secure locations, and therefore cannot be as rigorously isolated and secured, as is that of transmission utilities.
- *Lack of direct or timely feedback*: Distribution utilities cannot use direct monitoring and control typically used by SCADA systems for operating their own equipment. Instead, utilities will issue broadcast or multicast commands that do not necessarily include acknowledgments. This lack of feedback could impact how quickly the utilities might become aware of cyber security events and attacks, and could limit the types of mitigations that are deployed.
- *Inadequately security-trained personnel*: The NERC CIPs are requiring transmission utilities to train their personnel in security-related issues. The NERC CIPs are not mandatory for distribution utilities.

6.2.2 Level 4 Utility DER Operational Analysis: Categorization of Logical Interfaces

The utility DER applications interconnect with each other within the utility control center and/or back offices. The LIC related to all of these interconnections is LIC 5, interface

between control systems within the same organization, for example: between multiple DMS systems belonging to the same utility and between subsystems within DCS and ancillary control systems within a power plant:

- D01 – between DERMS and the GIS
- D02 – between DERMS and DMS
- U65 – between DERMS and DER SCADA
- U102 – between DMS and GIS
- U11 – between DMS and LM/DR
- U27 – between DMS and OMS
- U9 – between DMS and DER SCADA

6.3 Security Requirements for LIC 5: Between Control Systems within the Same Organization

All of the systems in Level 4 are control systems within a distribution organization, and therefore have the same cyber security requirements. The security requirements for the broader DMS functions have been addressed in other documents[8]; this document focuses on the security requirements for DER functions.

6.3.1 Unique Technical Security Requirements for LIC 5: Between Control Systems within the Same Organization

The unique technical security requirements associated with LIC 5: between control systems within the same organization, are shown in Table 6-1. Some additional unique technical security requirements that are not included in LIC 5 have been added since they are relevant to DER systems. These additional requirements are underlined in the table below. Comments on tailoring to DER analysis interactions are shown in the second column.

Table 6-1: Unique Technical Security Requirements for LIC 5

NISTIR 7628 Unique Technical Security Requirements	Tailoring for Interactions Between Control Systems within the Same Organization
SG.AC-14 Permitted Actions without Identification or Authentication	No actions should be permitted with DER-related applications without identification and authentication.

[8] The Advanced Security Acceleration Project for the Smart Grid (ASAP-SG) developed a security profile for Distribution Management: "*DM Security Profile - v1_0 – 20120220.* The document was prepared for the NIST SGIP Cyber Security Working Group and The UCAIug SG Security Working Group. The contract was managed by EnerNex Corporation, and supported by DOE and EPRI.

NISTIR 7628 Unique Technical Security Requirements	Tailoring for Interactions Between Control Systems within the Same Organization
SG.IA-4 User Identification and Authentication	Users interacting with DER-related applications should be individually identified and authenticated with access permissions established by their roles.
SG.IA-5 Device Identification and Authentication	All interactions between the DER-related applications should require authentication.
SG. IA-6 Authenticator Feedback	The authentication mechanism for user interactions within a utility should obscure passwords and other authentication information
Operational Latency[9]	Increased latency in exchanging information due to the use of cryptographic mechanisms should not impact the availability or degrade the operational performance of DER-related applications.
SG.SC-3 Security Function Isolation	Although not explicitly allocated to LIC 5, interactions involving the establishment and updating of security should be isolated from non-security interactions for DER-related applications.
SG.SC-7 Boundary Protection	A security boundary should be established around the DER-related applications. This security boundary should be protected to permit only authorized interactions, including from back office systems and any unprotected DER SCADA system.
SG.SC-8 Communication Integrity	Data exchanged among the DER-related applications should be protected to detect unauthorized modifications.
SG.SC-9 Communication Confidentiality	All security-relevant and sensitive data related to DER management should apply security techniques to ensure their confidentiality Sensitive data would include, for example, security updates, information, intellectual property, and personal data.
SG.SI-7 Software and Information Integrity	The DER software should monitor all modifications to data and applications for tampering.

6.3.2 Common Technical Security Requirements for LIC 5: Between Control Systems within the Same Organization

For DER-related applications within the utility control center, some common technical security requirements are more important than others and are identified in Table 6-2. There is one common technical security requirements that is not included in LIC 5 that has been added since it is relevant to DER systems. This requirement is underlined in the table below.

[9] There is no comparable NISTIR 7628 requirement.

Table 6-2: Common Technical Security Requirements for LIC 5 interfaces

NISTIR 7628 Common Technical Security Requirements	Tailoring for Interactions Between Control Systems within the Same Organization
SG.AC-7 Least Privilege	For DER-related applications, only the necessary rights and privileges should be assigned to each role, particularly for those involving access between different systems.
SG.AU-2 Auditable Events	DER-related applications should log all significant cyber security events that may indicate a cyber security attack. This will permit cyber security assessments to determine if an attack is occurring and the nature of the attack, as well as provide forensic data for after-the-fact evaluations and possible legal actions. Any attempts to access audit data by unauthorized users or software applications should be logged and notifications sent to security personnel. All changes and revocations to user and to role permissions should be logged. Appropriate users should be notified of unsuccessful login attempts.
SG.AU-3 Contents of Audit Records	The audit records of the DER-related applications should be synchronized and include an accurate time stamp, the type of security event, a description of the event, the context of the event, and the status of the system when the event took place.
SG.AU-16 Non-repudiation	All modifications to the messaging and security logs of interactions between the DER-related applications should be associated with a specific user and/or application identity.
SG.CM-7 Configuration for Least Functionality	The DER-related applications should be configured to provide only essential functionality. New, untested, and/or temporary applications should not be incorporated into operational systems and should have access restrictions.
SG.SA-10 Developer Security Testing	Because the DER-related applications are new and evolving in complexity, their vendors should provide security tests and security evaluation plans before these applications are incorporated into the utilities' DER control systems. The vendor/manufacturer of DER-related applications should verify the security and functionality of patches, should assess for malware, and should test on redundant or backup systems first (if possible), The vendor/manufacturer should develop procedures to rollback or de-install the patches.
SG.SA-11 Supply Chain Protection	Since any malware introduced in the supply chain could potentially affect large portions of the power grid, supply chain protection should be implemented to help ensure the new DER-related applications are secure. All applications should be digitally signed by their vendors or implementers.
SG.SC-11 Cryptographic Key Establishment and Management	The utility should establish and manage cryptographic keys for DER-related applications.

NISTIR 7628 Common Technical Security Requirements	Tailoring for Interactions Between Control Systems within the Same Organization
SG.SC-12 Use of Validated Cryptography	Interactions between the DER-related applications should: – Use validated cryptography, – Avoid implementing deprecated cryptographic suites in new systems beyond their expiration dates, and – Provide migration paths for older systems that still use deprecated cryptographic suites. These cryptographic methods should meet national or international standards, such as ISO/IEC 19790:2012, Information technology -- Security techniques -- Security requirements for cryptographic modules.
SG.SC-15 Public Key Infrastructure Certificates	The DER-related applications should use valid cyber security certificates that are updated as necessary and revoked in a timely manner.
SG.SC-19 Security Roles	Security role-based permissions should be established for different DER-related interactions, including security monitoring, security software updates and patching, and modifications to the security procedures and protection of the DER-related applications. Security role-based permissions should be established for interacting with each of the different DER-related applications, including security establishment, security key management, and management of security software updates and patching.
SG.SC-22 Fail in Known State	For defined safety and security failures, the DER-related applications should enter a well-defined failure state that may include changing functionality, limiting functionality, shutting down the network connections to these applications, resetting the applications, or other default actions. Failure in a known secure state helps prevent a loss of confidentiality, integrity, or availability in the event of a failure of the DER-related applications.
SG.SC-26 Confidentiality of Information at Rest	Passwords and other sensitive and security-relevant information in DER-related applications should be encrypted and protected against unauthorized disclosure.
SG.SI-8 Information Input Validation	All data being used by the DER-related applications should be validated for accuracy, completeness, validity and authenticity.
SG.SI-9 Error Handling	Error handling should include the ability to notify the utility users of errors.

6.3.3 Governance, Risk and Compliance (GRC) for LIC 5: Between Control Systems within the Same Organization

GRC security requirements are applicable to all LICs. However, some are more important than others for utility control systems. The more important GRCs are listed below in Table 6-3.

Table 6-3: Governance, Risk, and Compliance (GRC) Security Requirements for Utility DER-Related Applications

NISTIR 7628 GRC Security Requirements	Tailoring for Interactions Between Control Systems within the Same Organization
SG.AC-4 Access Enforcement	The utility should enforce access permissions that are assigned to different users, applications, and roles on the DER-related applications.
SG.AC-20 Publicly Accessible Content	The utility should ensure that personnel who may be primarily responsible for grid operations are aware of the privacy requirements related to DER information. DER information that is made public should not be personally identifiable information (PII). Alternatively, the data should be aggregated in such a way that no PII can be derived.
SG.AT-2 Security Awareness	The utility should promote security awareness and training among personnel involved with DER-related applications.
SG.AU-5 Response to Audit Processing Failures	The utility should log any failure of the security auditing process.
SG.AU-6 Audit Monitoring, Analysis and Reporting	The audit records of the DER-related applications should be synchronized. Time synchronization will permit different audit logs to be correlated.
SG.AU-8 Time Stamps	The utility should synchronize time across all DER-related applications to achieve adequate precision and accuracy to detect any compromise of the timestamps of audit logs. This ensures that a series of events are logged chronologically with the necessary time resolution.
SG.AU-9 Protection of Audit Information	The utility should detect and log any unauthorized modifications to audit logs. The user or application making the unauthorized modification should be logged. Any breach should be provided to affected parties,
SG.CM-5 Access Restrictions for Configuration Change	Security roles should be restricted in what security configuration settings they may modify or update. All configuration changes that affect DER-related applications should be logged.
SG.CM-9 Addition, Removal, and Disposal of Equipment	If DER-related applications are no longer utilized in grid operations, any sensitive or private information should be removed from their databases.
SG.CM-10 Factory Default Settings Management	The vendor/installer has security of the DER-related applications enabled “out of the box”, allowing modifications only by authenticated users. The DER-related applications should prevent the use of factory-set default access passwords after installation.
SG.CP-8 Alternate Telecommunication Services	If WAN telecommunications are needed between DER-related applications, the utility should identify alternate telecommunications capabilities in case of the loss of the primary telecommunications for longer than a critical time period.
SG.CP-11 Fail-Safe Response	If DER-related applications are not responding correctly, appropriate fail-safe procedures should be executed.
SG.IR-5 Incident Handling	The DER-related applications should reject any compromised data.

NISTIR 7628 GRC Security Requirements	Tailoring for Interactions Between Control Systems within the Same Organization
SG.IR-7 Incident Reporting	Since cyber incidents in DER-related applications could affect the resiliency of the power grid, any cyber incidents should be reported immediately to permit mitigating actions to be taken.
SG.MA-5 Maintenance Personnel	Maintenance of DER-related applications and analysis functions should be permitted only by authorized maintenance personnel.
SG.PL-4 Privacy Impact Assessment	The utility should assess the privacy requirements of DER information that is collected and aggregated for use by the DER analysis applications.
SG.PM-1 Security Policy and Procedures	The utility should develop the security policies for handling information exchanges between DER-related applications.
SG.PM-5 Risk Management Strategy	The utility should develop a risk management strategy for interactions between DER-related applications.
SG.PS-7 Contractor and Third-Party Personnel Security	The utility should establish and enforce the security requirements for contractor and third-party personnel for maintenance and upgrade functions of DER-related applications.
SG.RA-4 Risk Assessment	The utility should perform a security risk assessment to determine the impact of potentially compromised data in the DER-related applications.
SG.SA-5 Smart Grid Information System Documentation	The utility should require the security capabilities of the DER-related applications to be documented.
SG.SA-8 Security Engineering Principles	The utility should ensure that private DER information is not used during analysis in such a way that it can be publicly accessed or derived from the analysis results. The utility analysis software applications should be developed according to security engineering principles, taking into account that DER systems in aggregate can provide large amounts of energy and ancillary services, and can therefore affect the resilience of power grid operations. Security engineering principles include: – Creation of a documented and tested security response plan in the event a vulnerability is discovered; – Creation of a documented and tested privacy response plan in the event a vulnerability is discovered; and – Performance of a root cause analysis to understand the cause of identified vulnerabilities. – Creation of security response plan to detect and mitigate the impact of a cyber attack that is occurring.
SG.SI-2 Flaw Remediation	Cyber security patches to DER-related software applications, network interface software, and communication protocols should be applied using strong patch management procedures.
SG.SI-6 Security Functionality Verification	Start-up, restart, and anomalous events should cause the utility DER applications to perform a self-test of the security functionality.

7 LEVEL 5: DER INTEGRATION WITH TRANSMISSION AND MARKET OPERATIONS

7.1 Level 5: Information Exchange Requirements: Description

At Level 5, ISOs or RTOs and market operations can affect what the DER systems are requested or required to do, based on tariffs and other agreements. DER operations need to be integrated with the larger grid operations, including transmission and market operations. Distribution utilities may interact (either directly or indirectly) with their ISO/RTO as a wholesale market participant.

The Aggregator/Retail Energy Provider (#41) (also referred to as an ESP), manages aggregations of DER systems at multiple customer sites that may also act as “virtual power plants” that are bid into the electricity market for both energy and ancillary services. For the purposes of this architecture, the ESP manages the maintenance of these DER systems.

These interactions are shown in **Error! Reference source not found.** below.

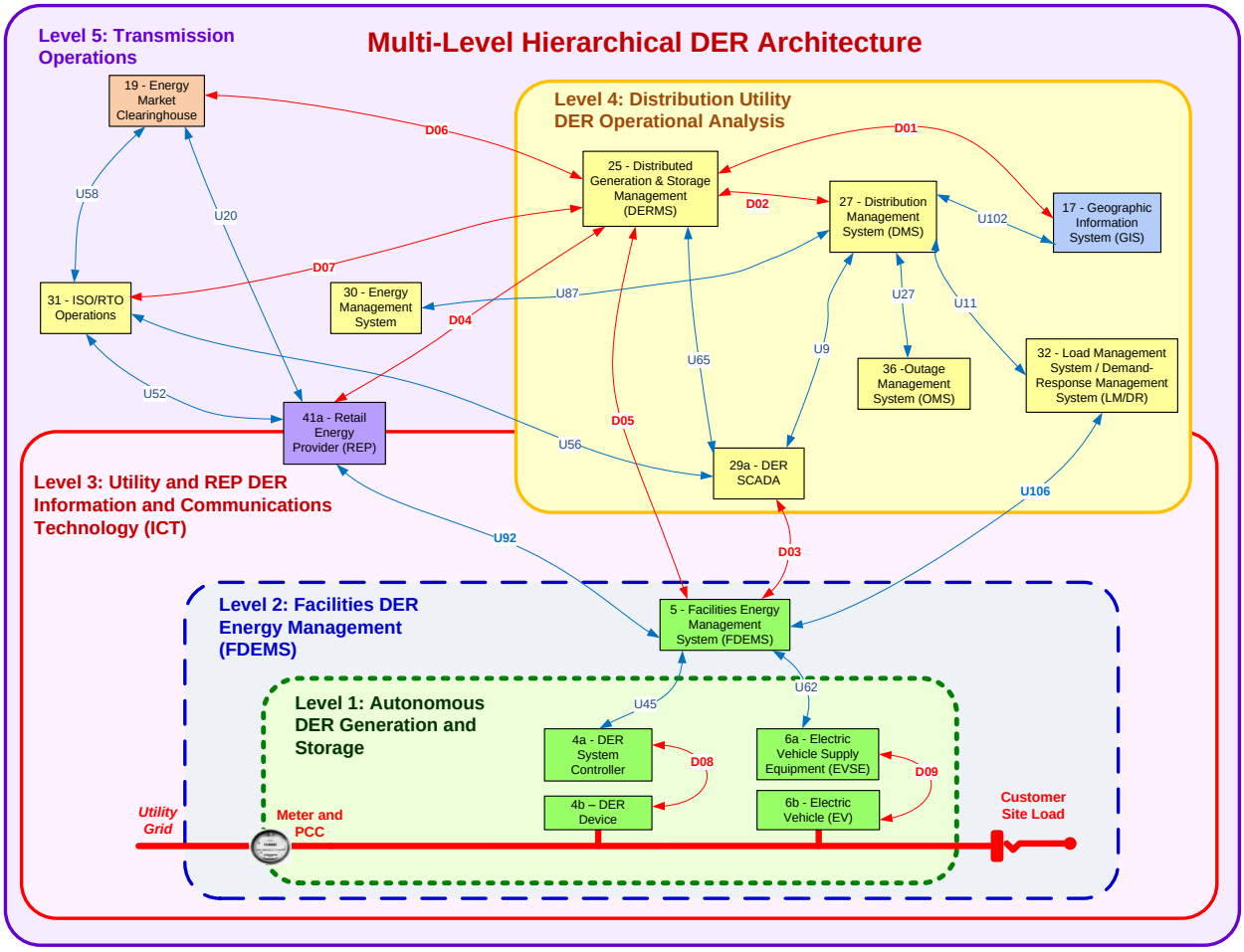

Figure 7-1: Level 5: DER Integration with Transmission and Market Operations Architecture

7.2 Level 5 DER Integration with Transmission and Market Operations: Cyber Security Requirements

Once a distribution utility has incorporated DER information into its DMS, the DMS interactions with transmission utilities and market operations are no different than without the DER information. Therefore, the cyber security requirements for DER-related aspects are identical to the cyber security requirements for DMS. These are addressed in other documents.

8 CONCLUSIONS AND RECOMMENDATIONS

8.1 Conclusions

DER systems are becoming an increasingly critical part of power system reliability. In 2012 in Germany, the inability of wind and solar DER systems to "ride-through" frequency anomalies caused enough grid instability that a number of major power outages occurred. Although those outages were caused by power system anomalies[10], similar outages could be caused by coordinated cyber security attacks.

In California, the DER interconnection rules may include cyber security requirements for all new DER installations. The NISTIR 7628 provides generic security recommendations, but these must be tailored into DER-specific security requirements for utilities, manufacturers, integrators, and owners/operators.

8.2 Recommended Next Steps

This document is a first step in the development of DER-specific security requirements. Two additional steps are needed when a utility develops specifications for installations and implements the cyber security controls:

- Utilities, DER manufacturers, and DER integrators should review the cyber security requirements in this document and ensure they are complete, implementable, and coordinated with the DER functional capabilities.
- DER security specifications should be developed that can be used by utilities for different types of installations and different communication protocols at each of the levels defined in this document.

[10] All "medium voltage" DER systems in Germany are being retrofitted to avoid future anomaly-caused outages.

APPENDIX A - LIST OF THE NISTIR 7628 SMART GRID CATALOG OF SECURITY REQUIREMENTS

The families of the NIST Smart Grid Catalog of Security Requirements are shown in Table 0-1, while a more detailed list of the requirements within each family is shown in Table 0-2. The complete NIST catalog can be found on the NIST web site[11].

Table 0-1: NIST Smart Grid Security Requirements Families

Ref.	NIST Smart Grid Security Requirements Families
SG.AC	Access Control
SG.AT	Security Awareness and Training
SG.AU	Audit and Accountability
SG.CM	Configuration Management
SG.ID	Information and Document Management
SG.IR	Incident Response
SG.MA	Smart Grid system Development and Maintenance
SG.MP	Media Protection
SG.MR	Monitoring and Reviewing Smart Grid System Security Policy
SG.PE	Physical and Environmental Security
SG.PL	Strategic Planning
SG.PM	Security Program Management
SG.PS	Personnel Security
SG.RA	Risk Management and Assessment
SG.SA	Smart Grid system and Services Acquisition
SG.SC	Smart Grid System and Communication Protection
SG.SI	Smart Grid System and Information Integrity

[11] http://csrc.nist.gov/publications/PubsNISTIRs.html

Table 0-2: Detailed NIST Catalog of Smart Grid Security Requirements

NIST Ref.	Catalog of SG Security Requirements
3.7 Access Control (SG.AC)	
SG.AC-1	Access Control Policy and Procedures
SG.AC-2	Remote Access Policy and Procedures
SG.AC-3	Account Management
SG.AC-4	Access Enforcement
SG.AC-5	Information Flow Enforcement
SG.AC-6	Separation of Duties
SG.AC-7	Least Privilege
SG.AC-8	Unsuccessful Login Attempts
SG.AC-9	Smart Grid Information System Use Notification
SG.AC-10	Previous Logon Notification ion
SG.AC-11	Concurrent Session Control
SG.AC-12	Session Lock
SG.AC-13	Remote Session Termination
SG.AC-14	Permitted Actions without Identification or Authentication
SG.AC-15	Remote Access
SG.AC-16	Wireless Access Restrictions
SG.AC-17	Access Control for Portable and Mobile Devices
SG.AC-18	Use of External Information Control Smart Grid systems
SG.AC-19	Control System Access Restrictions
SG.AC-20	Publicly Accessible Content
SG.AC-21	Passwords
3.8 Security Awareness and Training (SG.AT)	
SG.AT-1	Security Awareness and Training Policy and Procedures
SG.AT-2	Security Awareness
SG.AT-3	Security Training
SG.AT-4	Security Awareness & Training Records
SG.AT-5	Contact with Security Groups and Associations
SG.AT-6	Security Responsibility Testing
SG.AT-7	Planning Process Training
3.9 Audit and Accountability (SG.AU)	
SG.AU-1	Audit and Accountability Policy and Procedures
SG.AU-2	Auditable Events

NIST Ref.	Catalog of SG Security Requirements
SG.AU-3	Content of Audit Records
SG.AU-4	Audit Storage Capacity
SG.AU-5	Response to Audit Processing Failures
SG.AU-6	Audit Monitoring, Analysis, and Reporting
SG.AU-7	Audit Reduction and Report Generation
SG.AU-8	Time Stamps
SG.AU-9	Protection of Audit Information
SG.AU-10	Audit Record Retention
SG.AU-11	Conduct and Frequency of Audits
SG.AU-12	Auditor Qualification
SG.AU-13	Audit Tools
SG.AU-14	Security Policy Compliance
SG.AU-15	Audit Generation
SG.AU-16	Non-Repudiation
3.10 Security Assessment and Authorization (SG.CA)	
SG.CA-1	Security Assessment and Authorization Policy and Procedures
SG.CA-2	Security Assessments
SG.CA-3	Continuous Improvement
SG.CA-4	Smart Grid Information System Connections
SG.CA-5	Security Authorization to Operate
SG.CA-6	Continuous Monitoring
3.11 Configuration Management (SG.CM)	
SG.CM-1	Configuration Management Policy and Procedures
SG.CM-2	Baseline Configuration
SG.CM-3	Configuration Change Control
SG.CM-4	Monitoring Configuration Changes
SG.CM-5	Access Restrictions for Configuration Change
SG.CM-6	Configuration Settings
SG.CM-7	Configuration for Least Functionality
SG.CM-8	Component Inventory
SG.CM-9	Addition, Removal, and Disposal of Equipment
SG.CM-10	Factory Default Settings Management
SG.CM-11	Configuration Management Plan

NIST Ref.	Catalog of SG Security Requirements
3.12 Continuity of Operations (SG.CP)	
SG.CP-1	Continuity of Operations Policy and Procedures
SG.CP-2	Continuity of Operations Plan
SG.CP-3	Continuity of Operations Roles and Responsibilities
SG.CP-4	Continuity of Operations Training
SG.CP-5	Continuity of Operations Plan Testing
SG.CP-6	Continuity of Operations Plan Update
SG.CP-7	Alternate Storage Sites
SG.CP-8	Alternate Telecommunication Services
SG.CP-9	Alternate Control Center
SG.CP-10	Smart Grid Information System Recovery and Reconstitution
SG.CP-11	Fail-Safe Response
3.13 Identification and Authentication (SG.IA)	
SG.IA-1	Identification and Authentication Policy and Procedures
SG.IA-2	Identifier Management
SG.IA-3	Authenticator Management
SG.IA-4	User Identification and Authentication
SG.IA-5	Device Identification and Authentication
SG.IA-6	Authenticator Feedback
3.14 Information and Document Management (SG.ID)	
SG.ID-1	Information and Document Management Policy and Procedures
SG.ID-2	Information and Document Retention
SG.ID-3	Information Handling
SG.ID-4	Information Exchange
SG.ID-5	Automated Labeling
3.15 Incident Response (SG.IR)	
SG.IR-1	Incident Response Policy and Procedures
SG.IR-2	Incident Response Roles and Responsibilities
SG.IR-3	Incident Response Training
SG.IR-4	Incident Response Testing and Exercises
SG.IR-5	Incident Handling
SG.IR-6	Incident Monitoring
SG.IR-7	Incident Reporting
SG.IR-8	Incident Response Investigation and Analysis
SG.IR-9	Corrective Action
SG.IR-10	Smart Grid System Backup
SG.IR-11	Coordination of Emergency Response
3.16 Smart Grid System Development and Maintenance (SG.MA)	
SG.MA-1	Smart Grid System Maintenance Policy and Procedures
SG.MA-2	Legacy Smart Grid System Upgrades
SG.MA-3	Smart Grid Information System Maintenance
SG.MA-4	Maintenance Tools
SG.MA-5	Maintenance Personnel
SG.MA-6	Remote Maintenance
SG.MA-7	Timely Maintenance
3.17 Media Protection (SG.MP)	
SG.MP-1	Media Protection Policy and Procedures
SG.MP-2	Media Sensitivity Level
SG.MP-3	Media Marking
SG.MP-4	Media Storage
SG.MP-5	Media Transport
SG.MP-6	Media Sanitization and Disposal
3.18 Physical and Environmental Security (SG.PE)	
SG.PE-1	Physical and Environmental Security Policy and Procedures
SG.PE-2	Physical Access Authorizations
SG.PE-3	Physical Access
SG.PE-4	Monitoring Physical Access
SG.PE-5	Visitor Control
SG.PE-6	Visitor Records
SG.PE-7	Physical Access Log Retention
SG.PE-8	Emergency Shutoff Protection
SG.PE-9	Emergency Power
SG.PE-10	Delivery and Removal
SG.PE-11	Alternate Work Site
SG.PE-12	Location of Smart Grid System Assets
3.19 Strategic Planning (SG.PL)	
SG.PL-1	Strategic Planning Policy and Procedures
SG.PL-2	Smart Grid Information System Security Plan

NIST Ref.	Catalog of SG Security Requirements
SG.PL-3	Rules of Behavior
SG.PL-4	Privacy Impact Assessment
SG.PL-5	Security-Related Activity Planning
3.20 Security Program Management (SG.PM)	
SG.PM-1	Security Policy and Procedures
SG.PM-2	Security Program Plan
SG.PM-3	Senior Management Authority
SG.PM-4	Security Architecture
SG.PM-5	Risk Management Strategy
SG.PM-6	Security Authorization to Operate Process
SG.PM-7	Mission/Business Process Definition
SG.PM-8	Management Accountability
3.21 Personnel Security (SG.PS)	
SG.PS-1	Personnel Security Policy and Procedures
SG.PS-2	Position Categorization
SG.PS-3	Personnel Screening
SG.PS-4	Personnel Termination
SG.PS-5	Personnel Transfer
SG.PS-6	Access Agreements
SG.PS-7	Contractor and Third-Party Personnel Security
SG.PS-8	Personnel Accountability
SG.PS-9	Personnel Roles
3.22 Risk Management and Assessment (SG.RA)	
SG.RA-1	Risk Assessment Policy and Procedures
SG.RA-2	Risk Management Plan
SG.RA-3	Security Impact Level
SG.RA-4	Risk Assessment
SG.RA-5	Risk Assessment Update
SG.RA-6	Vulnerability Assessment and Awareness
3.23 Smart Grid System and Services Acquisition (SG.SA)	
SG.SA-1	Smart Grid System and Services Acquisition Policy and Procedures
SG.SA-2	Security Policies for Contractors and Third Parties
SG.SA-3	Life-Cycle Support
SG.SA-4	Acquisitions
SG.SA-5	Smart Grid System Documentation
SG.SA-6	Software License Usage Restrictions
SG.SA-7	User-Installed Software
SG.SA-8	Security Engineering Principles
SG.SA-9	Developer Configuration Management
SG.SA-10	Developer Security Testing
SG.SA-11	Supply Chain Protection
3.24 Smart Grid System and Communication Protection (SG.SC)	
SG.SC-1	Smart Grid System and Communication Protection Policy and Procedures
SG.SC-2	Communications Partitioning
SG.SC-3	Security Function Isolation
SG.SC-4	Information Remnants
SG.SC-5	Denial-of-Service Protection
SG.SC-6	Resource Priority
SG.SC-7	Boundary Protection
SG.SC-8	Communication Integrity
SG.SC-9	Communication Confidentiality
SG.SC-10	Trusted Path
SG.SC-11	Cryptographic Key Establishment and Management
SG.SC-12	Use of Validated Cryptography
SG.SC-13	Collaborative Computing
SG.SC-14	Transmission of Security Parameters
SG.SC-15	Public Key Infrastructure Certificates
SG.SC-16	Mobile Code
SG.SC-17	Voice-Over Internet Protocol
SG.SC-18	System Connections
SG.SC-19	Security Roles
SG.SC-20	Message Authenticity
SG.SC-21	Secure Name/Address Resolution Service
SG.SC-22	Fail in Known State
SG.SC-23	Thin Nodes
SG.SC-24	Honeypots
SG.SC-25	Operating Smart Grid system-Independent Applications
SG.SC-26	Confidentiality of Information at Rest
SG.SC-27	Heterogeneity
SG.SC-28	Virtualization Techniques
SG.SC-29	Application Partitioning
SG.SC-30	Smart Grid System Partitioning

NIST Ref.	Catalog of SG Security Requirements
3.25 Smart Grid System and Information Integrity (SG.SI)	
SG.SI-1	Smart Grid System and Information Integrity Policy and Procedures
SG.SI-2	Flaw Remediation
SG.SI-3	Malicious Code and Spam Protection

NIST Ref.	Catalog of SG Security Requirements
SG.SI-4	Smart Grid Information System Monitoring Tools and Techniques
SG.SI-5	Security Alerts and Advisories
SG.SI-6	Security Functionality Verification
SG.SI-7	Software and Information Integrity
SG.SI-8	Information Input Validation
SG.SI-9	Error Handling

APPENDIX B - ACRONYMS

AMI	Advanced Metering Infrastructure
ASAP-SG	Advanced Security Acceleration Project – Smart Grid
CIP	Critical Infrastructure Protection Standards
CIS	Customer Information System
CPS	Cyber Physical Systems
CPUC	California Public Utility Commission
DER	Distributed Energy Resources
DERMS	Distribution Utility DER Operational Analysis
DRGS	Distributed Renewable Generation and Storage
DMS	Distribution Management System
DOE	Department of Energy
DoS	Denial of Service
DR	Demand Response
EMS	Energy Management System
EPRI	Electric Power Research Institute
EPS	Electric Power System
ESI	Energy Services Interface
ESP	Energy Service Provider
EV	Electric Vehicle
EVSE	Electric Vehicle Supply Equipment
FDEMS	Facilities DER Energy Management Systems
GIS	Geographic Information System
GPRS	General Packet Radio Service
GRC	Governance, Risk, and Compliance
HAN	Home Area Network
HMI	Human Machine Interface
ICT	Information and Communications Technology
IDS	Intrusion Detection System
IED	Intelligent Electronic Device
ISO	Independent System Operator
kW	Kilowatts
LI	Logical Interface

LIC	Logical Interface Category
LM	Load Management
LM/DR	Load Management/Demand Response
MW	Megawatts
NERC	North American Electric Reliability Corporation
NESCOR	National Electric Sector Cybersecurity Organization Resource
NIST	National Institute of Standards and Technology
NISTIR	NIST Interagency Report
NSM	Network and System Management
OMS	Outage Management System
PCC	Point of Common Coupling
PII	Personally Identifiable Information
PUC	Public Utility Commissions
REP	Retail Energy Provider
RTO	Regional Transmission Organization
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SLA	Service Level Agreement
V2G	Vehicle to Grid
VPP	Virtual Power Plant
WAN	Wide Area Network