Distributed Energy Resources (DER) Cybersecurity Recommendations for DER System Stakeholders

DRAFT

April 18, 2013

Table of Contents

Table of Figures

Table of Tables

Introduction

This document is a publicly available document, being presented to the SGIP DRGS DEWG and to the SGIP SGCC for information and discussion, but also expected to be provided to other groups, including the IEC TC57 WG15 to act as input to a possible IEC Technical Report.

This document provides cyber security recommendations for the stakeholders of DER systems and the various applications and systems that help manage their safe, reliable, and efficient operations. These stakeholders include the manufacturers, the integrator/installers, the users, the information and communication technology (ICT) providers, the security managers, the testing and maintenance personnel, and other stakeholders involved in securing DER systems.

1. Overview of Key Cybersecurity Concepts

This document provides cybersecurity recommendations for the stakeholders of DER systems. These stakeholders include the manufacturers, the integrator/installers, the users, the communication network providers, the security managers, the testing and maintenance personnel, and other stakeholders involved in securing DER systems.

This document discusses the cybersecurity issues for Distributed Energy Resources (DER), building on the concepts and the hierarchical architecture described in the DRGS White Paper (ref).

- This first section covers key cybersecurity concepts and issues.
- The second section covers the cybersecurity issues of DER systems as cyber-physical systems, in which cyber attacks can affect physical systems.
- The third section covers the 5-level hierarchical architecture of DER systems
- The fourth through sixth sections cover the mitigations of cyber vulnerabilities and attacks for each of the first 3 levels, organized by stakeholder. ***Note: Only Level 1 and parts of Level 2 have been drafted as of April 18, 2013***
- The last section identifies commonly used communication standards in the power system industry, and identifies which types of cybersecurity functions are covered in these standards.

1.1 Cybersecurity Requirements

Users and DER systems have four basic security requirements, which protect them from four basic threats:

- Integrity – preventing the unauthorized modification or theft of information
- Availability – preventing the denial of service and ensuring authorized access to information
- Confidentiality – preventing the unauthorized access to information
- Non-Repudiation/Accountability – preventing the denial of an action that took place or the claim of an action that did not take place.

For DER systems, often **integrity** is the most important security requirements, although the others follow close behind. The reason for the importance of integrity is that the DER system must be able to operate safely and reliably, and some modifications to data located within the DER controller or sent to the DER controller may impact that safety and reliability.

Availability is viewed as less important because DER systems usually operate autonomously and should be able to enter a "default" mode if vital communications are lost.

Confidentiality is usually associated with market-related data and intellectual property. Competitors and thieves should not be able to access sensitive information.

Non-repudiation/Accountability is usually associated with financial transactions, such as responding to control commands or demand response requests. Providing time-stamped proof of receiving such a request and taking action on that request can be vital to billing and settling these transactions.

1.2 Security Threats in the Power Industry

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

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

Utilities are accustomed to worrying about equipment failures and safety-related carelessness. Natural disasters get some attention, particularly for utilities that commonly experience hurricanes, earthquakes, cyclones, ice storms, etc., even though these are looked upon as beyond the control of the utility. What is changing is the importance of protecting information, which is becoming an increasingly important aspect of safe, reliable, and efficient power system operations.

Security risk assessment is vital in determining exactly what needs to be secured against what threats and to what degree of security. The key is determining the cost-benefit: one size does not fit all (substations), layers of security are better than a single solution, and ultimately no protection against attacks can ever be completely absolute. Nonetheless, there is significant room between the extremes from doing nothing to doing everything, to provide the level of security needed for modern utility operations.

The benefits also can flow the other way. If additional security is implemented against possible deliberate attacks, this monitoring can be used to improve safety, minimize carelessness, and improve the efficiency of equipment maintenance.

The following sections discuss some of the most important threats to understand and to mitigate.

1.2.1 Deliberate Threats

Deliberate threats can cause more focused damage to facilities and equipment in substations than the inadvertent threats. The incentives for these deliberate threats are increasing as the results from successful attacks can have increasingly economic and/or "socio/political" benefits to the attackers. Sophisticated monitoring of facilities and

equipment can help prevent some of these threats, while ameliorating the impact of successful attacks through real-time notifications and forensic trails.

1.2.1.1 Disgruntled Employee

Disgruntled employees are one of the primary threats for attacks on power system assets, including DER systems. Unhappy employees who have the knowledge to do harm can cause significantly more damage than a non-employee, particularly in the power system industry where the DER equipment and supporting systems are unique to the industry.

1.2.1.2 Industrial Espionage

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

1.2.1.3 Vandalism

Vandalism can damage facilities and equipment with no specific gain to the attackers other than the act of doing it, and the proof to themselves and others that they can do it. Often, the vandals are unaware of or do not care about the possible consequences of their actions.

Again, DER systems may be particularly vulnerable to vandalism, partly because of their unprotected environments, but also because their generation capabilities can directly affect the power grid, including causing outages.

1.2.1.4 Cyber Hackers

Hackers are people who seek to breach cybersecurity for gain. This gain may be directly monetary, industrial knowledge, political, social, or just individual challenge to see if the hacker can gain access. Most hackers use the Internet as their primary gateway to entry, and therefore firewalls, isolation techniques, and other countermeasures can be used to separate DER systems from the Internet. However, DER systems may use the Internet for software updates, thus opening up a channel for cyber hackers.

1.2.1.5 Viruses and Worms

Like hackers, viruses and worms typically attack via the Internet. However, some viruses and worms can be embedded in software that is loaded into systems that have been isolated from the Internet, or could possibly be transmitted over secure communications from some insecure laptop or other system. They could include man-in-the-middle viruses, spyware for capturing power system data, and other Trojan horses. A famous (or infamous) example is the Stuxnet worm, which successfully attacked the Iranian uranium centrifuges. DER systems are equally vulnerable to such attacks.

1.2.1.6 Theft

Theft has a straightforward purpose – the attackers take something (equipment, data, or knowledge) that they are not authorized to take. Generally, the purpose has financial gain as the motive, although other motives are possible as well.

Monitoring access to locked facilities and alarming anomalies in the physical status and health of equipment (e.g. not responding or disconnected) are the primary methods for alerting personnel that theft is possibly being committed.

1.2.1.7 Terrorism

Terrorism is the least likely threat but the one with possibly the largest consequences since the primary purpose of terrorism is to inflict the greatest degree of physical, financial, and socio/political damage.

Monitoring and alarming anomalies to access (including physical proximity) to substation facilities is possibly the most effective means to alert personnel to potential terrorist acts, such as physically blowing up a substation or other facility. However, terrorists could become more sophisticated in their actions, and seek to damage specific equipment or render critical equipment inoperative in ways that could potentially do more harm to the power system at large than just blowing up one substation. Therefore, additional types of monitoring are critical, including the status and health of equipment.

1.2.2 Inadvertent Threats

1.2.2.1 Safety Failures

Safety has always been a primary concern for any power system facilities, and must be part of DER implementation and operation. In the power industry, meticulous procedures have been developed and refined to improve safety, but not all of these have yet been fully developed for DER systems. Autonomous safety measures such as protective relaying, are a primary defense, but monitoring of the status of key equipment and the logging/alarming of compliance to safety procedures can enhance safety to a significant degree.

1.2.2.2 Equipment Failures

Equipment failures are the most common and expected threats to the reliable operation of the power system. Often the monitoring of the physical status of DER equipment can also benefit maintenance efficiency, possible prevention of certain types of equipment failures, real-time detection of failures not previously monitored, and forensic analysis of equipment failure processes and impacts.

1.2.2.3 Carelessness or Lack of Knowledge

Carelessness or just a lack of knowledge is one of the “threats” to protecting DER systems, whether it is not locking doors or inadvertently allowing unauthorized personnel to access passwords, keys, and other security safeguards. Often this carelessness is due to complacency (“no one has ever harmed this DER system yet”) or inexperience (“I didn’t

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

1.2.2.4 Natural Disasters

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

1.3 Cybersecurity Vulnerabilities and Attacks

The threats can be realized by many different types of attacks, some of which are illustrated in Figure 1. Often an attack takes advantage of a vulnerability, which may be due to human carelessness, an inadequately designed system, or circumstances such as a major storm. As can be seen, the same type of attack can often be involved in different security threats. This web of potential attacks means that there is not just one method of meeting a particular security requirement: each of the types of attacks that present a specific threat needs to be countered.

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

- Lack of security: Security, even if it exists, is never "turned on".
- Indiscretions by personnel: Employees stick their passwords on their computer monitors or leave doors unlocked.
- Simple or easy-to-guess passwords: Employees use short alpha-only passwords or use their dog's name and/or their birthday as their password.
- Social engineering: An attacker uses personal information or subterfuge to learn a user's password, such as pretending to be from a bank or leaning over someone's shoulder as they type their password.
- Bypass controls: Employees turn off security measures, do not change default passwords, or everyone uses the same password to access all substation equipment. Or a software application is assumed to be in a secure environment, so does not authenticate its actions.
- Integrity violation: Data is modified without adequate validation, such that the modified data causes equipment to malfunction or allows access to unauthorized users or applications.
- Software updates and patches: The software is updated without adequate testing or validation such that worms, viruses, and Trojan Horses are allowed into otherwise

secure systems. Alternatively, security patches needed to fix vulnerabilities are not applied.

- Lack of trust: Different organizations have different security requirements and use different cybersecurity standards.

Some frequent types of attacks include:

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

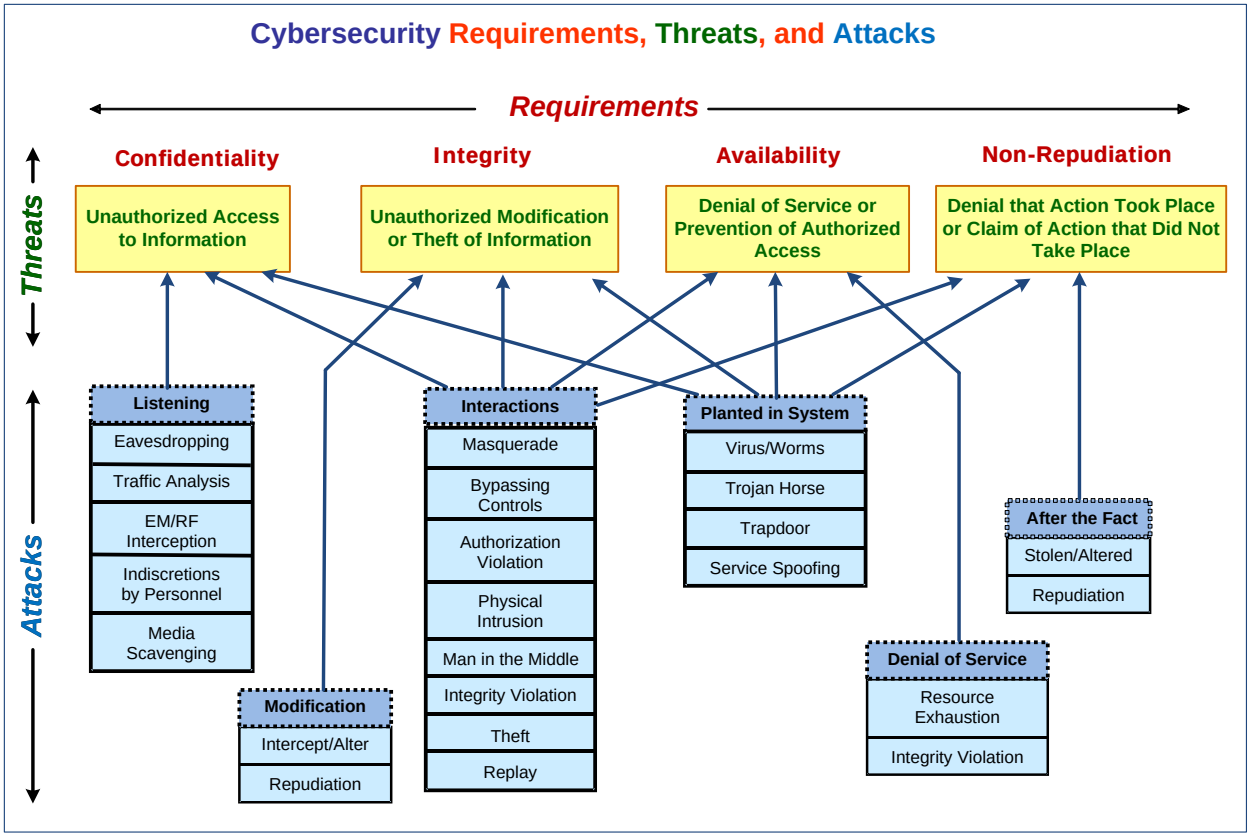


Figure 1: Security Requirements, Threats, and Possible Attacks

1.4 Mitigation Categories for Protection against Cybersecurity Attacks

Attack mitigations are often described as having five purposes. Associated security countermeasures can mitigate one or more of these purposes:

- **Deterrence and delay**, to try to avoid attacks or at least delay them long enough for counter actions to be undertaken. Often incorrectly described as "preventing attacks", deterrence can be the primary defense, but should not be viewed as the only defense.
- **Detection of attacks**, primarily those that were not deterred, but could include attempts at attacks. Detection is crucial to any other security measures since if an attack is not recognized, little can be done to prevent it. Intrusion detection capabilities can play a large role in this effort.
- **Assessment of attacks**, to determine the nature and severity of the attack. For instance, is the entry of a number of wrong passwords just someone forgetting or is it a deliberate attempt by an attacker to guess some likely passwords.
- **Communication and notification**, so that the appropriate authorities and/or computer systems can be made aware of the security attack in a timely manner. Network and system management can play a large role in this effort.

- **Response to attacks**, which includes actions by the appropriate authorities and computer systems to mitigate the effect of the attack in a timely manner. This response can then deter or delay a subsequent attack.

These mitigations are illustrated in Table 1.

Table 1: Mitigation Categories for Cyber-Physical Systems

	Category	*Description*	*Power System Examples*	*Cyber Examples*
Before Failure or Attack	**Protection against a failure or attack**	Active measures used in normal circumstances that are designed to prevent an attack	Erect substation fence; limit access to control center; validate data entry; deploy redundant equipment; perform contingency analysis studies; train personnel adequately	Isolate networks; require strong passwords; use role-based access control; encrypt messages; disable unneeded ports/services; validate patches before implementing them
	Deterrence to a failure or attack	Preparing for a possible failure or discouraging someone from engaging in an attack	Develop emergency operations plans; test emergency plans periodically; display signs indicating danger or private property; warn of legal actions; deploy CCTV cameras; change system settings for storms or other natural disasters; test new software and systems	Develop emergency network plans; display warnings when applications or data are modified; require legal acceptance when installing software
During Failure or Attack	**Detection of a failure or attack**	Identifying a failure or attack and notifying appropriate entities	Monitor power system status and measurements; enter events in event log; alarm operators; initiate cellphone call to on-duty person; provide quality flags for monitored data	Detect intrusions; check signatures; scan for viruses; monitor network configurations; alarm security personnel
	Response to a failure or attack	Stopping the spread of the failure or attack by using emergency measures	Trip breakers; shed load; isolate microgrids	Shut down network; turn off computer; isolate network
	Coping during a failure or attack	Initiating additional activities to mitigate the impact	Switch to backup systems; reconfigure feeders; start additional generation	Start manual activities to replace automated activities

	Category	*Description*	*Power System Examples*	*Cyber Examples*
After Failure or Attack	**Recovery from a failure or attack**	Restoring to normal operations after a failure has be corrected or an attack has been stopped	Test all failed or compromised power equipment; restore power; switch to primary systems; return to normal operations	Test all systems and networks; reconnect isolated networks and systems;
	Audit and legal actions to a failure or attack	Assessing the nature and consequences of a failure or attack	Analyze audit logs and other records	Debrief and post-mortem analysis; system re-configuration; policy changes

2. DER as Cyber-Physical Systems

2.1 Protecting Cyber-Physical Systems

DER systems are cyber-physical systems, so security breaches can have "real-world" impacts. However, generation systems have been protected against causing these real-world impacts since Thomas Edison pulled the switch in Pearl Station in 1882 to light up Wall Street for the first time in history. From the start, they included fuses to avoid voltage spikes from burning them down. They included voltage regulators to ensure the voltage remained in the proper range within the light bulbs. They used multiple generators so that one could be taken down while the other was maintained. Soon redundant cables were used, and red flags popped up if something was wrong.

Cyber controllers and embedded firmware have now been added to make modern DER systems, thus blurring the distinction between power system devices and information systems, but the fundamental design of these physical systems to protect themselves has not changed.

What has changed is that the cyber controllers and embedded firmware now need to be protected from cyber threats as well, especially those that could cause harm to the physical devices or to the power system they are interconnected with. This requirement for cybersecurity is well understood – what is not as well understood is the ability of the power system to continue to provide the mitigating capabilities built into its design and functions for over 100 years.

DER systems are cyber-physical systems which combine power system operational equipment with cyber-based control of that equipment. Cyber-physical systems are designed not only to provide the functions that the equipment was developed for, but also to protect that equipment against equipment failures and often against certain types of "mistakes". In addition, they are usually designed to operate in "degraded mode" if communications are lost or some other abnormal condition exists. "Coping" with attacks is also critical, since power system equipment cannot just be shut off if an attack is occurring, but must try to remain functional as much as possible. "Recovery" strategies after attacks are also critical, since again the power must remain on as much as feasible even if equipment is removed for repair. Finally, time-stamped forensic alarm and event logs need to capture as much information as possible about the attack sequences for both future protection and possible legal actions.

2.2 DER Systems as Cyber-Physical Systems

Cybersecurity for DER systems requires a different approach than for typical IT systems. As stated in the NISTIR 7628 "*Traditionally, cybersecurity for Information Technology (IT) focuses on the protection required to ensure the confidentiality, integrity, and availability of the electronic information communication systems. Cybersecurity 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. Cybersecurity 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]

2.3 Cyber-Physical Threats

Therefore, cybersecurity for cyber-physical systems are mostly the same as for purely cyber systems, but there are some important differences.

- **Physical impacts**: Cyber attacks (whether deliberate or inadvertent) can cause physical results, such as power outages and damaged equipment. So the threats are against the functions of these systems, not directly on the data itself. In other words, if an attack against data does not affect a function, then the attack is irrelevant. On the other hand, successful attacks that modify data not only may affect that data, but more importantly can cause some physical world impact.
- **Cyber-physical protections and mitigations**: Since cyber-physical systems already are designed with many protections against "equipment and software failures" (since these are common inadvertent problems), some cyber attacks may already be protected against or may simply invoke existing cyber-physical reactions to mitigate the impact of the attack. For instance, if the cyber-physical system validates data to be within acceptable ranges, then cyber attacks that change this data to unreasonable values would be detected and ignored or alarmed. Cyber-physical systems can mitigate attacks by using fault-tolerant designs, redundant equipment, and applications that model the physical systems using the laws of physics (e.g. power flow-based applications). For instance, if an attack causes one power system component to shut down, another redundant component would automatically take over the functions of the "failed" component. These intrinsic mitigations should be utilized and possibly enhanced to meet additional types of threats.
- **Impacts from cybersecurity**: Some types of cyber mitigation procedures and technologies can negatively impact cyber-physical systems. For example, if the time required to encrypt a message causes this message to arrive too late at the circuit breaker controller, that breaker might not trip in time and could cause a million-dollar transformer to explode. Therefore, the types of cybersecurity mitigations must be carefully woven into cyber-physical mitigations to ensure that the primary functionality is maintained, even during attacks.

2.4 Possible Mitigations of Attacks against Cyber-Physical Systems

DER systems are vulnerable to most of these cybersecurity threats. Of more direct interest are assessments of the severity of a cyber-physical attack and the possible countermeasures

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

available to mitigate these attacks – remembering that they will never be completely prevented, but that their impacts can be minimized.

Potential mitigations of "attacks" against cyber-physical systems need to include a combination of information cybersecurity measures and physical cybersecurity measures. An illustration of these mitigations is shown in Figure 2, in which physical measures can protect against cyber attacks, and cyber measures can protect against physical attacks.

The information in the Figure is also listed in Table 2 and Table 3.

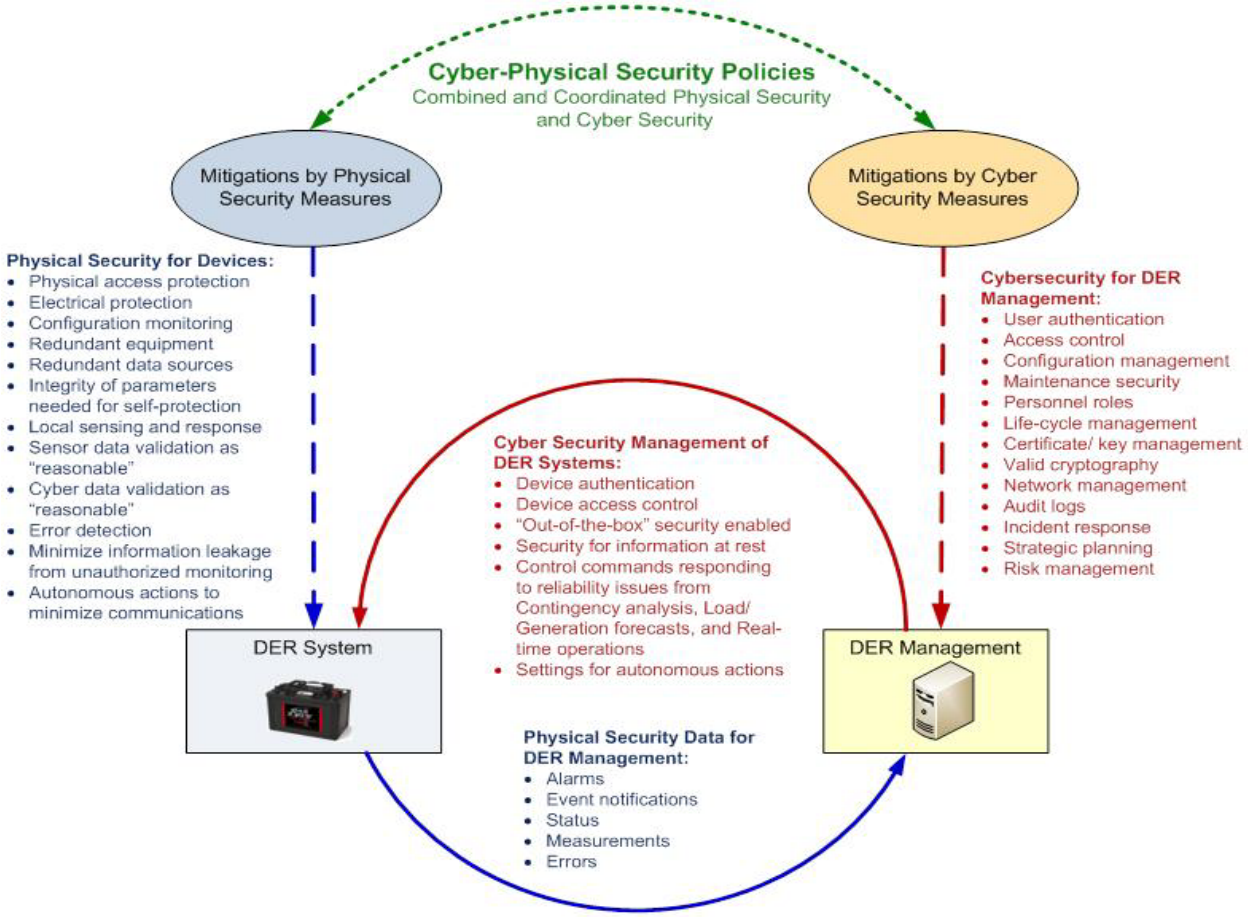


Figure 2: Mitigations by Physical and Cybersecurity Measures

Table 2: Mitigations by Physical and Cybersecurity Measures

Mitigations by Physical Security Measures	Mitigations by Cybersecurity Measures
Physical Security for Devices: • Physical access control, e.g. cages, locked doors, alarm systems, etc.	**Cybersecurity for DER Management:** • User authentication • Access control

Mitigations by Physical Security Measures	Mitigations by Cybersecurity Measures
• Electrical self-protection against cyber or physical attacks, such as "hardwired" limits, tripping off, disconnecting from grid, etc. • System self protection through "secured" parameters that cannot be remotely changed • Sensing and response to local conditions • Sensor data validation as "reasonable" • Cyber data validation as "reasonable" • Error detection • Alarms and events on physical changes • Redundant equipment • Redundant data sources • Redundant communication paths • Configuration monitoring • Data validation for "reasonability" • Securing the integrity of parameters that are needed for self-protection even from local access • Autonomous actions that minimize the need for communications	• Non-repudiation • System configuration management • Maintenance security • Personnel roles • Life-cycle management • Valid cryptography for confidentiality and integrity • Network management and control • Network configuration management • Intrusion detection in networks and controllers • Certificate / Key management • Audit logs • Incident response • Strategic planning • Risk management

Table 3: Security Management of DER Systems

Physical Security Data for DER Management	Cybersecurity Management of DER Systems
• Alarms • Event notifications • Status • Measurements • Errors	• Device authentication • Device access control • Authorization • "Out-of-the-box" security enabled • Security for information at rest • Non-repudiation • Valid cryptography for confidentiality and integrity • Results from State Estimation to validate DER status • Results from Contingency Analysis to manage DER systems • Power-flow-based applications for situational awareness, such as Load/Generation Forecasts, Real-time Operations, Contingency Analysis, etc. • Settings for autonomous actions

3. Cybersecurity Requirements to Mitigate DER Vulnerabilities and Attacks

DER systems have many stakeholders, including the original manufacturers, the implementers, the owners, the maintenance personnel, the utilities, and retail energy providers. How do these different stakeholders determine what DER vulnerabilities to protect against? What can they do to mitigate the likelihood and impact of a successful attack within their realm?

3.1 General DER Cybersecurity Requirements

Cybersecurity requirements to mitigate the possibility and/or the impact of attacks are described in many documents. The most relevant to DER cybersecurity is the NISTIR 7628[2]. However, that document is high-level and needs to be tailored for specific applications. Additional cybersecurity mitigation is also provided by specific standards, including communication standards that include cybersecurity or specific cybersecurity standards.

Briefly, cybersecurity requirements cover the following issues:

- Security policies to establish the concepts and overall security requirements
- Security procedures to establish the methods for achieving the security requirements described in the security policies
- Risk management to identify the possible impacts of attacks, the likelihood of such attacks, and the
- Defense in depth
- Identification, authentication, and role-based access control for users, applications, and systems
- Security perimeters at the different organizational and site-specific levels
- Security for communication protocols: media security, transport security, application security
- Intrusion detection and prevention
- Network and system management to monitor and control the health of networks and the computer systems
- Use of power system reliability mechanisms to detect and mitigate cyber attacks
- Prevention, detection, coping during an attack, recovery from an attack, documenting/logging attack events and actions
- Stakeholder responsibilities: security during manufacturing, implementation, installation, operation, maintenance, and removal

[2] NISTIR 7628

3.2 Five-Level DER Hierarchical Architecture (Overview)

Direct control by utilities is not feasible for the thousands if not millions of DER systems "in the field", so a hierarchical approach is necessary for utilities to interact with these widely dispersed DER systems. At the local level, DER systems must manage their own generation and storage activities autonomously, based on local conditions, pre-established settings, and DER owner preferences. However, 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 regional transmission organizations (RTOs) and/or independent system operators (ISOs) for reliability and market purposes. In some regions, retail energy providers (REPs) or other energy service providers (ESPs) are responsible for managing groups of DER systems.

Although in general DER systems will be part of a hierarchy, different scenarios will consist of different hierarchical levels and variations even within the same hierarchical level. For instance, small residential PV systems may not include sophisticated Facilities DER Energy Management Systems (FDEMS), while large industrial and commercial sites could include multiple FDEMS and even multiple levels of FDEMS. Some DER systems will be managed by Retail Energy Providers through demand response programs, while others may be managed (not necessarily directly controlled) by utilities through financial and operational contracts or tariffs with DER owners.

This hierarchical approach can be described as combinations of five levels, as illustrated in Figure 3[3] and described briefly below.

[3] Diagrams of these 5 levels have been discussed in the SGIP DRGS DEWG and the IEC TC57 WG17. They utilize the European Smart Grid Architecture Model (SGAM) structure. A White Paper can be found at https://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/DRGS/DRGS_Subgroup_B_White_Paper_-_Categorizing_Hierarchical_DER_Systems_v2.docx

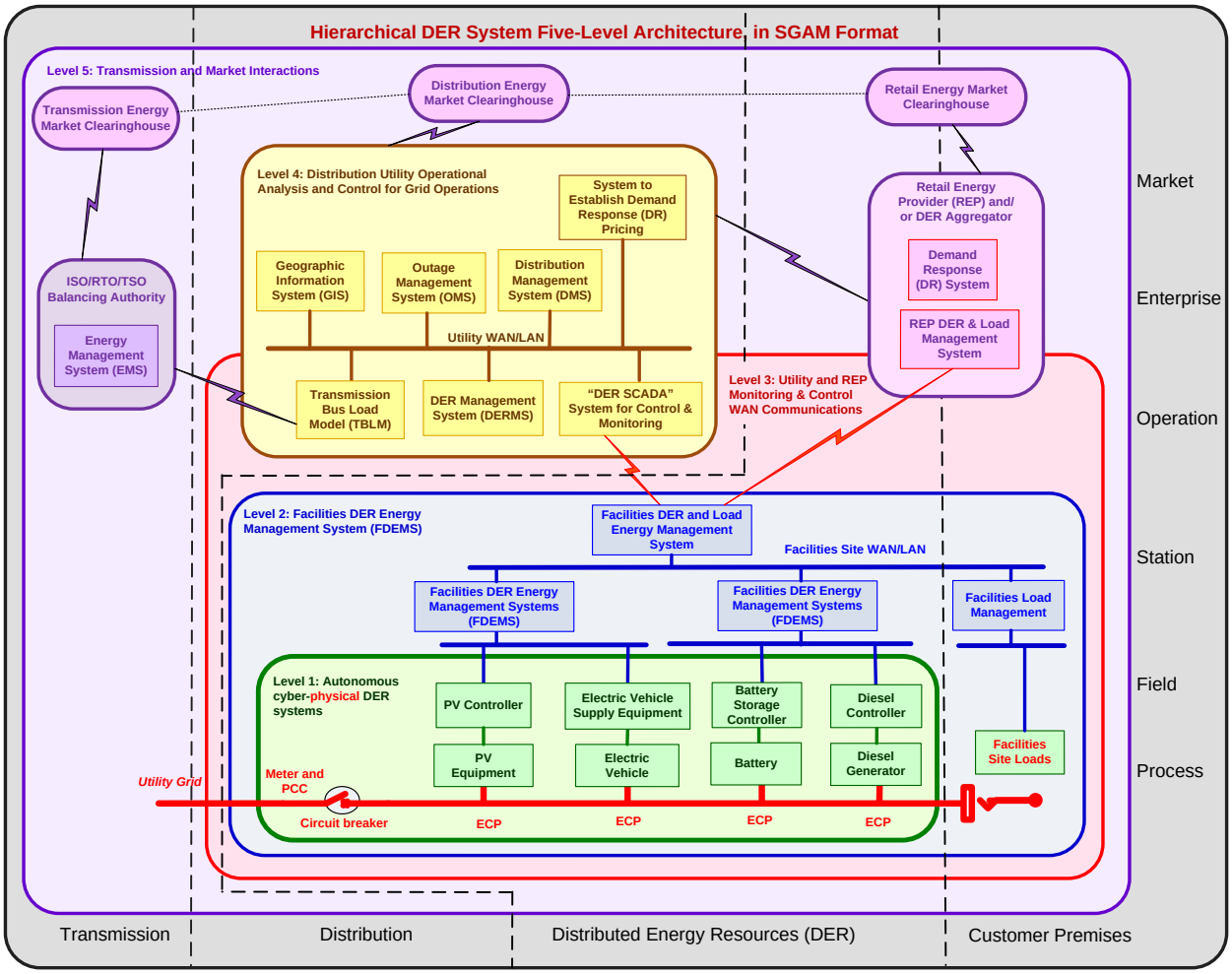


Figure 3: Five-Level Hierarchical DER System Architecture

1. **Level 1: DER Systems** (green in the Figure) is the lowest level and includes the actual cyber-physical DER systems themselves. These DER systems will be interconnected to the utility grid at Electrical Connection Points (ECPs) and will usually be operated autonomously. In other words, these DER systems will be running based on local conditions, such as photovoltaic systems operating when the sun is shining, wind turbines operating when the wind is blowing, electric vehicles charging when plugged in by the owner, and diesel generators operating when started up by the customer. This autonomous operation can be modified by DER owner preferences, pre-set parameter, and commands issued by utilities and aggregators.
2. **Level 2: Customer DER Management (FDEMS)** (blue in the Figure) is the next higher level in which a customer DER management system (FDEMS) manages the operation of the Level 1 DER systems. This FDEMS may be managing one or two DER systems in a residential home, but more likely will be managing multiple DER systems in commercial and industrial sites, such as university campuses and shopping malls. Utilities may also use a FDEMS to handle DER systems located at utility sites such as substations or power plant sites.

3. **Level 3: Utility and REP Operational WAN Communications** (red in the Figure) extends beyond the local site to provide the wide-area communications networks that support monitoring and control by utilities and retail energy providers (REPs). These communications networks provide the means to request or even command DER systems (typically through a FDEMS) to take specific actions, such as turning on or off, setting or limiting output, providing ancillary services (e.g. volt-var control), and other grid management functions. REP requests would likely be price-based focused on greater power system efficiency, while utility commands would also include safety and reliability purposes. The combination of this level and level 2 may have varying scenarios, while still fundamentally providing the same services.
4. **Level 4: Distribution Operational Analysis** (yellow in the Figure) applies to utility applications that are needed to determine what requests or commands should be issued to which DER systems. Utilities must monitor the power system and assess if efficiency or reliability of the power system can be improved by having DER systems modify their operation. This utility assessment involves many utility control center systems, including Geographical Information Systems, Distribution Automation Systems, Outage Management Systems, Demand Response systems, as well as DER database and management systems. Once the utility has determined that modified requests or commands should be issued, it will send these out as per Level 3.
5. **Level 5: Transmission and Market Operations** (purple in the Figure) is the highest level, and involves the larger utility environment where regional transmission operators (RTOs) or independent system operators (ISOs) may need information about DER capabilities or operations and/or may provide efficiency or reliability requests to the utility that is managing the DER systems within its domain. This may also involve the bulk power market systems, as well as retail energy providers.

In this document, only Levels 1, 2, and 3 are covered. Levels 4 and 5 are covered under general utility operations cybersecurity and are therefore beyond the scope of DER cybersecurity.

4. Level 1 Autonomous DER Cyber-Physical System Cybersecurity Requirements

4.1 Level 1 DER System: Architecture

As seen in Figure 4, 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. They 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 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 what is termed the Point of Common Coupling (PCC)[4].

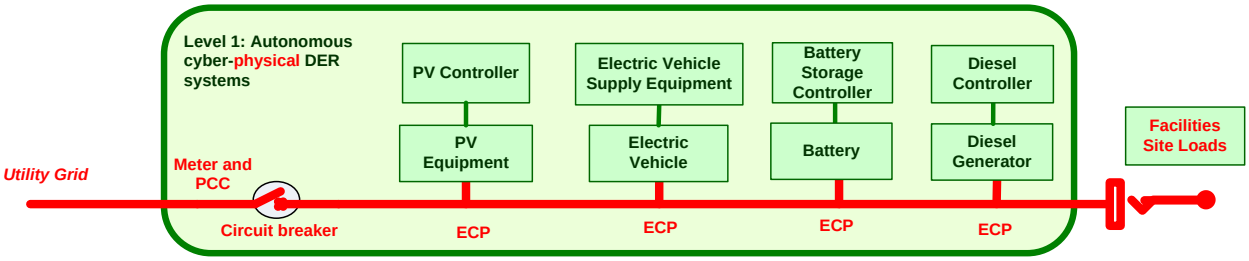


Figure 4: Level 1: Autonomous DER systems at smaller customer and utility sites

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 short green lines. 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 electric vehicle service element (EVSE) charger may be located in a garage or charging station parking spot, only a few feet from the electric vehicle, while the controller of 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) that 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 Point of Common Coupling (PCC) between the local EPS and the area EPS.

4.2 Level 1 DER System: Cybersecurity Vulnerabilities

4.3 Level 1 DER System: Impacts Due to DER Systems Failures

In the Level 1 environment, malicious attacks or inadvertent DER cyber-physical failures generally affect only one or a small number of DER systems. These DER systems are usually operating autonomously with minimal interactions with other systems. They are typically installed at one residential house or small commercial/industrial customer sites, such as stores, shopping centers, and buildings, or they may be located on utility sites such as substations.

In general, malicious attacks or other failures of autonomous DER systems may have large impacts on customer sites and customer equipment, but are not likely to impact utilities significantly or cause system-wide power system disruptions. As shown in Table 4, the major impacts are possible outages to customer sites and potential financial impacts to DER

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

owners. However, there are some impacts that could affect utilities, such as for a DER system located within utility facilities, or if the DER system is critical to utility operations.

Attacks or failures of DER systems may impact operations in a number of different ways.

- Denial of Service: The DER system could trip off or not provide the energy or ancillary services required
- Integrity violation: The DER system could use invalid settings and cause damage to itself or to the local electrical grid.
- Confidentiality / privacy violation: Confidential or private information could be taken from the DER system
- Non-repudiation violation: The DER system either repudiates an action or fails to confirm an action.

Table 4: Level 1 impact severities due to malicious attacks and failures of individual autonomous DER systems

Type of impact	Specific impacts	Severity
Scale impact	Single DER systems only	L
Safety impact	Outages of customer facilities could cause safety situations, such as criminal actions during the blackout Electrical causes of damage, such as electrocution or burning of property Loss of power at medically sensitive locations, causing harm or death of patients, including hospitals	M (H if medical impact)
Transmission power system operations impact	*None likely* If located on a feeder within a transmission substation, distribution power quality problems could affect transmission	L
Distribution power operations impact	Potential power quality impacts on the distribution feeder serving the customer facility, including voltage excursions, harmonics, and power outages of other customers on that feeder	L
Customer site(s) power system impact	Potential complete or partial outage of the facility	H
Utility financial impact	Any costs associated with power quality problems such as truck rolls or additional equipment inspections Possible legal costs if inadequate contingency analysis studies could be proved to have caused power outages to other customers on that feeder If equipment is destroyed or vandalized, the costs for repair or replacement	L L M
Utility reputation impact	Only if the utility were responsible for the security of the customer's DER management system	L

Type of impact	Specific impacts	Severity
DER owner financial impact	The costs for the replacement energy that would be purchased from the utility until the DER systems could be brought back on-line The costs for "cleaning up" the DER management system to delete any malware and to improve the cybersecurity mitigations If equipment is destroyed or vandalized, the costs for repair or replacement	H H H
DER owner privacy impact	If DER is connect to the HAN with other devices, then compromise of the DER could lead to compromises of other devices that have private information	L
DER ESP/ manager/ implementer reputation	The reputation of the manager of the DER management system could be hurt	M
Integrator financial and reputation impact	The integrator could have financial and reputation impacts if the unauthorized access to the DER management could be shown to be due to inadequate integrator-implemented cybersecurity. They would, at a minimum, require patching or upgrading systems in the field	M
Environmental impact	If the facility is directly managing environmental conditions such as a water treatment plant, loss of power could cause environmental damage Toxic material from damaged devices such as batteries could cause environmental harm people and locations Loss of power to life safety system in a manufacturing facility dealing with toxic material could cause environmental harm to people	L

4.4 Level 1 DER System: Cybersecurity Requirements and Possible Mitigations

The cybersecurity requirements and possible mitigations must reflect the need to design and install DER systems at sites where the DER owners have minimal cybersecurity expertise and where cost-effectiveness of the DER functions are their primary goal. Therefore, cybersecurity should be built into the DER system, enabled "out of the box", without the requirement for the DER owners to manage complex cybersecurity measures, and in fact only allowing advanced users from modifying cybersecurity measures.

The most important types of cybersecurity requirements are those that deter or defer attacks before they can cause any damage. Many of these involve policies and procedures, while a few involve the implementation of cybersecurity technologies. However, it is also very important to mitigate the impacts of an attack or failure during and after the event.

The following table describes cybersecurity requirements and mitigation techniques to take before, during, and after an attack or failure. The first column identifies the cybersecurity

requirements for mitigating the impacts. The second column lists the relevant NISTIR 7628 Catalog of Cybersecurity Requirements[5].

These table entries are organized by the following stakeholder categories:

1. Manufacturer: DER system design for self-protection security requirements
2. Integrator and installer: DER setup for meeting cybersecurity requirements
3. User (and device): access requirements
4. Information and communication technology (ICT) designers: cybersecurity requirements for media, networks, and protocols
5. Security managers: alarming, logging, and reporting cybersecurity requirements
6. Testing and maintenance personnel: cybersecurity requirements for testing, maintenance, and updating systems
7. Possible mitigations during a cyber attack or failure
8. Possible mitigations after a cyber attack or failure

4.4.1 Manufacturer: DER System Design for Self-protection Security Requirements

Any cyber-physical systems should have built-in self-protection designed and implemented by the manufacturer to prevent failures from common problems, such as electrical interference, voltage spikes, cold, heat, jostling during shipping, and many other physical protections. Their cyber components (microchips, communication modules, etc.) should also be protected against changes that are "operationally" unreasonable, harmful, or unsafe.

Table 5: Manufacturer-Established DER Self-Protection Cybersecurity Requirements

Cybersecurity Requirements for Mitigating Impacts Protection Measures Before an Attack or Failure	***NISTIR 7628 Catalog of Cybersecurity Requirements***
• The DER system is manufactured with the default that all access is authenticated	• *SG.SI-6 Security Functionality Verification*
• The DER system is hardened such that only essential software and applications are installed	• *SG.CM-7 Configuration for Least Functionality*
• The manufacturers of DER systems use penetration testing to ensure their systems are well-protected	• *SG.SI-6 Security Functionality Verification*
• The DER system establishes setting limits to ensure that no setting changes can exceed these limits and harm the equipment	• *SG.CM-2 Baseline Configuration* • *Cyber-Physical System security*

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

Cybersecurity Requirements for Mitigating Impacts Protection Measures Before an Attack or Failure	*NISTIR 7628 Catalog of Cybersecurity Requirements*
• The DER system is constrained in what functional and security settings can be changed remotely	• *SG.AC-15 Remote Access* • *SG.CM-5 Access Restrictions for Configuration Change*
• The DER system contains secure firmware or hardware memory for passwords and other embedded private or confidential information that is encrypted or otherwise secured against unauthorized access	• *SG.SI-7 Software and Information Integrity* • *SG.SC-26 Confidentiality of Information at Rest*
• The DER system validates even authorized changes to DER operational settings against what those settings are reasonably or contractually allowed to be	• *SG.CM-4 Monitoring Configuration Changes* • *SG.CM-6 Configuration Settings* • *SG.SI-8 Information Input Validation*
• The DER system rejects any compromised or invalid data, while that event is logged and appropriate entities (people or systems) notified	• *SG.AU-2 Auditable Events* • *SG.IR-7 Incident Reporting* • *SG.IR-9 Corrective Action* • *SG.SI-9 Error Handling*
• For important functionality, the DER system monitors more than one source of critical data and has an algorithm to determine the one that is "most likely" to be correct	• *SG.SC-5 Denial of Service Protection* • *SG.SC-8 Communication Integrity*
• The DER system detects internal errors and failures, and enters a default "failure" state, which may include limiting functionality, restarting, or shutting down	• *SG.SC-22 Fail in Known State*
• DER system components use heartbeat concepts to detect component failures	• *SG.SI-9 Error Handling*
• The DER system only provides non-sensitive data to non-authenticated requests	• *SG.CM-7 Configuration for Least Functionality*
• The DER system provides an emergency manual override capability that shuts down the system	• *SG.SI-9 Error Handling*

4.4.2 Integrator and Installer: DER Setup for Meeting Cybersecurity Requirements

Integrators and installers of DER systems should take the responsibility to ensure all appropriate cybersecurity measures are "turned on" when the DER system is installed. Since manufacturers usually include options for different types and levels of security, it is up to the integrators to meet the DER owner cybersecurity requirements (which may be mandated by the utility interconnection requirements) through the appropriate selection and testing of the cybersecurity cryptography suites, methods for establishing secure channels, and implementing appropriate key management processes.

Table 6: Integrator and installer Cybersecurity Requirements

Cybersecurity Requirements for Mitigating Impacts Protection Measures Before an Attack or Failure	*NISTIR 7628 Catalog of Cybersecurity Requirements*
• The integrator/installer selects and implements appropriate levels of security to meet the DER owner's and the utility's interconnection security requirements	• *SG.CM-2 Baseline Configuration*
• The integrator/installer has security of the DER system enabled "out of the box", allowing modifications only by authenticated advanced users	• *SG.CM-2 Baseline Configuration* • *SG.CM-3 Configuration Change Control* • *SG.CM-10 Factory Default Authentication Management*
• The integrator/installer ensures that unique cryptographic keys are used for each installation	• *SG.SC-11 Cryptographic Key Establishment and Management* • *SG.IA-5 Device Identification and Authentication*
• The integrator/installer ensures that separate security keys are used for different types of functions, such as for operations versus maintenance	• *SG.SC-11 Cryptographic Key Establishment and Management* • *SG.IA-5 Device Identification and Authentication*
• The integrator/installer Includes notices of legal actions that will be taken if a "threat agent" does try to manipulate DER system settings or access confidential/private information	• *SG.AC-9 Smart Grid Information System Use Notification*
• The integrator/installer provides instruction to DER owners on security requirements so they won't try to bypass security settings	• *SG.AT-2 Security Awareness* • *SG.AT-5 Contact with Security Groups and Associations*
• Installers are trained appropriately to ensure that the recommended security settings are implemented	• *SG.AT-3 Security Training*
• The integrator/installer uses validated cryptography, does not use deprecated cryptographic suites in new systems beyond their expiration dates, and provides migration paths for older systems using deprecated cryptographic suites	• *SG.SC-12 Use of Validated Cryptography*
• The integrator/installer certifies that they are supplying equipment from manufacturers who are certified as providing security-enabled equipment	• *SG.SA-2 Security Policies for Contractors and Third Parties* • *SG.SA-4 Acquisitions* • *SG.SA-11 Supply Chain Protection*
• The integrator/installer implements redundant DER systems for installations with critical load requirements	• *SG.CP-11 Fail-Safe Response* • *SG.SC-5 Denial of Service Protection*
• The integrators, installers, or manufacturers, in conjunction with utilities and regulators, establish, install, and test the default settings in the DER system for different failure/attack scenarios	• *SG.CP-11 Fail-Safe Response*

4.4.3 User (and Device): Access Requirements

Authentication of users and automated devices to the DER systems is the most critical communications cybersecurity requirement. Generally, confidentiality is less important, although privacy for customer-owned DER systems may be more important. Users may access DER systems directly through a local HMI while other devices may exist on the same local network. Remote access by users and devices would entail access via a network.

Table 7: User and Device Access Requirements

Cybersecurity Requirements for Mitigating Impacts Protection Measures Before an Attack or Failure	***NISTIR 7628 Catalog of Cybersecurity Requirements***
• Access security measures meet the utility interconnection requirements, if any, for autonomous DER systems	• *SG.AC-4 Access Enforcement*
• All access to the DER system requires authentication. Some access may require confidentiality as well. Some access may require non-repudiation via digital signatures	• *SG.AC-4 Access Enforcement* • *SG.IA-4 User Identification and Authentication* • *SG.IA-5 Device Identification and Authentication*
• Users and devices are individually identified and authenticated with access permissions established by their role	• *SG.IA-4 User Identification and Authentication* • *SG.IA-5 Device Identification and Authentication*
• The DER system requires unique username/ password access protection for all user interface interactions and prevents the use of factory-set default access passwords after installation	• *SG.IA-4 User Identification and Authentication* • *SG.AC-4 Access Enforcement* • *SG.AC-6 Separation of Duties* • *SG.AC-7 Least Privilege* • *SG.AC-21 Passwords*
• Only “advanced users” are allowed to make modifications through added layers of role-based access, password and certificate mechanisms	• *SG.CM-5 Access Restrictions for Configuration Change*
• The DER system only permits authorized devices to access its information and provide settings and commands, typically through certificates	• *SG.AC-4 Access Enforcement* • *SG.IA-5 Device Identification and Authentication*
• Role-based access permissions can be established for individual data elements, for groups of data elements, and for resources	• *SG.CM-11 Configuration Management Plan*
• Memory for passwords and other private or confidential information is encrypted or otherwise secured against unauthorized access	• *SG.SI-7 Software and Information Integrity* • *SG.SC-26 Confidentiality of Information at Rest*
• The privacy of information from or about customer-owned DER systems, including their functionality, output, and operational settings is maintained as appropriate	• *SG.PL-4 Privacy Impact Assessment* • *SG.SA-8 Security Engineering Principles*

Cybersecurity Requirements for Mitigating Impacts Protection Measures Before an Attack or Failure	*NISTIR 7628 Catalog of Cybersecurity Requirements*
• The confidentiality of information from or about DER systems, including their functionality, output, and operational settings is maintained as appropriate	• *SG.SA-8 Security Engineering Principles* • *SG.SC-9 Communication Confidentiality*
• Messages received or sent from DER systems cannot be repudiated	• *SG.AU-16 Non-Repudiation*

4.4.4 ICT Designers: Cybersecurity Requirements for DER Communications

Information and Communication Technologies (ICT) cover communication media, communication networks, communication protocols, and information modelling. Cybersecurity for these ICT elements is crucial to safe and reliable operation of DER systems.

DER systems can operate autonomously and are expected to do so most of the time. However DER owners and other authorized users may access the DER systems through a local network to modify settings, perform maintenance, update software, and test the systems.

Table 8: Communication Network and Protocols Cybersecurity Requirements

Cybersecurity Requirements for Mitigating Impacts Protection Measures Before an Attack or Failure	*NISTIR 7628 Catalog of Cybersecurity Requirements*
• Networks use gateways, secure routers, and firewall protection at domain boundaries, for instance using Energy Service Interfaces (ESIs) at customer service points	• *SG.SC-7 Boundary Protection*
• DER system information is exchanged only over secured network channels	• *SG.SC-7 Boundary Protection SG.CM-5 Access Restrictions for Configuration Change*
• Networks on shared media use secure technologies such as VPNs or MPLS to protect DER information	• *SG.SC-7 Boundary Protection*
• Network components are hardened with only essential applications installed and only necessary ports enabled	• *SG.CM-7 Configuration for Least Functionality*
• Communication networks will use Quality of Service (QoS) or other resource management techniques to ensure that higher priority traffic takes precedence over lower priority traffic	• *SG.SC-5 Denial of Service Protection*
• Network and system management capabilities with security are installed to monitor the status of all DER networks and all components connected to the networks, to detect intrusions, to protect against intrusions, to log all network changes, and to notify appropriate people of suspect changes	• *SG.AU-6 Audit Monitoring, Analysis, and Reporting* • *SG.AU-3 Content of Audit Records* • *SG.SC-5 Denial of Service Protection*

Cybersecurity Requirements for Mitigating Impacts Protection Measures Before an Attack or Failure	*NISTIR 7628 Catalog of Cybersecurity Requirements*
• Redundant networks are used for critical information flows	• *SG.SC-5 Denial of Service Protection*
• DER system network interface design prevents anyone from making insecure network settings	• *SG.CM-5 Access Restrictions for Configuration Change*
• Communication protocols are well-established international standards with security	• *SG.SA-8 Security Engineering Principles*
• Communication protocols used between DER system components are required to authenticate all messages, including their source and destinations	• *SG.IA-4 User Identification and Authentication* • *SG.IA-5 Device Identification and Authentication* • *SG.SC-20 Message Authenticity*
• Communication protocols used to manage DER systems validate the integrity of the data in transit, including protection against man-in-the-middle, replay, and non-repudiation. In particular, passwords are never sent in the clear	• *SG.SC-8 Communication Integrity*
• Communication protocols used for confidential or private information must ensure confidentiality of this information in transit	• *SG.SC-9 Communication Confidentiality* • *SG.SC-26 Confidentiality of Information at Rest*
• Communication protocols 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	• *SG.SC-12 Use of Validated Cryptography*
• Key management system ensures that the DER systems have valid cybersecurity certificates before communications are established	• *SG.SC-11 Cryptographic Key Establishment and Management*
• Key management system ensures that the DER systems have access to certificate revocation lists in a timely manner	• *SG.SC-11 Cryptographic Key Establishment and Management*
• DER system networks use communications partitioning to ensure DER systems cannot inadvertently connect to a rogue network	• *SG.SC-2 Communications Partitioning* • *SG.SC-18 System Connections*
• DER system settings are designed by integrators to ensure they are constrained from joining unauthorized networks	• *SG.SC-2 Communications Partitioning* • *SG.AC-16 Wireless Access Restrictions*
• A compromised DER system does not permit unauthorized access through the communications network to other DER systems or to other entities	• *SG.SC-2 Communications Partitioning*
• DER systems that may be accessed through the Internet has additional Internet security features including protection from malware	• *SG.SC-8 Communication Integrity* • *SG.SI-3 Malicious Code and Spam Protection*

Cybersecurity Requirements for Mitigating Impacts Protection Measures Before an Attack or Failure	*NISTIR 7628 Catalog of Cybersecurity Requirements*
• The DER system detects network and protocol permanent errors and failures, and enters a default "isolated" state, which may include changing functional settings, restarting the communication connection process, or shutting down	• *SG.SC-22 Fail in Known State*

4.4.5 Security Managers: Alarming, Logging, and Reporting Cybersecurity Requirements

Alarming of significant events is critical for real-time operations of cyber-physical systems so that security personnel, operational personnel, and other systems can be notified of potential failures and attacks. These alarms and other more routine events should also be logged for future reporting, particularly if forensic analysis is needed of anomalous activities. All cyber-physical and cybersecurity-related alarms should notify appropriate personnel, termed the "DER manager".

Table 9: Alarming, logging and reporting cybersecurity requirements

Cybersecurity Requirements for Mitigating Impacts Protection Measures Before an Attack or Failure	*NISTIR 7628 Catalog of Cybersecurity Requirements*
• One or more "DER security managers" are established who are responsible for receiving notifications of anomalous events, including cybersecurity events	• *SG.IR-2 Incident Response Roles and Responsibilities*
• The DER system issues alarms to notify the DER security manager when events occur that indicate significant situations or actions that were not commanded, or vice versa, lack of action in response to a command	• *SG.IR-7 Incident Reporting* • *SG.SI-4 Smart Grid Information System Monitoring Tools and Techniques*
• The DER system logs all significant events and ensures authorized access to these logs. These events include DER system events, physical events, power system events, manual overrides, communication network events, security events, user actions, actions triggered by other systems, and errors	• *SG.AU-2 Auditable Events* • *SG.AU-3 Content of Audit Records* • *SG.AU-6 Audit Monitoring, Analysis, and Reporting*
• Time synchronization provides adequate precision and accuracy to ensure that the timestamps of audit logs capture a series of events truly chronologically with the necessary time resolution	• *SG.AU-8 Time Stamps*
• The DER system prevents modifications to audit logs and/or logs all modifications to those logs	• *SG.AU-5 Response to Audit Processing Failures* • *SG.AU-9 Protection of Audit Information*
• The audit trail provides forensic information including back to the original audit entries	• *SG.AU-9 Protection of Audit Information*

4.4.6 Testing and Maintenance Personnel: Cybersecurity Requirements for Testing, Maintenance, and Updating Systems

All DER systems require testing both in the factory and once installed in the field to ensure that their functionality and security actually perform as designed and as required. Additional testing should take place after maintenance and after any updates before the DER system is certified as functional and secure.

Maintenance, particularly cyber maintenance such as software/firmware patching and upgrades, should involve stringent procedures, including factory functional and security testing, roll-back procedures, and re-testing of the systems after installation. In particular, security software/firmware maintenance should be thoroughly tested before installations

Table 10: Testing, maintenance, and updating cybersecurity requirements

Cybersecurity Requirements for Mitigating Impacts Protection Measures Before an Attack or Failure	***NISTIR 7628 Catalog of Cybersecurity Requirements***
• DER systems are factory tested for cyber-physical security issues	• *SG.SI-6 Security Functionality Verification*
• Purchased equipment and updated DER systems are tested for its security capabilities, any holes in its security through fuzzing and other methods, and the presence of any malware	• *SG.SI-3 Malicious Code and Spam Protection*
• Start-up, restart, and anomalous events cause the DER system to perform a self-test, including integrity and reasonability testing of all key functional and security settings	• *SG.SI-6 Security Functionality Verification* • *SG.SI-7 Software and Information Integrity*
• Maintenance schedules of any DER systems deemed "critical" to the utility are provided to and/or approved by the utility, as per interconnection contracts	• *SG.MA-3 Smart Grid Information System Maintenance*
• Maintenance is permitted only by security-certified maintenance organizations	• *SG.MA-3 Smart Grid Information System Maintenance*
• Maintenance tools are protected from unauthorized use	• *SG.MA-3 Smart Grid Information System Maintenance*
• Contractual arrangements with authorized integrators for software updates and patches, including applications, databases, and operating systems, are provided to ensure that these are managed properly and securely for the life of the DER system	• *SG.CM-3 Configuration Change Control*
• Remote access for maintenance uses 2-factor authentication or other strong authentication measures	• *SG.IA-4 User Identification and Authentication*
• Local access for maintenance requires that any laptops or other maintenance equipment connected to the DER system has been scanned for malware	• *SG.SI-3 Malicious Code and Spam Protection*

Cybersecurity Requirements for Mitigating Impacts Protection Measures Before an Attack or Failure	*NISTIR 7628 Catalog of Cybersecurity Requirements*
• Patches to DER system software are applied using strong patch management procedures, including certification by the integrator/manufacturer on its security and functionality, assessment by security anti-virus programs, testing on redundant or backup systems first (if possible), and ability to rollback or de-install the patch	• *SG.CM-3 Configuration Change Control* • *SG.CM-4 Monitoring Configuration Changes*
• Equipment is retested after maintenance for its security capabilities and the presence of any malware	• *SG.SI-3 Malicious Code and Spam Protection*
• All maintenance and testing events are captured in audit logs	• *SG.AU-3 Content of Audit Records*

4.4.7 Possible Mitigations During an Attack or Failure

Although the prevention of attacks or failures is the most effective approach, DER systems will be successfully attacked or will fail. Therefore it is critical to plan for those eventualities by preparing mitigation techniques and procedures.

The first requirement is to detect anomalous events that could signal an attack or failure. Then notifications of these anomalous events must be sent to the appropriate "DER manager". The DER system can then take steps to mitigate the impact of the situation.

Table 11: Possible mitigations during an attack or failure

Cybersecurity Requirements for Mitigating Impacts Protection Measures During an Attack or Failure	*NISTIR 7628 Catalog of Cybersecurity Requirements*
• When DER electrical output (voltage, vars, watts) is outside the "normal" range, it is logged and/or an alarm is sent to the "DER manager"	• *SG.AU-2 Auditable Events* • *SG.IR-7 Incident Reporting* • *SG.IR-9 Corrective Action* • *SG.SI-9 Error Handling*
• DER system monitors critical data from multiple sources and selects the one "most likely" to be correct	• *SG.SI-6 Security Functionality Verification*
• Backup versions of DER system software are available to restore the system at least to a default level	• *SG.SC-5 Denial-of-Service Protection*
• Loss of communications between DER components are timestamped, logged, and issued as an alarm to the "DER manager"	• *SG.AU-2 Auditable Events* • *SG.IR-7 Incident Reporting*
• All uncommanded or suspect network configuration changes are timestamped, logged, and issued as an alarm to the "DER manager"	• *SG.AU-2 Auditable Events* • *SG.IR-7 Incident Reporting*
• All invalid user access attempts to the DER system are timestamped, logged, and issued as an alarm to the "DER manager"	• *SG.AU-2 Auditable Events* • *SG.IR-7 Incident Reporting*

Cybersecurity Requirements for Mitigating Impacts Protection Measures During an Attack or Failure	*NISTIR 7628 Catalog of Cybersecurity Requirements*
• All uncommanded or suspect DER system setting changes are timestamped, logged, and issued as an alarm to the "DER manager"	• *SG.AU-2 Auditable Events* • *SG.IR-7 Incident Reporting*
• Where available, Intrusion Detection Systems (IDS) notifies the "DER manager" of suspected intrusions	• *SG.IR-7 Incident Reporting*
• Upon detection of an attack or failure, the DER system self-limits output to default output settings of reasonable or contractual limits, regardless of actual settings	• *SG.CP-11 Fail-Safe Response*
• Upon detection of an attack or failure, the DER system shuts down if default settings also fail to keep DER system within the "hard-wired" DER settings	• *SG.CP-11 Fail-Safe Response*
• If the DER system is still operational at the default output settings, but a communication network anomaly persists, the DER systems reverts to the default network configuration	• *SG.CP-11 Fail-Safe Response*
• If the attack or failure appears to be caused by the communications network, disconnect the DER system from any external networks and go into the default "isolated" state	• *SG.CP-11 Fail-Safe Response*
• If the attack still appears to be underway, disconnect DER system from the grid and turn it off	• *SG.CP-11 Fail-Safe Response*
• If the attack or failure is affecting the DER system operation, shut down the DER system	• *SG.CP-11 Fail-Safe Response*
• The DER system combines the information from an intrusion detection system with the state estimation information to determine which data may be compromised and not to be trusted	• *State estimation and intrusion detection*

4.4.8 Possible Mitigations After an Attack or Failure

After an attack or failure, the primary effort needs to be the restoration of the proper DER system operations after testing and verifying the security and safety of the DER system. Once the system is operational again, forensic analysis of the cause of the problem needs to be undertaken, while authorities need to be notified of the incident, particularly if the attack appears malicious.

Table 12: Possible mitigations after an attack or failure

Cybersecurity Requirements for Mitigating Impacts Protection Measures After an Attack or Failure	*NISTIR 7628 Catalog of Cybersecurity Requirements*
• Scan and disconnect any unauthorized entities connected to the DER system network (users, applications, viruses, etc.)	• *SG.IR-9 Corrective Action*
• Rerun initial installation network configuration	• *SG.IR-9 Corrective Action*
• Reset / restart / rerun all network security processes	• *SG.IR-9 Corrective Action*
• Re-establish known and authorized network configuration changes	• *SG.IR-9 Corrective Action*
• Restart DER system and monitor for any anomalous behavior	• *SG.IR-9 Corrective Action*
• Report incident to "authorities" such as utility, energy service provider, integrator, or other	• *SG.IR-7 Incident Reporting*
• Take any actions necessary to prevent incident from happening again	• *SG.IR-8 Incident Response Investigation and Analysis*
• If privacy or confidentiality is suspected of being compromised, notify all affected stakeholders	• *SG.SC-26 Confidentiality of Information at Rest*

5. Level 2: Facilities DER Energy Management (FDEMS) Cybersecurity Requirements

5.1 Level 2 FDEMS: Architecture

The Facilities DER Energy Management System (FDEMS) manages combinations of DER generation, DER storage, and customer loads at a residential, commercial, and industrial customer site as illustrated in Figure 5.

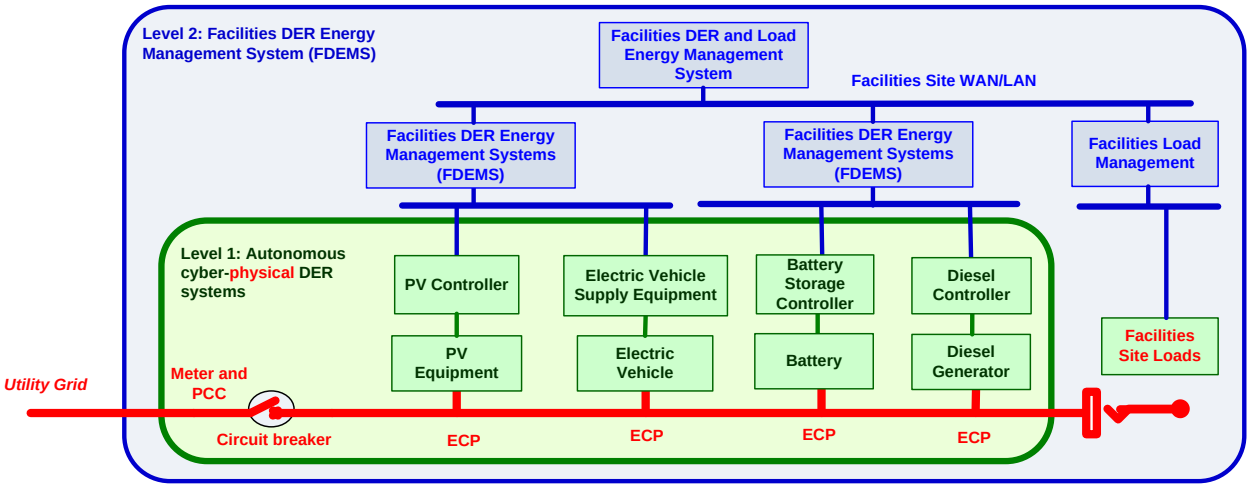


Figure 5: Level 2 FDEMS

The DER failure scenarios in this section focus on attacks by threat agents on a Facilities DER Energy Management system (FDEMS). These DER systems are typically installed at one residential home, a community of homes, or commercial/industrial customer sites, such as shopping centers, university campuses, and hospital complexes. They can act as microgrids that may still be connected to the grid, but can also operate in islanded mode. Layered FDEMS are typically connected via facility LANs or, if dispersed across larger territories, by WANS.

Attacks on the 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 integrator finances and reputation, and to a limited degree, utility reputation. The owners of these FDEMS generally do not have the sophistication to manage complex cybersecurity measures, while expensive security measures would typically not be cost-beneficial.

Attacks on larger FDEMS systems could impact utility operations by causing power system instability and potentially outages.

5.2 Level 2 FDEMS: Cybersecurity Vulnerabilities

FDEMS are located in customer sites with unknown security policies and security implementations. At the same time, they are generally general purpose systems (as

opposed to the specialized DER controller systems), whose operating systems, communication networks, and software applications have well-known vulnerabilities. They are also often not isolated to just connections with DER systems but also connected over the communication networks with other general computer systems.

This environment makes FDEMS very vulnerable to many types of attacks for many different purposes. These attack purposes could include:

- Attacks for personal notoriety or reputation:
  - Demonstrate personal ability to modify DER operations as an example of hacking expertise
  - Take revenge on utilities by disrupting DER operations
  - Demonstrate personal ability to cause harm to power system equipment by modifying DER safety systems
- Attacks for financial gain:
  - Steal intellectual property from the FDEMS on DER capabilities
  - Cause power outage of competitor by disabling the competitor's DER systems
  - Cause widespread outage that benefits the attacker's reputation or financial position
  - Send invalid market signals to competitor on the prices of energy and ancillary services, to gain market advantage
  - Modify the FDEMS applications and databases for managing its DER systems
  - Steal competitor's DER future plans and constraints to gain market advantage
- Terrorist attacks for political gain:
  - Cause local outages
  - Cause widespread outages by coordinated attacks against multiple FDEMS
  - Damage equipment
  - Harm personnel

In addition to deliberate attacks with specific purposes, inadvertent mistakes can also threaten the proper operation of the FDEMS

- Inadvertent mistakes
  - Cause local outages
  - Damage equipment
  - Harm personnel
  - Cause financial losses
  - Cause non-optimal participation in the market
  - Provide competitor with private/confidential information

5.3 Level 2 FDEMS: Impacts Due to FDEMS Failures

In the Level 2 environment, malicious attacks or inadvertent failures of a single FDEMS generally affect only a small number of DER systems. Typically these attacks or failures

would not affect the utility grid, but could cause serious electrical and/or financial problems for the site. In some cases where the FDEMS is particularly critical to reliable power grid operations, the attacks or failures could cause cascading electrical problems on the utility grid.

FDEMS attacks or failures may impact operations in a number of different ways.

- Denial of Service: The FDEMS could cease to provide the DER systems with updated information such as schedules.
- Integrity violation: The FDEMS could provide invalid settings to the DER systems or report invalid information to utilities or REPs.
- Confidentiality / privacy violation: Confidential or private information could be taken from the FDEMS
- Non-repudiation violation: The FDEMS either repudiates an action or fails to confirm an action.

Table 13: Level 2 impact severities due to malicious attacks and failures of FDEMS

Type of impact	Specific impacts	Severity
Scale impact	Single FDEMS only	L or M depending on facility generation size and locations
Safety impact	If the FDEMS failure causes DER failures, then outages of customer facilities could cause safety situations, such as machinery stoppage or criminal actions during the blackout Electrical causes of damage, such as electrocution or burning of property Loss of power at medically sensitive locations, causing harm or death of patients, such as at hospitals	M typically or H if medical impact
Transmission power system operations impact	If the FDEMS is managing large amounts of DER generation and/or storage, or is located within a transmission substation, outages and power quality problems could affect transmission	L typically or M if large facility
Distribution power operations impact	Potential power quality impacts on the distribution feeder serving the facility, including voltage excursions, harmonics, and power outages of other customers on that feeder	M
Facility site(s) power system impact	Potential complete or partial outage of the facility	H
Utility financial impact	Any costs associated with power quality problems such as truck rolls or additional equipment inspections Possible legal costs if inadequate contingency analysis studies could be proved to have caused power outages to other customers on that feeder If utility equipment is destroyed or vandalized, the costs for repair or replacement	L L M

Type of impact	Specific impacts	Severity
Utility reputation impact	Only if the utility were responsible for the security of the FDEMS	L typically M if utility responsible
FDEMS owner financial impact	If DER systems go into safe default modes, then only minimal financial costs on DER equipment. The costs for the replacement energy that would be purchased from the utility until the FDEMS could be brought back on-line The costs for "cleaning up" or even replacing the FDEMS to remove any malware and to improve the cybersecurity mitigation capabilities If DER equipment is destroyed or vandalized, the costs for repair or replacement	L H H H
FDEMS owner confidentiality or privacy impact	If the confidential or private information located within the FDEMS is compromised, then the impact could be medium or high, depending upon the sensitivity of that information	M-H
Reputation impact on FDEMS owner / manager/ implementer	The reputation of the owner of the FDEMS could be hurt, which could lead to loss of business if the FDEMS attack/failure affected the owner's customers. For instance, if a REP owns and manages FDEMS at customer sites, they could lose some of their customers.	M
Integrator financial and reputation impact	The integrator could have financial and reputation impacts if the attack on the FDEMS could be shown to be due to inadequate integrator-implemented cybersecurity. The results could require, at a minimum, the patching or upgrading of all other FDEMS in the field. It also could lead to loss of business and litigation	M-H
Environmental impact	If the facility is directly managing environmental conditions such as a water treatment plant, loss of power could cause environmental damage Toxic material from damaged devices such as batteries could cause environmental harm people and locations Loss of power to life safety system in a manufacturing facility dealing with toxic material could cause environmental harm to people	M

5.4 Level 2 FDEMS: Cybersecurity Requirements and Possible Mitigations

The cybersecurity requirements and possible mitigations must reflect the need to design and install FDEMS at sites where the FDEMS owners generally have minimal cybersecurity expertise and where cost-effectiveness of the FDEMS functions are their primary goal. Therefore, cybersecurity should be designed into the FDEMS system, enabled "out of the box", without the requirement for the FDEMS owners to manage complex cybersecurity measures, and in fact only allowing advanced users from modifying cybersecurity measures.

The most important types of cybersecurity requirements are those that deter or defer attacks before they can cause any damage. Many of these involve policies and procedures, while a few involve the implementation of cybersecurity technologies. However, it is also very important to mitigate the impacts of an attack or failure during and after the event.

The following table describes cybersecurity requirements and mitigation techniques to take before, during, and after an attack or failure. The first column identifies the cybersecurity requirements for mitigating the impacts. The second column lists the relevant NISTIR 7628 Catalog of Cybersecurity Requirements. The third column provides a checklist that could be used in utility specifications for FDEMS systems that are applying to be interconnected to the utility's grid.

These table entries are organized by the following categories:

1. Manufacturer design of FDEMS cybersecurity requirements
2. Integrators and installer cybersecurity requirements
3. User and system access requirements
4. Information and communication technology (ICT) cybersecurity requirements
5. Alarming, logging, and reporting cybersecurity requirements
6. Testing, maintenance, and updating cybersecurity requirements
7. Possible mitigations during a cyber attack or failure
8. Possible mitigations after a cyber attack or failure

5.4.1 Manufacturer: Design of FDEMS Cybersecurity Requirements

Although FDEMS are typically built from general purpose computers, they are acting as control systems. These control systems should have cybersecurity designed into their operating system, software applications, and ICT capabilities. Some of the cybersecurity requirements reflect the need to protect cyber-physical systems, such as the DER systems and the power grid, against malicious or inadvertent settings that could cause unsafe conditions, physical harm, or electrical consequences.

Table 14 identifies the key cybersecurity methods and technologies that the manufacturer of FDEMS should design into their applications and their systems, although the actual settings would be established during deployment and operations.

Table 14: Manufacturer Design of FDEMS Cybersecurity Requirements

Cybersecurity Requirements for Mitigating Impacts Protection Measures Before an Attack or Failure	***NISTIR 7628 Catalog of Cybersecurity Requirements***
• The FDEMS is designed such that all access by users and by external applications is authenticated, including the DER systems that the FDEMS manages.	• SG.IA-4 User Identification and Authentication • SG.IA-5 Device Identification and Authentication • SG.AC-14 Permitted Actions without Identification or Authentication
• The FDEMS is designed with the mandatory use of role-based access control that establishes role-based permissions for each of its applications, databases, and functions. Each external user and application must be identified and assigned to a role.	• SG.IA-4 User Identification and Authentication
• The FDEMS is designed such that only essential software and applications are installed and that unnecessary ports are deactivated.	• *SG.CM-7 Configuration for Least Functionality*
• The manufacturers of FDEMS use penetration testing to ensure their systems are well-protected	• *SG.SI-6 Security Functionality Verification*
• FDEMS applications are designed to check voltage, real power output, reactive power, and other power settings against valid limits before sending them to the DER systems that it manages, in order to prevent harm to the equipment.	• *SG.CM-2 Baseline Configuration*
• FDEMS applications are designed to check voltage, real power output, reactive power, and other power settings against ECP and PCC limits to ensure that no setting changes can exceed these limits at the ECPs and PCCs, and thus harm the power grid.	• *SG.CM-2 Baseline Configuration*
• The FDEMS is designed to constrain what security settings can be changed remotely, thus requiring some changes be permitted only within the security perimeter surrounding the FDEMS.	• *SG.AC-15 Remote Access* • *SG.CM-5 Access Restrictions for Configuration Change*
• The FDEMS contains secure firmware or hardware memory for passwords and other embedded private or confidential information that is encrypted or otherwise secured against unauthorized access	• *SG.SI-7 Software and Information Integrity* • *SG.SC-26 Confidentiality of Information at Rest*
• The FDEMS applications validate even authorized changes to DER operational settings against what those settings are reasonably or contractually allowed to be	• *SG.CM-4 Monitoring Configuration Changes* • *SG.CM-6 Configuration Settings* • *SG.SI-8 Information Input Validation*

Cybersecurity Requirements for Mitigating Impacts Protection Measures Before an Attack or Failure	*NISTIR 7628 Catalog of Cybersecurity Requirements*
• The FDEMS is designed to be able to reject any compromised or invalid data, while that event is logged and appropriate entities (people or systems) are notified.	• *SG.AU-2 Auditable Events* • *SG.IR-7 Incident Reporting* • *SG.IR-9 Corrective Action* • *SG.SI-9 Error Handling*
• For important functionality, the FDEMS is designed to be able to monitor more than one source of critical data and has an algorithm to determine the one that is "most likely" to be correct	• *SG.SC-5 Denial of Service Protection* • *SG.SC-8 Communication Integrity*
• FDEMS applications are designed to use heartbeat concepts to detect DER system failures.	• *SG.SI-9 Error Handling*
• The FDEMS is designed to be able to detect errors and failures in the DER systems it manages, and to establish a pre-set "failure" state for those failed DER systems, which may include limiting functionality, restarting, or shutting down	• *SG.SC-22 Fail in Known State*
• The FDEMS is designed to segregate different types of non-sensitive data, private data, commercially sensitive data, and other categories. The FDEMS applies appropriate role-based permissions to each type of data.	• *SG.CM-7 Configuration for Least Functionality*
• Security functions in the FDEMS are designed to be isolated from non-security functions.	• *SG.SC-3 Security Function Isolation*
• The FDEMS is designed to provide an emergency manual override capability that shuts down the system.	• *SG.SI-9 Error Handling*

5.4.2 Integrators and Installer: FDEMS Cybersecurity Requirements

Integrators and installers of FDEMS may or may not work for the manufacturer of the FDEMS, but regardless their roles and responsibilities are different.

Integrators and installers of FDEMS should take the responsibility to ensure that all appropriate cybersecurity measures are "turned on" when the FDEMS is installed, that role-based access control permissions are properly established, and that unnecessary ports and applications are removed or disabled. Since manufacturers usually include options for different types and levels of security, it is up to the integrators and installers to meet the FDEMS owner cybersecurity requirements (which may be mandated by the utility interconnection requirements) through the appropriate selection and testing of the cybersecurity cryptography suites, methods for establishing secure channels, and implementing appropriate key management processes.

Table 15 identifies the key cybersecurity settings that the integrator and installer of FDEMS should establish as they deploy the system.

Table 15: Integrator and Installer FDEMS Cybersecurity Requirements

Cybersecurity Requirements for Mitigating Impacts Protection Measures Before an Attack or Failure	***NISTIR 7628 Catalog of Cybersecurity Requirements***
• The integrator/installer ensures that security of the FDEMS is enabled "out-of-the-box.	• *SG.CM-2 Baseline Configuration* • *SG.CM-10 Factory Default Authentication Management*
• The integrator/installer implements the FDEMS so that all access by users, DER systems, and all external applications is authenticated.	• *SG.IA-4 User Identification and Authentication* • *SG.IA-5 Device Identification and Authentication* • *SG.AC-14 Permitted Actions without Identification or Authentication*
• The integrator/installer establishes the role-based access control roles and permissions, and links them to each of its applications, databases, and functions.	• *SG.IA-4 User Identification and Authentication* • *SG.AC-6 Separation of Duties*
• The integrator/installer ensures that at least one role is permitted to receive security alarms and to modify security settings.	• *SG.CM-5 Access Restrictions for Configuration Change*
• The integrator/installer ensures that only the necessary rights and privileges are assigned to each role that will have access to the FDEMS.	• *SG.AC-7 Least Privilege*
• Role-based access permissions can be established for individual data elements, for groups of data elements, and for resources.	• *SG.CM-11 Configuration Management Plan*
• The integrator/installer ensures that only strong passwords are permitted as authentication, and prevents the use of factory-set default access passwords after installation.	• *SG.AC-21 Passwords*
• If biometric or other authentication methods are used, the integrator/installer ensures that these are adequately strong.	• *SG.IA-4 User Identification and Authentication*
• The integrator/installer ensures that unsuccessful login attempts into the FDEMS are logged and the appropriate users are notified.	• *SG.AC-8 Unsuccessful login attempts*
• The integrator/installer ensures that logins should time out if there is no user activity within a preset period of time.	• *SG.AC-12 Session Lock*
• The integrator/installer ensures that modifications to the security settings can only be undertaken by users assigned to the security management role.	• *SG.CM-3 Configuration Change Control* • *SG.SC-29 Application Partitioning*
• The integrator/installer ensures that only essential software and applications are deployed and that unnecessary ports are deactivated.	• *SG.CM-7 Configuration for Least Functionality* • *SG.SC-7 Boundary Protection*

Cybersecurity Requirements for Mitigating Impacts Protection Measures Before an Attack or Failure	*NISTIR 7628 Catalog of Cybersecurity Requirements*
• The integrators/installers who maintain backdoor access to the FDEMS ensure this access is only available through role-based access control on a specific port.	• *SG.CM-7 Configuration for Least Functionality* • *SG.SC-7 Boundary Protection*
• The integrator/installer selects and implements appropriate levels of security to meet the FDEMS owner's and the utility's interconnection security requirements.	• *SG.CM-2 Baseline Configuration*
• The integrator/installer ensures that all modifications to FDEMS applications, settings, security audit logs and security parameters are associated with a specific identity through the role-based access process.	• *SG.AU-16 Non-repudiation*
• If pre-shared secret cryptographic keys are used for the DER systems that are managed by the FDEMS, the integrator/installer ensures that these cryptographic keys are securely protected during deployment.	• *SG.SC-11 Cryptographic Key Establishment and Management* • *SG.IA-5 Device Identification and Authentication*
• If PKI is used to establish cryptographic keys, the integrator/installer ensures the appropriate certificates are valid for the FDEMS and for the DER systems it manages.	• *SG.SC-11 Cryptographic Key Establishment and Management* • *SG.IA-5 Device Identification and Authentication*
• The integrator/installer ensures that separate security keys are used for different types of functions, such as for operations versus maintenance.	• *SG.SC-11 Cryptographic Key Establishment and Management* • *SG.IA-5 Device Identification and Authentication*
• The integrator/installer ensures that all data exchanged between the FDEMS and its DER systems is protected to detect and reject unauthorized modifications. These data exchanges are typically point-to-point, multi-drop, and/or across local networks.	• *SG.SC-8 Communication Integrity* • *SG.SC-20 Message Authenticity*
• The integrator/installer ensures that the FDEMS software validates all modifications to DER settings as reasonable, to avoid safety problems and/or equipment damage.	• *SG.SI-7 Software and Information Integrity*
• Since some DER information in the FDEMS is sensitive for privacy, intellectual property or financial reasons, the integrator/installer ensures this sensitive data is protected as confidential both within the FDEMS and whenever transmitted.	• *SG.SC-9 Communication Confidentiality* • *SG.SC-26 Confidentiality of Information at Rest*
• The integrator/installer ensures that security information (e.g. passwords and certificates) are strongly protected through cryptographic means.	• *SG.SC-26 Confidentiality of Information at Rest*
• The integrator/installer ensures that the FDEMS logs all significant cybersecurity events that may indicate a cyber security attack. These event logs permit cyber security assessments to determine if an attack is occurring and what the nature of the attacks is.	• *SG.AU-2 Auditable Events*

Cybersecurity Requirements for Mitigating Impacts Protection Measures Before an Attack or Failure	*NISTIR 7628 Catalog of Cybersecurity Requirements*
• The integrator/installer ensures that the FDEMS time is being synchronized with an adequate accuracy, and that all audit logs include an accurate time stamp, the type of event, a description of the event, the context of the event, the status of the system when the event took place.	• *SG.AU-8 Time Stamps* • *SG.AU-3 Contents of Audit Records*
• The integrator/installer includes notices of legal actions that will be taken if a "threat agent" does try to manipulate FDEMS settings or access confidential/private information.	• *SG.AC-9 Smart Grid Information System Use Notification*
• The integrator/installer provides instructions or training to FDEMS owners on security requirements so they won't try to bypass security settings.	• *SG.AT-2 Security Awareness* • *SG.AT-5 Contact with Security Groups and Associations*
• Installers are trained appropriately to ensure that the recommended security settings are implemented.	• *SG.AT-3 Security Training*
• The integrator/installer permits only validated cryptography to be deployed between the FDEMS and the DER systems, does not use deprecated cryptographic suites in new systems beyond their expiration dates, and provides migration paths for older DER systems or older FDEMS that are using deprecated cryptographic suites.	• *SG.SC-12 Use of Validated Cryptography*
• The integrator/installer certifies that they are supplying equipment from manufacturers who are certified as providing security-enabled equipment.	• *SG.SA-2 Security Policies for Contractors and Third Parties* • *SG.SA-4 Acquisitions* • *SG.SA-11 Supply Chain Protection*
• The integrator/installer implements redundant FDEMSs for installations with critical DER system management requirements.	• *SG.CP-11 Fail-Safe Response* • *SG.SC-5 Denial of Service Protection*
• The integrators, installers, or manufacturers, in conjunction with utilities and regulators, establish, install, and test the default settings in the FDEMS for different failure/attack scenarios.	• *SG.SA-10 Developer Security Testing* • *SG.CP-11 Fail-Safe Response*

5.4.3 Users and Applications: Access Requirements

During operations, the authentication of users and applications who are accessing the FDEMS is the most critical communications cybersecurity requirement. Generally, confidentiality is less important, although privacy for customer-owned DER systems may be more important. Particularly if the FDEMS is connected to the DER systems via a network that is used for other functions, authentication of all interactions is crucial to the safety and reliability of DER operations. For instance, a Home Area Network (HAN) may be used to network various appliances as well as the DER systems to a customer energy management

system which contains the FDEMS applications as well as washing machine management applications and home entertainment control functions.

Table 16 identifies the key cybersecurity requirements for users and applications that are accessing the FDEMS.

Table 16: User and Application Access Requirements

Cybersecurity Requirements for Mitigating Impacts Protection Measures Before an Attack or Failure	***NISTIR 7628 Catalog of Cybersecurity Requirements***
• All users and applications are uniquely identified.	• *SG.IA-4 User Identification and Authentication*
• Users create strong passwords, establish biometric identification methods, or utilize dongles or other strong authentication methods.	• *SG.AC-21 Passwords* • *SG.IA-4 User Identification and Authentication*
• Users login to the FDEMS via username and password or one of the other authentication methods.	• *SG.AC-4 Access Enforcement*
• All users and applications are assigned to one or more roles.	• *SG.AC-6 Separation of Duties* • *SG.AC-7 Least Privilege*
• All access and interactions with the FDEMS by users, DER systems, and external applications require authentication and an association with a role. Some access may also require confidentiality and some access may require non-repudiation via digital signatures.	• *SG.AC-4 Access Enforcement* • *SG.IA-4 User Identification and Authentication* • *SG.IA-5 Device Identification and Authentication*
• The FDEMS supports the requirement that passwords be changed periodically.	• *SG.AC-4 Access Enforcement* • *SG.AC-21 Passwords*
• The FDEMS only permits authenticated and authorized applications to access its information and modify settings and commands.	• *SG.AC-4 Access Enforcement* • *SG.IA-5 Device Identification and Authentication*
• Only users assigned to a security management role may make modifications to the security settings.	• *SG.CM-3 Configuration Change Control* • *SG.SC-29 Application Partitioning*
• Users assigned to a security management role should understand instructions or take training on security requirements.	• *SG.AT-2 Security Awareness* • *SG.AT-5 Contact with Security Groups and Associations*
• Users assigned to a security management role monitor the security situation, key management, and certificates, including any revocations, certificate expirations, and security alarms.	• *SG.AU-2 Auditable Events* • *SG.SC-11 Cryptographic Key Establishment and Management*
• Only users assigned to the “role modification” role are permitted to modify roles and/or to reassign users to different roles.	• *SG.CM-3 Configuration Change Control* • *SG.SC-29 Application Partitioning*

Cybersecurity Requirements for Mitigating Impacts Protection Measures Before an Attack or Failure	*NISTIR 7628 Catalog of Cybersecurity Requirements*
• Role-based access permissions can be established for individual data elements, for groups of data elements, and for resources	• *SG.CM-11 Configuration Management Plan*
• Only authenticated and authorized users and applications may access private and confidential information about DER systems, DER-owner/manager settings, etc. All transmission of this information is encrypted for confidentiality.	• *SG.PL-4 Privacy Impact Assessment* • *SG.SA-8 Security Engineering Principles* • *SG.SC-9 Communication Confidentiality*
• The role that receives security alarms or event notifications is always assigned to at least one user or application.	• *SG.AC-8 Unsuccessful login attempts* • *SG.AC-12 Session Lock*
• All modifications to FDEMS applications, settings, security audit logs and security parameters are associated with a specific identity through the role-based access process.	• *SG.AU-16 Non-repudiation*
• Certain types of messages received or sent from FDEMS can include digital signatures or other methods to ensure they cannot be repudiated.	• *SG.AU-16 Non-Repudiation*

5.4.4 ICT Designers: FDEMS Cybersecurity Requirements

The FDEMS communicates with sub-FDEMS and with the DER systems via communications networks using one or more communication protocols. The information models also may be different, depending upon the types of interactions and the design of the ICT systems. The communication media, communication networks, communication protocols, and information modelling should include cybersecurity to ensure secure operation of the FDEMS and the DER systems that it manages.

Table 17 identifies the key cybersecurity requirements for communications and protocols that are accessing the FDEMS.

Table 17: Communication Network and Protocols Cybersecurity Requirements

Cybersecurity Requirements for Mitigating Impacts Protection Measures Before an Attack or Failure	*NISTIR 7628 Catalog of Cybersecurity Requirements*
• Networks use gateways, secure routers, and firewall protection at domain boundaries, for instance using Energy Service Interfaces (ESIs) at customer service points	• *SG.SC-7 Boundary Protection*

Cybersecurity Requirements for Mitigating Impacts Protection Measures Before an Attack or Failure	*NISTIR 7628 Catalog of Cybersecurity Requirements*
• FDEMS and DER system information is exchanged only over secured network channels	• *SG.SC-7 Boundary Protection* • *SG.CM-5 Access Restrictions for Configuration Change*
• Networks on shared media use secure technologies such as VPNs or MPLS to protect DER information	• *SG.SC-7 Boundary Protection*
• Network components are hardened with only essential applications installed and only necessary ports enabled	• *SG.CM-7 Configuration for Least Functionality*
• Communication networks will use Quality of Service (QoS) or other resource management techniques to ensure that higher priority traffic takes precedence over lower priority traffic	• *SG.SC-5 Denial of Service Protection*
• Network and system management capabilities with security are installed to monitor the status of all FDEMS networks and all components connected to the networks, to detect intrusions, to protect against intrusions, to log all network changes, and to notify appropriate people of suspect changes	• *SG.AU-6 Audit Monitoring, Analysis, and Reporting* • *SG.AU-3 Content of Audit Records* • *SG.SC-5 Denial of Service Protection*
• Redundant networks are used for critical information flows	• *SG.SC-5 Denial of Service Protection*
• FDEMS network interface design prevents anyone from making insecure network settings	• *SG.CM-5 Access Restrictions for Configuration Change*
• Communication protocols are well-established international standards with security	• *SG.SA-8 Security Engineering Principles*
• Communication protocols used between the FDEMS and the DER systems are required to authenticate all messages, including their source and destinations	• *SG.IA-4 User Identification and Authentication* • *SG.IA-5 Device Identification and Authentication* • *SG.SC-20 Message Authenticity*
• Communication protocols used by the FDEMS to manage DER systems should validate the integrity of the data in transit, including protection against man-in-the-middle, replay, and non-repudiation. In particular, passwords are never sent in the clear	• *SG.SC-8 Communication Integrity*
• Communication protocols used for confidential or private information must ensure confidentiality of this information in transit.	• *SG.SC-9 Communication Confidentiality* • *SG.SC-26 Confidentiality of Information at Rest*

Cybersecurity Requirements for Mitigating Impacts Protection Measures Before an Attack or Failure	*NISTIR 7628 Catalog of Cybersecurity Requirements*
• Communication protocols 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.	• *SG.SC-12 Use of Validated Cryptography*
• Key management system ensures that the FDEMS and their DER systems have valid cybersecurity certificates or pre-shared keys before communications are established.	• *SG.SC-11 Cryptographic Key Establishment and Management*
• Key management system ensures that the DER systems have access to certificate revocation lists in a timely manner, either directly or via OCSP methods.	• *SG.SC-11 Cryptographic Key Establishment and Management*
• FDEMS networks use communications partitioning to ensure that none of the FDEMSs can inadvertently connect to a rogue network.	• *SG.SC-2 Communications Partitioning* • *SG.SC-18 System Connections*
• FDEMS settings are designed by integrators to ensure they are constrained from joining unauthorized networks.	• *SG.SC-2 Communications Partitioning* • *SG.AC-16 Wireless Access Restrictions*
• A compromised FDEMS does not permit unauthorized access through the communications network to other FDEMSs or to other entities.	• *SG.SC-2 Communications Partitioning*
• FDEMS that may be accessed through the Internet has additional Internet security features including strong protection against malware.	• *SG.SC-8 Communication Integrity* • *SG.SI-3 Malicious Code and Spam Protection*
• The FDEMS detects network and protocol permanent errors and failures, and enters a default “isolated” state, which may include changing functional settings, restarting the communication connection process, or shutting down	• *SG.SC-22 Fail in Known State*

6. Level 3: Utility/REP WAN Information & Communications Technology (ICT) Cybersecurity Requirements

TDB

6.1 Level 3 WAN ICT: Architecture

6.2 Level 3 WAN ICT: Cybersecurity Vulnerabilities

Most FDEMS will connect to external systems, possibly utility systems or market-based energy service providers (see Level 3). These connections may be over special well-protected networks or may utilize the Internet. In either case, the interactions will transverse the customer site perimeter and will necessitate the protection of systems on the customer site from external systems.

Level 3 communications 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 attacks since these attacks could cause injury to personnel, damage to equipment, and unstable power system conditions. Cyber attacks on financially-based control commands could cause financial losses as well as legal and regulatory actions.

Despite the vulnerabilities of these control commands to cyber attacks, utilities cannot generally use the same types of secure control as they use for utility-owned power system equipment. The reasons include:

- Different ownership: In general, utilities do not own the FDEMS equipment that they must interact with (the exception is if 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 trust that adequate and "well-known" protections are in place. However, since FDEMS are not owned by utilities, they cannot trust the cyber security protections to the same degree as they trust their own operational interactions.
- Different security domains: Since FDEMS are located in customer facilities, information exchanges between utility systems and FDEMS must cross security perimeters. These security perimeters must be protected against unauthorized access.
- Utilities cannot use the direct monitoring and control typically used by their SCADA systems for operating their own equipment. Instead, utilities would issue broadcast or multicast commands which often would not even include acknowledgments.
- Some information exchanges, particularly between REPs and FDEMS, may rely on the Internet, providing additional attack possibilities.

6.3 Level 3 WAN ICT: Impacts

TBD

Table 18: Level 1 impact severities due to malicious attacks and failures of individual autonomous DER systems

Type of impact	Specific impacts	Severity
Scale impact	Single DER systems only	L
Safety impact	Outages of customer facilities could cause safety situations, such as criminal actions during the blackout Electrical causes of damage, such as electrocution or burning of property Loss of power at medically sensitive locations, causing harm or death of patients, including hospitals	M unless medical impact: H
Transmission power system operations impact	*None likely* If located on a feeder within a transmission substation, distribution power quality problems could affect transmission	L
Distribution power operations impact	Potential power quality impacts on the distribution feeder serving the customer facility, including voltage excursions, harmonics, and power outages of other customers on that feeder	L
Customer site(s) power system impact	Potential complete or partial outage of the facility	H
Utility financial impact	Any costs associated with power quality problems such as truck rolls or additional equipment inspections Possible legal costs if inadequate contingency analysis studies could be proved to have caused power outages to other customers on that feeder If equipment is destroyed or vandalized, the costs for repair or replacement	L L M
Utility reputation impact	Only if the utility were responsible for the security of the customer's DER management system	L
DER owner financial impact	The costs for the replacement energy that would be purchased from the utility until the DER systems could be brought back on-line The costs for "cleaning up" the DER management system to delete any malware and to improve the cybersecurity mitigations If equipment is destroyed or vandalized, the costs for repair or replacement	H H H
DER owner privacy impact	If DER is connect to the HAN with other devices, then compromise of the DER could lead to compromises of other devices that have private information	L
DER ESP/ manager/ implementer reputation	The reputation of the manager of the DER management system could be hurt	M
Integrator financial and reputation impact	The integrator could have financial and reputation impacts if the unauthorized access to the DER management could be shown to be due to inadequate integrator-implemented cybersecurity. They would, at a minimum, require patching or upgrading systems in the field	M

Type of impact	Specific impacts	Severity
Environmental impact	If the facility is directly managing environmental conditions such as a water treatment plant, loss of power could cause environmental damage Toxic material from damaged devices such as batteries could cause environmental harm people and locations Loss of power to life safety system in a manufacturing facility dealing with toxic material could cause environmental harm to people	L

6.4 Level 3 WAN ICT: Cybersecurity Requirements and Possible Mitigations

The cybersecurity requirements and possible mitigations must reflect the need to design and install DER systems at sites where the DER owners have minimal cybersecurity expertise and where cost-effectiveness of the DER functions are their primary goal. Therefore, cybersecurity should be built into the DER system, enabled "out of the box", without the requirement for the DER owners to manage complex cybersecurity measures, and in fact only allowing advanced users from modifying cybersecurity measures.

The most important types of cybersecurity requirements are those that deter or defer attacks before they can cause any damage. Many of these involve policies and procedures, while a few involve the implementation of cybersecurity technologies. However, it is also very important to mitigate the impacts of an attack or failure during and after the event.

The following table describes cybersecurity requirements and mitigation techniques to take before, during, and after an attack or failure. The first column identifies the cybersecurity requirements for mitigating the impacts. The second column lists the relevant NISTIR 7628 Catalog of Cybersecurity Requirements[6]. The third column provides a checklist that could be used in utility specifications for DER systems that are applying to be interconnected to the utility's grid.

These table entries are organized by the following categories:

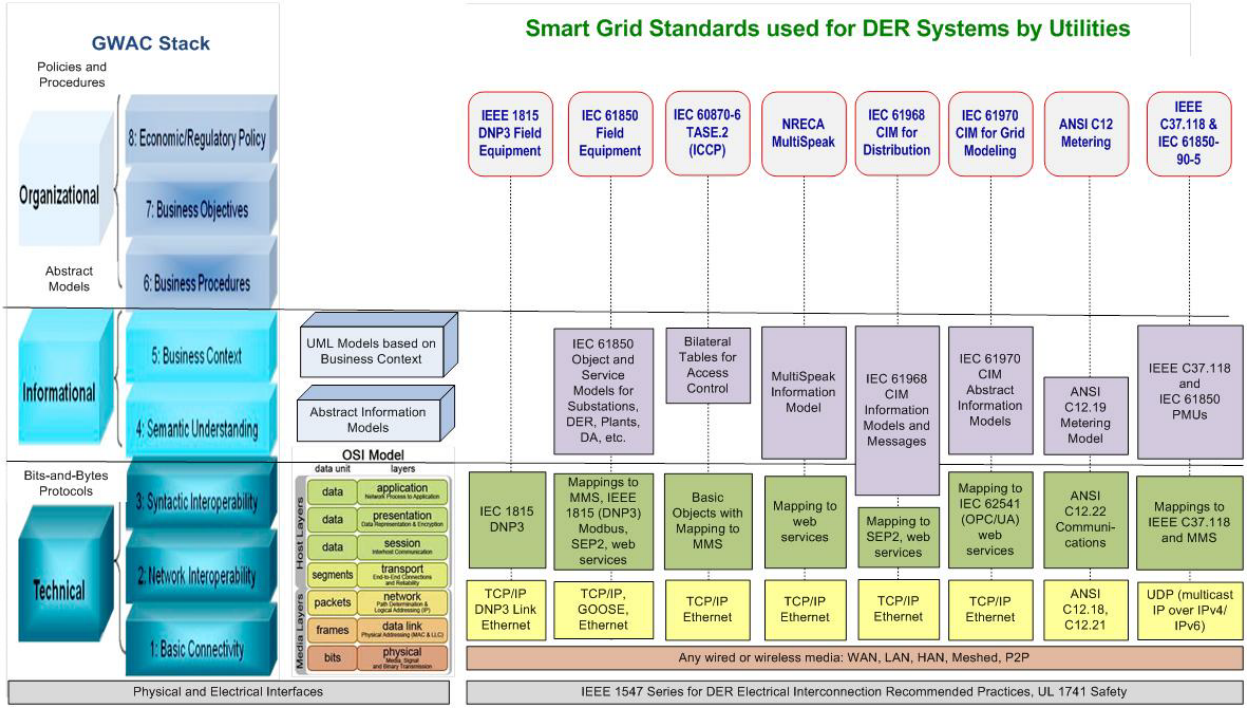
1. Manufacturer network design security requirements
2. Integrator and installer cybersecurity requirements
3. User and device access requirements
4. Communication network and protocols cybersecurity requirements
5. Alarming, logging, and reporting cybersecurity requirements
6. Testing, maintenance, and updating cybersecurity requirements
7. Possible mitigations during a cyber attack or failure
8. Possible mitigations after a cyber attack or failure

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

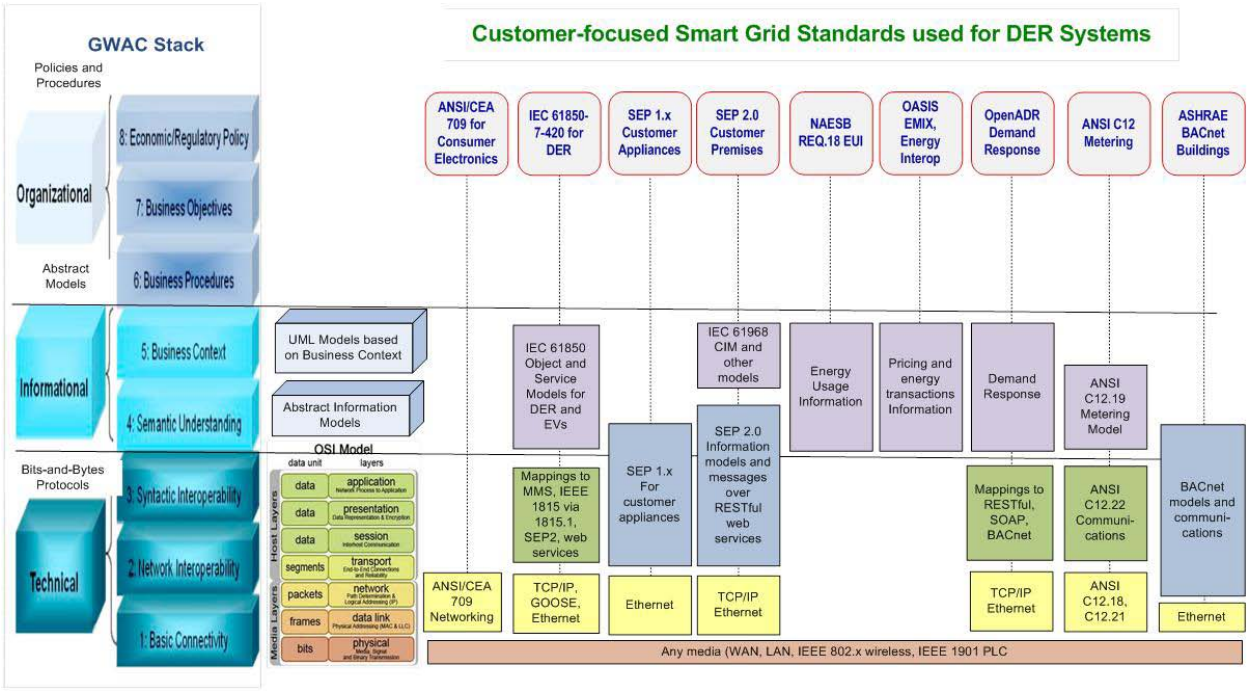
7. Cybersecurity for Communication Protocols Used with DER Systems

- Identify and characterize the communication protocols
  - Purpose and focus of the standard
  - GWAC Stack and/or ISO RM layers covered
  - Common profiles
- Cybersecurity capabilities either directly included in each standard or identified as provided by profiles or expected to be provided outside the scope of the standard
  - Security policy
  - Risk management
  - Role-based access control
  - Registration of devices
  - Establishing connections
  - Authentication
  - Integrity of data
  - Confidentiality of data
  - Updating and patching software
  - Key management
  - Audit logging

7.1 Communication Protocols used by Utilities



7.2 Communication Protocols Used in Customer Sites



7.3 Security Profile for DER using IEC 61850 Standards

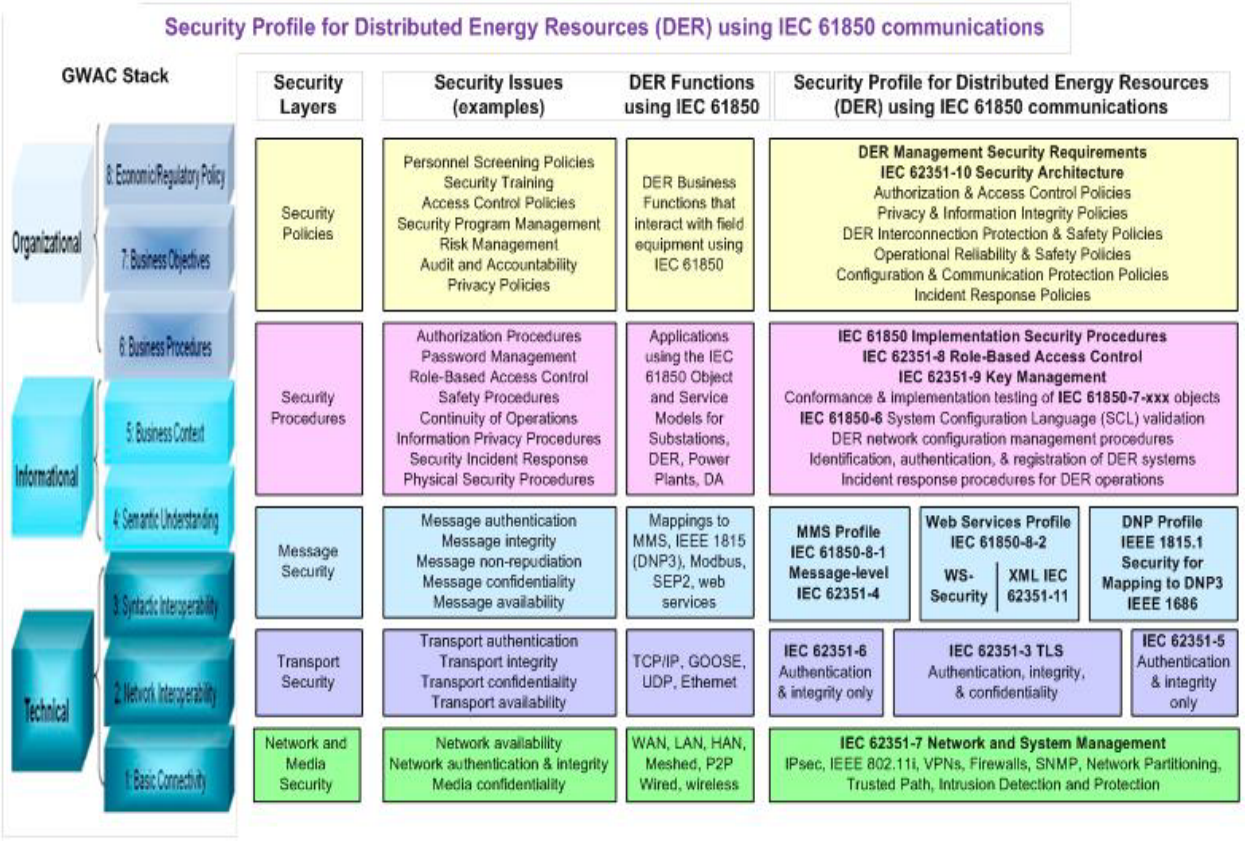


Figure 6: Security Profile for DER using IEC 61850 Standards