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

April 28, 2013

Table of Contents

Table of Figures

Table of Tables

1. 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.

2. 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.

2.1 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.

2.2 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.

2.2.1 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.

2.2.1.1 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.

2.2.1.2 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.

2.2.1.3 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.

2.2.1.4 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.

2.2.1.5 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.

2.2.1.6 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.

2.2.1.7 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.

2.2.2 Inadvertent Threats

2.2.2.1 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.

2.2.2.2 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.

2.2.2.3 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").

2.2.2.4 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.

2.3 Cybersecurity Vulnerabilities and Attacks

The threats can be realized by many different types of attacks, some of which are illustrated in **Error! Reference source not found.**. 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.

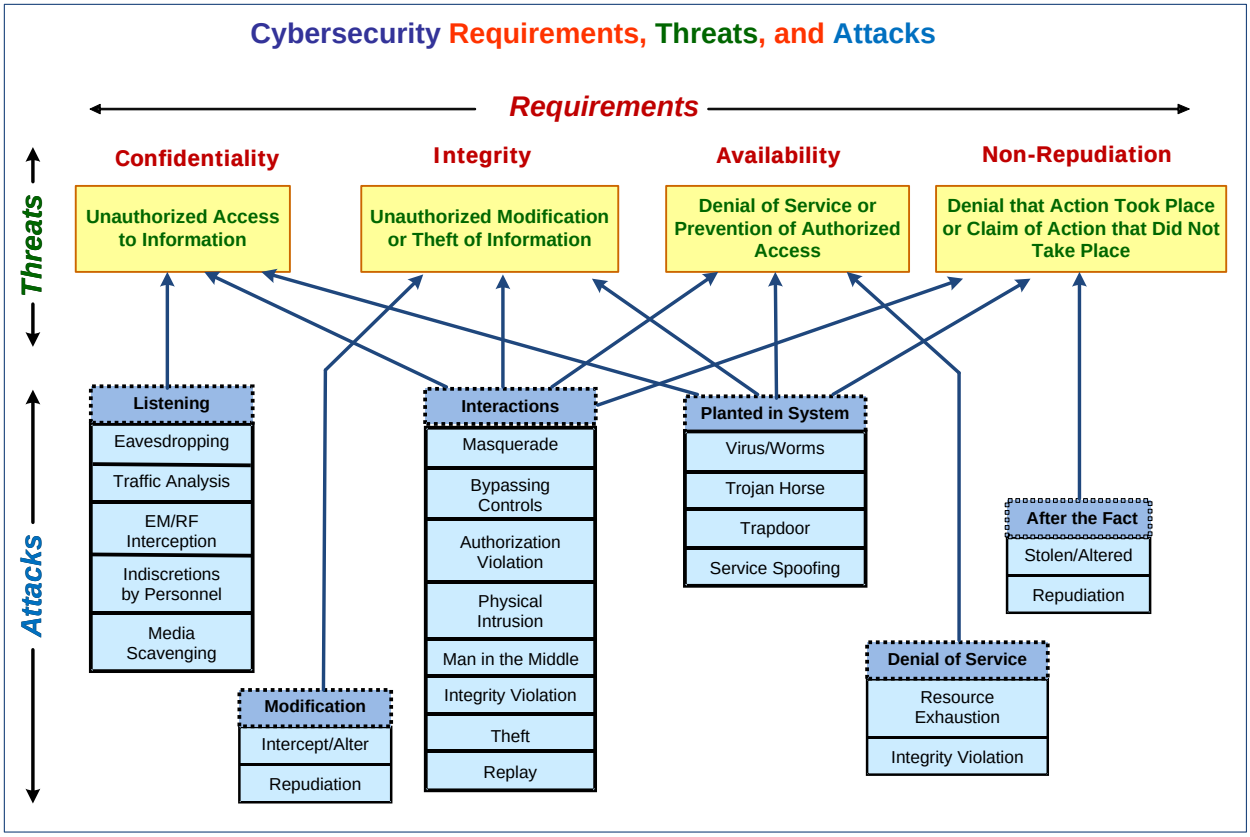


Figure 1: Security Requirements, Threats, and Possible Attacks

2.4 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 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
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;

	Category	Description	Power System Examples	Cyber Examples
	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

2.5 General Cybersecurity Requirements for Human Users and Software Applications Which Interact with Automation Systems

Users who interact with the automation systems should be required to follow security policies and procedures. These security requirements should cover both the human users and the software applications that interact with each other in response to the automation system designs, user actions, and external monitored events.

The security requirements for human users and software applications are different from the purely technical security requirements found in many communication and device standards. For user security standards, more emphasis must be on "policy and procedures" and "roles and authorization" rather than "bits and bytes" cryptographic techniques that should be included in Information and Communications Technology (ICT).

Some of the key security requirements that could be addressed (as appropriate to their scope) by standards and specifications include the following. This is just a checklist, so not all standards or specifications should include all items.

2.5.1 General Cybersecurity Considerations

These general cyber security considerations should be discussed in the standard and specifications as appropriate.

- Rely on **normative references to standards** as much as possible, with the selection of alternatives or options normatively stated.
  - Any discussions or explanations that are used to help with understandings should be clearly identified as informative.
  - Use "shall" for normative statements and "should", "could", or "may" for informative statements.
  - Preferably normative and informative information should be in separate clauses, although simple introductory informative sentences are reasonable in a normative clause.
- Start by identifying the major **security threats** and their possible **impacts**:
  - Which threats have highest likelihood? Which threats have the most serious impacts? Which threats may not be preventable but could be mitigated? How can

successful attacks be coped with? What audit logs are needed to record possible or successful attacks?

  - Taking into account the possible cost of countermeasures, which threats are the most important to prevent, mitigate, cope with, and log?
  - The results of this step do not need to be included specifically in the standard, but may be very useful during its development to solidify the security requirements and/or may included as informative

- Require or recommend that **security policies and procedures** be developed for all users covered in the standard (e.g. companies, vendors, implementers, employees, guests, contractors, customers, etc.)
  - NISTIR 7628 Volume 1, Chapter 3, Security Requirements provides a very useful list of areas that could be covered (depending upon the scope of the standard).
- State the **major cyber security requirements** – the first four rely on cryptography:
  - **Authentication** of the systems, devices, and applications that are sending and receiving data, is generally the most important.
  - **Data integrity** of all interactions and of information within the systems, is also critical. Data integrity of messages usually implies detecting tampering since it is not possible to prevent messages from being destroyed or modified, but it is possible to detect these actions.
  - **Confidentiality** is usually for financial, corporate, or private data, but not usually for normal power system operational data exchanges.
  - **Non-repudiation** ensures that some entity cannot deny having received or acted upon a message.
  - **Availability** of the interactions can range from milliseconds to hours or days. Unlike the other cyber security requirements, availability generally relies on configuration design and engineering practices.

2.5.2 User-Focused Cybersecurity Procedures and Techniques

The following items need to be addressed in standards and specifications that are addressing the high level requirements, but do not need to get into cryptographic details.

- **Establish the identity of users and devices**:
  - For authentication, trust must be established that the users are who they say they are.
  - Users need to be identified through the organization or group they belong to (company, vendor, customer, guest, etc.)
  - These organizations and groups must also establish their identities and be trusted by the other stakeholders in transactions.

  - Users provide passwords, biometric data, or other security mechanisms that tie the user to their identity in the organization/group.
  - These identifications can be used assigning users to “roles”.
- Establish the authorizations and privileges of each role in **Role-Based Access Control (RBAC)** (reference IEC 62351-8):
  - Each (human) user should be assigned to one or more of the roles, thus acquiring the associated authorizations and privileges (read data, issue commands, write data, modify data, delete data, execute applications) that are assigned to those roles.
  - Some roles ought to be mutually exclusive in order to ensure the separation of duties in order to eliminate conflicts of interest and to ensure independence in the responsibilities.
  - Users may be assigned to multiple roles so long as they are not mutually exclusive.
  - Software applications should also be assigned to roles in RBAC so that they too have the associated authorizations and privileges.
- **Require the authentication** of all interactions between users and applications, and between different applications, based on the trusted identities of these users and applications.
  - Authentication of interactions can include the use of passwords, application tokens, digital signatures, certificates, message authentication codes (hashes), etc.
  - Avoid specifying cryptographic algorithms (such as AES) if the standard is focused only on user requirements, but ensure some standard does cover the appropriate cryptographic technologies for all system designs.
  - Whenever possible and appropriate, reference existing standards, such as the IEC 62351 series and the security-related IETF RFCs.
- Focus on the **integrity of information**:
  - Data entry by users and software applications should be checked for validity as much as possible, including reasonability of values, and where possible, cross-checked by algorithms, visual displays, testing, or other mechanisms.
  - Integrity of information should apply also for message exchanges, database access, software patches, and software updates.
- Determine **availability requirements** for all types of interactions:
  - What timing latency is allowed for different types of interactions: milliseconds, seconds, minutes, or even days?
  - How closely monitored must that timing be? Issue an alarm? Log it? Ignore?

  - What kind of redundancy (or other methods) should be used to improve this availability?
  - What actions are required if those timing requirements are not met?
- Identify those interactions that require **confidentiality**:
  - These interactions usually involve corporate, financial, customer, and market information.
  - Privacy (personal information) can also be considered confidential, but may require additional management if aggregations are used for planning or other functions
- Determine if **non-repudiation and/or accountability** are necessary for different types of transactions:
  - Event logs can capture the fact that a transaction was initiated, while a similar, time-synchronized event log of the recipient of the transaction is necessary for non-repudiation of that transaction.
  - Authenticated responses to transactions can also provide non-repudiation records.
- **Revoke user access** and/or privileges through RBAC and disable the user's passwords.
  - Ensure revocations are made available to all affected systems in a timely manner
- **Deregister applications** and revoke any certificates or tokens.
  - Ensure revocations are made available to all affected systems in a timely manner
- Establish **alarm and event logs** content, synchronicity of timestamping, and security requirements
  - Ensure all alarms are assigned to one or more roles.
  - For higher priority alarms, ensure that at least one user has logged on in one of the assigned roles.
  - Synchronize the timestamps across all systems within the necessary accuracy (milliseconds or seconds).
  - Prevent or log all modifications to logs.
  - Archive logs for appropriate lengths of time.
  - Provide relevant logs to security personnel.

2.6 Information and Communication Technology (ICT) Cryptographic Techniques

In standards and specifications that focus on specific Information and Communication Technology (ICT) requirements such as communication protocols and interactions with "intelligent" equipment, the following security requirements could be directly included or

could include normative references to other standards, as appropriate (this is just a checklist, so not all standards or specifications should include all items):

2.6.1 Best practices for Specifying Cryptography

Some of the best practices for specifying cryptography used for confidentiality, authentication, and/or digital signatures are:

- Use **normative references to cryptographic standards** rather than describing the cryptography (except for informative purposes). If there are alternatives or options within the referenced standards, indicate which are mandatory, which are recommended, which are optional, and which must not be used.
- Cipher suites are always evolving, so specifying only one can be self-defeating over time. However, one cipher suite can be mandated for interoperability, with other cipher suites permitted and negotiated at startup.
- Because cipher suites get broken or "weaken" over time as computer speeds increase and hacker capabilities improve, only cipher suites of "adequate strength" should be permitted. Options for improved cipher suites over time should also be permitted.
- The permitted cryptographic algorithms should not be listed as deprecated by leading security organizations, such as NIST. NIST lists the deprecation dates of certain cryptographic algorithms in NIST SP800-131a.
- Legacy equipment may be allowed to use deprecated cryptographic algorithms so long as "mitigating" countermeasures are included. No new implementations should be permitted to implement deprecated cryptographic algorithms.
- Key management and certificate management requirements should be included, either directly or by normative reference.
- Implementation considerations include when "session" keys should be updated, how certificate expirations should be handled (ignored? Warning? Stop interactions?), and how certifications that have been revoked should be provided to affected systems.

2.6.2 Cryptographic Methods

The following cryptography methods are commonly specified. Normative references should be used where possible. More information on NIST cryptographic toolkit can be found at http://csrc.nist.gov/groups/ST/toolkit/index.html.

- The most common block cipher is the **Advanced Encryption Standard (AES),** usually either AES-128 or AES-256. NIST has identified it as the preferred block cipher. Neither DES nor Triple DES (3DES) should be specified anymore.
- **Confidentiality** (but not authentication) is provided by block cipher modes. Block ciphers only encrypt one block, so block cipher modes are used to string together the encryption of messages that are longer than one block while still using the same

cryptographic key. The most common block cipher modes are cipher-block chaining (CBC) mode and counter (CTR) mode.

- **Authentication** and **integrity** are provided by digital signatures and/or by "hashing" messages with cryptographic keys. These methods do not provide confidentiality – the messages can be read by anyone – but they do provide authentication of the sender and the ability to determine if the message has be tampered with. They require less "compute" processing than the block cipher modes.
  - **Digital signatures** algorithms include RSA-based signature schemes, such as RSA-PSS or RSA ANS x9.31, and DSA and its elliptic curve variant ECDSA, e.g. ECDSA ANS X9.62
  - The **cryptographic hashing** methods or "codes" are called Message Authentication Codes (MAC). To avoid some confusion with the term "Media Access Control (MAC)", they are sometimes called Message Integrity Codes (MIC). The most common include the Keyed-Hash Message Authentication Code (HMAC), CBC-MAC (CMAC), and Galois/Counter Mode (GCM) and GMAC. These can be further specified as to which hashing ciphers and size to use, such as HMAC-SHA256 or AES-GMAC-128.
- Combinations of confidentiality and authentication modes are called authenticated encryption (AE). Examples of AE modes are CCM (NIST SP800-38C), GCM (NIST SP800-38D), CWC, EAX, IAPM, and OCB.
- **Certificates** are issued **by Certificate Authorities (CA)** as a method for certifying the validated identity of a device or software application – the equivalent to a birth certificate or passport for a human. Most certificates use the ITU X.509 format for public key certificates, which bind a public key to the certified device or application, which contains (and guards) the corresponding secret key. **Public Key Infrastructure (PKI)** is the most commonly used method.

2.6.3 Internet Cryptography

Internet cryptography uses cryptographic profiles defined in RFCs by the IETF. The predominant RFCs include:

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

- **Hypertext Transfer Protocol Security (HTTPS)** is a combining of HTTP over TLS, and in formalized in RFC 2818.
- **Internet Protocol Security (IPsec)** authenticates and encrypts each IP packet as well as providing mutual authentication at the start of a session, thus providing security at the Network Layer rather than at the Transport Layer.
- **Virtual Private Network (VPN)** creates a "tunnel" through the Internet (or other network) in which the entire IP packet is encrypted and then encapsulated into another IP packet.

2.6.4 Wireless Cryptography

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

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

The **Extensible Authentication Protocol (EAP)** is an authentication framework frequently used in wireless networks and point-to-point connections. It is defined in RFC 3748 and was updated by RFC 5247. EAP is one of the possible authentication schema of the more general IEEE 801.1x standard that is the de-facto mandatory standard for WiFi enterprise deployment, and it is also applicable to wired LANs. When applied to wired LANs, 802.1x can allow a logical segregation of VLAN inside the same physical infrastructure. 802.1x is a role based Network Access Control mechanism and brings the RBAC model to LAN access control.

2.6.5 Public Key Cryptography

Public Key Cryptography is the cryptographic system that requires two keys, a public key and private key that are mathematically linked so that when one key is used to encrypt a message, the other key can decrypt the message. The public key can be made widely available, which the private key must be kept secret. Although mathematically linked, if the keys are long enough the private key cannot be derived from the public key, making it secure. The public keys used in the RSA system are the product of two very large prime numbers with the secret key being one of those prime numbers. A relatively new algorithm for creating keys, the **Elliptic Curve Cryptography (ECC)** system may permit shorter keys to be used. This public-private key concept is used in TLS and most other cryptographic methods.

The Public Key Infrastructure (PKI) key management process entails a number of steps. IEC 62351-9, Key Management, is identifying and standardizing these techniques for the power industry:

- **Register with Registration Authority (RA)**: Entities (systems, devices, and software applications) must be "registered" usually through an RA to confirm their identities. This registration can occur on manufacturing, on installation, on connection to a network, or off-line. Manufacturers often provide the initial registration of their entities using their corporate identity as proof.
- **Generate public/private key pair**: Either the entity generates its own public/private key pair if it has that capability, or a key pair is (securely) installed in the entity.
- **Request certificate from a Certificate Authority (CA)**: Once entities are registered and have generated their key pairs, a CA can provide these entities with security certificates that bind their identity to their public cryptographic key. The CA verifies this binding by using its own digital signature. Certificates usually have an expiration date, so updated certificates should be requested before the previous certificate expires.
- **Chain certificates by enrollment**: The identity of an entity can be chained from the initial registration by using the initial certificate to validate subsequent requests for additional certificates, as the entity's ownership or function is changed over time. Thus, the manufacturer's certificate can be used to create an integrator's certificate which can be used to create a utility's certificate, etc. This enrollment process may be through different CAs, so the CAs digital signatures are used to establish trust with each other. A common method for enrollment is the Simple Certificate Enrollment Protocol (SCEP) but this may be replaced in the near future by an updated method.
- **Assign RBAC roles**: The enrolled devices and software applications should be assigned to their RBAC roles, identifying what permissions and privileges they have, and what actions they permit other roles.
- **Create (and update) session keys**: The public/private keys can be used by two (or more) entities to authenticate each to the other and to create session keys that are used to exchange information between the entities for the length of a session, for instance between a user and their on-line banking web site or between two protective relays. In the latter example, the session keys will need to be periodically updated to ensure the keys are not compromised over the many hours and years that the relays interact.
- **Use session keys**: Session keys can be used to hash messages (authentication and integrity only), provide digital signatures (authentication, integrity, and non-repudiation), or encrypt the message payloads to provide confidentiality. Each of these processes has different cryptographic requirements and performance characteristics.
- **Revoke certificates**: Certificates can be revoked if the private key has been compromised or if the entity must no longer be used in its current role.
- **Access Certificate Revocation Lists (CRL):** CRLs are used for general revocation information when systems are able to access CA sites. For power system equipment,

alternate methods must often be used, such as OCSP servers. White listing (namely only permitting access by entities on the white list) can also be used to verify the current status of an entity.

- Some devices can use **pre-shared keys** installed (securely) to act as the source for managing their keys, so they do not undertake all the steps, but still need to be authenticated, enrolled, assigned RBAC roles, create and update their session keys, and include a method for revocating their participation in information exchanges.

2.6.6 Group Keys (GDOI)

2.6.7 Design Secure Network Configurations

Design network configurations for improved security:

- Networks that are dedicated to different scopes should be **physically and/or logically isolated** (e.g. industrial networks and corporate networks).
- Access points to the **Internet** should either be prevented or very carefully managed.
- **Firewalls** should be used at "security boundaries" to permit only authorized traffic to go through
- **Unused ports** in routers should be disabled to prevent denial of service attacks and other malicious attacks.
- **Intrusion detection and/or intrusion prevention systems (IDS/IPS)** should be deployed.
- **Redundant communication paths** should be provided for applications that require high availability.
- **Service level agreements (SLA)** with any third party communication providers should include very stringent security requirements.

2.6.8 Network and System Management (NSM)

Establish network and system management (NSM) for all communication networks (reference IEC 62351-7).

- **Alarms and events** from power system operations and equipment should be able to be time-synchronized and coordinated with security alarms and events, in order to provide a complete picture of possible threats and attacks.
- **Monitor the traffic flows** and detect/alarm abnormal conditions, such as communication circuit temporary and permanent failures.
- **Provide intrusion detection** and, for more critical circuits, intrusion prevention.
- **Detect both communication and end equipment operational anomalies**, such as failures, internal alarms, security alarms, etc.

- **Determine what automatic and/or manual actions** should be taken for each type of equipment or circuit anomaly

2.6.9 Security Testing and Validation Procedures

Establish testing and validation procedures for all software applications and all interactions between users and applications, and between different applications

- Testing of all new systems and devices should include testing of security measures.
- The validity of software applications should be tested to ensure they perform their functions correctly and do not have embedded malware or security vulnerabilities.
- Testing requirements could include both static and dynamic code analysis.
- Guidelines from the Open Web Application Security Project (OWASP) could be used to better ensure that web applications are secure.
- The NISTIR report 7920 (2012) discusses software testing and references the software testing standard, ISO/IEC 29119.
- Validation should include checking all data inputs at least as “reasonable”, with possible cross-checking against other data or algorithms for higher priority data.
- Testing should cover initial installations, and after any updates or patching.
- Security procedures should also be tested and validated to ensure they perform the security functions they are designed for.

2.6.10 Security Interoperability

Clearly identify how the interoperability of the security requirements is to be managed. This is particularly important if different organizations are involved.

- What steps must each organization take? For instance is there a pre-established list of Certificate Authorities that are trusted by each as well as all affected stakeholders? What will the different RBAC roles be and what are their privileges? What security testing is required?
- What are the default security technologies? Which additional ones may be used? Which are deprecated?
- Determine how time synchronizations across all organizations are to be handled?
- What happens if suspicious actions are noted? Who must be informed? What actions are taken? How must people and systems cope with the impacts of suspected security attacks?

2.6.11 Some Additional Cybersecurity Techniques

Some additional cybersecurity techniques include the following:

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

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[1]. 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

[1] 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 2[2] and described briefly below.

[2] 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

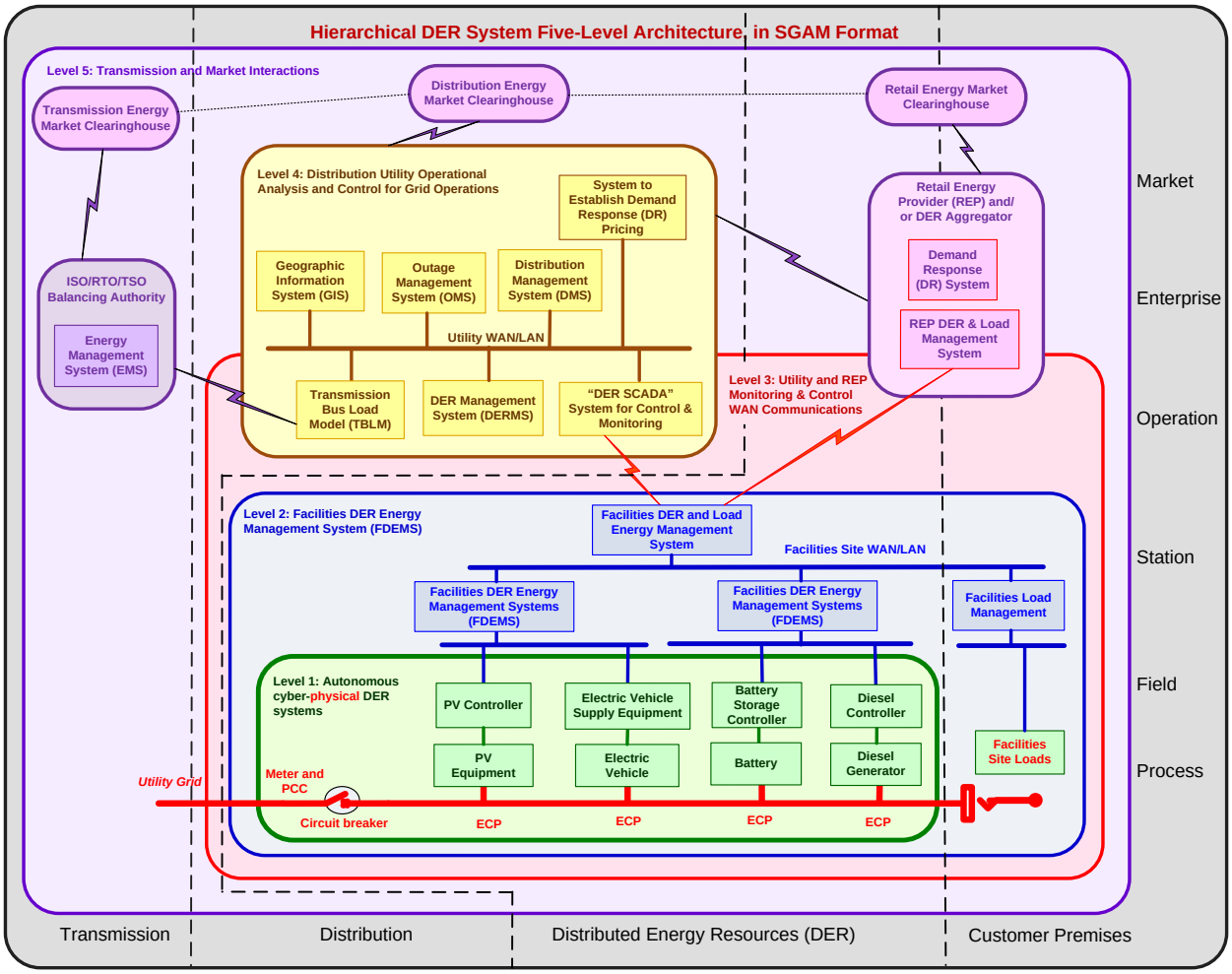


Figure 2: Five-Level Hierarchical DER System Architecture

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: Facilities 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 Information and Communications Technologies (ICT)** (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. DER as Cyber-Physical Systems

4.1 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.

4.2 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."[3]

4.3 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.

4.4 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

[3] 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 3, 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 2 and 3.

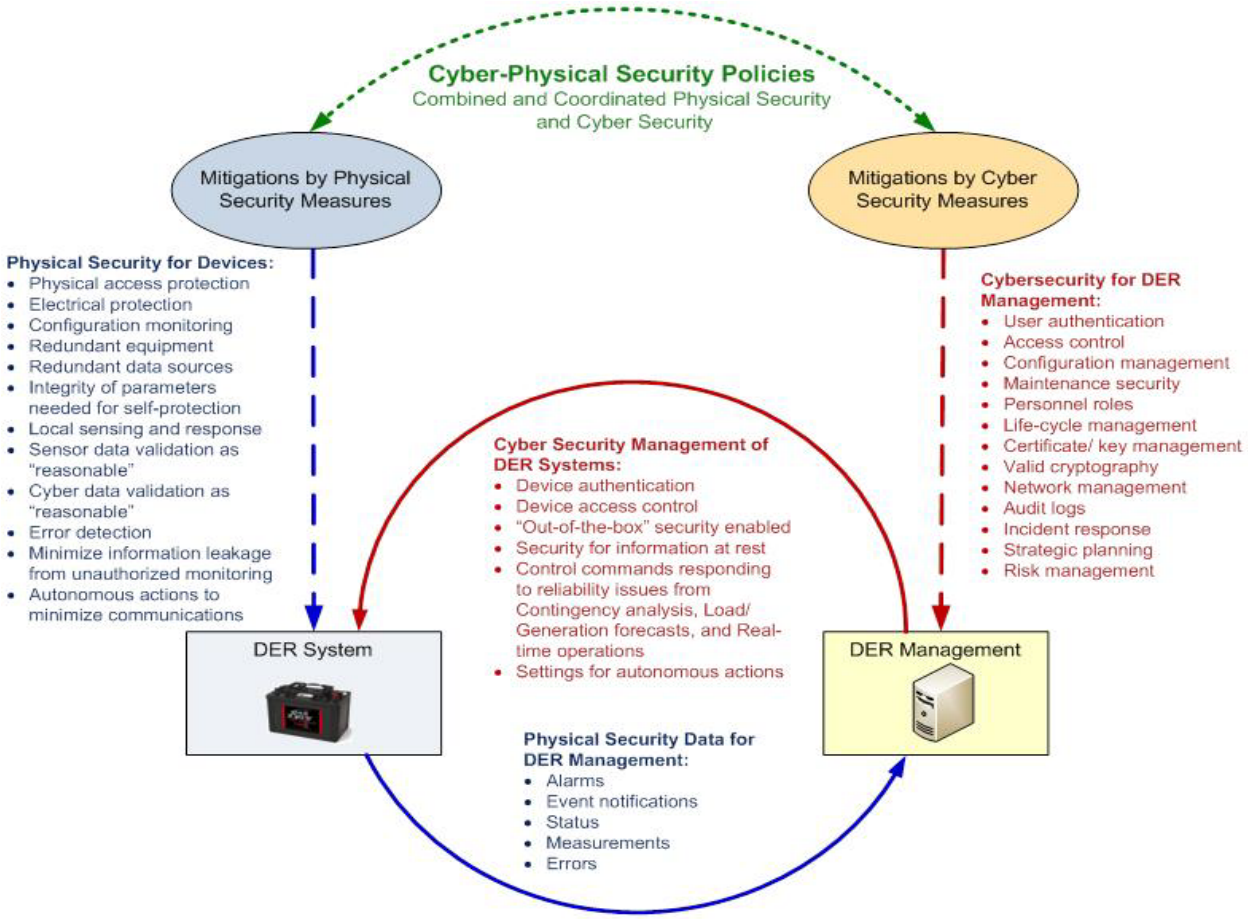


Figure 3: Mitigations by Physical and Cybersecurity Measures

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

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	• Access control • 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	Device authentication
Event notifications	Device access control
Status	Authorization
Measurements	"Out-of-the-box" security enabled
Errors	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

Physical Security Data for DER Management	Cybersecurity Management of DER Systems
	awareness, such as Load/Generation Forecasts, Real-time Operations, Contingency Analysis, etc. Settings for autonomous actions

4.5 Power System Engineering and Functions for Mitigating Cyber-Physical Attacks

Utilities have developed many different engineering practices, functions, configurations, checks, and operational methods to help ensure the reliability and safety of the power system. Although not strictly cybersecurity measures, they do provide mitigations against many of the same types of attacks, and indeed provide defense-in-depth and coping methods that cybersecurity measures cannot achieve. From a power system security perspective, it does not matter if cyber tools are used or if power system reliability tools are used – in fact they complement each other and should always be used in conjunction with each other.

Just as with any engineering, the costs for including any particular protection must be weighed against the likelihood and possible impact of a failure that could have been prevented or mitigated by that protection.

The NISTIR 7628 provides examples of these power system engineering practices and functions in Appendix B. Similar ones for DER systems are listed in the following sections.

4.5.1 DER System Engineering Practices and Configurations

DER systems are engineered and configured with reliability as a major design factor. Single DER systems can include hardened or redundant components, while multiple DER systems can be deployed such that they can support or back each other up. Some examples of these DER system engineering practices and configurations include:

- Redundant equipment (e.g., redundant DER systems, redundant components, spares)
- Redundant communication networks (e.g., multiple communication paths, redundant wireless nodes, redundant interconnections to a backhaul network)
- Redundant automation systems (e.g., redundant controllers, redundant FDEMS, redundant SCADA computers systems, backup systems that can be quickly switched in)
- Validation of information input for format and reasonability, including that the input is in the correct format, that values are within limits, that the values are not beyond the capabilities of the DER system.
- Redundant information sources (e.g., redundant sensors, voltage measurements from multiple sources such as at the ECP, the PCC, or even the feeder substation)

- Redundant or backup control systems (e.g., multiple FDEMS that can be assigned to manage different DER systems, SCADA systems in physically different locations),
- Redundant power system configurations (e.g., networked grids, multiple feeds to customer site from different substations, microgrid formation)
- Redundant logs and databases with mirrored or frequent updates
- DER systems connected at different locations on the grid
- Reserve generation capacity (DER or bulk power) available to handle the loss of a DER system
- Configuration setting development procedures, including remedial relay settings
- Post-event engineering forensic analysis capabilities

4.5.2 Power System Equipment Monitoring, Analysis, and Control

DER systems are part of the larger power system grid, and therefore the reliability of the grid is critical to the reliability of the DER systems.

- Sensors on substation and feeder equipment monitor volts, VARs, current, temperature, vibrations, etc. – eyes and ears for monitoring the power system
- Control capabilities for local control, either automatically (e.g., breaker trip) or manually (e.g., substation technician raises the voltage setting on a tap changer)
- Volt/var regulation by local equipment to ensure voltages and vars remain within prescribed limits and are coordinated with DER systems volt/var settings
- Protective relaying to respond to system events (e.g., power system fault) by tripping breakers
- Reclosers which reconnect after a “temporary” fault by trying to close the breaker 2-3 times before accepting it as a “permanent” fault. Their actions need to be coordinated with DER “ride-through” settings
- Manual or automatic switching to reconfigure the power system in a timely manner by isolating the faulted section, then reconnecting the unfaulted sections. These actions need to be coordinated with DER microgrid formation and DER volt/var settings, since connection to different sections can necessitate different settings
- Device event logs capture all significant power system events, including DER status changes
- Digital fault recorders capture wave forms of anomalous behavior of the grid
- Power quality (PQ) harmonics recorders
- Time synchronization to the appropriate accuracy and precision is used by all power system equipment to ensure that the events captured in logs can be synchronized across all locations.

4.5.3 Centralized Monitoring and Control

- SCADA systems have approximately 99.98% availability with 24x7 monitoring,
- SCADA systems continuously monitor generators, substations, and feeder equipment (e.g., every second and/or report status and measurements “by exception”),
- SCADA systems perform remote control actions on generators, substations, and feeder equipment in response to operator commands or software application commands,
- Automatic Generation Control (AGC) issues control commands to generators to maintain frequency and other parameters within limits,
- Load Shedding commands can drop feeders, substations, or other large loads rapidly in case of emergencies,
- Load Control commands can “request” or command many smaller loads to turn off or cycle off,
- Disturbance analysis (rapid snapshots of power system during a disturbance for future analysis),
- Alarm processing, with categorization of high priority alarms, “intelligent” alarm processing to determine the true cause of the alarm, and events, and
- Comparisons of device settings against baseline settings.

4.5.4 Centralized Power System Analysis and Control

Energy Management Systems (EMS) and Distribution Management Systems (DMS) (along with the DERMS and other control center systems) use many software functions to analyze the real-time state and probable future state of the power system. These software functions include:

- “Power Flow” models of the transmission system, bulk generators, and loads simulate the real-time or future (or past) power system scenarios
- “Power Flow” models of the distribution system simulate real-time or future power system scenarios, and include the characteristics and status of DER systems either individually or in aggregate
- State estimation uses redundant measurements from the field to “clean up” or estimate the real measurements from sometimes noisy, missing, or inaccurate sensor data. Since many smaller DER systems will not be directly monitored, state estimation can provide estimated values.
- Power flow applications use the state estimated data to better simulate real-time conditions
- Load and renewable generation forecasts based on weather, history, day-type, and other parameters will forecast the generation requirements

- Contingency Analysis (Security Analysis) assesses the power flow model for single points of failure (n-1) as well as any linked types of failures, and flags possible problems
- Generation reserve capacity is available for instantaneous, short term, and longer term supply of generation in the event of the loss of generation
- Ancillary services from bulk generation are available to handle both efficiency and emergency situations (e.g. generator is set to “follow load” for improved efficiency, generator is capable of a “black start” namely to start up during an outage without needing external power)
- Fault Location, Isolation, and Service Restoration (FLISR) analyze fault information in real-time to determine what feeder section to isolate and how to best restore power to unfaulted sections
- Volt/VAR/Watt Optimization determine the optimal voltage, VAR, and generation levels usually for efficiency, but also to handle contingencies and emergency situations
- Direct control of DER and loads (load management) for both efficiency and reliability
- Indirect control of DER and loads (pre-established settings, broadcasts, demand response) for both efficiency and reliability
- Ancillary services from DER for both efficiency and reliability (e.g., var support from inverters, managed charging rates for PEVs).

4.5.5 Testing

Testing of DER systems for their functionality, and their role in the power system once installed, is critical to reliable operations. Some types of testing include:

- Lab and field testing of all power system and automation equipment minimizes failure rates
- Software system factory, field, and availability testing
- Rollback capability for database updates
- Configuration testing
- Relay coordination testing
- Communication network testing, including near power system faults.

4.5.6 Training

Training of operators and other stakeholders who are involved with DER systems is vital to ensuring that they are operated reliably and safely:

- Dispatcher training simulator, using snapshots of real events as well as scenarios set up by trainers
- Operational training using case studies, etc.

- Training in using new technologies
- Security training.

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

5.1 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].

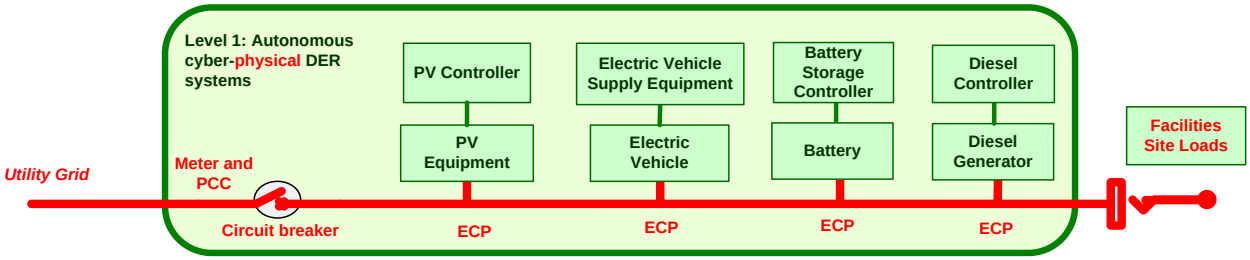


Figure 4: Level 1: Autonomous DER systems at smaller customer and utility sites

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

5.2 Level 1 DER System: Cybersecurity Vulnerabilities

5.3 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 4, the major impacts are possible outages to customer sites and potential financial impacts to DER 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)

Type of impact	Specific impacts	Severity
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

Type of impact	Specific impacts	Severity
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

5.4 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:

- Manufacturer: DER system design for self-protection security requirements
- Integrator and installer: DER setup for meeting cybersecurity requirements

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

- User (and device): access requirements
- Information and communication technology (ICT) designers: cybersecurity requirements for media, networks, and protocols
- Security managers: alarming, logging, and reporting cybersecurity requirements
- Testing and maintenance personnel: cybersecurity requirements for testing, maintenance, and updating systems
- Possible mitigations during a cyber attack or failure
- Possible mitigations after a cyber attack or failure

5.4.1 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
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

Cybersecurity Requirements for Mitigating Impacts Protection Measures Before an Attack or Failure	NISTIR 7628 Catalog of Cybersecurity Requirements
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

5.4.2 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

Cybersecurity Requirements for Mitigating Impacts Protection Measures Before an Attack or Failure	NISTIR 7628 Catalog of Cybersecurity Requirements
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

5.4.3 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
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

Cybersecurity Requirements for Mitigating Impacts Protection Measures Before an Attack or Failure	NISTIR 7628 Catalog of Cybersecurity Requirements
Messages received or sent from DER systems cannot be repudiated	SG.AU-16 Non-Repudiation

5.4.4 ICT Designers: Cybersecurity Requirements for DER Communications

Information and Communication Technologies (ICT) cover communication media, communication networks, communication protocols, and information modeling. 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
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

Cybersecurity Requirements for Mitigating Impacts Protection Measures Before an Attack or Failure	NISTIR 7628 Catalog of Cybersecurity Requirements
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
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

5.4.5 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

5.4.6 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
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

5.4.7 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
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

Cybersecurity Requirements for Mitigating Impacts Protection Measures During an Attack or Failure	NISTIR 7628 Catalog of Cybersecurity Requirements
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

5.4.8 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

Cybersecurity Requirements for Mitigating Impacts Protection Measures After an Attack or Failure	NISTIR 7628 Catalog of Cybersecurity Requirements
If privacy or confidentiality is suspected of being compromised, notify all affected stakeholders	SG.SC-26 Confidentiality of Information at Rest

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

6.1 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 5.

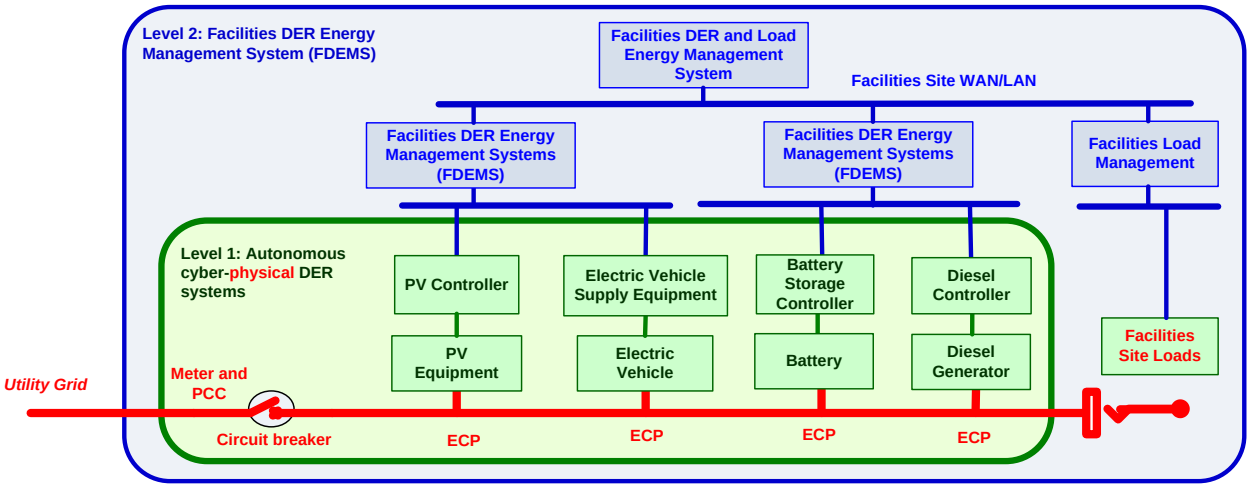


Figure 5: Level 2 FDEMS

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.

6.2 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

6.3 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

Type of impact	Specific impacts	Severity
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
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

6.4 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:

- Manufacturer design of FDEMS cybersecurity requirements
- Integrators and installer cybersecurity requirements
- User and system access requirements
- Information and communication technology (ICT) cybersecurity requirements
- Alarming, logging, and reporting cybersecurity requirements
- Testing, maintenance, and updating cybersecurity requirements
- Possible mitigations during a cyber attack or failure
- Possible mitigations after a cyber attack or failure

6.4.1 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.

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

6.4.2 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

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 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
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

6.4.3 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

Cybersecurity Requirements for Mitigating Impacts Protection Measures Before an Attack or Failure	NISTIR 7628 Catalog of Cybersecurity Requirements
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
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

6.4.4 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
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

Cybersecurity Requirements for Mitigating Impacts Protection Measures Before an Attack or Failure	NISTIR 7628 Catalog of Cybersecurity Requirements
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

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

TDB

7.1 Level 3 WAN ICT: Architecture

7.2 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.

7.3 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

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

7.4 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:

- Manufacturer network design security requirements
- Integrator and installer cybersecurity requirements
- User and device access requirements
- Communication network and protocols cybersecurity requirements
- Alarming, logging, and reporting cybersecurity requirements
- Testing, maintenance, and updating cybersecurity requirements
- Possible mitigations during a cyber attack or failure
- Possible mitigations after a cyber attack or failure

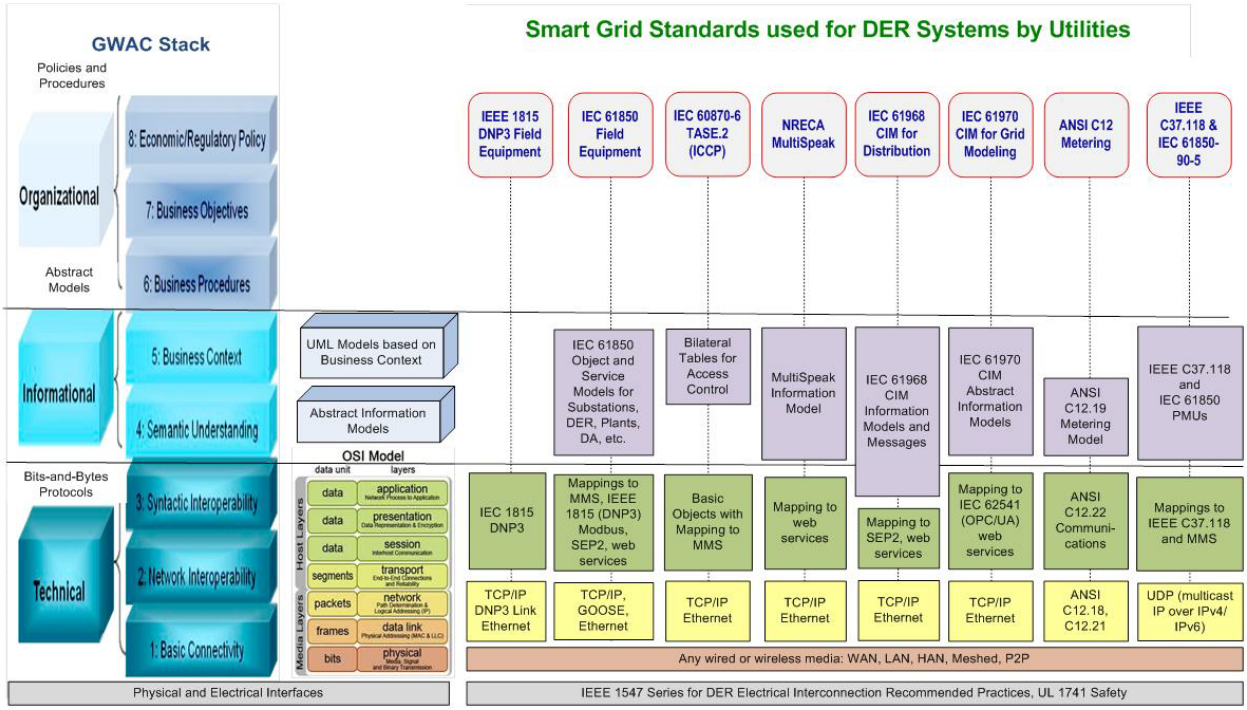
8. Cybersecurity for Communication Protocols Used with DER Systems

- 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

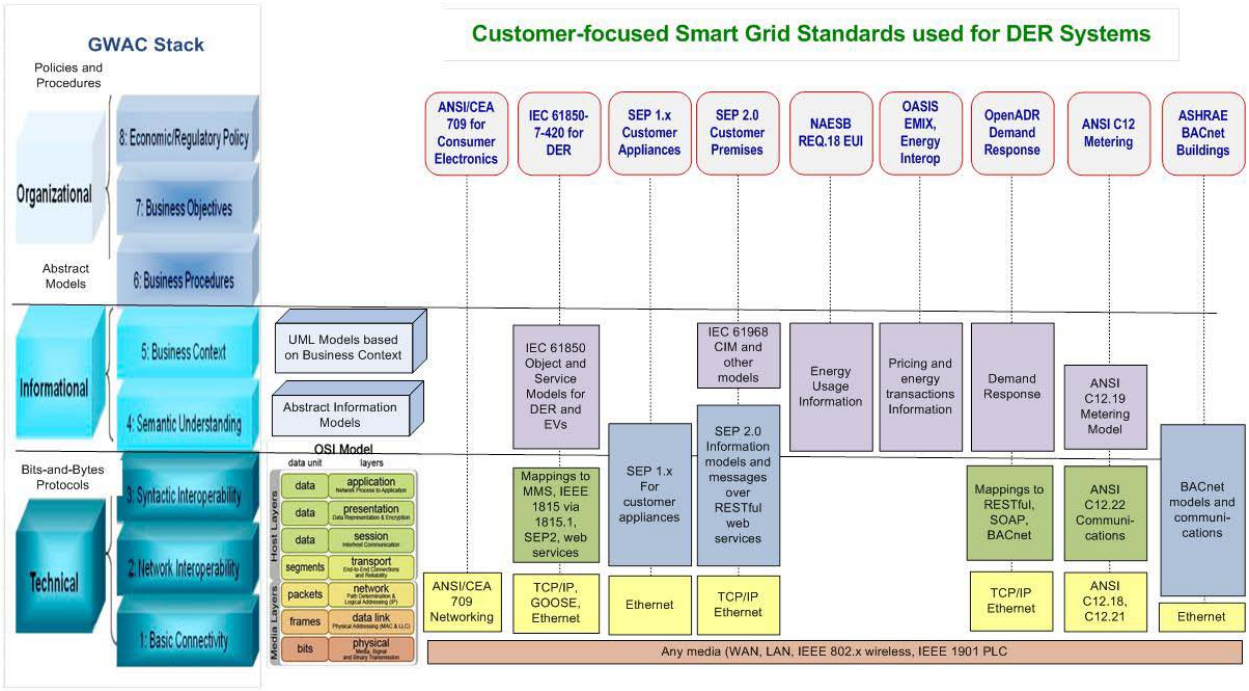
[6] NISTIR 7628 Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements, 2010

- Integrity of data
- Confidentiality of data
- Updating and patching software
- Key management
- Audit logging

8.1 Communication Protocols used by Utilities



8.2 Communication Protocols Used in Customer Sites



8.3 Security Profile for DER using IEC 61850 Standards

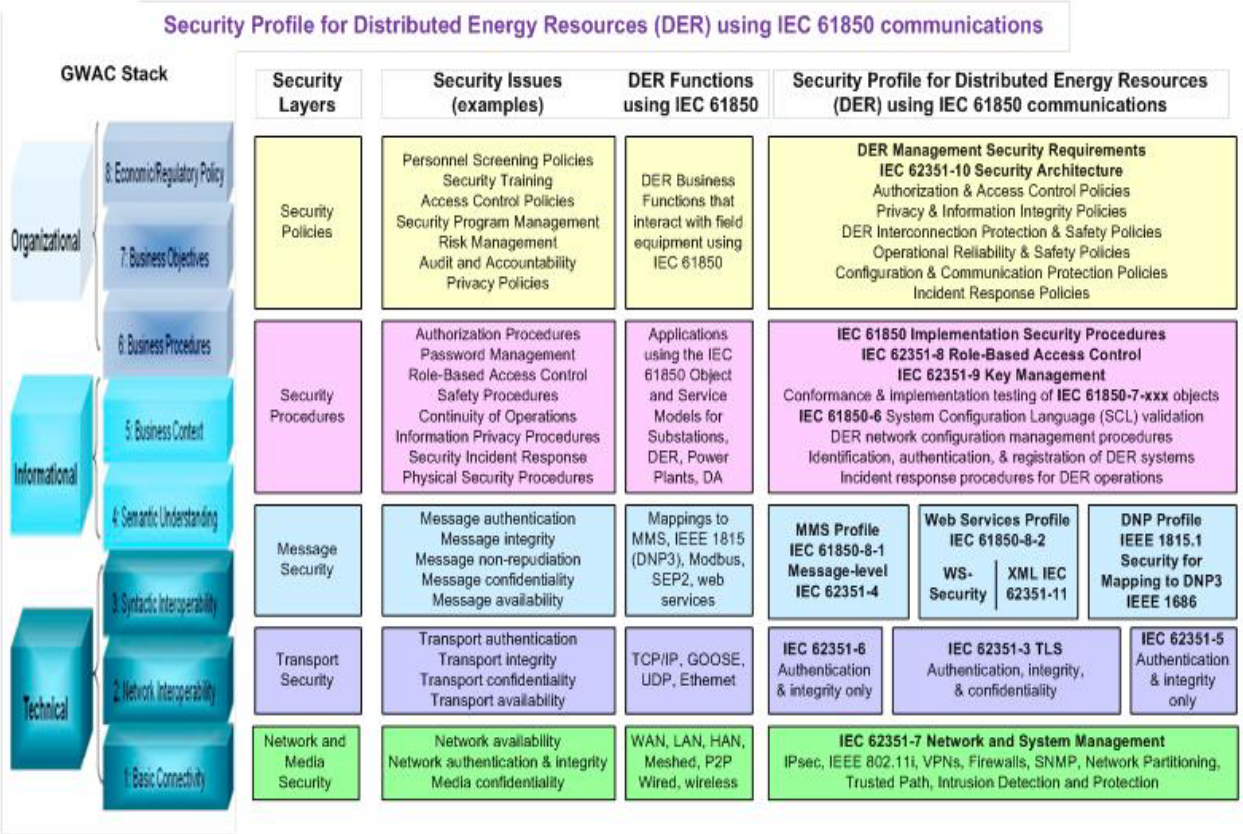


Figure 6: Security Profile for DER using IEC 61850 Standards

Appendix A - List of the NISTIR 7628 Smart Grid Catalog of Security Requirements

The families of the NIST Smart Grid Catalog of Security Requirements are shown in 19, while a more detailed list of the requirements within each family is shown in Table 20. The complete NIST catalog can be found on the NIST web site[7].

Table 19: NIST Smart Grid Security Requirements Families

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

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

Table 20: Detailed NIST Catalogue of Smart Grid Security Requirements

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

NIST Ref.	Catalog of SG Security Requirements
SG.AU-8	Time Stamps
SG.AU-9	Protection of Audit Information
SG.AU-10	Audit Record Retention
SG.AU-11	Conduct and Frequency of Audits
SG.AU-12	Auditor Qualification
SG.AU-13	Audit Tools
SG.AU-14	Security Policy Compliance
SG.AU-15	Audit Generation
SG.AU-16	Non-Repudiation
3.10 Security Assessment and Authorization (SG.CA)	
SG.CA-1	Security Assessment and Authorization Policy and Procedures
SG.CA-2	Security Assessments
SG.CA-3	Continuous Improvement
SG.CA-4	Smart Grid Information System Connections
SG.CA-5	Security Authorization to Operate
SG.CA-6	Continuous Monitoring
3.11 Configuration Management (SG.CM)	
SG.CM-1	Configuration Management Policy and Procedures
SG.CM-2	Baseline Configuration

NIST Ref.	Catalog of SG Security Requirements
SG.CM-3	Configuration Change Control
SG.CM-4	Monitoring Configuration Changes
SG.CM-5	Access Restrictions for Configuration Change
SG.CM-6	Configuration Settings
SG.CM-7	Configuration for Least Functionality
SG.CM-8	Component Inventory
SG.CM-9	Addition, Removal, and Disposal of Equipment
SG.CM-10	Factory Default Authentication Management
SG.CM-11	Configuration Management Plan
3.12 Continuity of Operations (SG.CP)	
SG.CP-1	Continuity of Operations Policy and Procedures
SG.CP-2	Continuity of Operations Plan
SG.CP-3	Continuity of Operations Roles and Responsibilities
SG.CP-4	Continuity of Operations Training
SG.CP-5	Continuity of Operations Plan Testing
SG.CP-6	Continuity of Operations Plan Update
SG.CP-7	Alternate Storage Sites
SG.CP-8	Alternate Telecommunication Services
SG.CP-9	Alternate Control Center

NIST Ref.	Catalog of SG Security Requirements
SG.CP-10	Smart Grid Information System Recovery and Reconstitution
SG.CP-11	Fail-Safe Response
3.13 Identification and Authentication (SG.IA)	
SG.IA-1	Identification and Authentication Policy and Procedures
SG.IA-2	Identifier Management
SG.IA-3	Authenticator Management
SG.IA-4	User Identification and Authentication
SG.IA-5	Device Identification and Authentication
SG.IA-6	Authenticator Feedback
3.14 Information and Document Management (SG.ID)	
SG.ID-1	Information and Document Management Policy and Procedures
SG.ID-2	Information and Document Retention
SG.ID-3	Information Handling
SG.ID-4	Information Exchange
SG.ID-5	Automated Labeling
3.15 Incident Response (SG.IR)	
SG.IR-1	Incident Response Policy and Procedures
SG.IR-2	Incident Response Roles and Responsibilities
SG.IR-3	Incident Response Training

NIST Ref.	Catalog of SG Security Requirements
SG.IR-4	Incident Response Testing and Exercises
SG.IR-5	Incident Handling
SG.IR-6	Incident Monitoring
SG.IR-7	Incident Reporting
SG.IR-8	Incident Response Investigation and Analysis
SG.IR-9	Corrective Action
SG.IR-10	Smart Grid System Backup
SG.IR-11	Coordination of Emergency Response
3.16 Smart Grid System Development and Maintenance (SG.MA)	
SG.MA-1	Smart Grid System Maintenance Policy and Procedures
SG.MA-2	Legacy Smart Grid System Upgrades
SG.MA-3	Smart Grid Information System Maintenance
SG.MA-4	Maintenance Tools
SG.MA-5	Maintenance Personnel
SG.MA-6	Remote Maintenance
SG.MA-7	Timely Maintenance
3.17 Media Protection (SG.MP)	
SG.MP-1	Media Protection Policy and Procedures
SG.MP-2	Media Sensitivity Level
SG.MP-3	Media Marking

NIST Ref.	Catalog of SG Security Requirements
SG.MP-4	Media Storage
SG.MP-5	Media Transport
SG.MP-6	Media Sanitization and Disposal
3.18 Physical and Environmental Security (SG.PE)	
SG.PE-1	Physical and Environmental Security Policy and Procedures
SG.PE-2	Physical Access Authorizations
SG.PE-3	Physical Access
SG.PE-4	Monitoring Physical Access
SG.PE-5	Visitor Control
SG.PE-6	Visitor Records
SG.PE-7	Physical Access Log Retention
SG.PE-8	Emergency Shutoff Protection
SG.PE-9	Emergency Power
SG.PE-10	Delivery and Removal
SG.PE-11	Alternate Work Site
SG.PE-12	Location of Smart Grid System Assets
3.19 Strategic Planning (SG.PL)	
SG.PL-1	Strategic Planning Policy and Procedures
SG.PL-2	Smart Grid Information System Security Plan
SG.PL-3	Rules of Behavior
SG.PL-4	Privacy Impact Assessment
SG.PL-5	Security-Related Activity Planning

NIST Ref.	Catalog of SG Security Requirements
3.20 Security Program Management (SG.PM)	
SG.PM-1	Security Policy and Procedures
SG.PM-2	Security Program Plan
SG.PM-3	Senior Management Authority
SG.PM-4	Security Architecture
SG.PM-5	Risk Management Strategy
SG.PM-6	Security Authorization to Operate Process
SG.PM-7	Mission/Business Process Definition
SG.PM-8	Management Accountability
3.21 Personnel Security (SG.PS)	
SG.PS-1	Personnel Security Policy and Procedures
SG.PS-2	Position Categorization
SG.PS-3	Personnel Screening
SG.PS-4	Personnel Termination
SG.PS-5	Personnel Transfer
SG.PS-6	Access Agreements
SG.PS-7	Contractor and Third-Party Personnel Security
SG.PS-8	Personnel Accountability
SG.PS-9	Personnel Roles
3.22 Risk Management and Assessment (SG.RA)	
SG.RA-1	Risk Assessment Policy and Procedures
SG.RA-2	Risk Management Plan
SG.RA-3	Security Impact Level
SG.RA-4	Risk Assessment

NIST Ref.	Catalog of SG Security Requirements
SG.RA-5	Risk Assessment Update
SG.RA-6	Vulnerability Assessment and Awareness
3.23 Smart Grid System and Services Acquisition (SG.SA)	
SG.SA-1	Smart Grid System and Services Acquisition Policy and Procedures
SG.SA-2	Security Policies for Contractors and Third Parties
SG.SA-3	Life-Cycle Support
SG.SA-4	Acquisitions
SG.SA-5	Smart Grid System Documentation
SG.SA-6	Software License Usage Restrictions
SG.SA-7	User-Installed Software
SG.SA-8	Security Engineering Principles
SG.SA-9	Developer Configuration Management
SG.SA-10	Developer Security Testing
SG.SA-11	Supply Chain Protection
3.24 Smart Grid System and Communication Protection (SG.SC)	
SG.SC-1	Smart Grid System and Communication Protection Policy and Procedures
SG.SC-2	Communications Partitioning
SG.SC-3	Security Function Isolation
SG.SC-4	Information Remnants

NIST Ref.	Catalog of SG Security Requirements
SG.SC-5	Denial-of-Service Protection
SG.SC-6	Resource Priority
SG.SC-7	Boundary Protection
SG.SC-8	Communication Integrity
SG.SC-9	Communication Confidentiality
SG.SC-10	Trusted Path
SG.SC-11	Cryptographic Key Establishment and Management
SG.SC-12	Use of Validated Cryptography
SG.SC-13	Collaborative Computing
SG.SC-14	Transmission of Security Parameters
SG.SC-15	Public Key Infrastructure Certificates
SG.SC-16	Mobile Code
SG.SC-17	Voice-Over Internet Protocol
SG.SC-18	System Connections
SG.SC-19	Security Roles
SG.SC-20	Message Authenticity
SG.SC-21	Secure Name/Address Resolution Service
SG.SC-22	Fail in Known State
SG.SC-23	Thin Nodes

NIST Ref.	Catalog of SG Security Requirements
SG.SC-24	Honeypots
SG.SC-25	Operating Smart Grid system-Independent Applications
SG.SC-26	Confidentiality of Information at Rest
SG.SC-27	Heterogeneity
SG.SC-28	Virtualization Techniques
SG.SC-29	Application Partitioning
SG.SC-30	Smart Grid System Partitioning
3.25 Smart Grid System and Information Integrity (SG.SI)	

NIST Ref.	Catalog of SG Security Requirements
SG.SI-1	Smart Grid System and Information Integrity Policy and Procedures
SG.SI-2	Flaw Remediation
SG.SI-3	Malicious Code and Spam Protection
SG.SI-4	Smart Grid Information System Monitoring Tools and Techniques
SG.SI-5	Security Alerts and Advisories
SG.SI-6	Security Functionality Verification
SG.SI-7	Software and Information Integrity
SG.SI-8	Information Input Validation
SG.SI-9	Error Handling