PD IEC/TR 62351-12:2016

BSI Standards Publication

Power systems management and associated information exchange — Data and communications security

Part 12: Resilience and security recommendations for power systems with distributed energy resources (DER) cyber-physical systems

National foreword

This Published Document is the UK implementation of IEC/TR 62351-12:2016.

The UK participation in its preparation was entrusted to Technical Committee PEL/57, Power systems management and associated information exchange.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Published by BSI Standards Limited 2016

ISBN 978 0 580 92310 4
ICS 33.200

Compliance with a British Standard cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 30 April 2016.

Amendments/corrigenda issued since publication

Date	Text affected

PD IEC/TR 62351-12:2016

IEC TR 62351-12

Edition 1.0 2016-04

TECHNICAL REPORT

colour inside

Power systems management and associated information exchange – Data and communications security – Part 12: Resilience and security recommendations for power systems with distributed energy resources (DER) cyber-physical systems

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 33.200

ISBN 978-2-8322-3255-2

Warning! Make sure that you obtained this publication from an authorized distributor.

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

POWER SYSTEMS MANAGEMENT AND ASSOCIATED INFORMATION EXCHANGE – DATA AND COMMUNICATIONS SECURITY –

Part 12: Resilience and security recommendations for power systems with distributed energy resources (DER) cyber-physical systems

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.

2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.

3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.

4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.

5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.

6) All users should ensure that they have the latest edition of this publication.

7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.

8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.

9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

The main task of IEC technical committees is to prepare International Standards. However, a technical committee may propose the publication of a technical report when it has collected data of a different kind from that which is normally published as an International Standard, for example "state of the art".

IEC TR 62351-12, which is a technical report, has been prepared by IEC technical committee 57: Power systems management and associated information exchange.

The text of this technical report is based on the following documents:

Enquiry draft	Report on voting
57/1637/DTR	57/1664/RVC

Full information on the voting for the approval of this technical report can be found in the report on voting indicated in the above table.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

A list of all parts of the IEC 62351 series, under the general title: *Power systems management and associated information exchange – Data and communications security*, can be found on the IEC website.

The committee has decided that the contents of this publication will remain unchanged until the stability date indicated on the IEC website under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

A bilingual version of this publication may be issued at a later date.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

Resilience and Cyber Security

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

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

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

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

Background to Resilience Issues

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

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

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

On the other hand, the sophisticated cyber-physical capabilities of smart DER systems could actually improve power system resilience if these smart DER capabilities were properly secure and coordinated with power system management through communications. DER systems can actually compensate for some of the problems they cause, such as riding through temporary spikes and dips in voltage or frequency that could be caused by their fluctuating behavior. DER functions such as volt-VAr management can smooth these fluctuations as well. In addition, networked DER systems (e.g. microgrids), and the bulk power system can serve as mutual backups during excessive peak loads or during disaster conditions. As illustrated in Figure 1, if both the cyber and the physical components of these DER systems were well designed and implemented with embedded cyber security, and were interconnected and operated using good engineering strategies, they would significantly improve the resilience of the power system.

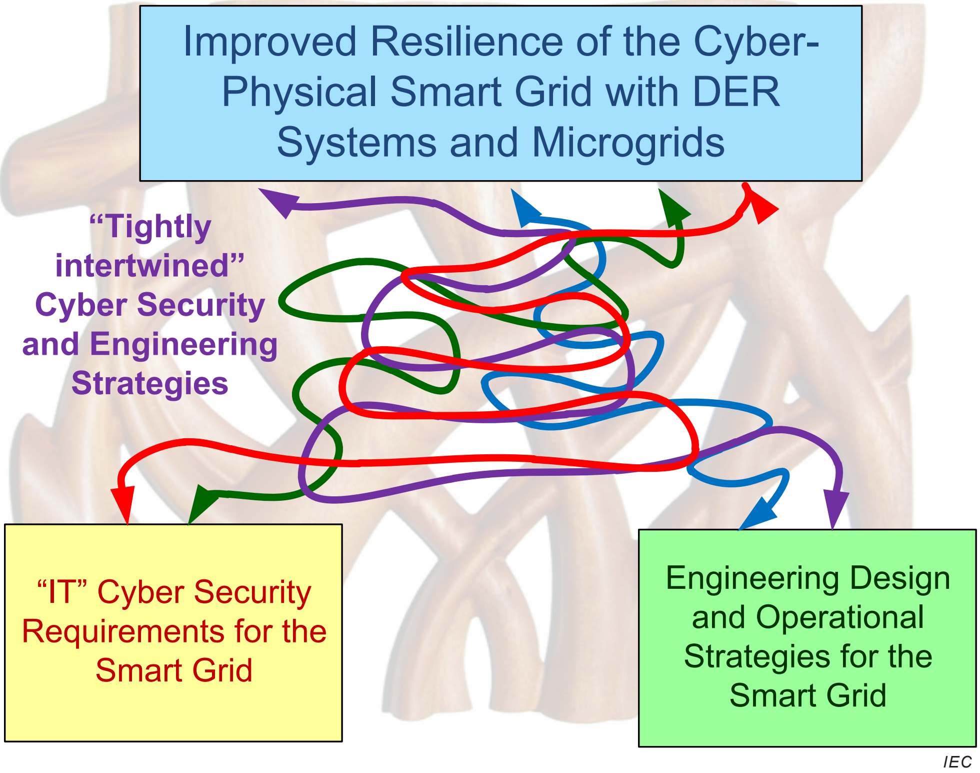

Improved Resilience of the Cyber-Physical Smart Grid with DER Systems and Microgrids
"Tightly intertwined" Cyber Security and Engineering Strategies
"IT" Cyber Security Requirements for the Smart Grid
Engineering Design and Operational Strategies for the Smart Grid
IEC

Figure 1 – Smart grid resilience: intertwined IT cyber security and engineering strategies

It is not just the utilities who must take responsibility for achieving this resilience goal. Many stakeholders are involved in the design, implementation, and operation of DER systems, including manufacturers, integrator/installers, users, information and communication technology (ICT) providers, security managers, testing and maintenance personnel, and ultimately utility regulators. However, given this new cyber-physical environment, often these stakeholders do not fully understand or appreciate the types of cyber security and engineering strategies that could or should be used.

POWER SYSTEMS MANAGEMENT AND ASSOCIATED INFORMATION EXCHANGE – DATA AND COMMUNICATIONS SECURITY –

Part 12: Resilience and security recommendations for power systems with distributed energy resources (DER) cyber-physical systems

1 Scope

This part of IEC 62351, which is a technical report, discusses cyber security recommendations and engineering/operational strategies for improving the resilience of power systems with interconnected Distributed Energy Resources (DER) systems. It covers the resilience requirements for the many different stakeholders of these dispersed cyber-physical generation and storage devices, with the goal of enhancing the safety, reliability, power quality, and other operational aspects of power systems, particularly those with high penetrations of DER systems.

The focus of this technical report is describing the impact of DER systems on power system resilience, and covers the cyber security and engineering strategies for improving power system resilience with high penetrations of DER systems.

While recognizing that many other requirements exist for improving power system resilience, this technical report does not address general power system configurations, operations, manual power restoration activities or the many other non-DER-specific issues. For instance, power system reliability relies on well-coordinated protective relays, stable power system designs, and well-trained field crews, while control center cyber security relies on many best practices for communication network design and firewalls. However, this technical report only addresses the additional reliability and resilience issues caused by 3rd-party managed DER systems which may not be as well-secured or operated with the same reliability as the utility-managed power system.

This technical report discusses the resilience issues for cyber-physical DER systems interconnected with the power grid, building on the concepts and the hierarchical architecture described in the Smart Grid Interoperability Panel (SGIP) draft *DRGS Subgroup B White Paper – Categorizing Use Cases in Hierarchical DER Systems 01-14-2014.docx*[2].

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 62351-9, *Power systems management and associated information exchange – Data and communications security – Part 9: Cyber security key management for power system equipment*[3]

[2] http://members.sgip.org/apps/org/workgroup/sgip-drgs-b/download.php/2984/DRGS%20Subgroup%20B%20White%20Paper%20-%20Categorizing%20Use%20Cases%20in%20Hierarchical%20DER%20Systems%2001-14-2014.docx

[3] Under consideration.

IEC 62443-3-3, *Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels*

NIST Special Publication (SP) 800-30, *Guide for Conducting Risk Assessments*

NISTIR 7628:2010, *Guidelines for Smart Grid Cyber Security*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

NOTE For the sake of transparency certain terms, taken from different sources, are provided with slightly different definitions in Annex D, Glossary of terms.

3.1
anti-islanding
detecting an island and ceasing to energize that island

3.2
cease to energize
cessation of energy outflow capability

[SOURCE: IEEE 1547:2003]

3.3
cyber-physical systems
engineered systems that are built from and depend upon the synergy of computational and physical components

[SOURCE: National Science Foundation]

3.4
electric power system
EPS
facilities that deliver electric power to a load

Note 1 to entry: This may include generation units.

[SOURCE:IEEE 1547:2003]

3.5
electric power system, area
area EPS
electric power system (EPS) that serves Local EPSs

Note 1 to entry: Typically, an Area EPS has primary access to public rights-of-way, priority crossing of property boundaries, etc. and is subject to regulatory oversight.

[SOURCE:IEEE 1547:2003]

3.6
electric power system, local
local EPS
EPS contained entirely within a single premises or group of premises

[SOURCE: IEEE 1547:2003]

3.7
island
condition in which a portion of an Area EPS is energized solely by one or more Local EPSs through the associated PCCs while that portion of the Area EPS is electrically separated from the rest of the Area EPS

[SOURCE: IEEE 1547:2003]

3.8
microgrid
small electrical grid that can manage the generation, storage, and load within its domain. It may remain connected to the area electrical power system for financial or reliability reasons, but may disconnect from the area EPS and operate as an islanded grid.

3.9
resilience
ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents

[SOURCE: US Presidential Policy Directive – Critical Infrastructure Security and Resilience]

3.10
threat
potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm

[SOURCE: RFC 2828]

3.11
threat agent
intent and method targeted at the intentional exploitation of a vulnerability, or a situation and method that may accidentally trigger a vulnerability

[SOURCE: FIPS 200; SP 800-53; SP 800-53A; SP 800-37]

3.12
vulnerability
flaw or weakness in a system’s design, implementation, or operation and management that could be exploited to violate the system’s integrity or security policy

[SOURCE: RFC 2828]

4 Abbreviations and acronyms

AGC	Automatic Generation Control
DER	Distributed Energy Resource
DERMS	DER Management System
DMS	Distribution Management System
DSO	Distribution System Operator
ECP	Electrical Connection Point
EMS	Energy Management System
EPS	Electric Power System
ESI	Energy Service Interface

FDEMS	Facility DER Management System
HAN	Home Area Network
HMI	Human-Machine Interface
ICT	Information and Communication Technology
ISO	Independent System Operator
MAC	Message Authentication Code
MPLS	Multiprotocol Label Switching
NSM	Network and System Management
OCSP	Online Certificate Status Protocol
PCC	Point of Common Coupling
PKI	Public-Key Infrastructure
PQ	Power Quality
QoS	Quality of Service
RBAC	Role-Based Access Control
REP	Retail Energy Provider (Aggregator)
RTO	Regional Transmission Operator
TSO	Transmission System Operator
VAr	Volt-ampere reactive

5 DER architectures and DER cyber-physical concepts

5.1 Resiliency challenge for power systems with DER systems

Ensuring the resilience of the power system with integrated DER systems is an evolving and complex challenge. Unlike traditional power system management, DER systems involve many stakeholders, including the original DER manufacturers, the DER system implementers, the DER owners, the DER operators, the DER maintenance personnel, the retail energy providers (REP) or aggregators who manage groups of DER systems, and, finally, the utilities. Within the utilities, the distribution system operator (DSO) is the front line for interactions with DER systems, but the transmission system operator (TSO) can also be affected by either large DER systems or aggregations of smaller DER systems. In addition, the primary purpose of DER systems is often not to support power system operations, but to provide energy services to the DER owner.

The resilience challenges for all these stakeholders are to:

- Assess the risks associated with the products and services provided by each stakeholder. Risk assessment consists of:
  - – Understanding the impacts of DER systems on the power grid due to their natural characteristics, including the normal fluctuations of output due to renewable sources of energy. These impacts could also reflect the decisions of DER operators, the response of DER operators to pricing signals, and normal maintenance decisions;
  - – Identifying the threats that might affect the products and services of each stakeholder. These threats may be malicious attackers, but more often are inadvertent mistakes, failures, or natural disasters;
  - – Understanding the possible vulnerabilities that could allow these threats to materialize and to cause undesired events;
  - – Evaluating the likelihood of such an undesired event actually occurring;
  - – Determining the possible impacts of this event in terms of safety, power system reliability, power system quality, financial repercussions, privacy, and environmental consequences;

- Assess possible mitigation policies, procedures, and technologies that could help prevent, deter, cope with, and/or recover from normal such threat-caused events;
- Balance the likelihood and impact of threats against the costs to implement the mitigation measures. This balancing assessment may include using mitigations that address many different types of threats, but may also involve specific mitigation techniques;
- Develop coordinated resilience recommendations for each of the stakeholders for implementing those mitigation measures that are within their purview. These resilience recommendations should be coordinated across the stakeholders, since only partial implementation by one stakeholder could leave additional vulnerabilities for other stakeholders.

Subclauses 5.2 to 5.5 describe the multi-level DER architecture, the cyber-physical nature of DER systems, and the different types of stakeholders.

5.2 Five-level DER hierarchical architecture

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 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 need to be coordinated with other DER systems and distribution grid devices. In addition, the distribution system operators (DSOs) need to interact with regional transmission organizations (RTOs) and/or independent system operators (ISOs) for reliability and market purposes. In some regions, aggregators or other energy service providers (ESPs) are responsible for managing groups of DER systems. In some situations DER systems might be controlled both by aggregators for commercial or market purposes and by grid operators (RTOs/DSOs/ISOs) for controlling grid stability, requiring close coordination to avoid conflicts and possible security impacts.

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, based on a selected set of domains, layers, and zones of the European M/490 Smart Grid Architecture Model (SGAM) (see Figure 2), as illustrated in Figure 3 and described briefly below. Specifically, the 5-layer DER model includes four of the five domains and all of the zones, while it selects only the information layer to be included.

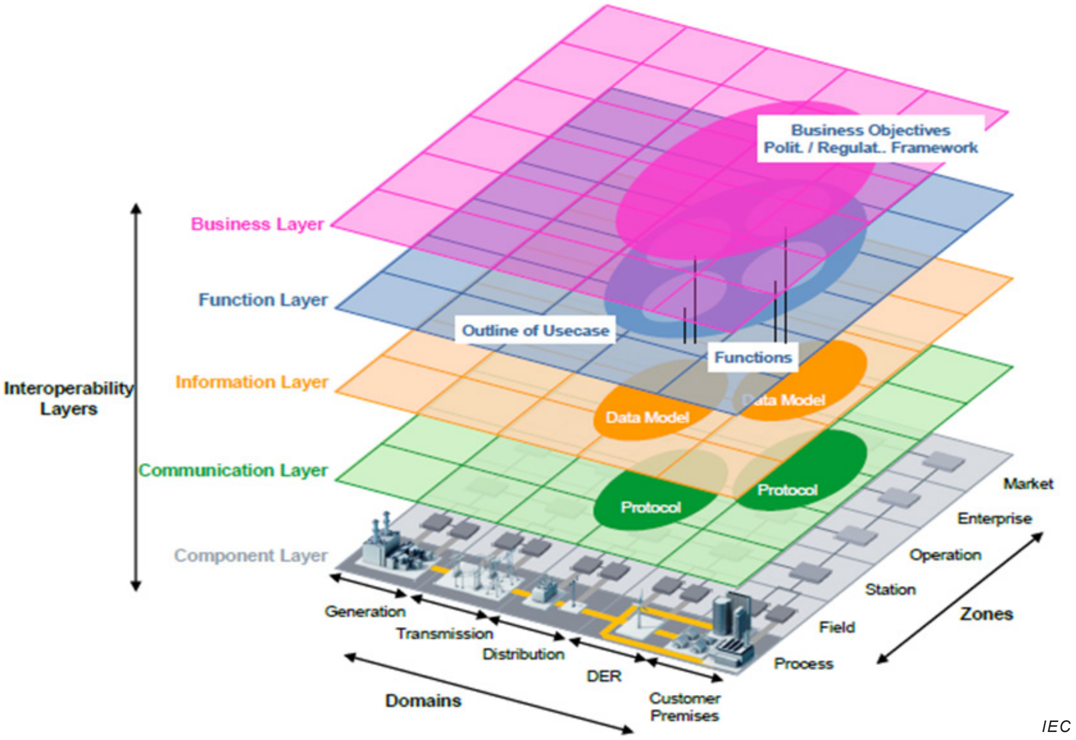


Figure 2 – Smart Grid Architecture Model (SGAM)

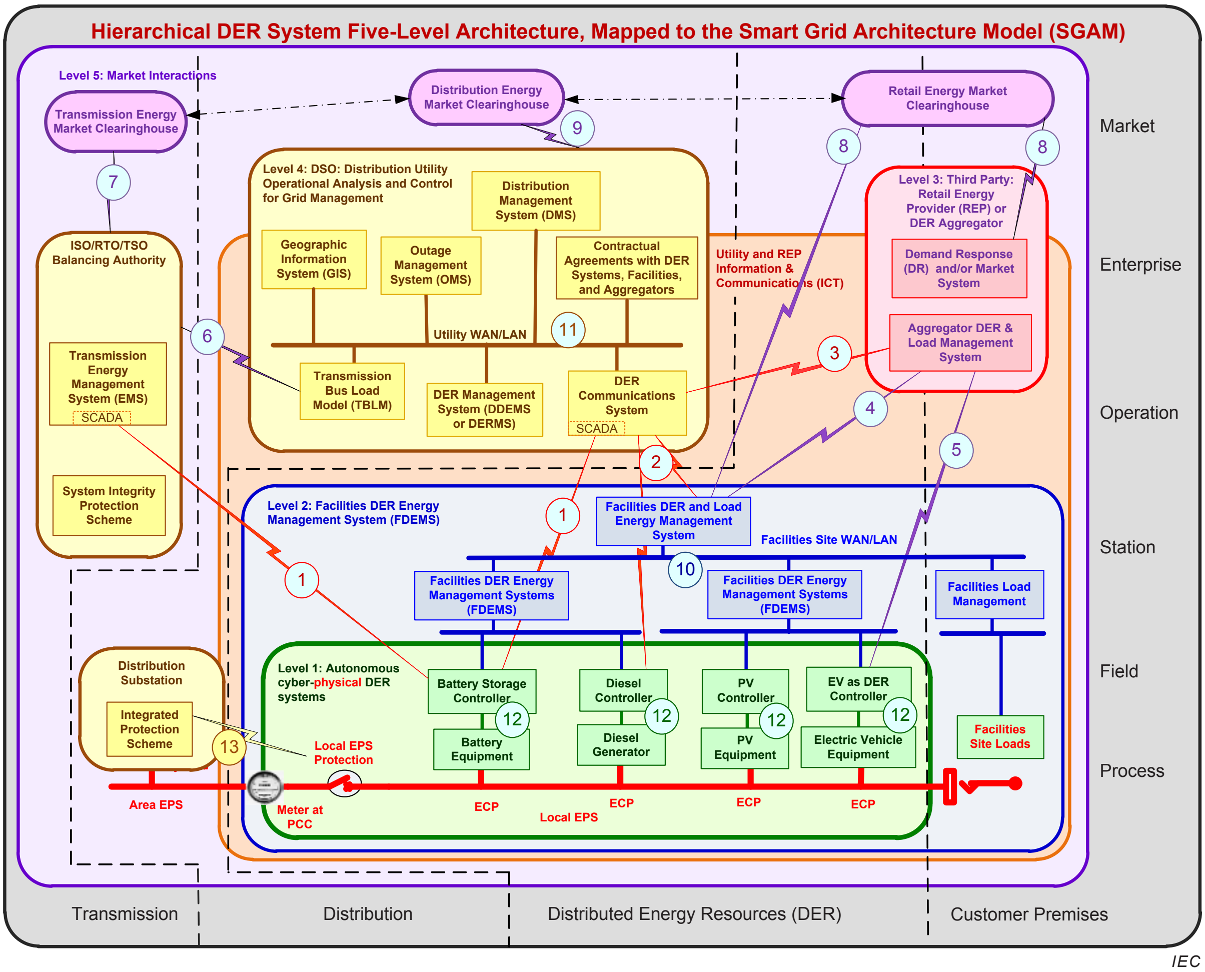

Hierarchical DER System Five-Level Architecture, Mapped to the Smart Grid Architecture Model (SGAM)
Level 5: Market Interactions
Transmission Energy Market Clearinghouse
Distribution Energy Market Clearinghouse
Retail Energy Market Clearinghouse
Market
7
9
8
8
ISO/RTO/TSO Balancing Authority
Transmission Energy Management System (EMS)
SCADA
System Integrity Protection Scheme
Level 4: DSO: Distribution Utility Operational Analysis and Control for Grid Management
Distribution Management System (DMS)
Geographic Information System (GIS)
Outage Management System (OMS)
Contractual Agreements with DER Systems, Facilities, and Aggregators
Utility WAN/LAN
11
Transmission Bus Load Model (TBLM)
DER Management System (DDEMS or DERMS)
DER Communications System
SCADA
Utility and REP Information & Communications (ICT)
Level 3: Third Party: Retail Energy Provider (REP) or DER Aggregator
Demand Response (DR) and/or Market System
Aggregator DER & Load Management System
Enterprise
Operation
6
3
4
5
2
Level 2: Facilities DER Energy Management System (FDEMS)
Facilities DER and Load Energy Management System
Facilities Site WAN/LAN
1
1
10
Facilities DER Energy Management Systems (FDEMS)
Facilities DER Energy Management Systems (FDEMS)
Facilities Load Management
Station
Level 1: Autonomous cyber-physical DER systems
Battery Storage Controller
Battery Equipment
Diesel Controller
Diesel Generator
PV Controller
PV Equipment
EV as DER Controller
Electric Vehicle Equipment
12
12
12
12
Facilities Site Loads
Field
Distribution Substation
Integrated Protection Scheme
13
Local EPS Protection
Process
Area EPS
Meter at PCC
ECP
Local EPS
ECP
ECP
ECP
Transmission
Distribution
Distributed Energy Resources (DER)
Customer Premises
IEC

Figure 3 – Five-level hierarchical DER system architecture

- **Level 1: Cyber-physical DER systems** (green in Figure 3) is the lowest level and includes the actual cyber-physical DER systems themselves (*SGAM: Process and Field Zones within the Customer and DER Domains*). These DER systems will be interconnected to local grids at Electrical Connection Points (ECPs) and to the utility grid through the Point of Common Coupling (PCC) (the ECP and the PCC may be the same if the DER is directly grid-connected). These DER systems will usually be operated autonomously. In other words, these DER systems will be running based on local conditions, such as photovoltaic systems operating when the sun is shining, wind turbines operating when the wind is blowing, electric vehicles charging when plugged in by the owner, and diesel generators operating when started up by the facility operator. This autonomous operation can be modified by DER owner preferences, pre-set parameter, and commands issued by utilities and aggregators.
- **Level 2: Facilities DER management (FDEMS)** (blue in Figure 3) is the next higher level in which a Facility DER Management System (FDEMS) manages the operation of the Level 1 DER systems (*SGAM Station Zone within the Customer and DER Domains*). 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.
- **Level 3 Third parties: retail energy provider or aggregators** (red in Figure 3) shows market-based aggregators and retail energy providers (REP) who request or even command DER systems (either through the facility's FDEMS or via aggregator-provided direct communication links) to take specific actions, such as turning on or off, setting or limiting output, providing ancillary services (e.g. volt-VAr control), and other grid management functions. Aggregator DER commands would likely be price-based either to minimize customer costs or in response to utility requirements for safety and reliability

purposes. The combination of this level and level 2 may have VArying scenarios, while still fundamentally providing the same services.

- **Level 4: Distribution operational analysis** (yellow in Figure 3) applies to utility applications that are needed to determine what requests or commands should be issued to which DER systems (*SGAM: Operations and Enterprise Zones for the Distribution Domain*). DSOs monitor the power system and assess if efficiency or reliability of the power system can be improved by having DER systems modify their operations. This utility assessment involves many utility control centre 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 either directly to a DER system, indirectly through the FDEMS, or indirectly through the REP/Aggregator.
- **Level 5: Transmission and market operations** (purple in Figure 3) is the highest level, and involves the larger utility environment where Transmission System Operators (TSOs), regional transmission operators (RTOs) or independent system operators (ISOs) may need information about DER capabilities or operations and/or may request aggregated services for the bulk power system from DER systems through the distribution utility or through the REP/Aggregators. These aggregated services may be through contracts, tariffs, or market operations. (*SGAM: Operations and Enterprise Zones for the Transmission Domain* and *SGAM: Market Zone for the Customer, DER, Distribution, and Transmission Domains*).

In this technical report, only Levels 1, 2, 3, and 4 are covered. Level 5 is covered under transmission utility operations and/or market cyber security and engineering strategies, and is therefore beyond the scope of resilience for distribution power systems with DER (even though it is recognized that DER systems can impact transmission operations).

5.3 DER system interfaces

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 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 aggregators and utilities through financial and operational contracts or tariffs with DER owners.

The management of DER systems involves multiple levels of information exchanges (see circled numbers in Figure 3):

- **Interface 1** – Direct DSO interactions with DER systems between Level 4 and Level 1. These direct DSO interactions usually imply that the DER system is under contract to be managed by the DSO, such as providing energy storage for smoothing fluctuations or counteracting spikes and sags. The DSO generally uses its SCADA system for these interactions. Interaction latency requirements are typically a few seconds.
- **Interface 2** – DSO interactions with FDEMS between Level 4 and Level 2. These interactions may be for the purpose of the DSO monitoring the aggregated generation and load, usually at the PCC, with the ability of the DSO to request ancillary services, such as reactive power support, frequency support, or limiting real power output at the PCC. The DSO could also request data on generation capabilities, load forecasts, and other longer term information. The DSO could also provide updated settings and schedules for specific advanced functions, such as volt-VAr control or frequency-watt control. It could also include pricing signals. These DSO-FDEMS interactions would probably not use the real-time SCADA system (due to concerns about the volumes of data and cyber security) and could be every few minutes, or hourly, weekly, or seasonally
- **Interface 3** – DSO interactions with aggregators between Level 4 and Level 5. These interactions would be primarily for the DSO to monitor aggregated groups of DER systems

that are under the aggregator's management. These groups of DER systems would be established by the DSO, such as all DER systems on a particular feeder or feeder segment, or all DER system capable of performing the volt-VAr function. The DSO could then issue commands (or requests, depending upon the contractual relationships) to specific groups of DER systems via the aggregator.

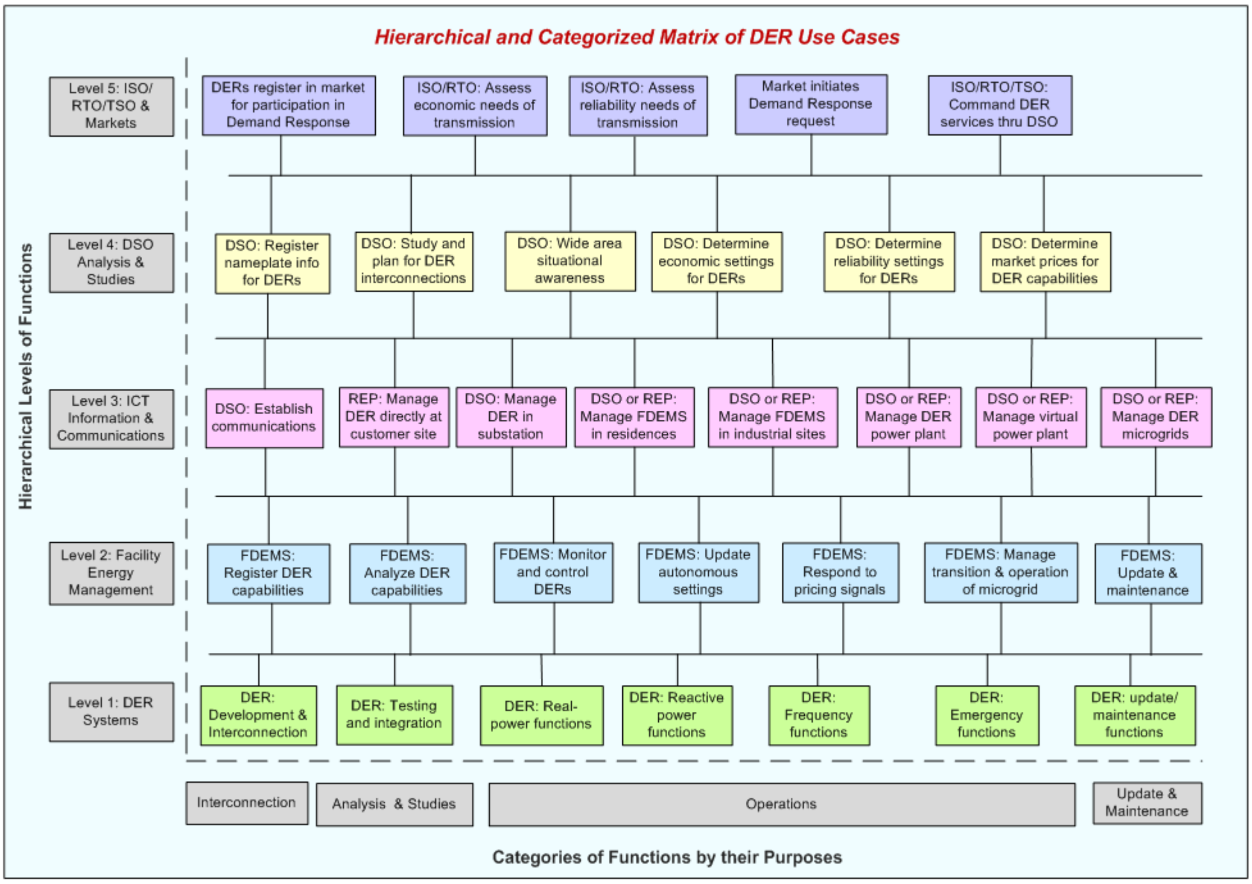
- **Interfaces 4 and 5** – Aggregator interactions with DER systems or FDEMS between Level 5 and Levels 3 and 4 (respectively). These interactions consist of monitoring and control (or requests) so that the aggregator has visibility of all DER or FDEMS under its management.
- **Interface 6** – DSO interactions with the TSO or ISO/RTO between Level 4 and Level 5. These interactions provide the TSO with the ability to request ancillary services from DER systems, FDEMS, and/or aggregators, usually by going through the DSO or any third party which can control aggregated DER systems. The TSO can also request forecasts, information on emergency situations, and other DER-related data.
- **Interfaces 7, 8, and 9** – Market interactions by the TSO, aggregators, FDEMS, and DSO (respectively) within Level 5. These interactions would be for sending and receiving market offers, bids, and/or pricing signals.
- **Interface 10** – DER management system interactions within Level 2 with multiple DER systems managed or coordinated by a FDEMS. Peer to peer interactions can also occur between DER controllers, such as between a PV controller and a battery storage controller. The FDEMS has a more global vision of all the DER systems under its control, and can allocate tasks to different DER systems, depending upon the facility operator's requests, load conditions within the facility, and possibly demand response pricing signals. It understands the overall capabilities of the DER systems under its management but may not have (or need) detailed data. FDEMS can issue direct commands but will primarily update the autonomous settings for each DER system. Interaction frequency may be seconds to minutes, hours, or even weeks.
- **Interface 11** – Internal DSO interactions among applications and systems involved with DER systems within Level 4. These interactions between applications provide the capability of the DSO to make decisions on operating the distribution system with DER systems.
- **Interface 12** – Autonomous DER behaviour in which the controller responds to sensors that sense local conditions within Level 1. Controllers are focused on direct and rapid monitoring and control of the DER hardware. Common types of autonomous DER controls include managing one or more inverters, such as a small PV system, a battery storage system, or an electric vehicle service element (EVSE). In addition to basic control, this autonomous behaviour can perform advanced "smart inverter" functions using one or more of the pre-set modes and/or schedules that respond to locally sensed conditions, such as voltage, frequency, and/or temperature. Responses could include anti-islanding ride-through protective actions, volt-VAr control, frequency-watt control, ramping from one setting to another per a schedule, soft-restart, and other functions that may be pre-set. Interaction latency requirements are typically milliseconds to seconds.
- **Interface 13** – Protection signals between substations and DER systems to permit the coordination of local and area protection schemes.

5.4 Resilience at different DER architectural levels

The different approaches to resilience reflect the various implementations of DER systems both at the different hierarchical levels and for different functional purposes. Hundreds if not thousands of different combinations of implementation configurations and functional purposes of these DER systems exist – these can be captured in use cases, but developing detailed use cases for all such configurations is impractical and counterproductive. However, for the purposes of discussing resilience requirements, DER use cases can be categorized to limit the number of variations.

DER use cases may be categorized by DER Level and by the purposes they support. The DER systems in the different categories may participate in various power system functions for different purposes. They range from initial development and interconnection of DER systems, to testing, to planning studies and analysis, to operations in near-time and real-time, to maintenance and updates. These functions can be defined as primary (local) control functions and as secondary (central) control functions. The secondary control functions use the primary control functions as actuators. Cyber security requirements for different categories of purposes may vary considerably.

These categorizations may be envisioned as shown in Figure 4. The DER use cases for operations are the most numerous and complex, but the other use cases are equally important for ensuring power system resilience.


Hierarchical and Categorized Matrix of DER Use Cases
Hierarchical Levels of Functions
Level 5: ISO/ RTO/TSO & Markets
DERs register in market for participation in Demand Response
ISO/RTO: Assess economic needs of transmission
ISO/RTO: Assess reliability needs of transmission
Market initiates Demand Response request
ISO/RTO/TSO: Command DER services thru DSO
Level 4: DSO Analysis & Studies
DSO: Register nameplate info for DERs
DSO: Study and plan for DER interconnections
DSO: Wide area situational awareness
DSO: Determine economic settings for DERs
DSO: Determine reliability settings for DERs
DSO: Determine market prices for DER capabilities
Level 3: ICT Information & Communications
DSO: Establish communications
REP: Manage DER directly at customer site
DSO: Manage DER in substation
DSO or REP: Manage FDEMS in residences
DSO or REP: Manage FDEMS in industrial sites
DSO or REP: Manage DER power plant
DSO or REP: Manage virtual power plant
DSO or REP: Manage DER microgrids
Level 2: Facility Energy Management
FDEMS: Register DER capabilities
FDEMS: Analyze DER capabilities
FDEMS: Monitor and control DERs
FDEMS: Update autonomous settings
FDEMS: Respond to pricing signals
FDEMS: Manage transition & operation of microgrid
FDEMS: Update & maintenance
Level 1: DER Systems
DER: Development & Interconnection
DER: Testing and integration
DER: Real-power functions
DER: Reactive power functions
DER: Frequency functions
DER: Emergency functions
DER: update/ maintenance functions
Interconnection
Analysis & Studies
Operations
Update & Maintenance
Categories of Functions by their Purposes

IEC

Figure 4 – Structure of use cases within the DER hierarchy

5.5 DER Systems as cyber-physical systems

5.5.1 Protecting cyber-physical DER systems

DER systems are a prime example of cyber-physical systems which combine power system operational equipment with cyber-based control of that equipment. Cyber security for DER systems, as for all cyber-physical systems, requires a different approach than for typical IT systems. As stated in the NISTIR 7628[4], *“Traditionally, cyber security for Information Technology (IT) focuses on the protection required to ensure the confidentiality, integrity, and availability of the electronic information communication systems. Cyber security needs to be appropriately applied to the combined power system and IT communication system domains to maintain the reliability of the Smart Grid and privacy of consumer information. Cyber security in the Smart Grid must include a balance of both power and cyber system*

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

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."

DER systems are cyber-physical systems where resilience to adverse external forces is a primary goal. Both physical and cyber actions can have "real-world" impacts. Physically, 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 more capable and reliability. For instance, these DER 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., This combination of cyber and physical equipment in DER systems is 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 can also be the cause real-world impacts due to both malicious cyber attacks as well as inadvertent events. These cyber systems need to be protected from cyber threats, especially those that could cause harm to the physical devices or to the power system they are interconnected with. This requirement for cyber security of cyber assets is well understood – what is not as well understood is how best to combine the protections provided by cyber technologies with the physical engineering technologies built into power system design and functions for over 100 years to provide the required resilience.

So cyber-physical systems should be designed to protect themselves not only from inadvertent failures and mistakes, but also from deliberate cyber attacks. They should also be designed to "cope" with attacks, since power system equipment cannot just be shut off if an attack is occurring, but should try to remain functional as much as possible. "Recovery" strategies after attacks are also important, since again the power should remain on as much as feasible even if equipment is removed for repair. Finally, time-stamped forensic alarm and event logs should capture as much information as possible about the attack sequences for both future protection and possible legal actions. Therefore both cyber and engineering strategies should focus on preventing cyber attacks and mitigating the impacts of successful attacks.

5.5.2 Cyber-physical threats

Cyber security for cyber-physical systems is mostly the same as for purely cyber systems, but there are some important differences that can affect the resilience of the cyber-physical systems.

- Physical impacts: Cyber attacks (whether deliberate or inadvertent) can cause physical results, such as power outages and damaged equipment. Successful attacks that modify data may not only affect that data, but more importantly can cause some physical world impact either immediately or in the future.
- Cyber-physical protections and mitigations: Since cyber-physical systems already are designed with engineering 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 cyber security: 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 cyber security mitigations should be carefully woven into cyber-physical engineering mitigations to ensure that the primary functionality is maintained, even during attacks.

5.5.3 Resilience measures for cyber-physical systems

Resilience measures for cyber-physical systems need to include a combination of information cyber security measures and physical engineering strategies. An illustration of resilience for cyber-physical systems is shown in Figure 5, in which engineering strategies (designs and operations) can help protect against cyber attacks, and cyber security measures can help protect against engineering failures, mistakes, and natural disasters. The information is also listed in Table 1 and Table 2.

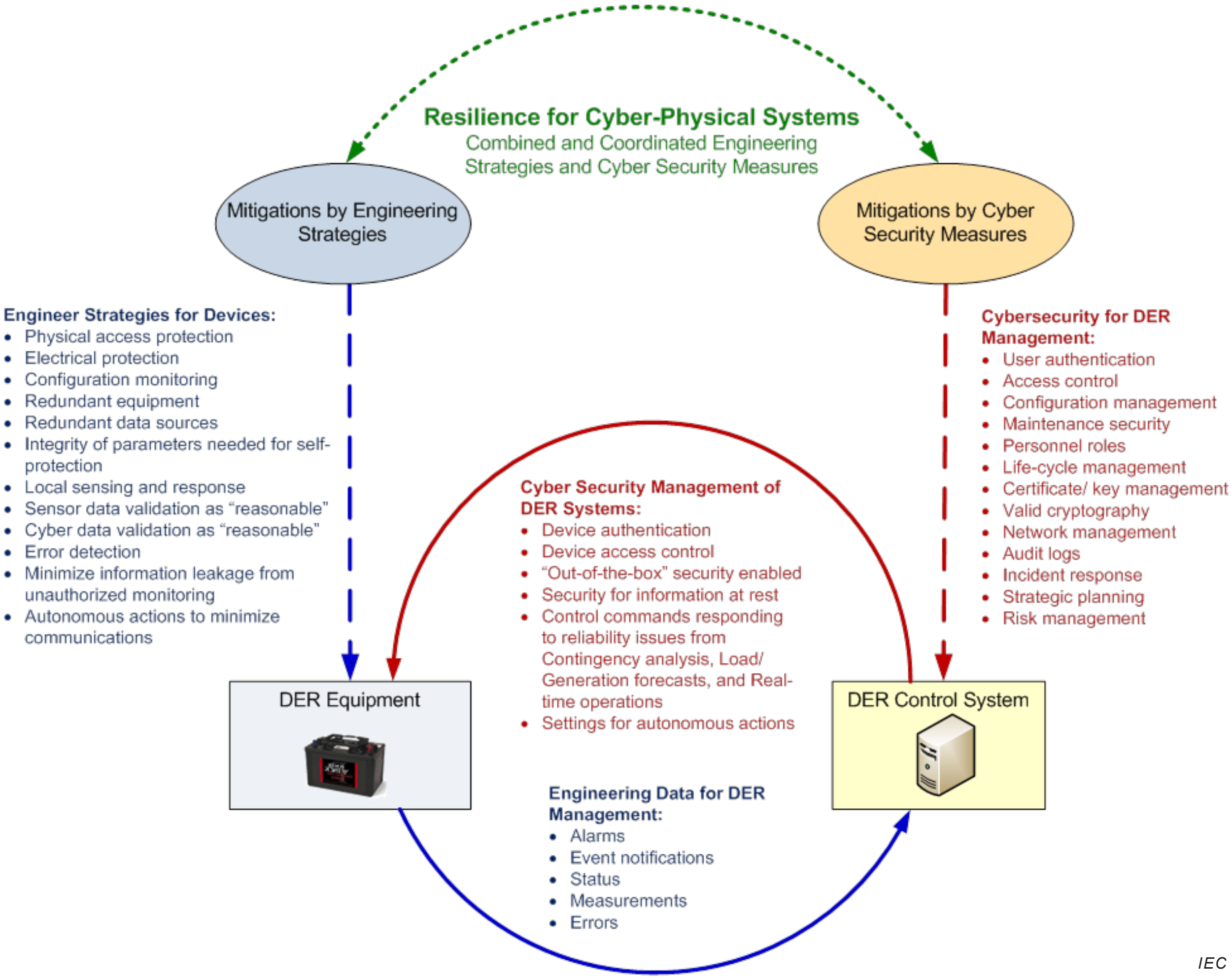

Resilience for Cyber-Physical Systems
Combined and Coordinated Engineering Strategies and Cyber Security Measures
Mitigations by Engineering Strategies
Mitigations by Cyber Security Measures
Engineer Strategies for Devices:
Physical access protection
Electrical protection
Configuration monitoring
Redundant equipment
Redundant data sources
Integrity of parameters needed for self-protection
Local sensing and response
Sensor data validation as "reasonable"
Cyber data validation as "reasonable"
Error detection
Minimize information leakage from unauthorized monitoring
Autonomous actions to minimize communications
Cybersecurity for DER Management:
User authentication
Access control
Configuration management
Maintenance security
Personnel roles
Life-cycle management
Certificate/ key management
Valid cryptography
Network management
Audit logs
Incident response
Strategic planning
Risk management
Cyber Security Management of DER Systems:
Device authentication
Device access control
"Out-of-the-box" security enabled
Security for information at rest
Control commands responding to reliability issues from Contingency analysis, Load/ Generation forecasts, and Real-time operations
Settings for autonomous actions
DER Equipment
DER Control System
Engineering Data for DER Management:
Alarms
Event notifications
Status
Measurements
Errors
IEC

Figure 5 – Mitigations by engineering strategies and cyber security measures

Table 1 – Examples of mitigations by engineering strategies and cyber security techniques

Mitigations by engineering strategy techniques	Mitigations by cyber security techniques
Physical access control, e.g. cages, locked doors, alarm systems, etc. 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” Calculated data validation as “reasonable” Error detection Alarms and events on physical changes Redundant equipment Redundant data sources Redundant communication paths Configuration validation and monitoring Securing the integrity of parameters that are needed for self-protection even from local access Autonomous actions that minimize the need for communications	User identity and authentication Role-based access control Access control management Authorization Non-repudiation System configuration management Maintenance security Personnel roles Life-cycle management Valid cryptography for authentication, 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 Configuration protection

Table 2 – Engineering and cyber security data for managing the resilience of DER systems

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

6 Threats, vulnerabilities, and impacts on power system resilience

6.1 Threats – engineering and cyber

6.1.1 Physical and electrical threats – mostly but not entirely inadvertent

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

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

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

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

- Anti-islanding failures. Under certain circumstances DER systems may not properly disconnect when the grid does experience an outage, thus failing to detect an electrical "island". This situation can be a serious safety hazard.
- Power system instability. Variations in DER generation due to unmanaged and unmonitored DER systems can cause power system instability and possibly widespread power outages.
- Fluctuating energy output. Fluctuations in DER energy output due to Variable renewable energy sources or responses to local loads can cause changes in voltage and frequency which may cause them to exceed their normal ranges.
- Unnecessary DER disconnections. If voltage and/or frequency exceed their normal ranges, DER systems may cease energizing the grid and disconnect, thus worsening a situation that might otherwise have been recovered from.
- Reverse power flows. Unmonitored DER output can cause back-feeding in substations that are not designed for reverse power flows.

6.1.2 Cyber threats – inadvertent and deliberate

6.1.2.1 General

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

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

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.

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

Threat agents can be defined as one of the following:

- Malicious person *[malicious]* who is deliberately attacking systems for financial, power, revenge, or other gain
- Inadvertent mistake *[error]* caused by a person who either failed to pay attention or did not recognize the consequences of their action. Computer applications can also have “bugs” or other flaws that cause them to mis-operate. Poorly designed systems and inadequate operating procedures also fall In this category.
- Equipment failure *[failure]* that was not any person’s fault, but reflects the fact that electronic and mechanical devices can fail. Equipment that responds in unexpected ways to normal conditions can also be placed in this category.
- Natural disasters *[disaster]* caused by events completely outside the control of humans.

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

6.1.2.2 Inadvertent threats

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

- Safety failures: Safety has always been a primary concern for any power system facilities, and should 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 defence, but monitoring of the status of key equipment and the logging/alarming of compliance to safety procedures can enhance safety to a significant degree.

- Equipment failures: Equipment failures are the most common and expected threats to the reliable operation of the power system. Often the monitoring of the physical status of DER equipment can also benefit maintenance efficiency, possible prevention of certain types of equipment failures, real-time detection of failures not previously monitored, and forensic analysis of equipment failure processes and impacts.
- Software/firmware malfunctions: Software and firmware malfunctions (e.g. bugs, crashes, and incorrect results) can still occur even if systems are thoroughly tested, often due to the complexity of the software and how it interacts with the operating system or other software applications. Newly implemented or upgraded software applications are particularly vulnerable to malfunctions, while patches and upgrades to reliable software can sometimes cause malfunctions.
- Mistakes, carelessness, or lack of knowledge: Mistakes caused by carelessness or just a lack of knowledge is one of the “threats” to protecting DER systems, whether it is not locking doors or inadvertently allowing unauthorized personnel to access passwords, keys, and other security safeguards. Often this carelessness is due to complacency (“no one has ever harmed this DER system yet”) or inexperience (“I didn’t realize that the email did not come from the DER manufacturer, and so I provided the attacker with my password into the DER system”).
- Natural disasters: Natural disasters, such as storms, hurricanes, and earthquakes, can lead to widespread power system failures, safety breaches, and opportunities for theft, vandalism, and terrorism. Monitoring of the physical and cyber status of DER systems in real-time can provide the “eyes and ears” to understand what is taking place and to take ameliorating actions with respect to the utilization of DER to minimize the impact of these natural disasters on power system operations.

6.1.2.3 Deliberate threats

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

- Disgruntled employee: Disgruntled employees are an important threat for attacks on power system assets, including DER systems. Unhappy employees who have the detailed knowledge to do harm can cause significantly more damage than a non-employee, particularly in the power system industry where the DER equipment and supporting systems are unique to the industry.
- Industrial espionage: Industrial espionage in the power system industry is becoming more of a threat as deregulation and competition involving millions of dollars provide growing incentives for unauthorized access to information – and the possible damaging of equipment for nefarious purposes. DER systems are particularly vulnerable since they are usually located in relatively unprotected environments on customer property. In addition to financial gains, some attackers could gain “socio/political” benefits through “showing up” the incompetence or unreliability of competitors.
- Vandalism: Vandalism can damage facilities and equipment with no specific gain to the attackers other than the act of doing it, and the proof to themselves and others that they can do it. Often, the vandals are unaware of or do not care about the possible consequences of their actions.
- Again, DER systems may be particularly vulnerable to vandalism, partly because of their unprotected environments, but also because their generation capabilities can directly affect the power grid, including causing outages.
- Cyber hackers: Cyber hackers are people who seek to breach cyber security for gain. This gain may be directly monetary, industrial knowledge, political, social, or just individual

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

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

6.2 Vulnerabilities – engineering and cyber vulnerabilities

6.2.1 General

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

6.2.2 Power system vulnerabilities and attacks

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

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

Some of the causes of these types of vulnerabilities include:

- Equipment vulnerabilities: Equipment failures could cause improper operations. For instance, a circuit breaker fails to trip during a short circuit event, causing power equipment to overload and burn, and personnel to be electrocuted.
- Complexity of analysis: Complexity of analysis of large numbers of DERs could provide incorrect results. For example, engineers who set protective relay parameters have not taken into account certain types of contingencies, so that one event causes a second event, and causes a cascading failure of the power system, resulting in major outages.
- Lack of standardized operating procedures: Lack of standardized operating procedures could cause misunderstandings and results in incorrect actions, incorrect responses to situations, and confusion during emergencies.
- Incorrect settings: Incorrect settings could cause incorrect responses to power system situations. For instance, DER systems have not included appropriate voltage and frequency ride-through settings, which results in numerous outages whenever voltage and frequency fluctuations occur due to storms or rapid changes in sunlight or wind.
- Inability to detect loss of grid power: The inability of DER systems to detect the loss of grid power could cause safety concerns as well as uncertainty and delay in addressing emergency situations. For example, DER systems which are supposed to disconnect upon the loss of the grid power, do not disconnect because their traditional anti-islanding methods fail to detect the loss of power due to masking by other DER systems or their own smart DER volt-VAr functions, causing safety problems and equipment damage.
- Inadequate analysis capabilities: Inadequate analysis capabilities of software applications could result in sending invalid pricing signals, control settings, and control commands to DER systems. For instance, inadequate analysis of the location and amount of DER generation causes over or under voltage or frequency events and results in large scale outages.
- Inadequate personnel training: Inadequate personnel training could result in poor judgment on actions. For example, inadequately trained crews fail to disconnect DER systems during system maintenance activities, or inadequately trained fire and police on how to cope with DER systems, leading to safety problems and outages.
- Manipulated or mistaken market prices: Manipulated or mistaken market prices could result in uneconomical or unfair actions. For instance, market pricing signals call for decreased generation when actually more generation is needed, leading to higher prices for spot generation or even outages.
- Inadequately structured authority hierarchy: Inadequately structured authority or contractual hierarchy could cause confusion during emergencies. For example, a DER operator ignores utility-set limits and generates more than the utility circuit can handle, damaging substation equipment and causing outages.
- Degradation in analysis accuracy: Degradation over time in analysis accuracy due to the rapid growth and resulting increasingly complex interactions between DER systems, could cause increasing reliability and power quality problems. For instance, DER systems are expanding rapidly in their number and types of deployments, resulting in increasingly complex interactions between them and also between these DER systems and other grid equipment, leading to incorrect settings and non-optimal actions by operators.
- Incomplete testing of complex intelligent DER systems: Multiple DER systems, each with complex intelligent behaviour, could cause unsafe or unexpected actions because their complexity inhibits the testing of all possible combinations of situations. For instance, intelligent DER systems capable of undertaking many new functionalities, tend to have more design and operational errors because development is more complex and testing just cannot cover all possible types of interactions. Often there are unintended

consequences to actions in complex environments that may not be evident in simpler environments.

- Inadequately specified requirements: Inadequately specified requirements for DER systems cause unsafe or unexpected actions, because the systems that are not well understood could lead to errors in development and performance. For instance, the requirements for managing high penetrations of DER systems in coordination with existing distribution equipment are still under extensive study.
- Mismatched assumptions between organizations: Mismatched assumptions between organizations could result in confused or incorrect actions. For instance, if one organization uses encryption techniques or some settings not supported by another organization, then the expected interactions will not take place.
- Lack of confidence in analysis results: Lack of confidence in analysis could result in slow responses to problems. For example, some power flow studies or DER generation forecasts or other complex analyses may not be trusted by operators, possibly due to previous failures or inexperience with the type of analysis, leading to personnel responding slowly or taking incorrect actions.
- Inadequate change management procedures: Inadequate change management could cause decisions to be made on inaccurate data. For example, inadequate management of changes to systems, which should include pre-testing of the changes and the ability to restore a previous version if the changed system fails to operate correctly, could cause failures and incorrect results.

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

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

6.2.3 Cyber security vulnerabilities and attacks

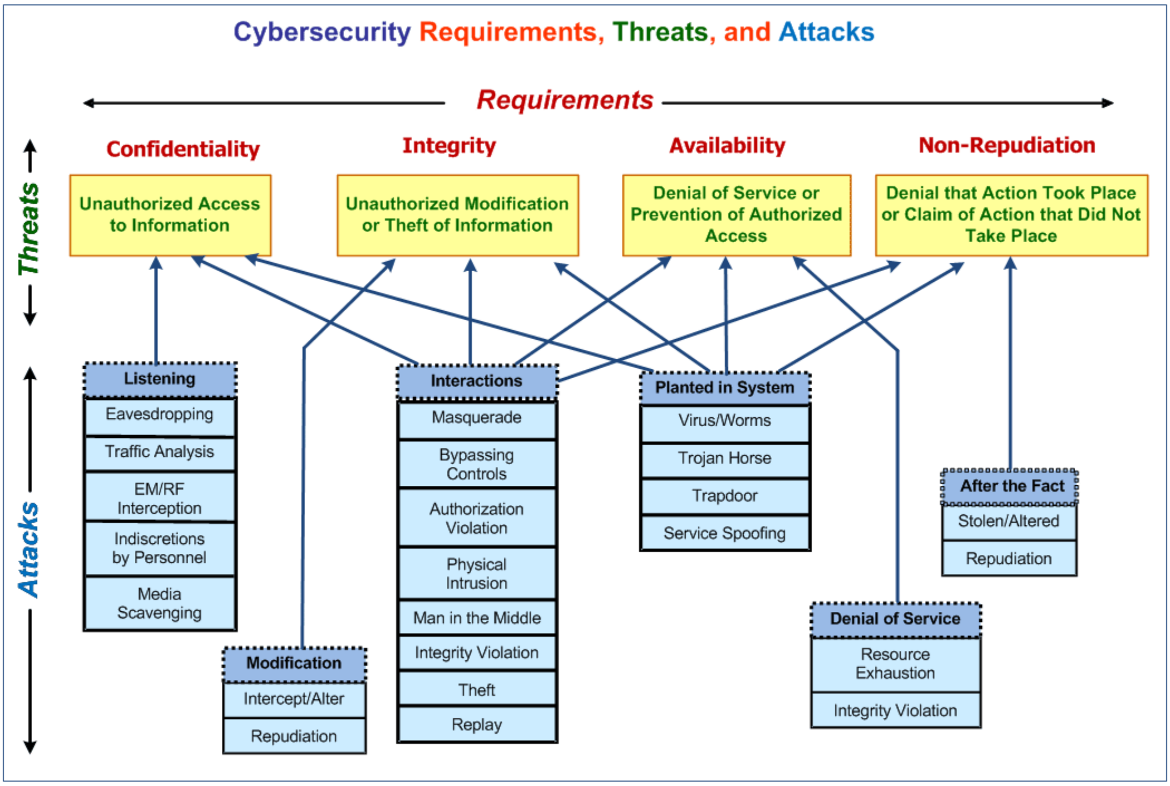
The threats can be realized by many different types of attacks, some of which are illustrated in Figure 6. Often an attack takes advantage of a vulnerability, which may be due to human carelessness, an inadequately designed system, or circumstances such as a major storm. As can be seen, the same type 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 features, even if they exist, are never “turned on”.
- Indiscretions by personnel: Employees write down their username and passwords and place them in their desk drawer.
- Simple or easy-to-guess passwords: Employees use short alpha-only passwords or use their dog’s name and/or their birthday as their password.
- Social engineering: An attacker uses personal information or subterfuge to learn a user’s password, such as pretending to be from a bank or leaning over someone’s shoulder as they type their password.
- Bypass controls: Employees turn off security measures, do not change default passwords, or everyone uses the same password to access all substation equipment. Alternatively, a software application is assumed to be in a secure environment, so does not authenticate its actions.
- Integrity violation: Data is modified without adequate validation, such that the modified data causes equipment to malfunction or allows access to unauthorized users or applications.
- Software updates and patches: The software is updated without adequate testing or validation such that worms, viruses, and Trojan Horses are allowed into otherwise secure systems. Alternatively, security patches needed to fix vulnerabilities are not applied.
- Lack of trust: Different organizations have different security requirements and use different cyber security standards.

Some common types of attacks include:

- Eavesdropping: a hacker “listens” to confidential or private data as it is transmitted, thus stealing the information. This is typically used to access intellectual property, market and financial data, personnel data, and other sensitive information.
- Masquerade: a hacker uses someone else’s credentials to pretend to be an authorized user, and thus able to steal information, take unauthorized actions, and possibly “plant” malware.
- Man-in-the-middle: a gateway, data server, communications channel, or other non-end equipment is compromised, so the data that is supposed to flow through this middle node is read or modified before it is sent on its way.
- Resource exhaustion: equipment is inadvertently (or deliberately) overloaded and cannot therefore perform its functions. Alternatively, a certificate expires and prevents access to equipment. This denial of service can seriously impact a power system operator trying to control the power system.
- Replay: a command being sent from one system to another is copied by an attacker. This command is then used at some other time to further the attacker’s purpose, such as tripping a breaker or limiting generation output.
- Trojan horse: the attacker adds malware to a system, possibly as part of an innocent-appearing enhancement or application, and possibly during the supply chain (e.g. during component manufacturing or system integration or shipping or during installation). This malware does nothing until some circumstance locally or remotely triggers it to cause an unauthorized action.



IEC

Figure 6 – Security requirements, threats, and possible attacks

6.3 Risk management and mitigation techniques

6.3.1 Risk handling

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

- The risk can be accepted (no measures taken to mitigate it) because the expected likelihood and impact of an event does not appear to be worth the cost of implementing mitigation measures. For instance, requiring redundant communications to all DER systems would most likely not be worth the cost of implementing such redundancy.
- The risk can be shared, for instance by paying an insurance company to take on the risk. This approach is often used for protection against the loss of physical assets such as buildings and the physical DER equipment.
- The risk can be transferred, for instance by contracting a third party to take responsibility for operating and maintaining DER systems.
- The risk can be mitigated to different levels. For instance, some DER systems may require only the use of username/password for access control protection, while other DER systems may require two-party authentication and cryptographic certificate verification for any access.

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

6.3.2 Risk mitigation categories

Mitigations against the effects of attacks and failures are often described as having eight categories. Associated security countermeasures can mitigate one or more of these purposes; these mitigations are illustrated in Table 3:

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

Table 3 – Examples of mitigation categories for cyber-physical systems

	Category	Description	Power engineering examples	Cyber examples

Protection and deterrence before failure or attack	**Preparation and protection against a failure or attack**	Active measures used in normal circumstances that are designed to prevent an attack	Erect substation fences;
			Limit access to control center;
			Specify robust, hardened equipment
			Design the power system with adequate flexibility to handle anomalous situations;
			Deploy redundant equipment;
			Establish default system settings to failures;
			Establish autonomous modes of operation in case of lack or loss of communications;
			Perform contingency analysis studies on power system conditions;
			Design communication networks to be isolated from each other;
			Train personnel adequately
				Design systems and applications to handle anomalous situations;
				Test all software applications for both normal operations and anomalous situations;
				Validate data entry;
				Require message authentication;
				Require strong passwords;
				Use role-based access control;
				Encrypt confidential messages;
				Disable unneeded ports/services;
				Require non-repudiation methods;
				Validate patches before implementing them;

	Deterrence to a failure or attack	Preparing for a possible failure or discouraging someone from engaging in an attack	Develop emergency operations plans and procedures; Test emergency plans periodically; Display signs indicating danger or private property; Warn of legal actions; Deploy CCTV cameras; Change system settings for storms or other natural disasters; Test new software and systems; Assess potential failure impacts of all additions to the power system	Develop emergency plans for network failures; Display warnings when applications or data are modified; Require legal acceptance when installing software
Detection, assessment, response, and coping during failure or attack	**Detection of a failure or attack**	Identifying a failure or attack and notifying appropriate entities	Monitor power system status and measurements; enter events in event log; alarm operators; initiate cellphone call to on-duty person; provide quality flags for monitored data	Detect intrusions; check signatures; scan for viruses; monitor network configurations; alarm security personnel

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

6.4 Impacts on power system resilience

6.4.1 Safety impacts

Safety is the overarching concern of power system management. Any threat that could involve the safety of utility crews or the general public is taken very seriously, and mitigations to that threat are required.

The most serious safety concerns involve people contacting "live" power lines or equipment, with the danger of them being electrocuted or badly burned. Additional safety concerns from "live" power are reactions to otherwise non-fatal electric shocks, such as falling from a ladder or causing a heart attack.

DER systems, if they do not disconnect in a timely manner upon loss of external power (anti-islanding), could become a significant cause of these safety events. DER system configurations, particularly of mixed DER types that compensate for each other, that result in close-to-zero power flow at the PCC might not detect an (unintentional) islanded situation. If a cyber attack causes DER systems to remain connected by subverting the normal settings and sending “stay connected” signals, these DER systems could continue to output power and thus cause harm to people and equipment.

Safety impacts are not only from live power lines, but from the loss of power. Aggregations of DER systems, if they disconnect too rapidly after some anomalous voltage or frequency events, can cause cascading power outages. Some examples of people and situations that have their safety impacted by power outages include:

- People who rely on uninterrupted power for health reasons, such as medical ventilator systems for breathing
- Patients in hospitals who are being operated on or whose life is being sustained by electrical equipment
- Workers in environments that need electrical equipment for health, such as ventilator fans in mines
- Industrial or research plants that rely on negative pressure areas to prevent airborne diseases or harmful chemicals from dispersing into the atmosphere
- Nuclear power plants that rely on electrically driven water pumps to keep the nuclear fuel cool
- Traffic management signals that direct cars and trains to avoid crashes
- Loss of street lighting in urban areas exacerbates the possibility of looting, riots, and other crimes

6.4.2 Power outage impacts

Power outages can have many additional impacts than just safety. Predominantly, they affect the finances of businesses who rely on electricity to keep their shops open, on computers, or on electrically-driven equipment.

Even residential customers who may not have direct financial impacts from the loss of power can feel quality-of-life impacts, including cold, heat, fear of the dark, lack of mobility if they use elevators, loss of refrigerated food, inability to use computers or television, and other impacts that reliance on electricity has fostered.

Most outages are local, thus affecting only small groups of people for short durations. However, some outages (often caused by natural disasters like Hurricanes Katrina and Sandy and the Japanese earthquake of 2011) can affect millions of people for days or weeks. These long duration outages can aggravate already devastating circumstances. People have to leave their homes to seek shelter, warmth, food, clean water, and protection.

Aggregations of even the smaller DER systems can cause power outages, particularly during low-load situations, by causing reverse power flows on lines and into substations that have not been designed to handle this backflow. Since renewable DER systems often have major fluctuations in their output, they may cause power outage events if bulk generation cannot compensate in a timely manner. DER systems are often used to meet the load within a facility, but the utility may not be aware of the magnitude of that load, and might not be able to compensate upon loss of the DER systems. Cyber attacks on individual large DER systems or aggregations of DER systems can cause these systems to disconnect unexpectedly and potentially cause local or wide-spread outages.

It is expected that the risk of local and even wide-scale outages will increase in the near future, until the coordination issues between large aggregations of DER systems and bulk generation are studied and better managed, and/or microgrids can provide local islands of power.

6.4.3 Power quality impacts

Power quality covers the divergence of the power from “nominal” values, including voltage spikes and sags, frequency fluctuations, undesired VArs, harmonics, and other anomalous power characteristics. Power quality problems are usually caused by customer equipment such as customer motors, battery chargers, utility capacitor bank switching, and industrial equipment that involves rapid switching or load changes. (Power quality is sometimes defined as including power outages, but for impact purposes, outages are treated separately).

Power quality anomalies typically do not have as much of an impact as outages, but can cause damage to equipment, particularly utility transformers and the increasingly sensitive equipment used in hospitals, factories, and research facilities. This equipment can show incorrect results or can shut down or fail, causing loss of productivity. Some power quality anomalies can harm air conditioners and decrease the life of light bulbs.

Utilities often try to implement Conservation Voltage Reduction (CVR) to lower the total amount of energy used, while still maintaining the system voltage within normal limits. This lower voltage approach means that anomalies in voltage and VArs could cause voltage sags more easily.

Renewable DER systems can cause power quality impacts simply because their output is determined by the sun or wind energy which can vary significantly within seconds. These output fluctuations can cause harmonics as well as voltage spikes and sags and even frequency variations. Although active voltage management by DER systems are expected to improve power quality, some configurations of multiple DER systems trying to manage voltage may actually cause voltage oscillations if they are not properly coordinated. DER systems that actively respond to local conditions may also cause distribution equipment such as load tap changers and voltage regulators to oscillate as well. The coordination required to establish appropriate settings and timings for all these devices will require significant analysis.

Even the reconnection of power after an outage can have power quality impacts. Rapid connections can cause voltage spikes or frequency fluctuations that can harm equipment. Particularly after long duration outages, situations can occur where people have forgotten the on/off status of equipment. For instance, when some people left a pizza box on an electric stove during an outage, their kitchen burned when the power came on in the middle of the night.

Aggregations of DER systems can cause power quality impacts by all of them connecting or disconnecting from the grid at the same time, either due to poor planning or because of a cyber attack. DER systems can also aggravate power quality if their output does not try to compensate for the local power quality anomalies.

6.4.4 Financial impacts

The most obvious impacts of power system anomalies are financial, although getting a true estimate of these financial impacts is virtually impossible. For utilities, outages can cause loss of revenue but more importantly can require the expenses of truck rolls and maintenance crews. For commercial and industrial customers, power outages can directly affect their revenue streams and may increase their costs, particularly if they have to generate their own backup power. For police, outages can require additional police presence. If major blackouts occur, there could be major financial impacts on a country’s Gross Domestic Product (GDP).

However, other types of financial impacts also should be recognized. If more expensive generators need to be used during peak loads or upon the failure of less expensive generators or for reserve power, then the total cost of generation increases. Demand response can mitigate this cost by providing incentives for customers to decrease their loads.

Alternatively DER systems (including storage units) can increase their output. So the loss of DER systems through cyber attacks or unnecessary disconnections can impact the overall cost of power, as well as the cost to the DER owner.

6.4.5 Regulatory and legal impacts

Most utilities are regulated by national, state, municipal, or other regulators. If regulations are not followed or regulation goals are not adequately met, these regulators could impose penalties. Currently DER systems are not generally directly regulated, but their impact on utility operations can have regulatory impacts. For instance, if voltage is not maintained within normal limits or too many DER-caused outages affect the utility's CAIDI or SAIFI indices, regulators may take actions.

Where market-driven approaches are permitted by regulations, these markets could make operating the power system more uncertain. For instance, if a specific price is set for generation during one hour, it is the DER owners, not the DSO, who will determine whether or not to generate, leaving the DSO uncertain on how much generation will actually be available. If market approaches are also applied to ancillary services such as load following or frequency management, then these additional uncertainties may make the DSO generation/load balancing activity more inaccurate. If cyber attacks on the energy market cause incorrect prices to be issued, then not only could there be financial impacts for some of the stakeholders, but the DSO may not easily manage the consequences.

6.4.6 Environmental impacts

Bulk power generators are subject to environmental regulations for air pollution and water pollution. Environmental requirements also limit the amount of harmful substances (including NOx, particulate matter, CO, CO_2, and noise pollution) that DER systems, particularly diesel generators, can emit over time. If these limits are not met, penalties can be assessed against the generator owners.

6.4.7 Goodwill and other "soft" impacts

Some impacts, such as "goodwill", are not really quantifiable. If customers do not believe that utilities or DER owners are acting in the best interests of the society as a whole, they can start to push against them. For instance, in some regions, the installation of automated metering systems has been fought against as either a health concern and/or an invasion of privacy. Owners of DER systems, although responsible for the capital expenditures for installing the DER systems, can be viewed as no longer equally sharing the burden of paying for electricity over time, leaving that burden on those who cannot afford to install DER systems.

6.5 DER stakeholders' resilience responsibilities

Different DER stakeholders have different responsibilities for meeting the resilience requirements for interconnecting and operating DER systems within the utility power system and for mitigating impacts before, during, and after an attack or failure. These stakeholders include:

- Manufacturers: Manufacturers should design and implement DER systems, including their software and firmware applications, to meet self-protection and grid protection requirements and should provide the tools and hooks for other stakeholders to apply additional cyber and engineering security.
- Integrators and installers: Integrators can combine DER systems with other power components to design "turn-key systems" or to develop microgrids at a facility. All software and firmware applications in these integrated systems should be designed according to resilience requirements. Installers of individual DER systems as well as these integrated systems should ensure that configurations, communications, and startup settings are tested and conform to the resilience requirements of the DSO power system interconnection obligations.

- Testing personnel: Testing personnel should test DER systems not only for their ability to correctly perform functions, but also to handle or respond to anomalous situations, including cyber attacks, component failures, performance degradations, and availability degradations.
- DER owners and users: DER owners and other non-operational users should be constrained by role-based access control (RBAC) requirements to only have permissions for actions associated with their roles. Since these DER owners and users are often not power system experts or resilience experts, the RBAC permissions should be carefully defined and strongly sustained. For smaller DER installations, these access controls could be fixed during manufacturing or installation, while larger DER installations could provide flexibility for on-site assignment of roles and access rights.
- Information and communication technology (ICT) designers: ICT designers should ensure that the communications infrastructures are designed for resilience, including internal DER communications, intra-facility communications, communications to DSOs, communications to retail energy providers, and communications with any external users. For each of these areas, the ICT resilience designs should cover the media, networks, protocols, and cyber security management.
- DER operators: DER operators should ensure that those DER systems under their control meet the resilience operational requirements while operating DER systems and should initiate mitigations during and after a cyber attack or engineering failure.
- DSO operators: DSO operators should ensure that DER systems that interconnect to their power system meet the resilience requirements. They should also ensure that DER systems are operated according to resilience requirements, and should initiate mitigations during and after a cyber attack or engineering failure.
- Maintenance personnel: Maintenance personnel should ensure that any maintenance activities, particularly any updated software, firmware, hardware, and data, meet the resilience requirements.
- Security and forensic engineers: Security and forensic engineers should ensure that all the alarming, logging, and reporting meet the resilience requirements for capturing all anomalous events and that the appropriate mitigations were activated during and after a cyber attack or engineering failure.
- Training personnel: Training personnel should ensure that key civil servants such as firefighters, police, and security personnel are trained to understand what safety methods should be used for interacting with DER systems.

6.6 Resilience Measures for DER systems to counter threats

6.6.1 General IT cyber security approach for DER systems

Information technology (IT) cyber security is typically seen as providing confidentiality, integrity, and availability to cyber assets, while power system security is based on engineering design and operational strategies. IT and power system security should be combined to provide the resilience of the cyber-physical power system.

Cyber-physical DER systems and their interactions with cyber-physical power systems have five basic security requirements, which protect them from five basic threats:

- Authentication – preventing unauthorized interactions
- Integrity – preventing the unauthorized modification or theft of 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.
- Availability/Resilience – preventing the denial of service and ensuring authorized access to information. This concept is extended in cyber-physical concepts to include the resilience of the power system: preventing outages if possible, coping with those outages, and recovering rapidly from outages

The first four security requirements are generally met by cyber security technologies, while the fifth security requirement of preventing denial of service is usually best met through engineering strategies. However, a tightly entwined combination of cyber and engineering strategies can build on each other to provide defense-in-depth and defense-in-breadth.

For DER systems, authentication and integrity are the most important security requirements, although the others follow close behind. Authentication ensures that only authorized interactions can take place, while integrity assures that DER systems 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.

Confidentiality is usually associated with market-related data and intellectual property, as well as managing security procedures and techniques. 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, signed, and logged proof of receiving such a request, including who signed off of that request, and taking action on that request can be vital to billing and settling these transactions.

Although arguably the resilience of individual DER systems can be seen as less important than the resilience of a single large bulk power generator, in fact the combined resilience of aggregations of large numbers of even small DER systems can ultimately be more critical than a single bulk generator in the overall resilience of the power system.

6.6.2 Resilience by engineering designs and operational strategies

Ever since Edison first installed electric lights in 1882, utilities have developed many different engineering practices, functions, configurations, checks, and operational methods to help ensure the reliability and resilience of the power system. Although not “IT” cyber security measures, they do provide mitigations against many of the same types of attacks, and indeed provide defense-in-depth and coping methods that cyber security measures cannot achieve. From a power system resilience perspective, it does not matter if cyber tools are used or if power system reliability and operations 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 should be weighed against the likelihood and possible impact of a failure that could have been prevented or mitigated by that protection.

7 Level 1 DER System resilience recommendations

7.1 General

DER systems should be designed and configured with resilience as a major design factor. Resilient designs of DER controllers can protect against incorrect or unreasonable inputs and outputs. Single DER systems can be made more resilient by including hardened or redundant components, while multiple DER systems can be deployed such that they can support or back each other up.

7.2 Level 1 DER system: architecture

As seen in Figure 7, 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)[5]. The communications between DER controllers and their components is shown as (12) in Figure 7.

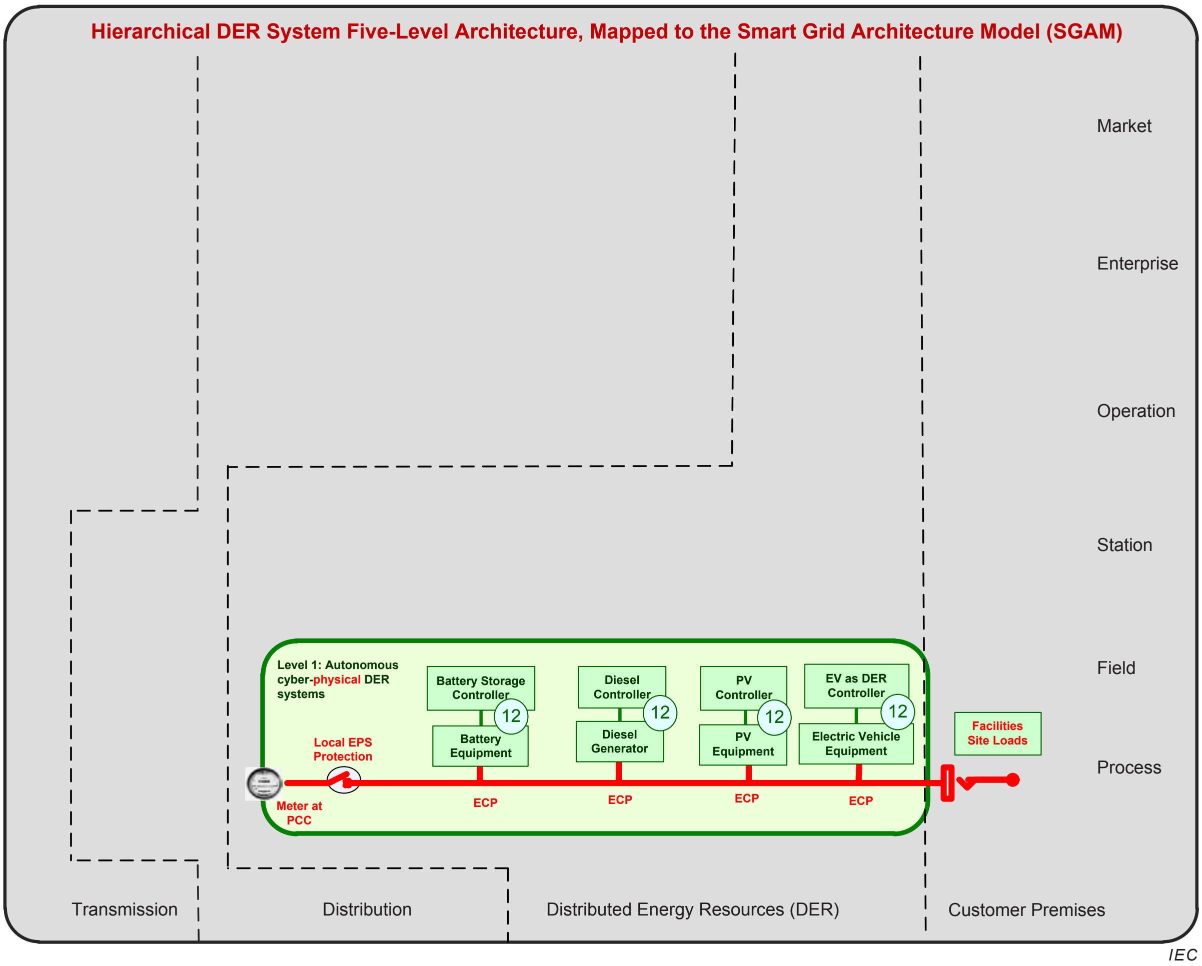


Figure 7 – Level 1: Autonomous DER systems at smaller customer and utility sites

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.

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

7.3 Level 1 DER system: vulnerabilities

7.3.1 General

Level 1 DER vulnerabilities cover cyber, engineering, and operational vulnerabilities. Cyber vulnerabilities are related to communications which consist primarily of a local HMI and local connections between the DER controller and the DER “prime mover” such as solar panels or wind turbines. In many units, such as diesel generators (gen-sets), the controller is embedded in the unit.

The engineering design and development vulnerabilities are related mostly to the manufacturer and integrator of the DER software and firmware, while the deployment and operational vulnerabilities relate to the DER system once it is operational in the field.

7.3.2 Cyber vulnerabilities

Cyber vulnerabilities cover the problems that can use cyber security techniques to minimize the likelihood of an attack/failure or to mitigate the impact of an attack/failure:

- Lack of mandatory access control through the HMI to the DER system
- Insecure communication protocol between the user interface and the DER system that allows unauthenticated changes to sensitive parameters
- Weak or no authentication on the wireless network allows an unauthorized entity to gain control of DER system through the Internet
- The wireless network allows systems to join without appropriate authorization
- The DER system does not have adequate access control to prevent unauthorized access by threat agents
- Inadequate personnel security control procedures in the vendor factory or during implementation
- The communications protocol does not provide adequate confidentiality
- The communications protocol does not notify anyone that the information has been intercepted
- Communication protocol does not protect against replay attacks (either through no security or inadequate security)
- The communication protocol used to issue the curtailing command lacks non-repudiation
- Lack of redundant access to the Certification authority (CA) when needed

7.3.3 Engineering design and development vulnerabilities

Engineering design and development vulnerabilities cover the problems that can best use engineering strategies to minimize the likelihood of an attack/failure or to mitigate the impact of an attack/failure:

- Lack of mandatory change from default password
- Poor configuration design of the DER system that permits unauthorized changes to anti-islanding protection
- Inadequate validation of software/firmware
- Inadequate testing of all DER functions
- The supply chain allows embedded malware
- The design of the application-to-application messaging scheme does not protect against changing the sequence of commands
- The time synchronization communication protocol is not secured against invalid clock changes

- Lack of adequate protection against modifying audit logs
- Lack of validation of invalid messages
- Lack of alarm notification on invalid messages
- Lack of alarm on messages that were expected but not received within the appropriate time window
- Lack of default DER energy output actions upon an invalid or missing messages

7.3.4 Deployment and operational vulnerabilities

Deployment and operational vulnerabilities cover the problems that can best use installation methodologies and operational strategies to minimize the likelihood of an attack/failure or to mitigate the impact of an attack/failure:

- Inadequate physical protection of the DER user interface where it is deployed
- The installation organization allows the installation of malware
- An inept installer incorrectly sets the security features or engineering protections
- The DER system allows itself to connect to rogue or non-authorized networks
- Commands from users do not provide any indication of failures of the DER system
- The DER system as a critical asset does not require redundant confirmation of time changes
- The DER system does not notify or request confirmation of changes from the utility DER management system before taking actions
- Lack of local monitoring of the power system to detect a possible transformer overload condition
- Poor choice of default operational mode for coping with an anomalous situation
- The maintenance organization allows the installation of malware

7.4 Level 1 DER system: impacts

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. The failures of individual DER systems within power plants are likely to have only very minimal impacts.

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

However, there are some impacts that could affect utilities. Safety is a major concern if a DER system fails to disconnect during a grid outage (e.g. if the anti-islanding mechanism fails), and a person gets electrocuted from a downed power line. If the utility owns or directly operates a DER system, such as a DER system within a substation, the utility is liable for its correct operation. If a DER system is critical to the reliability of operations, its failure could affect the utility's reliability ratings (CAIDI and SAIDI).

Some attacks and failures of individual DER systems could also impact distribution grid operations. If the utility owns or directly operates a DER system, such as a DER system within a substation, the utility is liable for its correct and safe operation. If a DER system is critical to the reliability of operations, its failure could affect the utility's reliability ratings (CAIDI and SAIDI). In addition, if a cyber attack or invalid setting affects large groups of DER systems, then utility operations could be seriously impacted (aggregations of DER systems are covered in Level 3)

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

- Loss of resilience (denial of service): The DER system trips off or does not provide the energy or ancillary services required, causing loss of power that could harm people (e.g. hospital power, signal lights, etc.) and equipment.
- Safety violation: The DER system does not disconnect from the grid when required, causing potential harm to people who may come in contact with live power lines.
- Integrity violation: The DER system uses invalid operational settings and causes damage to itself or to the local electrical grid.
- Confidentiality violation: The financial or market information related to the DER system is compromised, causing financial and/or reputation losses
- Privacy violation: Private information about the owner or about the operation of the DER system is compromised, leading to privacy violations and possible criminal actions.
- Non-repudiation violation: The DER system either repudiates an action or fails to confirm an action, leading to the possibility of revenue impacts or law suits.

Table 4 identifies impacts at Level 1, and indicates possible severity degrees: Low (L), Medium (M), and High (H).

Table 4 – Level 1 impact severities due to attacks and failures of 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 Failure to disconnect from otherwise de-energized power lines, could cause electrocution	M in general H if medical impact H if failure to disconnect
Transmission power system operations impact	None likely from a single DER system 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	L
	Possible legal costs if inadequate contingency analysis studies could be proved to have caused power outages to other customers on that feeder	L
	If equipment is destroyed or vandalized, the costs for repair or replacement	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	H
	The costs for “cleaning up” the DER management system to delete any malware and to improve the cyber security mitigations	H
	If equipment is destroyed or vandalized, the costs for repair or replacement	H
DER owner privacy impact	Compromise of DER usage and marketing information could impact the DER owner	M
	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 cyber security. 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	L
	Toxic material from damaged devices such as batteries could cause environmental harm people and locations	M
	Loss of power to life safety system in a manufacturing facility dealing with toxic material could cause environmental harm to people	M

7.5 Level 1 DER system: resilience recommendations

7.5.1 General

The DER resilience recommendations and possible mitigations reflect the need to design and install DER systems at sites where the DER owners have minimal cyber security expertise and where cost-effectiveness of the DER functions are their primary goal. Therefore, cyber security should be built into the DER system, enabled "out of the box", without the requirement for the DER owners to manage complex cyber security measures, and in fact only allowing advanced users from modifying cyber security measures. In addition, the DER engineering should provide measures against inadvertent actions by inexperienced users and for validity and reasonability checking of all data.

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

7.5.2 Manufacturer: DER system design for resilience recommendations

Manufacturers should design DER systems with cyber-physical-electrical resilience as the first step of the chain to develop resilient power systems with high penetrations of DER systems.

All DER systems should have built-in physical-electrical self-protection that is 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 protections. In addition, all DER systems that are interconnected to the utility grid should include grid protection schemes, such as anti-islanding disconnection or intentional microgrid islanding.

DER systems should also have their cyber components (microchips, communication modules, etc.) protected against changes that are "operationally" unreasonable, harmful, or unsafe. In addition, components should include "proof-of-identity" to counter imitations and to provide accountability. The following is a list of DER resilience recommendations for manufacturers:

Engineering strategies

A-1. Hardware or firmware designs prevent software applications or settings from harming these hardware/firmware components. For instance, hardware switches or sensors prevent the software from running the equipment if it would overheat the equipment or while critical self-check operations are taking place.

A-2. The DER system includes setting limits to ensure that no setting changes can exceed these limits and harm the equipment.

A-3. Sensors are included to monitor critical status and measurements, such as switch status, component temperature, speed, vibration, flow, pressure, etc.

A-4. Feedback is provided for actions and commands, including success or failure as well as resulting status or measurement values.

A-5. The DER system is constrained in what hardware settings can be changed by software in the factory.

A-6. The DER system is hardened such that only essential software and applications are installed in the product.

A-7. The settings that can be changed remotely are limited to those that do not impact safety of the DER system or the grid.

A-8. Default settings that "do no harm" are used if no explicit settings are provided.

A-9. Default actions are performed upon detection of different types of anomalous conditions or failures.

A-10. The DER system validates even authorized changes to DER operational settings against what those settings are reasonably or contractually allowed to be.

A-11. The DER system rejects any compromised or invalid data, while that event is logged and appropriate entities (people or systems) notified.

A-12. 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.

A-13. The DER system detects internal errors and failures, and enters a default “failure” state, which may include limiting functionality, restarting, or shutting down.

A-14. DER system components use heartbeat concepts to detect component failures.

A-15. The DER system provides an emergency manual override capability that shuts down the system.

A-16. Information input is validated for format and reasonability, including checking that the input is in the correct format, that values are within limits, that the values are not beyond the capabilities of the system, that timing constraints are met, etc.

A-17. Logs capture significant events, along with timestamps, significant data values, status of related equipment, etc. Forensic assessment tools are used to extract possible problems.

A-18. DER settings are designed such that they do not adversely affect distribution equipment operational settings, such as load tap changers, voltage regulators, and recloser settings.

Cyber security

A-19. All DER components are provided with unique cryptographic device identifications by the manufacturer.

A-20. The DER system is manufactured with the default that all access shall be authenticated.

A-21. The DER system includes pre-defined roles for DER owner, DER operator, aggregator, utility normal operations, and utility emergency operations, as a minimum, with pre-defined default permissions for each role. These default permissions could be updated by implementation-specific profiles for rights.

A-22. Purchased components are tested for their security capabilities, any holes in their security through fuzzing and other security assessment methods, and the presence of any malware.

A-23. The manufacturers of DER systems use penetration testing to ensure their systems are well-protected against cyber attacks.

A-24. The DER system contains secure firmware or hardware memory (hardware security module) for cryptographic material, passwords and other embedded private or confidential information that is encrypted or otherwise secured against unauthorized access.

A-25. The DER system is designed to permit only non-sensitive data to be provided to non-authenticated requests.

A-26. Logs capture all cyber security events, including security parameter changes, changes in certificate status, invalid login attempts, detection of malware, etc.

A-27. Post-event engineering forensic analysis capabilities include the security-related actions of DER systems.

7.5.3 Integrator and installer: DER setup for meeting resilience recommendations

Integrators and installers of DER systems should take the responsibility to ensure all appropriate cyber security 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 cyber security requirements (which may be mandated by the utility interconnection requirements) through the appropriate selection and testing of the cyber security cryptography suites, methods for establishing secure channels, and implementing appropriate key management processes.

Engineering strategies

A-28. DER systems are connected at different locations on the grid for redundancy and balancing generation/load profiles.

A-29. The integrator/installer implements redundant DER systems for installations with critical load requirements.

A-30. 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.

A-31. Redundant equipment is designed into the system (e.g., redundant DER systems, redundant components, spares) if availability of the system is critical.

A-32. Redundant communication networks are able to be utilized in a timely manner (e.g., multiple communication paths, redundant wireless nodes, redundant interconnections to a backhaul network) to meet the required communications availability.

A-33. Redundant automation systems are able to be utilized in a timely manner (e.g., redundant controllers, redundant FDEMS, redundant SCADA computers systems, backup systems) to meet the required system availability.

A-34. Redundant information sources are able to be utilized in a timely manner (e.g., redundant sensors, voltage measurements from multiple sources such as at the ECP, the PCC, or even the feeder substation) to meet the required system availability.

A-35. Redundant or backup control systems are able to be utilized in a timely manner (e.g., multiple FDEMS that can be assigned to manage different DER systems, SCADA systems in physically different locations) to meet the required system availability.

A-36. Redundant power system configurations are able to be utilized in a timely manner (e.g., networked grids, multiple feeds to customer site from different substations, microgrid formation) to meet the required system availability.

A-37. Redundant logs and databases are available with mirrored or frequent updates.

Cyber security

A-38. The integrator/installer ensures that the DER systems are factory tested for cyber-physical security issues.

A-39. The integrator/installer selects and implements appropriate levels of security to meet the DER owner’s and the utility’s interconnection security requirements.

A-40. The integrator/installer has security of the DER system enabled “out of the box”, allowing modifications only by authenticated advanced users.

A-41. The integrator/installer ensures that unique cryptographic keys are used for each installation.

A-42. The integrator/installer ensures that separate security keys are used for different types of functions, such as for operations versus maintenance.

A-43. The integrator/installer updates the roles and permissions to reflect the implementation configuration and contractual agreements.

A-44. 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.

A-45. The integrator/installer provides instruction to DER owners on security requirements so they won’t try to bypass security settings.

A-46. Installers are trained appropriately to ensure that the recommended security settings are implemented.

A-47. 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.

A-48. The integrator/installer certifies that they are supplying equipment from manufacturers who are certified as providing security-enabled equipment.

7.5.4 Testing personnel: resilient DER system interconnection testing recommendations

Utilities have rigorous interconnection requirements before DER systems are permitted to connect to the grid. Most of these interconnection requirements necessitate testing and certification[6]. Some testing occurs at manufacturer sites or in testing laboratories while some tests have to be done in the field while the DER system is being interconnected. These lab and field tests helps to ensure that the DER settings and actions are compliant with the interconnection requirements, thus helping to minimize equipment failure rates and validate the coordination between DER system settings and the distribution grid equipment settings.

Some types of testing include:

Engineering strategies

A-49. Functional testing ensures that the equipment operates correctly for all valid commands and settings, according to testing standards if these are available.

A-50. Error testing ensures that erroneous settings, commands, and combinations of settings are detected and that default actions are taken.

A-51. Safety testing ensures the equipment take the appropriate actions, such as disconnecting from the grid, when necessary for safety.

A-52. Performance testing ensures that extreme conditions are handled appropriately, such as high or low temperatures, rapid and large number of commands, rapidly changing power conditions.

A-53. Field testing ensures the equipment operates correctly under real conditions in the field, which may include the impacts of other equipment on the power system and on the operations of this equipment.

A-54. Availability testing ensures the equipment (software and hardware) continues to operate over long periods of time.

A-55. Database rollback capability ensures that invalid input in database updates can be recovered from.

A-56. Configuration testing ensures that changes in the equipment’s configuration and network connections do not incorrectly affect the equipment’s operations and capabilities.

A-57. Relay coordination testing ensures that DER settings are coordinated with other protective equipment.

A-58. Communication network testing, including near power system faults, ensures that communications are operating reliably and correctly.

Cyber security

A-59. Cyber security access control is tested for all roles and their rights/permissions, including switching between utility normal operations and utility emergency operations.

[6] In North America, DER systems are expected to be certified as compliant with UL1741 testing criteria.

A-60. Any secure firmware or hardware memory used to store sensitive information is tested to ensure that information is not accessible except to authorized users.

A-61. Any communication protocols used to interact with the DER system are tested for meeting the protocol’s cyber security requirements.

7.5.5 DER user: access recommendations

Authentication of users and automated devices to the DER systems is the most critical communications cyber security 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.

Engineering strategies

A-62. Users may have access to the DER system through a local HMI.

A-63. Users have the ability to modify settings, subject to reasonability and safety of those settings.

A-64. Forensic assessment tools for logs are available to extract possible problems.

Cyber security

A-65. The DER system requires unique and high quality username/ password access protection for all user interface interactions and prevents the use of factory-set default access passwords after installation.

A-66. Users and devices are individually identified and authenticated with access permissions established by their role.

A-67. Access security measures meet the utility interconnection requirements, if any, for autonomous DER systems.

A-68. All access to the DER system requires authentication. Some access may require confidentiality as well. Some access may require non-repudiation via digital signatures.

A-69. Only “advanced users” are allowed to make modifications through added layers of role-based access, password and certificate mechanisms.

A-70. The DER system only permits authorized users and other systems to access its information and provide settings and commands, typically through certificates.

A-71. Role-based access permissions can be established for individual data elements, for groups of data elements, and for resources.

A-72. The privacy of information from or about customer-owned DER systems, including their functionality, output, and operational settings is maintained as appropriate.

A-73. The confidentiality of information from or about DER systems, including their functionality, output, and operational settings is maintained as appropriate.

A-74. Messages received or sent from DER systems cannot be repudiated.

7.5.6 ICT designers: requirements for local DER communications

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

Engineering strategies

A-75. 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.

A-76. Redundant networks are used for critical information flows

A-77. DER system network interface design prevents anyone from making invalid network settings.

A-78. Communication protocols are well-established international standards with security.

Cyber security

A-79. Networks use gateways, secure routers, and firewall protection at domain boundaries, for instance using Energy Service Interfaces (ESIs) at customer service points.

A-80. DER system information is exchanged only over secured network channels.

A-81. Networks on shared media use secure technologies such as TLS, VPNs, or MPLS to protect DER information

A-82. Network components are hardened with only essential applications installed and only necessary ports enabled.

A-83. 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.

A-84. Communication protocols used between DER system components are required to authenticate all messages, including their source and destinations.

A-85. 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.

A-86. Communication protocols used for confidential or private information shall ensure confidentiality of this information in transit.

A-87. 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.

A-88. Key management system ensures that the DER systems have valid public-key certificates before communications are established

A-89. Key management system ensures that the DER systems have access to certificate revocation lists in a timely manner.

A-90. DER system networks use communications partitioning and segmentation to ensure DER systems cannot inadvertently connect to a rogue network or networks using insecure cryptographic algorithms.

A-91. DER system settings are designed by integrators to ensure they are constrained from joining unauthorized networks, specifically wireless networks.

A-92. A compromised DER system does not permit unauthorized access through the communications network to other DER systems or to other entities, including the FDEMS and DSO systems.

A-93. DER systems that may be accessed through the Internet has additional Internet security features including protection from malware.

A-94. 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.

7.5.7 Security managers: alarming, logging, and reporting cyber security recommendations

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 cyber security-related alarms should notify appropriate personnel, termed the "DER manager".

Cyber security

A-95. One or more "DER security managers" are established who are responsible for receiving notifications of anomalous events, including cyber security events.

A-96. 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.

A-97. 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, excessive unsuccessful login attempts, and errors.

A-98. Time synchronization provides adequate precision and accuracy, including security against attacks on clocks and the time synch protocol, to ensure that the timestamps of audit logs capture a series of events truly chronologically with the necessary time resolution.

A-99. The DER system prevents modifications to audit logs and/or logs all modifications to those logs.

A-100. The audit trail provides forensic information including back to the original audit entries.

7.5.8 Maintenance personnel: resilience recommendations for maintenance, updating and re-testing, 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, configuration testing, parameter change testing, roll-back procedures, and re-testing of the systems after installation. In particular, security software/firmware maintenance should be thoroughly tested before installations.

Engineering strategies

A-101. 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.

A-102. Maintenance schedules of any DER systems deemed "critical" to the utility are provided to and/or approved by the utility, as per interconnection contracts.

A-103. All maintenance and testing events are captured in audit logs. Forensic assessment tools for logs are available to extract possible problems.

Cyber security

A-104. Maintenance is permitted only by security-certified maintenance organizations. The security requirements for maintenance organizations (e.g. patched maintenance systems, up-to-date malware protection, security clearance for personnel etc.) are included in maintenance contracts. The fulfilment of these requirements is regularly tested or audited.

A-105. Maintenance tools are protected from unauthorized use.

A-106. Purchased equipment and updated DER systems are tested for its security capabilities, any holes in its security through security reviews, penetration tests and other methods, and the presence of any malware.

A-107. 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.

A-108. Remote access for maintenance uses 2-factor authentication or other strong authentication measures.

A-109. Local access for maintenance requires that any laptops or other maintenance equipment connected to the DER system has been scanned for malware, that the software installation on the maintenance equipment is up-to-date, and that the latest security patches are installed.

A-110. 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.

A-111. Equipment is retested after maintenance for its security capabilities and the presence of any malware.

7.5.9 Recommended coping actions 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 are sent to the appropriate “DER manager”. The DER system can then take steps to mitigate the impact of the situation.

Engineering strategies

A-112. 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”.

A-113. DER system monitors critical data from multiple sources and selects the one “most likely” to be correct.

A-114. Backup versions of DER system software, including configuration data and parameter settings, are available to restore the system at least to a default level.

A-115. Loss of communications between DER components are timestamped, logged, and issued as an alarm to the “DER manager”.

A-116. All uncommanded or suspect network configuration changes are timestamped, logged, and issued as an alarm to the “DER manager”.

A-117. 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.

A-118. 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.

A-119. If the DER system is still operational at the default output settings, but a communication network anomaly persists, the DER systems revert to the default network configuration.

A-120. 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.

A-121. If the attack still appears to be underway, disconnect DER system from the grid and turn it off, so long as this action (as previously determined) would not affect grid stability.

A-122. If the attack or failure is affecting the DER system operation, shut down the DER system.

A-123. 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.

Cyber security

A-124. All invalid user access attempts to the DER system are timestamped, logged, and issued as an alarm to the "DER manager".

A-125. All uncommanded or suspect DER system setting changes are timestamped, logged, and issued as an alarm to the "DER manager".

A-126. Where available, Intrusion Detection Systems (IDS) notifies the "DER manager" of suspected intrusions.

7.5.10 Recommended recovery and analysis actions 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.

Engineering strategies

A-127. Rerun initial installation network configuration.

A-128. Re-establish known and authorized network configuration changes.

A-129. Restart DER system and monitor for any anomalous behavior.

A-130. Take any actions necessary to prevent incident from happening again. Forensic assessment tools for logs are available to extract possible problems.

Cyber security

A-131. Scan and disconnect any unauthorized entities connected to the DER system network (users, applications, viruses, etc.).

A-132. Reset / restart / rerun all network security processes.

A-133. Report incident to "authorities" such as utility, energy service provider, integrator, or other.

A-134. If privacy or confidentiality is suspected of being compromised, notify all affected stakeholders.

8 Level 2: Facilities DER energy management (FDEMS) resilience recommendations

8.1 Level 2 FDEMS: architecture

The Facilities DER Energy Management System (FDEMS) manages combinations of DER generation, DER storage, and customer loads at a residential, commercial, and industrial customer site as illustrated in Figure 8. As such, an FDEMS may be very small and co-located with a single DER system, or may be very large and sophisticated, with networks of sub-

FDEMS that manage subgroups of DER systems and local loads. In some cases, FDEMS may also manage microgrids, and thus able to balance generation, storage, and load in an islanded situation. The communications between the FDEMS and the DER systems is shown as (10) in the figure.

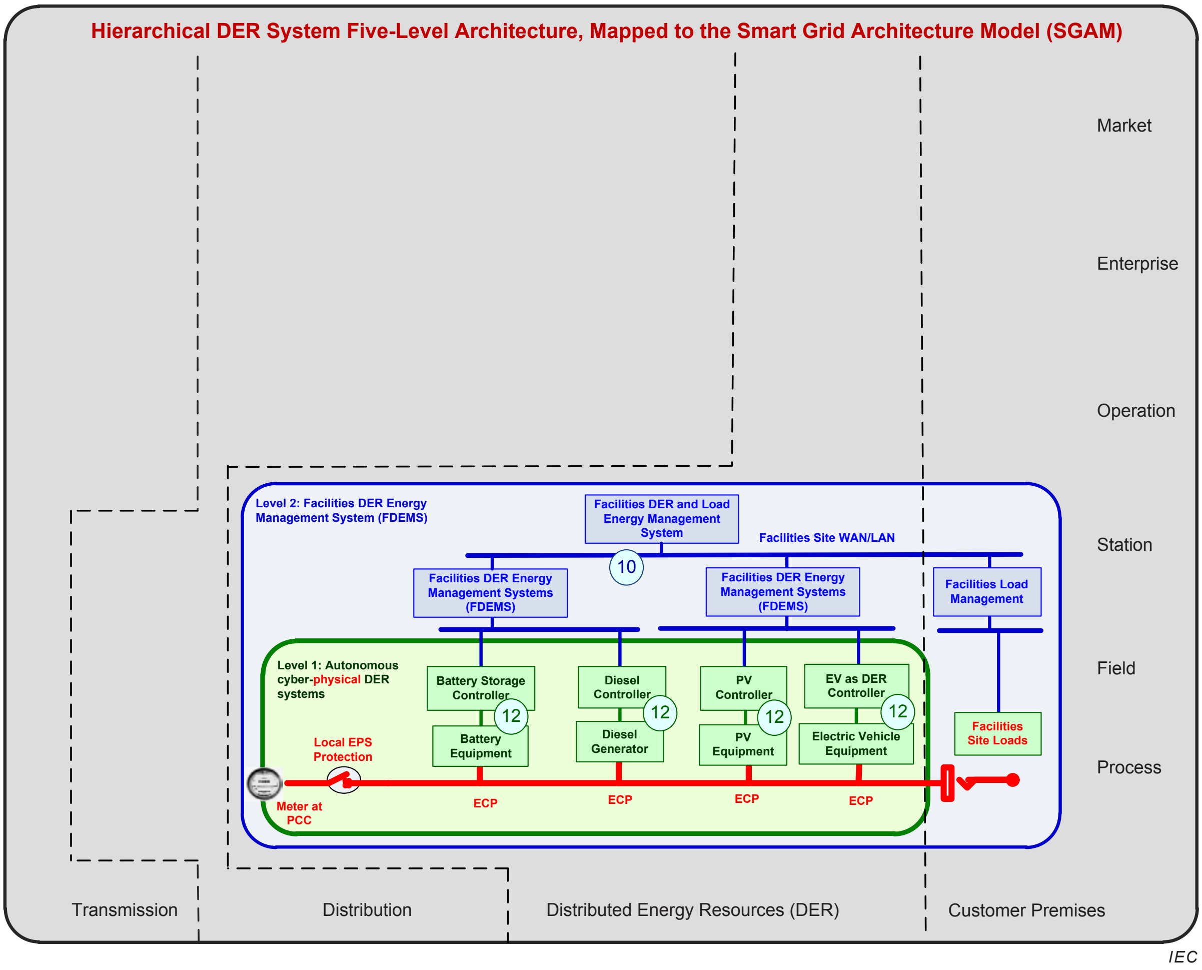

Hierarchical DER System Five-Level Architecture, Mapped to the Smart Grid Architecture Model (SGAM)
Market
Enterprise
Operation
Station
Field
Process
Level 2: Facilities DER Energy Management System (FDEMS)
Facilities DER and Load Energy Management System
Facilities Site WAN/LAN
10
Facilities DER Energy Management Systems (FDEMS)
Facilities DER Energy Management Systems (FDEMS)
Facilities Load Management
Level 1: Autonomous cyber-physical DER systems
Battery Storage Controller
12
Battery Equipment
Diesel Controller
12
Diesel Generator
PV Controller
12
PV Equipment
EV as DER Controller
12
Electric Vehicle Equipment
Facilities Site Loads
Local EPS Protection
Meter at PCC
ECP
ECP
ECP
ECP
Transmission
Distribution
Distributed Energy Resources (DER)
Customer Premises
IEC

Figure 8 – Level 2 FDEMS architecture

The DER attack and 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 micrograms 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 cyber security 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.

8.2 Level 2 FDEMS: Vulnerabilities

FDEMS are located in customer sites with unknown security policies and security implementations. At the same time, they are typically 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

8.3 Level 2 FDEMS: Impacts

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 5 identifies impacts at Level 2, and indicates possible severity degrees: Low (L), Medium (M), and High (H).

Table 5 – Level 2 impact severities due to malicious attacks and failures of FDEMS

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

Type of impact	Specific impacts	Severity
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 an aggregator 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 cyber security. 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

8.4 Level 2 FDEMS: Resilience recommendations

8.4.1 General

The FDEMS resilience requirements reflect the need to design and install FDEMS at sites where the FDEMS owners generally have minimal cyber security expertise and where cost-effectiveness of the FDEMS functions are their primary goal. Therefore, FDEMS systems should be designed and configured for resilience, and cyber security should be designed into the FDEMS system and enabled “out of the box”. FDEMS owners should not be required to manage complex resilience measures, and in fact only allowing advanced users from modifying cyber security measures.

The most important types of Cyber Security 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 cyber security technologies. However, it is also very important to mitigate the impacts of an attack or failure during and after the event.

8.4.2 Manufacturer: Design of FDEMS resilience recommendations

Although FDEMS are typically built from general purpose computers, they are acting as control systems. These control systems should have cyber security designed into their operating system, software applications, and ICT capabilities. Some of the cyber security 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.

The following list identifies the key resilience 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.

Engineering strategies

B-1. 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.

B-2. 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.

B-3. The FDEMS applications validate even authorized changes to DER operational settings against what those settings are reasonably or contractually allowed to be.

B-4. 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.

B-5. 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.

B-6. The FDEMS is designed to collect detailed and/or aggregated operational information on all DER systems under its management, for use in contingency analysis and assessing current resilience capabilities.

B-7. 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.

B-8. The FDEMS is designed to provide an emergency manual override capability that shuts down the system.

Cyber security

B-9. The FDEMS is designed such that all access by users and by external applications is authenticated, including the DER systems that the FDEMS manages.

B-10. The FDEMS is designed with the mandatory use of role-based access control (RBAC) that includes default roles and permissions, which can be modified to associate roles to access permissions and to link these permissions for each of its applications, databases, and functions. Each external user and application shall be identified and assigned to a role.

B-11. Role-based access permissions can be established for individual data elements, for groups of data elements, and for resources.

B-12. The FDEMS is designed such that only essential software and applications are installed and that unnecessary ports are deactivated.

B-13. The manufacturers of FDEMS use penetration testing to ensure their systems are well-protected.

B-14. 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.

B-15. 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.

B-16. FDEMS applications are designed to use heartbeat concepts to detect DER system failures.

B-17. 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.

B-18. Security functions in the FDEMS are designed to be isolated from non-security functions.

8.4.3 Integrators and installer: FDEMS implementation for meeting resilience recommendations

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 should configure the FDEMS appropriately for managing the DER systems and ensuring the FDEMS can monitor and control those DER systems. If the FDEMS contains any analysis applications, the integrators should ensure the necessary information and scheduling is appropriately configured.

They should take the responsibility to ensure also and that all appropriate cyber security 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 cyber security requirements (which may be mandated by the utility interconnection requirements) through the appropriate selection and testing of the cyber security cryptography suites, methods for establishing secure channels, and implementing appropriate key management processes.

The following list identifies the key resilience settings that the integrator and installer of FDEMS should establish as they deploy the system.

Engineering strategies

B-19. The integrator/installer configures the FDEMS for all DER systems under its management.

B-20. The integrator/installer configures any FDEMS analysis applications for performing contingency assessments.

B-21. The integrator/installer implements redundant FDEMSs for installations with critical DER system management requirements.

B-22. Forensic assessment tools for logs are available to extract possible problems.

Cyber security

B-23. The integrator/installer ensures that security of the FDEMS is enabled "out-of-the-box", and that the security configuration is documented and available in machine readable format.

B-24. The integrator/installer implements the FDEMS so that all access by users, DER systems, and all external applications is authenticated.

B-25. The integrator/installer associates users with RBAC roles and may modify the default role-based access control roles and permissions.

B-26. The integrator/installer ensures that at least one role is permitted to receive security alarms and to modify security settings.

B-27. The integrator/installer ensures that only the necessary permissions are assigned to each role that will have access to the FDEMS.

B-28. The integrator/installer ensures that only strong passwords are permitted as authentication, and prevents the use of factory-set default access passwords after installation.

B-29. If biometric or other authentication methods are used, the integrator/installer ensures that these are adequately strong.

B-30. The integrator/installer ensures that unsuccessful login attempts into the FDEMS are logged and the appropriate users are notified.

B-31. The integrator/installer ensures that logins should time out if there is no user activity within a preset period of time.

B-32. The integrator/installer ensures that modifications to the security settings can only be undertaken by users assigned to the security management role.

B-33. The integrator/installer ensures that only essential software and applications are deployed and that unnecessary ports are deactivated.

B-34. The integrators/installers who maintain maintenance access to the FDEMS ensure that this access is documented and only available through authenticated role-based access control on a specific port. Default credentials for such maintenance access should be changed to secure values.

B-35. The integrator/installer selects and implements appropriate levels of security to meet the FDEMS owner's and the utility's interconnection security requirements.

B-36. 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.

B-37. 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.

B-38. 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.

B-39. The integrator/installer ensures that separate security keys are used for different types of functions, such as for operations versus maintenance.

B-40. 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.

B-41. The integrator/installer ensures by an appropriate network design and segmentation that the communication between FDEMS and other systems is only possible through secure gateway systems.

B-42. The integrator/installer ensures that the FDEMS software validates all modifications to DER settings as reasonable, to avoid safety problems and/or equipment damage.

B-43. 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.

B-44. The integrator/installer ensures that security information (e.g. passwords, secret keys, and private keys) are strongly protected through cryptographic means.

B-45. The integrator/installer ensures that the FDEMS logs all significant cyber security 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.

B-46. 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.

B-47. 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.

B-48. The integrator/installer provides instructions or training to FDEMS owners on security requirements so they won't try to bypass security settings.

B-49. Installers are trained appropriately to ensure that the recommended security settings are implemented.

B-50. 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.

B-51. The integrator/installer certifies that they are supplying equipment from manufacturers who are certified as providing security-enabled equipment.

B-52. 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.

8.4.4 Testing personnel: Resilient FDEMS testing recommendations

Utilities have rigorous interconnection requirements before DER systems are permitted to connect to the grid. Most of these interconnection requirements necessitate testing and certification. Some testing occurs at manufacturer sites or in testing laboratories while some tests have to be done in the field while the DER system is being interconnected. These lab and field tests helps to ensure that the DER settings and actions are compliant with the interconnection requirements, thus helping to minimize equipment failure rates and validate the coordination between DER system settings and the distribution grid equipment settings.

Some types of testing include:

Engineering strategies

B-53. Functional testing ensures that the equipment operates correctly for all valid commands and settings.

B-54. Error testing ensures that erroneous settings, commands, and combinations of settings are detected and that default actions are taken.

B-55. Safety testing ensures the equipment take the appropriate actions, such as disconnecting from the grid, when necessary for safety.

B-56. Performance testing ensures that extreme conditions are handled appropriately, such as high or low temperatures, rapid and large number of commands, rapidly changing power conditions.

B-57. Field testing ensures the equipment operates correctly under real conditions in the field, which may include the impacts of other equipment on the power system and on the operations of this equipment.

B-58. Availability testing ensures the equipment (software and hardware) continues to operate over long periods of time.

B-59. Database rollback capability ensures that invalid input in database updates can be recovered from.

B-60. Configuration testing ensures that changes in the equipment’s configuration and network connections do not incorrectly affect the equipment’s operations and capabilities.

B-61. Relay coordination testing ensures that DER settings are coordinated with other protective equipment.

B-62. Communication network testing, including near power system faults, ensures that communications are operating reliably and correctly.

Cyber security

B-63. Cyber security testing ensures that the role-based access control mechanisms are correctly established.

B-64. Cyber security testing ensures that all security requirements are met, as per the integration and installer requirements.

8.4.5 FDEMS users: Access recommendations

During operations, the authentication of users and applications who are accessing the FDEMS is the most critical communications cyber security 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.

The following items identify the key resilience requirements for users and applications that are accessing the FDEMS.

Cyber security

B-65. All users and applications are uniquely identified.

B-66. Users create strong passwords, establish biometric identification methods, or utilize dongles or other strong authentication methods.

B-67. Users login to the FDEMS via username and password or one of the other authentication methods.

B-68. All users and applications are assigned to one or more roles.

B-69. 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. Some critical actions may require dual approval by two authorized users.

B-70. The FDEMS supports the requirement that passwords be changed periodically.

B-71. The FDEMS only permits authenticated and authorized applications to access its information and modify settings and commands.

B-72. Only users assigned to a security management role may make modifications to the security settings.

B-73. Users assigned to a security management role should understand instructions or take training on security requirements.

B-74. Users assigned to a security management role monitor the security situation, key management, and certificates, including any revocations, certificate expirations, and security alarms.

B-75. Only users assigned to the “role modification” role are permitted to modify roles and/or to reassign users to different roles.

B-76. Role-based access permissions can be established for individual data elements, for groups of data elements, and for resources.

B-77. 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.

B-78. The role that receives security alarms or event notifications is always assigned to at least one user or application.

B-79. All modifications to FDEMS applications, settings, security audit logs and security parameters are associated with a specific identity through the role-based access process.

B-80. Certain types of messages received or sent from FDEMS can include digital signatures or other methods to ensure they cannot be repudiated.

8.4.6 FDEMS ICT designers: Resilience recommendations

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 modeling should include cyber security to ensure secure operation of the FDEMS and the VArious sub-FDEMS and DER systems that it manages.

The following items identify the key resilience requirements for ICT communications and protocols that are accessing the FDEMS.

Engineering strategies

B-81. 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.

B-82. Redundant networks are used for critical information flows.

B-83. DER system network interface design prevents anyone from making invalid network settings.

B-84. Communication protocols are well-established international standards with security.

Cyber security

B-85. Networks use gateways, secure routers, and firewall protection at domain boundaries, for instance using Energy Service Interfaces (ESIs) at customer service points.

B-86. FDEMS and DER system information is exchanged only over secured network channels.

B-87. Networks on shared media use secure technologies such as TLS, VPNs, or MPLS to protect DER information.

B-88. Network components are hardened with only essential applications installed and only necessary ports enabled.

B-89. 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.

B-90. 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.

B-91. Redundant networks are used for critical information flows.

B-92. FDEMS network interface design prevents anyone from making insecure network settings.

B-93. Communication protocols are well-established international standards with security.

B-94. Communication protocols used between the FDEMS and the DER systems are required to authenticate all messages, including their source and destinations.

B-95. 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.

B-96. Communication protocols used for confidential or private information shall ensure confidentiality of this information in transit.

B-97. 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.

B-98. Key management system ensures that the FDEMS and their DER systems have valid public-key certificates or pre-shared keys before communications are established.

B-99. Key management system ensures that the DER systems have access to certificate revocation lists in a timely manner, either directly or via OCSP methods.

B-100. FDEMS networks use communications partitioning to ensure that none of the FDEMSs can inadvertently connect to a rogue network or networks using insecure cryptographic algorithms.

B-101. FDEMS settings are designed by integrators to ensure they are constrained from joining unauthorized networks, particularly wireless networks.

B-102. A compromised FDEMS does not permit unauthorized access through the communications network to other FDEMSs or to other entities.

B-103. FDEMS that may be accessed through the Internet has additional Internet security features including strong protection against malware.

B-104. 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.

8.4.7 Security managers: Alarming, logging, and reporting recommendations

Alarming of significant events is critical for real-time operations of FDEMS 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 alarms should notify appropriate personnel, termed the “FDEMS manager”.

Cyber security

B-105. One or more “FDEMS security managers” are established who are responsible for receiving notifications of anomalous power system and cyber events.

B-106. The FDEMS issues alarms to notify the FDEMS security manager when events occur on its DER systems and when DER systems have taken actions that were not commanded, or vice versa, the lack of action by a DER system in response to an FDEMS command.

B-107. The FDEMS logs all significant events and ensures authorized access to these logs. These events include FDEMS computer events, physical events, power system events, manual overrides, communication network events, security events, user actions, actions triggered by other systems, and errors.

B-108. Time synchronization provides adequate precision and accuracy, including security against attacks on clocks and the time synch protocol, to ensure that the timestamps of audit logs capture a series of events truly chronologically with the necessary time resolution.

B-109. The FDEMS prevents modifications to audit logs and/or logs all modifications to those logs.

B-110. The FDEMS audit trail provides forensic information including links back to the original audit entries.

8.4.8 Maintenance personnel: Resilience recommendations for maintenance, updating and re-testing, systems

All FDEMS 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 FDEMS 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, configuration testing, parameter change testing, roll-back procedures, and re-testing of the systems after installation. In particular, security software/firmware maintenance should be thoroughly tested before installations.

Engineering strategies

B-111. Start-up, restart, and anomalous events cause the FDEMS to perform a self-test, including integrity and reasonability testing of all key functional and security settings.

B-112. Maintenance schedules of any DER systems managed by the FDEMS which are deemed “critical” to the DSO are provided to and/or approved by the DSO, as per interconnection contracts.

B-113. Forensic assessment tools for logs are available to extract possible problems.

Cyber security

B-114. Maintenance is permitted only by security-certified maintenance organizations. The security requirements for maintenance organizations (e.g. patched maintenance systems, up-to-date malware protection, security clearance for personnel etc.) are included in maintenance contracts. The fulfilment of these requirements is regularly tested or audited.

B-115. Maintenance tools are protected from unauthorized use and are tested for unauthorized updates.

B-116. Replacement equipment and updated FDEMS components are tested for their security capabilities, any holes in its security through security reviews, penetration tests and other methods, and the presence of any malware.

B-117. Contractual arrangements with authorized vendors 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 FDEMS.

B-118. Remote access for maintenance uses 2-factor authentication or other strong authentication measures.

B-119. Local access for maintenance requires that any laptops or other maintenance equipment connected to the FDEMS has been scanned for malware, that the software installation on the maintenance equipment is up-to-date, and that the latest security patches are installed.

B-120. Patches to FDEMS 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.

B-121. The FDEMS is retested after maintenance for its security capabilities and the presence of any malware.

B-122. All maintenance and testing events are captured in audit logs.

8.4.9 Recommended coping actions during an attack or failure

Although the prevention of attacks or failures is the most effective approach, FDEMS 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 are sent to the appropriate “FDEMS manager”. The FDEMS can then take steps to mitigate the impact of the situation.

Engineering strategies

B-123. If an outage of the area EPS is occurring and if the FDEMS can handle an islanded situation, the FDEMS should disconnect its DER systems and loads from the area EPS and form an islanded microgrid.

B-124. If an outage of the area EPS is occurring but if the FDEMS cannot handle an islanded situation, the FDEMS should disconnect its DER systems and loads from the area EPS and should verify that all DER systems have actually disconnected.

B-125. If the FDEMS determines that a DER system’s electrical output (voltage, VArs, watts) is outside the “normal” range, it is logged and/or an alarm is sent to the “FDEMS manager”.

B-126. When the FDEMS is determining what actions to take in an emergency situation, it should monitor critical data from multiple sources and selects the one “most likely” to be correct.

B-127. The FDEMS should 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.

B-128. Backup versions of FDEMS software, including configuration data and parameter settings, are available to restore the system at least to a default level.

B-129. Loss of communications between FDEMS subsystems and DER systems are timestamped, logged, and issued as an alarm to the “FDEMS manager”.

B-130. All uncommanded or suspect network configuration changes are timestamped, logged, and issued as an alarm to the “FDEMS manager”.

Cyber security

B-131. All invalid user access attempts to the FDEMS are timestamped, logged, and issued as an alarm to the “FDEMS manager”.

B-132. All uncommanded or suspect FDEMS setting changes are timestamped, logged, and issued as an alarm to the “FDEMS manager”.

B-133. Where available, Intrusion Detection Systems (IDS) notifies the “FDEMS manager” of suspected intrusions.

B-134. Upon detection of an attack or significant failure, the FDEMS issues commands to its DER systems to go to default output settings of reasonable or contractual limits, regardless of actual settings.

B-135. If an attack or failure appears to be caused by the communications network, the FDEMS should disconnect from any external communication networks and go into the default “isolated” state.

B-136. If the attack or failure is significantly affecting the FDEMS, shut down the FDEMS.

8.4.10 Recommended recovery and analysis actions after an attack or failure

After an attack or failure, the primary effort needs to be the restoration of the FDEMS and operation of its DER systems, but only after testing and verifying their security and safety. Once the FDEMS 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.

Engineering strategies

B-137. Save all audit logs and other records of the FDEMS operations just before and during the attack or failure.

B-138. Scan and disconnect any unauthorized entities connected to the FDEMS network, particularly wireless networks (users, applications, viruses, etc.).

B-139. Rerun initial installation network configuration.

B-140. Reset / restart / rerun all network security processes.

B-141. Re-establish known and authorized network configuration changes.

B-142. Restart the FDEMS and its DER systems, and monitor for any anomalous behavior. Forensic assessment tools for logs are available to extract possible problems.

Cyber security

B-143. Report incident to “authorities” such as utility, energy service provider, integrator, or other.

B-144. Take any actions necessary to prevent incident from happening again.

B-145. If privacy or confidentiality is suspected of being compromised, notify all affected stakeholders.

9 Level 3: Third parties: Retail energy provider or aggregators resilience recommendations

9.1 Level 3: Third parties: ICT architecture

Level 3: Third parties: Retail energy provider or aggregators extends beyond the local site to third parties: the retail energy providers (REPs) and other DER aggregators. These third parties use information and communication technologies (ICT) to request or even command DER systems (possibly directly but usually 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. Aggregator 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 3 and Level 2 may have VArying scenarios[7], while still fundamentally providing the same services.

The internal security of third parties is not addressed in this document – the focus is on the ICT networks between the third parties and the FDEMS and/or DER systems, shown as communications (4) and (5) in Figure 9.

[7] See the SGIP DRGS Subgroup B White Paper, "*DRGS Subgroup B White Paper – Categorizing Use Cases in Hierarchical DER Systems*", available through the SGIP.org website.

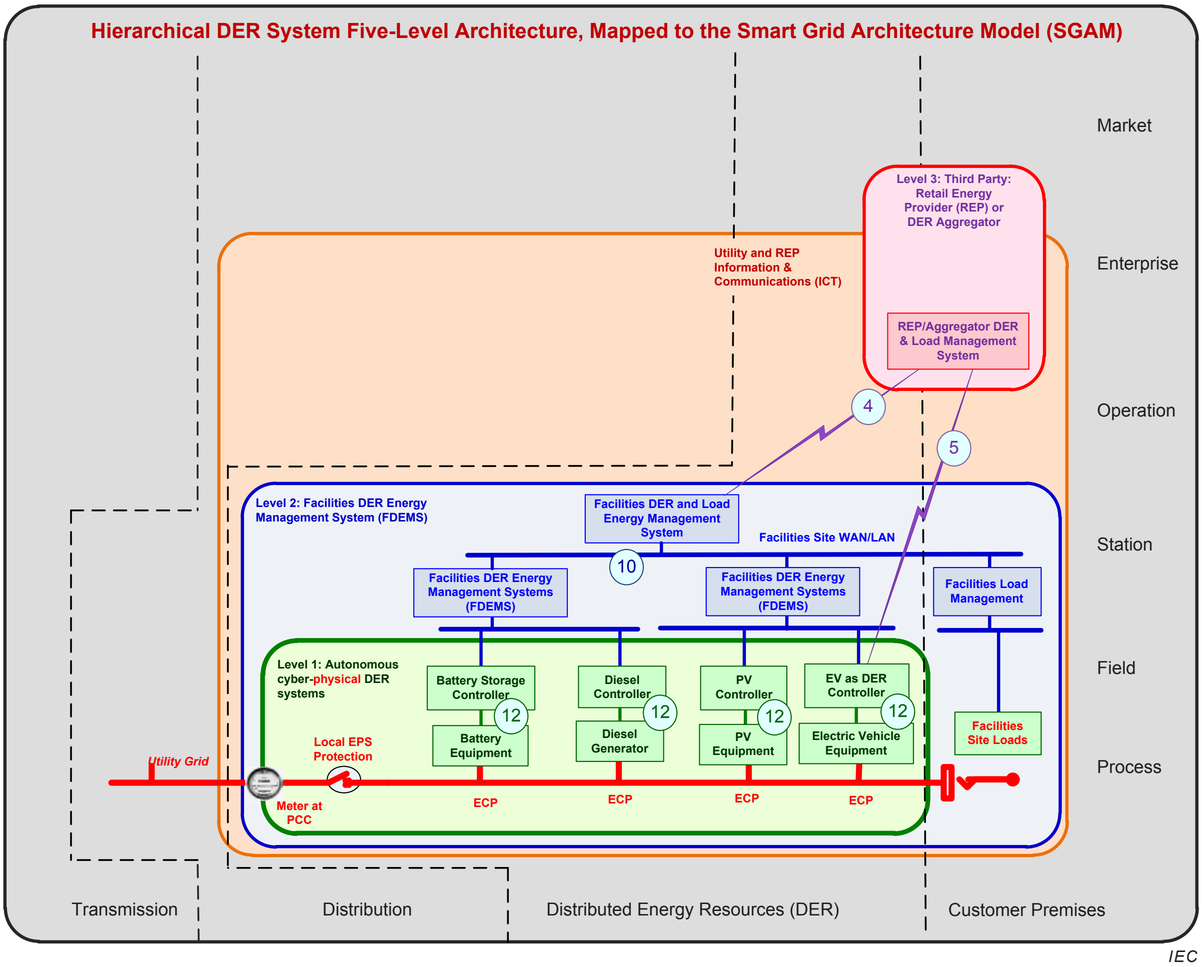

Hierarchical DER System Five-Level Architecture, Mapped to the Smart Grid Architecture Model (SGAM)
Market
Enterprise
Operation
Station
Field
Process
Level 3: Third Party: Retail Energy Provider (REP) or DER Aggregator
REP/Aggregator DER & Load Management System
Utility and REP Information & Communications (ICT)
4
5
Level 2: Facilities DER Energy Management System (FDEMS)
Facilities DER and Load Energy Management System
Facilities Site WAN/LAN
10
Facilities DER Energy Management Systems (FDEMS)
Facilities DER Energy Management Systems (FDEMS)
Facilities Load Management
Level 1: Autonomous cyber-physical DER systems
Battery Storage Controller
Battery Equipment
Diesel Controller
Diesel Generator
PV Controller
PV Equipment
EV as DER Controller
Electric Vehicle Equipment
12
12
12
12
Facilities Site Loads
Utility Grid
Local EPS Protection
Meter at PCC
ECP
ECP
ECP
ECP
Transmission
Distribution
Distributed Energy Resources (DER)
Customer Premises
IEC

Figure 9 – DER third parties: Retail energy provider or aggregators architecture

9.2 Level 3: Third parties: ICT vulnerabilities

Most DER systems and FDEMS will need to connect to external systems, possibly utility systems or market-based energy service providers, using information and communication technologies (ICT). These DER ICT systems may consist of special utility well-protected networks or may utilize public telecommunication services such as cellphone networks, or may use the Internet. This wide range of types and locations of ICT systems makes them open to many vulnerabilities.

DER ICT systems 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 these vulnerabilities, utilities cannot generally use the same types of secure control as they use for ICT systems to their own substations and other utility facilities, even if the ICT systems are utility-owned. The reasons include:

- Different ownership of the end systems: In general, utilities do not own the DER or FDEMS equipment that they interact with (the exception is if the ICT is used for a utility-owned DER system in a substation). Therefore they are limited in the amount of cyber security or operational control they have over the DER systems.

- 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 and DER systems are generally not owned by utilities, they cannot trust the cyber security protections or DER responses to failures to the same degree as they trust their own operational interactions.
- Different security domains: Even if the FDEMS or DER systems are located in secured facilities, the ICT information exchanges between utility systems and FDEMS cross security perimeters. These security perimeters may not be adequately 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 could issue broadcast or multicast commands to FDEMS that may in turn issue different information to the DER systems as it tries to allocate the commands to appropriate DER systems. However these multi-tier interactions may cause misinformation and incorrect results.
- Some ICT information exchanges, particularly between REPs and FDEMS, may rely on the Internet, providing additional attack possibilities.

9.3 Level 3: Third parties: ICT impacts

In the Level 3 environment, the information and communications systems (ICT) provided by third parties to interact with FDEMS and DER systems are vulnerable to many types of malicious attacks or inadvertent failures. Although such attacks or failures might only affect a small number of FDEMS and DER systems, it is also quite likely that they could affect all FDEMS and DER systems served by the ICT system, and could therefore cause wide area and cascading electrical problems on the utility grid.

DER ICT attacks or failures may impact grid operations in a number of different ways.

- Denial of Service: The lack of ICT messaging could prevent utilities from providing the DER systems with commands and updated information such as schedules. In some situations, communications could be designed to allow certain DER functions to operate, so the lack of communications could prevent these DER functions from operating. REPs could be prevented from providing pricing information.
- Integrity violation: The ICT could transmit invalid commands or settings to the DER systems or report invalid information to utilities or REPs.
- Confidentiality / privacy violation: The ICT could transmit confidential or private information to unauthorized parties.
- Non-repudiation violation: The ICT could allow the DER, the FDEMS, or the utility to repudiate an action or fail to confirm an action.

Table 6 identifies impacts at Level 3, and indicates possible severity degrees: Low (L), Medium (M), and High (H).

Table 6 – Level 3 impact severities due to malicious attacks and failures of DER ICT

Type of impact	Specific impacts	Severity
Scale impact	Potentially wide-spread, affecting all DER systems using the ICT	H if ICT impacts all DER systems M if ICT impacts a small subset of DER systems
Safety impact	If the ICT attack or failure causes DER failures or disconnections, 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, such as at hospitals and homes with people reliant on medical equipment, can cause harm or death	M typically since most DER operate autonomously or H if medical impact
Transmission power system operations impact	If the failed ICT is used to manage or coordinate large amounts of DER generation and/or storage, outages and power quality problems could affect the transmission power system	L typically since most DER operate autonomously or M if large amount of DER
Distribution power operations impact	If the failed ICT is used to manage or coordinate large amounts of DER generation and/or storage, outages and power quality problems, including voltage excursions, harmonics, and excess power, could affect portions of the distribution power system. Potential power quality impacts on the distribution feeder serving the facility, and power outages of other customers on that feeder	H for distribution circuits affected by the ICT attack or failure
Facility site(s) power system impact	If the failed ICT is used to directly manage the facility, then there could be complete or partial outage of the facility. If the failed ICT is only used for updates of settings and/or schedules, the facility may not be affected much.	H for facilities under direct management via ICT L for facilities primarily managed autonomously
Utility financial impact	If the attacked or failed ICT is owned by the utility, the utility would bear the costs associated with restoring the ICT capabilities. If the attacked or failed ICT necessitated truck rolls or additional equipment inspections, the utility would bear these repair costs. The utility might have legal costs if inadequate cyber security or ICT design could be proved to have caused power outages or power quality problems. If utility equipment is destroyed or vandalized, the utility would bear the costs for repair or replacement	H if ICT is utility-owned L if only repairs are necessary H if negligence could be proved
Utility reputation impact	If the utility could be shown as negligent in designing or securing the ICT, the utility reputation could be harmed	L typically M if utility is shown to be responsible
ICT owner financial impact	The ICT owner would bear the costs associated with restoring the ICT capabilities and might have legal costs if inadequate cyber security or ICT design could be proved to have caused power outages or power quality problems.	M if ICT is utility-owned H if negligence could be proved
Environmental impact	If the ICT is used to directly manage DER systems for controlling environmental conditions such as a water treatment plant, loss of power could cause environmental damage	M

9.4 Level 3: Third parties ICT: Resilience recommendations

9.4.1 Third party ICT designers: Resilience recommendations

The ICT is comprised of communications networks using one or often more than one communication protocol. The information models also may be different, depending upon the types of interactions and the design of the ICT systems. Each layer of the communications network, from the communication media, communication transport protocols, communication application protocols, and semantic information modeling should include cyber security to ensure secure interactions between the utility and the DER sites.

The following items identify the key resilience requirements for ICT communications and protocols that are used between utilities and the DER systems (FDEMS and/or DER systems).

Engineering strategies

C-1. Communication networks should use Quality of Service (QoS) or other resource management techniques to ensure that higher priority traffic takes precedence over lower priority traffic.

C-2. Network and system management capabilities should be installed to monitor the status of all communication 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.

C-3. Redundant networks should be used for critical information flows.

C-4. Communication protocols should be well-established, mature international standards with security capabilities, that have been well tested in large numbers of implementations.

Cyber security

C-5. Networks should use gateways, secure routers, and firewall protection at domain boundaries, for instance using Energy Service Interfaces (ESIs) at customer service points.

C-6. Networks on shared media should use secure technologies such as TLS, VPNs, or MPLS to protect DER information.

C-7. Network components are hardened with only essential applications installed and only necessary ports enabled.

C-8. The design of the network interface should prevent users from making invalid, unsafe, or insecure network settings.

C-9. Communication protocols should validate the integrity of the data in transit, including protection against man-in-the-middle, replay, and non-repudiation. In particular, passwords and secret kyes should never be sent in the clear.

C-10. Communication protocols used for confidential or private information should ensure confidentiality of this information in transit.

C-11. Communication protocols should use validated cryptography, should not use deprecated cryptographic suites in new systems beyond their expiration dates, and provide migration paths for older systems using deprecated cryptographic suites to implement up-to-date cryptographic suites.

C-12. Information exchanges should authenticate sources and destination, and permit only authorized access to data.

C-13. The key management system should ensure that the DER systems have valid public-key certificates or pre-shared keys before communications are established.

C-14. The key management system should ensure that the DER systems have access to certificate revocation lists in a timely manner, either directly or via OCSP methods.

C-15. The networks should use communications partitioning to ensure that none of the DER systems can inadvertently connect to a rogue network or any other unauthorized network or networks using insecure cryptographic algorithms.

C-16. A compromised DER system should not permit unauthorized access through the communications network to the utility or other DER systems.

C-17. If the Internet or other public network is used, additional Internet security features should be activated, including strong protection against malware.

C-18. If the utility or any DER system detects network and protocol permanent errors and failures, it should notify appropriate entities and take security steps such as entering into a default "isolated" state, changing functional settings, restarting the communication connection process, or shutting down.

9.4.2 ICT users: Access recommendations

During operations, the authentication of users and applications which are accessing the communications networks is the most critical communications cyber security requirement. Generally, confidentiality is less important, although privacy for customer-owned DER systems may be more important. Particularly if the utility is connected to the DER systems via a communications network that is used for other functions, authentication of all interactions is crucial to the safety and reliability of utility and DER operations.

The following items identify the key resilience requirements for users and applications that are accessing the communications network between the utility and the DER systems.

Cyber security

C-19. All users and applications should be uniquely identified and authorized to use the communications network.

C-20. Users should create strong passwords, establish biometric identification methods, or utilize dongles or other strong authentication methods.

C-21. Applications should use cryptographic key-based methods for authentication purposes.

C-22. Users and applications should be required to use strong authentication methods in order to access the communications network.

C-23. All users and applications are assigned to one or more roles that are associated with permissions for interacting with data across the network, such as read access, write access, delete access, etc.

C-24. Some access by users and applications may also require confidentiality and some access may require non-repudiation via digital signatures. Some critical actions may require dual approval by two authorized users.

C-25. The utility and/or DER systems should support the requirement that passwords be changed periodically.

C-26. Only users assigned to a security management role may make modifications to the security settings.

C-27. Users assigned to a security management role should understand instructions or take training on security requirements.

C-28. Users assigned to a security management role should monitor the security situation, key management, and certificates, including any revocations, certificate expirations, and security alarms.

C-29. Only users assigned to the "role modification" role should be permitted to modify roles and/or to reassign users to different roles.

C-30. Role-based access permissions should be established for individual data elements, for groups of data elements, and for resources.

C-31. Only authenticated and authorized users and applications should be able to access private and confidential information about DER systems, DER-owner/manager settings, etc. All transmission of this information is encrypted for confidentiality.

C-32. The role that receives security alarms or event notifications should always be assigned to at least one user or application.

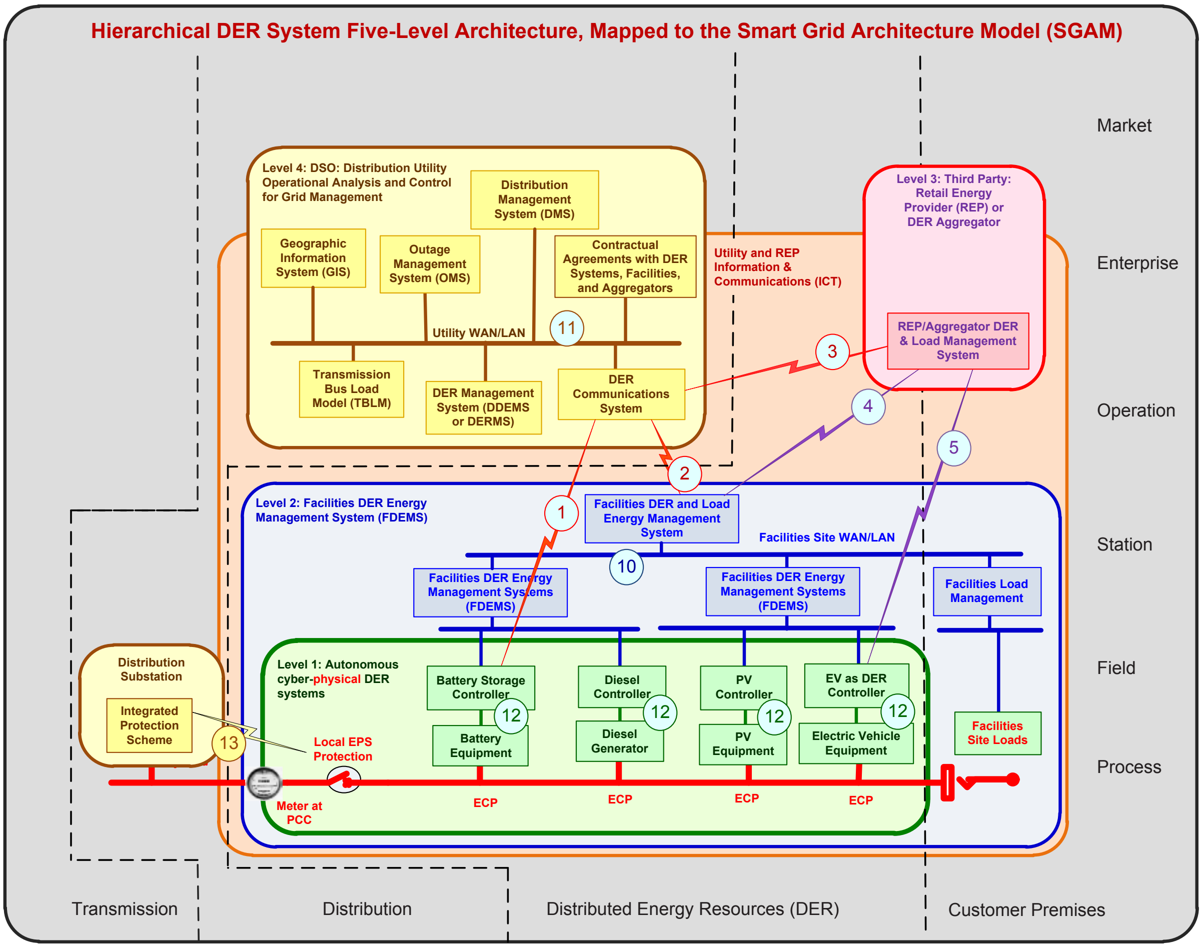
C-33. All modifications to communications software, settings, security audit logs and security parameters should be associated with a specific identity through the role-based access process.

C-34. Certain types of messages received or sent via the communications protocols shall be able to include digital signatures or other methods to ensure they cannot be repudiated.

10 Level 4: Distribution operations analysis resilience recommendations

10.1 Level 4 DSO analysis: Architecture

Level 4: Distribution operational analysis applies to utility applications that are needed to determine what requests or commands should be issued to which DER systems. Distribution system operators (DSOs) monitor the power system and assess if the efficiency, reliability, or resilience of the both the distribution and the transmission power system can be improved by having DER systems modify their operations. This DSO assessment can involve many utility control center systems, including distribution management system (DMS), DER management system (DERMS), “DER SCADA” (not necessarily the same as the distribution SCADA), and the associated geographical information systems, transmission bus load model, outage management systems, and demand response systems. Once the DSO has determined that modified requests or commands should be issued, it will send these out over the ICT as per Level 3 (see Figure 10).


Hierarchical DER System Five-Level Architecture, Mapped to the Smart Grid Architecture Model (SGAM)
Market
Enterprise
Operation
Station
Field
Process
Level 4: DSO: Distribution Utility Operational Analysis and Control for Grid Management
Distribution Management System (DMS)
Geographic Information System (GIS)
Outage Management System (OMS)
Contractual Agreements with DER Systems, Facilities, and Aggregators
Utility WAN/LAN
11
Transmission Bus Load Model (TBLM)
DER Management System (DDEMS or DERMS)
DER Communications System
Utility and REP Information & Communications (ICT)
Level 3: Third Party: Retail Energy Provider (REP) or DER Aggregator
REP/Aggregator DER & Load Management System
3
4
5
2
1
Level 2: Facilities DER Energy Management System (FDEMS)
Facilities DER and Load Energy Management System
Facilities Site WAN/LAN
10
Facilities DER Energy Management Systems (FDEMS)
Facilities DER Energy Management Systems (FDEMS)
Facilities Load Management
Distribution Substation
Integrated Protection Scheme
13
Level 1: Autonomous cyber-physical DER systems
Battery Storage Controller
12
Battery Equipment
Diesel Controller
12
Diesel Generator
PV Controller
12
PV Equipment
EV as DER Controller
12
Electric Vehicle Equipment
Facilities Site Loads
Local EPS Protection
Meter at PCC
ECP
ECP
ECP
ECP
Transmission
Distribution
Distributed Energy Resources (DER)
Customer Premises

IEC

Figure 10 – Distribution operations architecture

10.2 Level 4 DSO analysis: Vulnerabilities

Utility DMS and DERMS are responsible for managing the distribution system, including sending appropriate signals (market signals or control commands) via the “DER SCADA” to the DER systems that are interconnect to their grid. These DMS and DERMS systems are typically within protected utility areas, behind firewalls and within secured locations. However, they are vulnerable to external attacks through the DER SCADA and the widespread ICT, and are as vulnerable as other utility systems to internal attacks and equipment failures.

Level 4 utility DMS and DERMS systems assess power system existing status and any possible future contingencies. If any of these assessment functions are compromised, these systems could issue incorrect, possibly damaging, and potentially catastrophic signals to the DER systems. Compromised control commands from DMS and DERMS systems are particularly sensitive since invalid commands could cause injury to personnel, damage to equipment, and unstable power system conditions. Cyber attacks on market signals from a DERMS could cause financial losses as well as legal and regulatory actions.

Despite the protections accorded to DMS and DERMS systems if they are within utility control centers, they can still be 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 DERMS 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
- Cause the DERMS to send invalid market signals to competitor on the prices of energy and ancillary services, to gain market advantage
- Modify the DERMS 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 coordinating attacks against the DERMS with other power system attacks that could cause power system emergency conditions
- Damage equipment
- Harm personnel

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

- 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

10.3 Level 4 DSO analysis: Impacts

In the Level 4 environment, the utility distribution management systems (DMS) and/or the DER Management Systems (DERMS) are vulnerable to certain types of malicious attacks and inadvertent failures. Such attacks or failures could affect all FDEMS and DER systems that are monitored and controlled by these utility systems, and could therefore cause wide area and cascading electrical problems on the utility grid, particularly during alert and emergency situations when the utilities are most likely to be contractually permitted and/or required to manage the DER systems.

DMS and/or DERMS attacks or failures may impact grid operations in a number of different ways.

- Denial of Service: The failures of DMS or DERMS could prevent utilities from providing the DER systems with the necessary commands and updated settings during alert and emergency situations.
- Integrity violation: The DMS or DERMS could issue invalid commands or settings to the DER systems or report invalid information to utilities.
- Confidentiality / privacy violation: The DMS or DERMS could permit confidential or private information to be accessed by unauthorized parties.
- Non-repudiation violation: The DMS or DERMS failure could allow the DER, the FDEMS, or the utility to repudiate an action or fail to confirm an action.

Table 7 identifies impacts at Level 4, and indicates possible severity degrees: Low (L), Medium (M), and High (H).

Table 7 – Level 4 impact severities due to malicious attacks and failures of DMS or DERMS

Type of impact	Specific impacts	Severity
Scale impact	Potentially wide-spread, affecting all DER systems controlled by the DMS or DERMS	H if DERMS impacts all DER systems M if DERMS impacts a small subset of DER systems
Safety impact	If the DMS or DERMS attack or failure causes DER failures or disconnections, 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, such as at hospitals and homes with people reliant on medical equipment, can cause harm or death	M typically since most DER operate autonomously for safety or H if medical impact
Transmission power system operations impact	If the failed DMS or DERMS is used to manage or coordinate large amounts of DER generation and/or storage, the resulting outages and power quality problems could affect the transmission power system	H if incorrect commands are issued during emergencies
Distribution power operations impact	If the failed DERMS is used to manage or coordinate large amounts of DER generation and/or storage, outages and power quality problems, including voltage excursions, harmonics, and excess power, could affect large portions of the distribution power system. Potential power quality impacts on the distribution feeder serving the facility, and power outages of other customers on that feeder	H for distribution circuits affected by the DERMS attack or failure
Facility site(s) power system impact	If the failed DERMS is used to directly manage the facility, then there could be complete or partial outage of the facility. If the failed DERMS is only used for updates of settings and/or schedules, the facility may not be affected much.	H for facilities under direct management by DERMS L for facilities primarily managed autonomously
Utility financial impact	Since the attacked or failed DERMS is owned by the utility, the utility would bear the costs associated with restoring the DERMS capabilities. If DERMS causes FDEMS or DER damage, the utility would bear these repair costs. The utility might have legal costs if inadequate cyber security or DERMS design could be proved to have caused power outages or power quality problems, or even environmental damage. If utility equipment is destroyed or vandalized, the utility would bear the costs for repair or replacement	H for DERMS repair L if only DER repairs are necessary H if negligence could be proved
Utility reputation impact	If the utility could be shown as negligent in designing or securing the DERMS, the utility reputation could be harmed	L typically M if utility is shown to be responsible
DERMS vendor financial impact	If shown to be associated with inadequate design, the DERMS vendor would bear the costs associated with restoring the DERMS capabilities and might have legal costs if inadequate cyber security or DERMS design could be proved to have caused power outages or power quality problems.	L if no negligence can be proved H if negligence could be proved
Environmental impact	If the DERMS is used to directly manage DER systems for controlling environmental conditions such as a water treatment plant, loss of power could cause environmental damage	M for societal impact

10.4 Level 4 DSO analysis: Resilience recommendations

10.4.1 Resilient design of distribution grid equipment with DER systems

DER systems are part of the power grid, and therefore the resilience of the rest of the equipment managing the grid is also critical. Most of that resilience is already built into distribution grid design and operation, but some additional resilience requirements should be implemented when high penetrations of DER systems are combined with distribution equipment.

Engineering strategies

D-1. Sensors on substation and feeder equipment should monitor volts, VArs, current, temperature, vibrations, etc. to determine the impact of DER systems on feeder generation and load profiles.

D-2. Control capabilities should be available for initiating reactive and proactive control of distribution equipment, either automatically (e.g., breaker trip), via communications (adjust recloser settings), or manually (e.g., substation technician changes the nominal voltage setting on a tap changer).

D-3. Volt/VAr regulation by distribution equipment should be coordinated with the volt/VAr settings of DER systems to ensure feeder voltages and VArs remain within prescribed limits.

D-4. Protective relaying should respond to system events (e.g., power system fault) by tripping breakers in coordination with the DER ride-through and anti-islanding settings.

D-5. The timing of recloser attempts to reconnect after a “temporary” fault (by trying to close the breaker 2-3 times before accepting it as a “permanent” fault) should be coordinated with DER “ride-through” and anti-islanding settings.

D-6. Manual or automatic switching should 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.

D-7. Reserve generation capacity (DER or bulk generation) is available in a timely manner to handle the loss of one or groups of DER systems.

D-8. Device event logs should capture all significant power system events, including the status and output changes of larger DER systems or aggregations of smaller DER systems. Forensic assessment tools for logs are available to extract possible problems.

D-9. Digital fault recorders should capture wave forms of anomalous behavior of the grid, with the ability to identify contributions from DER systems if possible.

D-10. Power quality (PQ) harmonics recorders should capture PQ results of DER systems where necessary.

D-11. Time synchronization to the appropriate accuracy and precision, including security against attacks on clocks and the time synch protocol, should be used by all power system equipment and DER systems to ensure that the events captured in logs can be synchronized across all locations.

10.4.2 Resilience through DSO grid operations with DER systems

DSOs will need to operate the distribution power system differently once there are high penetrations of DER systems. This new paradigm for power system operations will require significantly different capabilities and resilience methods than in the past, including:

Engineering strategies

D-12. The DSO should collect critical information on all DER systems (or aggregations of DER systems) and link that information to their electrical location.

D-13. Before DER systems are interconnected to the grid, they should be assessed for their capabilities and the appropriate settings should be established for all DER autonomous functions.

D-14. Monitoring and control capabilities should be provided to DSOs (may be separate from the distribution SCADA system that monitors distribution equipment) so that key larger DER systems or aggregations of DER systems can be more visible, particularly during rapid changes of status or output.

D-15. These DSO SCADA systems should have approximately high availability with 24x7 monitoring, similar to TSO SCADA systems.

D-16. DSO SCADA systems should be able to perform remote control actions on DER systems and distribution equipment in response to operator commands or software application commands.

D-17. The DSO should be able to issue Automatic Generation Control (AGC) control commands to key DER systems, DER power plants, and/or aggregations of smaller DER systems to maintain frequency and other parameters within limits.

D-18. For managing voltage emergencies, the DER voltage ride-through settings should be coordinated with other distribution equipment trip settings.

D-19. For managing frequency emergencies, the DER frequency ride-through settings should be coordinated with load shedding settings to ensure these actions are compatible.

D-20. Load control or demand response actions should be coordinated with DER control and demand response.

D-21. Disturbance analysis (rapid snapshots of power system during a disturbance for future analysis) should include the information from key DER systems or aggregations of DER systems.

D-22. Alarm processing should include the categorization of high priority alarms, as well as “intelligent” alarm processing that combines different data elements into useful information to better determine the true cause of events.

D-23. Comparisons of device settings against baseline settings.

10.4.3 Resilience through power system analysis

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:

Engineering strategies

D-24. “Power Flow” models of the transmission system, bulk generators, and loads simulate the real-time or future (or past) power system scenarios.

D-25. “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.

D-26. 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.

D-27. Synchrophasors or phasor measurement units provide more granular and accurate data on the state of the grid.

D-28. Power flow applications use the state estimated data to better simulate real-time conditions.

D-29. Load and renewable generation forecasts based on weather, history, day-type, and other parameters will forecast the generation requirements.

D-30. 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.

D-31. Generation reserve capacity is available for instantaneous, short term, and longer term supply of generation in the event of the loss of generation.

D-32. 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).

D-33. 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.

D-34. Volt/VAR/Watt Optimization determine the optimal voltage, VAR, and generation levels usually for efficiency, but also to handle contingencies and emergency situations.

D-35. Direct control of DER and loads (load management) for both efficiency and reliability.

D-36. Indirect control of DER and loads (pre-established settings, broadcasts, demand response) for both efficiency and reliability.

D-37. Ancillary services from DER for both efficiency and reliability (e.g., VAr support from inverters, managed charging rates for PEVs).

D-38. Reliability Coordinators and Independent System Operators provide a regional perspective on the state of the grid in which DER will operate.

10.4.4 Resilience by stakeholder training

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

Engineering strategies

D-39. Dispatcher training simulator, using snapshots of real events as well as scenarios set up by trainers.

D-40. Operational training using case studies, etc.

D-41. Training in using new technologies.

D-42. Security classroom training complemented by participation in local, regional, and national grid security exercises (e.g., the NERC Grid Ex series of annual exercises).

Annex A
(informative)

NISTIR 7628 Smart Grid Catalog of Security Requirements

A.1 NISTIR 7628 families of security requirements

The families of the NISTIR 7628 Smart Grid Catalog of Security Requirements are shown in Table A.1. A more detailed list of the NISTIR 7628 security requirements within each family is shown in Table A.2. The complete NISTIR 7628 document can be found on the NIST web site[8].

Table A.1 – NIST Smart Grid Security Requirements Families

Ref.	NIST Smart Grid security requirements families
SG.AC	Access Control
SG.AT	Awareness and Training
SG.AU	Audit and Accountability
SG.CA	Security Assessment and Authorization
SG.CM	Configuration Management
SG.CP	Continuity of Operations
SG.IA	Identification and Authentication
SG.ID	Information and Document Management
SG.IR	Incident Response
SG.MA	Smart Grid Information System Development and Maintenance
SG.MP	Media Protection
SG.PE	Physical and Environmental Security
SG.PL	Planning
SG.PM	Security Program Management
SG.PS	Personnel Security
SG.RA	Risk Management and Assessment
SG.SA	Smart Grid Information System and Services Acquisition
SG.SC	Smart Grid Information System and Communication Protection
SG.SI	Smart Grid Information System and Information Integrity

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

A.2 Detailed NISTIR 7626 Catalogue of Smart Grid Security Requirements

Table A.2 – Detailed NIST Catalogue of Smart Grid Security Requirements

NIST Ref.	Catalogue 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 Systems
SG.AC-19	Control System Access Restrictions
SG.AC-20	Publicly Accessible Content
SG.AC-21	Passwords
3.8 Awareness and Training (SG.AT)	
SG.AT-1	Awareness and Training Policy and Procedures
SG.AT-2	Security Awareness
SG.AT-3	Security Training
SG.AT-4	Security Awareness and 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
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

NIST Ref.	Catalogue of SG Security Requirements
SG.AU-12	Auditor Qualification
SG.AU-13	Audit Tools
SG.AU-14	Security Policy Compliance
SG.AU-15	Audit Record Generation
SG.AU-16	Non-Repudiation
3.10 Security Assessment and Authorization (SG.CA)	
SG.CA-1	Security Assessment and Authorization Policy and Procedures
SG.CA-2	Security Assessments
SG.CA-3	Continuous Improvement
SG.CA-4	Smart Grid Information System Connections
SG.CA-5	Security Authorization to Operate
SG.CA-6	Continuous Monitoring
3.11 Configuration Management (SG.CM)	
SG.CM-1	Configuration Management Policy and Procedures
SG.CM-2	Baseline Configuration
SG.CM-3	Configuration Change Control
SG.CM-4	Monitoring Configuration Changes
SG.CM-5	Access Restrictions for Configuration Change
SG.CM-6	Configuration Settings
SG.CM-7	Configuration for Least Functionality
SG.CM-8	Component Inventory
SG.CM-9	Addition, Removal, and Disposal of Equipment
SG.CM-10	Factory Default Settings Management
SG.CM-11	Configuration Management Plan
3.12 Continuity of Operations (SG.CP)	
SG.CP-1	Continuity of Operations Policy and Procedures
SG.CP-2	Continuity of Operations Plan
SG.CP-3	Continuity of Operations Roles and Responsibilities
SG.CP-4	Continuity of Operations Training
SG.CP-5	Continuity of Operations Plan Testing
SG.CP-6	Continuity of Operations Plan Update
SG.CP-7	Alternate Storage Sites
SG.CP-8	Alternate Telecommunication Services
SG.CP-9	Alternate Control Center
SG.CP-10	Smart Grid Information System Recovery and Reconstitution
SG.CP-11	Fail-Safe Response
3.13 Identification and Authentication (SG.IA)	
SG.IA-1	Identification and Authentication Policy and Procedures
SG.IA-2	Identifier Management
SG.IA-3	Authenticator Management
SG.IA-4	User Identification and Authentication
SG.IA-5	Device Identification and Authentication
SG.IA-6	Authenticator Feedback
3.14 Information and Document Management (SG.ID)	
SG.ID-1	Information and Document Management Policy and Procedures
SG.ID-2	Information and Document Retention
SG.ID-3	Information Handling
SG.ID-4	Information Exchange

NIST Ref.	Catalogue of SG Security Requirements
SG.ID-5	Automated Labeling
3.15 Incident Response (SG.IR)	
SG.IR-1	Incident Response Policy and Procedures
SG.IR-2	Incident Response Roles and Responsibilities
SG.IR-3	Incident Response Training
SG.IR-4	Incident Response Testing and Exercises
SG.IR-5	Incident Handling
SG.IR-6	Incident Monitoring
SG.IR-7	Incident Reporting
SG.IR-8	Incident Response Investigation and Analysis
SG.IR-9	Corrective Action
SG.IR-10	Smart Grid Information System Backup
SG.IR-11	Coordination of Emergency Response
3.16 Smart Grid Information System Development and Maintenance (SG.MA)	
SG.MA-1	Smart Grid Information System Maintenance Policy and Procedures
SG.MA-2	Legacy Smart Grid Information System Upgrades
SG.MA-3	Smart Grid Information System Maintenance
SG.MA-4	Maintenance Tools
SG.MA-5	Maintenance Personnel
SG.MA-6	Remote Maintenance
SG.MA-7	Timely Maintenance
3.17 Media Protection (SG.MP)	
SG.MP-1	Media Protection Policy and Procedures
SG.MP-2	Media Sensitivity Level
SG.MP-3	Media Marking
SG.MP-4	Media Storage
SG.MP-5	Media Transport
SG.MP-6	Media Sanitization and Disposal
3.18 Physical and Environmental Security (SG.PE)	
SG.PE-1	Physical and Environmental Security Policy and Procedures
SG.PE-2	Physical Access Authorizations
SG.PE-3	Physical Access
SG.PE-4	Monitoring Physical Access
SG.PE-5	Visitor Control
SG.PE-6	Visitor Records
SG.PE-7	Physical Access Log Retention
SG.PE-8	Emergency Shutoff Protection
SG.PE-9	Emergency Power
SG.PE-10	Delivery and Removal
SG.PE-11	Alternate Work Site
SG.PE-12	Location of Smart Grid Information System Assets
3.19 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
3.20 Security Program Management (SG.PM)	
SG.PM-1	Security Policy and Procedures

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

NIST Ref.	Catalogue of SG Security Requirements
SG.SA-1	Smart Grid Information 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 Information 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 Information System and Communication Protection (SG.SC)	
SG.SC-1	Smart Grid Information System and Communication Protection Policy and Procedures
SG.SC-2	Communications Partitioning
SG.SC-3	Security Function Isolation
SG.SC-4	Information Remnants
SG.SC-5	Denial-of-Service Protection
SG.SC-6	Resource Priority
SG.SC-7	Boundary Protection
SG.SC-8	Communication Integrity
SG.SC-9	Communication Confidentiality
SG.SC-10	Trusted Path
SG.SC-11	Cryptographic Key Establishment and Management

NIST Ref.	Catalogue of SG Security Requirements
SG.SC-12	Use of Validated Cryptography
SG.SC-13	Collaborative Computing
SG.SC-14	Transmission of Security Parameters
SG.SC-15	Public-Key Infrastructure Certificates
SG.SC-16	Mobile Code
SG.SC-17	Voice-Over Internet Protocol
SG.SC-18	System Connections
SG.SC-19	Security Roles
SG.SC-20	Message Authenticity
SG.SC-21	Secure Name/Address Resolution Service
SG.SC-22	Fail in Known State
SG.SC-23	Thin Nodes
SG.SC-24	Honeypots
SG.SC-25	Operating 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 Information System Partitioning
3.25 Smart Grid Information System and Information Integrity (SG.SI)	
SG.SI-1	Smart Grid Information 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

Annex B
(informative)

IT security guidelines

B.1 Overview of cyber security issues for DER systems

Briefly, cyber-physical resilience measures should cover possible requirements in the following key areas:

G-1. Security policies to establish the concepts and overall security requirements

G-2. Security procedures to establish the methods for achieving the security requirements described in the security policies

G-3. Risk management to identify the possible impacts of attacks, the likelihood of such attacks (including the cost to the attacker), and the possible cost to mitigate their impacts and/or likelihood

G-4. Defense-in-depth and defense-in-breadth designs and configurations

G-5. Identification, authentication, and role-based access control for users, applications, and systems

G-6. Security perimeters at the different organizational and site-specific levels

G-7. Security for communication protocols: media security, transport security, application security

G-8. Intrusion detection and prevention

G-9. Network and system management to monitor and control the health of networks and the computer systems

G-10. Use of power system reliability mechanisms to detect and mitigate cyber attacks

G-11. Operating the power grid and its security systems differently and unpredictably during attack to maintain power grid reliability

G-12. Prevention, detection, coping during an attack, recovery from an attack, documenting/logging attack events and actions

G-13. Stakeholder responsibilities: security during manufacturing, implementation, installation, operation, maintenance, and removal

B.2 Security guidelines and policies across organizational boundaries

Security policies and procedures are critical to establishing the security environment and ensuring well-integrated security measures. These security policies and procedures should cover both the human users, devices, and the software applications that interact with each other in response to the automation system designs, user actions, and external monitored events.

Within an organization, the security policy-makers can define specific approaches. For instance, utilities could require their systems use specific role-based access control categories and privileges and to implement certain cryptographic procedures.

However, for interactions involving DER systems, security policies and procedures extend across organizational boundaries. It would be impractical to try to have a single set of security policies and procedures for all the stakeholders of DER systems. For instance, it may be possible in an organization to specify a specific set of cryptographic algorithms, but that may not be possible across different organizations. Nonetheless it is critical that adequate security policies and procedures extend across these organizational boundaries.

Therefore more high-level security guidelines and policies may need to be developed. In those situations, some high level cyber security guidelines could be developed that would apply to all stakeholders. Some key recommendations in those security policy guidelines could include:

G-14. Use normative references to standards as much as possible, with the selection of alternatives or options normatively stated. Do not re-invent security requirements if they can be found in well-established standards. Some high level security standards that focus on the electric power industry include:

- **ISO/IEC 27019**: Information technology — Security techniques — Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy industry
- **NISTIR 7628**: Guidelines for Smart Grid Cyber security
- **NERC CIP 2-11**: Critical Infrastructure Protection
- **IEC 62351 series**: Power systems management and associated information exchange – Data and communications security
- **IEC 62443**: Industrial communication networks – Network and system security

G-15. Start by identifying the major security threats and failure scenarios, including assessing their likelihood and their possible impacts (risk assessment):

- Many documents provide guidelines on assessing risks, including the CEN-Cenelec-ETSI “SGIS Toolbox”[9] and the NIST “Guide for Conducting Risk Assessments”[10].
- Identify examples of security breaches and failure scenarios, and develop use cases that illustrate the failures and can be used to identify the most likely threats, impacts, and mitigations.
- 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 attempted but unsuccessful 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 be included as informative

G-16. 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, High-Level Security Requirements, provides a very useful list of areas that could be covered (depending upon the scope of the standard).

G-17. Discuss the major cyber security requirements as they apply to the standard – the first four rely on cryptography and require key management methods, while resilience may rely more on engineering strategies and other non-cryptographic methods:

[9] CEN-CENELEC-ETSI “Smart Grid Coordination Group Smart Grid Information Security”, November 2012.

[10] NIST SP-800-30 Rev 1, “Guide for Conducting Risk Assessments, September 2012.

- Authentication of the systems, devices, and applications that are sending and receiving data, is generally the most important security requirement.
- 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.
- Authorization for all interactions to ensure that only authorized actions are allowed. Role-Based Access Control (RBAC) is the most effective methodology to handle authorization.
- Confidentiality is usually for financial, corporate, or private data, but not usually for normal power system operational data exchanges.
- Non-repudiation (accountability) ensures that some entity cannot deny having received or acted upon a message.
- Resilience (including availability) of the interactions can range from milliseconds to hours or days. Unlike the other cyber security requirements, resilience generally relies on engineering design, configuration management, redundancy, functional analysis, communication network analysis, engineering and operating practices.

G-18. Security shall be end-to-end and therefore the different security solutions and implementations by different vendors should be interoperable.

B.3 User and device authentication

All entities, including human users, devices, and software applications, should be authenticated before they are allowed to interact with any systems. The following include the steps that should be taken.

G-19. Validate and register the identity of users and devices:

- For authentication, trust shall 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 shall 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.
- Devices, usually when manufactured, shall be provided with security certificates, pre-established secret keys, or other security tokens for establishing their identity. Care shall be taken to ensure security certificates are not counterfeit or stolen.
- These identifications can be used assigning users and devices to “roles”.

G-20. Establish the authorizations and privileges of each role in Role-Based Access Control (RBAC) (reference IEC 62351-8):

- Each (human) user, software application, and device 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, to eliminate conflicts of interest, and to ensure independence in the responsibilities.
- Users, applications, and devices may be assigned to multiple roles so long as they are not mutually exclusive.
- RBAC privileges should be linked to the data wherever it is located, such as in a device or a database.

- The ability to log user, application, or device role execution along with role violation alerts should be provided

G-21. 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 (MAC hashes), etc. All authentication methods rely on cryptography (even passwords if they are transmitted between systems) and thus necessitate key management (see clause B.8). Public-Key Infrastructure (PKI) is the most commonly used for key management, but may not be applicable in all situations.
- Avoid specifying cryptographic algorithms (such as RSA) if the standard is focused only on user requirements, since there are many valid cryptographic methods. However, there should be a reference to a cryptographic standard that does cover the appropriate cryptographic technologies for these user requirements.
- Whenever possible and appropriate, reference existing standards, such as the IEC 62351 series and the security-related IETF RFCs.

G-22. Focus on the integrity of information:

- Integrity of information relies on cryptography, specifically message authentication codes (MAC hashes) which use cryptographic keys to ensure that any tampering of information can be detected (not prevented). Often integrity cryptography is combined with authentication, such as with digital signatures with certificates. Integrity cryptography (MAC) is also usually included in confidentiality which combines tamper detection with encryption for prevention of eavesdropping.
- Key management is required for integrity.
- 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, software updates, and configuration.
- Integrity violations should be logged

G-23. Identify those interactions that require confidentiality:

- Confidentiality relies on encryption algorithms which use cryptographic keys to prevent eavesdropping. Usually these encryption algorithms are combined with integrity cryptography to ensure both confidentiality and integrity.
- Key management is required for confidentiality.
- These interactions usually involve corporate, financial, customer, and market information.
- Privacy (personal information) should also be considered confidential. If personal data is aggregated, that aggregated data should still be considered private unless individual personal data cannot reasonably be derived from it.,
- Avoid specifying cryptographic algorithms (such as RSA) if the standard is focused only on user requirements, but ensure some standard does cover the appropriate cryptographic technologies for all system designs.

G-24. Determine availability requirements for all types of interactions:

- Availability is mostly affected by configuration design and management. Therefore, normally key management is not necessary for availability.
- What timing latency is allowed for different types of interactions: milliseconds, seconds, minutes, or even days?
- How closely monitored does that timing need to 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?

G-25. 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.

G-26. Revoke user access and/or privileges when a user or an application's role changes

- Revoke access through RBAC and disable the user's passwords.
- Ensure revocations are made available to all affected systems in a timely manner
- For temporary assignment of users to roles, ensure that a deadline is associated with that assignment and the user is revoked at the deadline.

G-27. Deregister applications and revoke any certificates or tokens if an application is decommissioned or its security is compromised

- Ensure revocations are made available to all affected systems in a timely manner, usually within a day or so.

G-28. Establish alarm and event logs content, accuracy of the timestamps, synchronicity of timestamping, and security requirements:

- Log and timestamp all anomalous events
- Ensure all alarms are assigned to one or more roles so that they will be viewable.
- For higher priority alarms, ensure that at least one user has logged on in one of the assigned roles.
- Track user interactions with applications and systems, as appropriate
- Synchronize the timestamps across all systems within the necessary accuracy (milliseconds or seconds).
- Prevent alteration of the time source and issue an alarm if the time source becomes unavailable or appears to be tampered with (e.g. significant change in time)
- Implement methods to detect and mitigate time spoofing (e.g., by cross checking against and failover to a trusted time source).
- Prevent or log all modifications to logs.
- Ensure log storage capacity is adequate for audit purposes
- Issue alarms when the audit log capacity is close to full and when it is exceeded
- Issue an alarm if an audit logging process has failed
- Archive logs for appropriate lengths of time.
- Have the capability to write audit logs to write-once media
- Provide relevant logs to security personnel.
- Provide methods for correlating different types of events – sort/search

B.4 Good practices for specifying and implementing cryptography

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

G-29. 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 shall not be used.

G-30. Only experts should implement cryptography, since non-experts often implement it incorrectly and thus leave the systems open to well-known attacks.

G-31. 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.

G-32. 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. For instance, AES-128 and SHA-256 are currently commonly used. However, what is understood as "adequate strength" changes over time as systems become more capable – and hackers become more sophisticated. Therefore, options for improved cipher suites over time should also be permitted.

G-33. 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.

G-34. Legacy equipment may be allowed to use deprecated cryptographic algorithms so long as "mitigating" countermeasures are included. Mitigating countermeasures might include constraining the legacy communications to be within an electronically secure perimeter, tunneling legacy protocols through VPNs or limiting what functions that legacy equipment is permitted to do. No new implementations should be permitted to implement deprecated cryptographic algorithms.

G-35. Key management and certificate management requirements should be included, either directly or by normative reference. All cryptographic methods rely on cryptographic keys which need, at a minimum, to be initially installed in equipment (e.g. as the equipment's private or secret key). Typically the secret keys used in sessions shall be periodically updated or recalculated. Certificates that bind a public key to a private key may also need to be re-issued if they are about to expire. Certificate revocation provides the critical ability to prevent any future interactions if the private key has been compromised.

G-36. 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.

B.5 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.

G-37. 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.

G-38. 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.

G-39. 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.

G-40. 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.

G-41. 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 private key. Public-Key Infrastructure (PKI) is the most commonly used method for managing certificates.

G-42. NSA Suite B identifies the strongest security algorithms available for civilian use. It consists of the following:

- Encryption: Advanced Encryption Standard (AES) – FIPS PUB 197 (with keys sizes of 128 and 256 bits)
- Key Exchange: The Ephemeral Unified Model and the One-Pass Diffie Hellman (referred to as ECDH) – NIST Special Publication 800-56A (using the curves with 256 and 384- bit prime moduli)
- Digital Signature: Elliptic Curve Digital Signature Algorithm (ECDSA) – FIPS PUB 186-3 (using the curves with 256 and 384-bit prime moduli)
- Hashing: Secure Hash Algorithm (SHA) – FIPS PUB 180-4 (using SHA-256 and SHA-384)

B.6 Cryptography used for transport layer security on networks

Cryptography used for transport layer security often uses the cryptographic profiles defined in RFCs by the IETF. The predominant RFCs include:

G-43. 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.

G-44. Hypertext Transfer Protocol Security (HTTPS) is a combining of HTTP over TLS, and in formalized in RFC 2818.

G-45. 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.

G-46. 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.

B.7 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:

G-47. Using centrally managed WiFi infrastructures and the authentication

G-48. Adopting the IEEE 801.1x authentication infrastructure

G-49. 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.

B.8 Key management using 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 the private key is used in the digital signature generation process; the corresponding public key is used in the digital signature valuation process. The public key can be made widely available, while the private key is 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. A Public-Key Infrastructure (PKI) certificate management process can be used to certify and manage the public keys.

The public key cryptography process, often using PKI in some of the steps, entails a number of steps. IEC 62351-9, Key Management, is identifying and standardizing these techniques for the power industry:

G-50. Register with Registration Authority (RA): Entities (systems, devices, and software applications) shall 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.

G-51. 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, preferably via hardware mechanisms.

G-52. Request certificate from a Certification 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.

G-53. Chain subsequent 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.

G-54. 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.

G-55. Create (and update) session keys: Although public/private keys can be used by two (or more) entities to authenticate each to the other and to then exchange information, a more efficient and secure purpose of these public/private keys can be to create session keys. These session keys can be 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.

G-56. Use session keys: Session keys can be used to hash messages (authentication and integrity only) or encrypt the message payloads to provide confidentiality. Each of these processes has different cryptographic requirements and performance characteristics.

G-57. Revoke certificates: Certificates can be revoked if the private key has been compromised ,if the entity shall no longer be used in its current role, or other reasons for preventing the further use of the certificate.

G-58. Access Certificate Revocation Lists (CRL): CRLs are used for general revocation information when systems are able to access CA sites.

G-59. Provide Online Certificate Status Protocol (OCSP) servers for revoked certificates: For power system equipment, alternate methods shall often be used, such as OCSP servers.

G-60. White listing (namely only permitting access by entities on the white list) can also be used to verify the current status of an entity. In particular, self-signed certificates should usually be white listed as added authentication.

G-61. 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, and assigned to RBAC roles. These pre-shared keys can be used to create and update session keys, and should include a method for revoking their participation in information exchanges.

B.9 Multicast and group keys

For peer-to-peer or multicast interactions of entities which have stringent performance requirements, group key management is more efficient that pair-wise key management. Group key management uses a combination of asymmetric and symmetric cryptography. The security process steps include:

G-62. One system or device is designated as group controller.

G-63. The group controller authenticates other entities via their certificates or pre-shared keys.

G-64. The group controller establishes of a group-based key.

G-65. The group controller distributes the group key to all authenticated entities.

B.10 Device and platform integrity

Security can be enhanced in devices and platforms using technologies such as:

G-66. A manufacturer certificate or other identity token is installed on every component of a system or device. This can be used for identification and trust purposes when certificates and/or cryptographic keys are provided to the device

G-67. Tamper-resistant design of firmware and software by logging all changes or attempts to change data

G-68. Digitally signed firmware/software images are provided, particularly during firmware/software upgrades

G-69. Secure storage of cryptography credentials and other sensitive data is provided, including tamper detection

G-70. Secure code development practices include ensuring the chain of supply is secured, particularly for components that could contain malware or similar vulnerabilities

G-71. Installation integrity includes site tests, protection or elimination of vendor backdoors

B.11 Resilient network configurations

Network configurations can be designed for resilience:

G-72. Networks that are dedicated to different scopes should be physically and/or logically isolated (e.g. industrial networks and corporate networks).

G-73. Access points to the Internet should either be prevented or very carefully managed.

G-74. Firewalls should be used at “security boundaries” to permit only authorized traffic to go through

G-75. Unused ports in routers should be disabled to prevent denial of service attacks and other malicious attacks.

G-76. Intrusion detection and/or intrusion prevention systems (IDS/IPS) should be deployed.

G-77. Redundant communication paths should be provided for applications that require high availability.

G-78. Service level agreements (SLA) with any third party communication providers should include very stringent security requirements.

B.12 Network and system management (NSM)

Network and system management (NSM) should be implemented for all communication networks (reference IEC 62351-7), using protocols such as the Simple Network Management Protocol (SNMP).

G-79. Alarms and events from power system operations and equipment should be able to be time-synchronized, timestamped, and coordinated with security alarms and events, in order to provide a complete picture of possible threats and attacks.

G-80. Monitor and control the traffic flows as well as detect/alarm abnormal conditions, such as communication circuit temporary and permanent failures. Ensure that denial of service attacks on one network does not cause applications to overload other critical networks.

G-81. Provide intrusion detection and, for more critical circuits, intrusion prevention.

G-82. Detect both communication and end equipment operational anomalies, such as failures, internal alarms, security alarms, operations outside of design specifications, etc.

G-83. Determine what automatic and/or manual actions should be taken for each type of equipment or circuit anomaly

B.13 Some additional cyber security techniques

Some additional cyber security techniques that could be used include the following:

G-84. 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.

G-85. Access Control Lists (ACL) are used in routers to limit which ports and/or IP addresses are permitted to be accessed by which entities.

G-86. 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.

G-87. The Group Domain Of Interpretation (GDOI) method defined in RFC 6407 supports the distribution of a symmetric group key to all pre-configured or otherwise enrolled entities, typically devices.

B.14 Security testing procedures

Security testing procedures should be established for all software applications and all interactions between users and applications, and between different applications

G-88. Only experts should implement cryptography to avoid implementation mistakes

G-89. Testing of all new systems and devices should include testing of security measures.

G-90. Software applications and firmware should be tested to ensure they do not have embedded malware, including at their entry and exit points. Notifications of suspected malware should be alarmed and logged.

G-91. Testing requirements could include both static and dynamic code analysis.

G-92. Guidelines from the Open Web Application Security Project (OWASP) could be used to better ensure that web applications are secure.

G-93. Security testing standards should be used. The NISTIR report 7920 (2012) discusses software testing and references the software testing standard, ISO/IEC 29119.

G-94. Security testing should be undertake during initial installations and after any updates or patching.

G-95. Security procedures should also be tested to ensure they perform the security functions they are designed for.

B.15 Security interoperability

Particularly for cross-organizational security, it is important to clearly identify how the coordination and interoperability of the security requirements are to be managed. Questions to resolve include the following:

G-96. Security design and implementation steps: What steps should 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?

G-97. Cryptographic technologies: What are the default certificate and key management technologies? Which additional ones may be used? Which are deprecated?

G-98. Time synchronization: Determine how time synchronizations across all organizations are to be handled, including security against attacks on clocks and the time synch protocol?

G-99. Incidence response: What happens if suspicious actions are noted? Who should be informed? What actions are taken? How should people and systems cope with the impacts of suspected security attacks?

G-100. Remote session termination. Should remote sessions between two organizations be terminated after a time of inaction? What time should that be? Should concurrent sessions be limited to a specific number of users?

G-101. Mitigation strategies during and after an attack: Are there security response plans at the organizational, inter-organizational, and regional level?

G-102. Protection across untrusted networks: What security mechanisms should be used to protect information that is traversing untrusted networks between two zones or organizations?

Annex C
(informative)

Mapping between IEC 62443-3-3, NISTIR 7628, and IEC TR 62351-12

C.1 Mapping table

Table C.1 provides a mapping between IEC 62443-3-3, NISTIR 7628, and this document, IEC TR 62351-12. IEC 62443-3-3 and the NISTIR 7628 are both high level guidelines for smart grid cyber security, and are very similar in scope and even guideline titles. They do not explicitly focus on DER systems or engineering strategies, although some engineering strategies can be implied from the requirements.

On the other hand, the present technical report focuses on power systems with interconnected DER systems, and identifies both cyber security measures and engineering strategies with the goal of enhancing power system resilience. It identifies far more detailed recommendations than the high level guideline documents, but since it is focused on DER, it does not cover all areas of those documents. At the same time, it addresses additional detailed areas that are not included in the guideline documents. Therefore there is not an easily recognized one-to-one mapping between them. For this reason, the IEC TR 62351-12 mapping includes some explanatory comments.

In the present technical report, Clause 7.4 contains the “A-xx” references, Clause 8.4 contains the “B-xx” references, Clause 9.4 contains the “C-xx” references, Clause 10.4 contains the “D-xx” references, and Annex B contains the “G-xx” references.

Table C.1 – Mapping between IEC 62443-3-3, NISTIR 7628, and IEC TR 62351-12

IEC 62443-3-3 versus NISTIR 7628 versus IEC TR 62351-12			
IEC 62443-3-3	**IEC 62443-3-3, Subclause**	**NISTIR 7628**	**IEC TR 62351-12**
FR 1 – Identification and authentication control (IAC)			
SR 1.1 – Human user identification and authentication	5.3	SG.IA-4 User Identification and Authentication	A-66, A-68, A-108, B-28, B29, B-65, B-66, B-67, B-68, B-69, B-118, C-19, C-20, C-22, G-5, G-17, G-19, G-21
SR 1.1 RE 1 – Unique identification and authentication	5.3.3.1		A-66, B-65, B-76, C-19
SR 1.1 RE 2 – Multifactor authentication for untrusted networks	5.3.3.2		A-108, B-118 *For remote maintenance*
SR 1.1 RE 3 – Multifactor authentication for all networks	5.3.3.3		*Not necessary for all networks*
SR 1.2 – Software process and device identification and authentication	5.4	SG.IA-5 Device Identification and Authentication	A-19, A-20, A-68, A-108, B-9, B-11, B-28, B29, B-66, B-67, B-69, B-94, B-118, C-20, C-21, C-22, C-30, G-5, G-17, G-19, G-21, G-22, G-39, G-40, G-43, G-45, G-47, G-48, G-56, G-60
SR 1.2 RE 1 – Unique identification and authentication	5.4.3.1		A-19, A-65, A-66, B-9, B-11, C-21
SR 1.3 – Account management	5.5	SG.AC-3 Account Management	A-21, A-65, B-10, B-14, B-24, C-23
SR 1.3 RE 1 – Unified account management	5.5.3.1		B-24, C-23
SR 1.4 – Identifier management	5.6	SG.IA-2 Identifier Management	A-66, B-65, C-19
SR 1.5 – Authenticator management	5.7	SG.IA-3 Authenticator Management	A-40, A-43, A-67, A-69, B-14, B-25, B-26, B-27, B-35, B-72, B-75, B-105, C-25, C-26, C-29
SR 1.5 RE 1 – Hardware security for software process identity credentials	5.7.3.1		A-24, A-60, B-15
SR 1.6 – Wireless access management	5.8	SG.AC-16 Wireless Access Restrictions SG.AC-17 Access Control for Portable and Mobile Devices	A-32, G-47, G-48, G-49
SR 1.6 RE 1 – Unique identification and authentication	5.8.3.1		G-47
SR 1.7 – Strength of password-based authentication	5.9	SG.AC-21 Passwords	A-24, A-65, A-69, A-85, B-15, B-28, B-29, B-44, B-66, B-67, B-70, B-95, C-9, C-20, C-25, G-19, G-21, G-26
SR 1.7 RE 1 – Password generation and lifetime restrictions for human users	5.9.3.1		B-28, B-70, C-25, G-26
SR 1.7 RE 2 – Password lifetime restrictions for all users	5.9.3.2		B-28, B-70, C-25, G-26

IEC 62443-3-3 versus NISTIR 7628 versus IEC TR 62351-12			
IEC 62443-3-3	**IEC 62443-3-3, Subclause**	**NISTIR 7628**	**IEC TR 62351-12**
SR 1.8 – Public-Key Infrastructure certificates	5.10	SG.SC-15 Public-Key Infrastructure Certificates	A-26, A-69, A-70, A-88, A-89, B-38, B-44, B-74, B-98, B-99, C-13, C-14, C-28, G-27, G-35, G-41, G-52, G-53, G-57, G-59, G-60, G-63, G-66
SR 1.9 – Strength of public key authentication	5.11	SG.SC-11 Cryptographic Key Establishment and Management SG.SC-12 Use of Validated Cryptography	A-19, A-41, A-47, A-87, B-37, B-38, B-44, B-50, B-97, C-11, C-21, G-21, G-22, G-23, G-29, G-33, G-34, G-35, G-38, G-39, G-43, G-52, G-56, G-66,G-69, G-88, G-97
SR 1.9 RE 1 – Hardware security for public key authentication	5.11.3.1		A-24, A-60, B-15, G-51
SR 1.10 – Authenticator feedback	5.12	SG.IA-6 Authenticator Feedback	A-85, A-86, B-95, B-96, C-9, C-10, G-21, G-26, G-27
SR 1.11 – Unsuccessful login attempts	5.13	SG.AC-8 Unsuccessful Login Attempts	A-26, A-97, B-30, B-31, B-67
SR 1.12 – System use notification	5.14	SG.AC-9 Smart Grid Information System Use Notification	A-72, A-95, B-78, B-105, C-32
SR 1.13 – Access via untrusted networks	5.15	SG.AC-14 Permitted Actions without Identification or Authentication	A-123, B-41, B-60, B-83, B-86, B-90, B-92
SR 1.13 RE 1 – Explicit access request approval	5.15.3.1		A-123, B-41, B-60, B-83, B-86, B-90, B-92
FR 2 – Use control (UC)			
SR 2.1 – Authorization enforcement	6.3	SG.AC-4 Access Enforcement	A-10, A-24, A-60, A-70, A-91, A-92, A-97, A-105, A-107, A-131, B-3, B-15, B-40, B-71, B-77, B-101, B-102, B-107, B-115, B-117, B-138, C-12, C-15, C-16, C-19, C-31, G-17, G-20, G-74, G-84
SR 2.1 RE 1 – Authorization enforcement for all users	6.3.3.1		A-10, A-24, A-60, A-70, A-91, A-92, A-97, A-105, A-107, A-131, B-3, B-15, B-40, B-71, B-77, B-101, B-102, B-107, B-115, B-117, B-138, C-12, C-15, C-16, C-19, C-31, G-17, G-20, G-74, G-84
SR 2.1 RE 2 – Permission mapping to roles	6.3.3.2		A-21, A-43, A-59, A-66, A-69, A-71, A-124, B-10, B-11, B-17, B-25, B-26, B-27, B-32, B-34, B-36, B-63, B-69, B-72, B-75, C-23, C-26, C-29, G-20, G-26, G-54
SR 2.1 RE 3 – Supervisor override	6.3.3.3		A-15, A-97, B-8, B-107
SR 2.1 RE 4 – Dual approval	6.3.3.4		B-69, C-24
SR 2.2 – Wireless use control	6.4	SG.AC-16 Wireless Access Restrictions	G-47, G-48, G-49
SR 2.2 RE 1 – Identify and report unauthorized wireless devices	6.4.3.1		A-91, A-131, B-101, B-102, B-138, C-15, C-16

IEC 62443-3-3 versus NISTIR 7628 versus IEC TR 62351-12			
IEC 62443-3-3	**IEC 62443-3-3, Subclause**	**NISTIR 7628**	**IEC TR 62351-12**
SR 2.3 – Use control for portable and mobile devices	6.5	SG.AC-17 Access Control for Portable and Mobile Devices	*Not explicitly addressed for mobile devices, but covered under RBAC requirements and network connection requirements*
SR 2.3 RE 1 – Enforcement of security status of portable and mobile devices	6.5.3.1		A-91, A-131, B-101, B-102, B-138, C-15, C-16
SR 2.4 – Mobile code	*6.6*	SG.SC-16 Mobile Code	A-6, A-107, A-109, A-110, B-12, B-33, B-117, B-119, B-120, G-22, G-68 *Applicable for all code, not just mobile code*
SR 2.4 RE 1 – Mobile code integrity check	*6.6.3.1*		G-67, G-68, G-90
SR 2.5 – Session lock	*6.7*	SG.AC-12 Session Lock	*Not applicable for DER systems*
SR 2.6 – Remote session termination	*6.8*	SG.AC-13 Remote Session Termination	G-100
SR 2.7 – Concurrent session control	*6.9*	SG.AC-11 Concurrent Session Control	G-100
SR 2.8 – Auditable events	*6.10*	SG.AU-2 Auditable Events	A-98, A-99, A-100, A-103, B-36, B-46, B-79, B-108, B-109, B-110, B-122, B-137, C-33, G-15
SR 2.8 RE 1 – Centrally managed, system-wide audit trail	*6.10.3.1*		A-98, B-46, B-108, D-11, G-28, G-79, G-98
SR 2.9 – Audit storage capacity	*6.11*	SG.AU-4 Audit Storage Capacity	G-28
SR 2.9 RE 1 – Warn when audit record storage capacity threshold reached	6.11.3.1		G-28
SR 2.10 – Response to audit processing failures	6.12	SG.AU-5 Response to Audit Processing Failures	G-28
SR 2.11 – Timestamps	6.13	SG.AU-8 Time Stamps	A-17, A-98, A-115, A-116, A-124, A-125, B-108, B-129, B-130, B-131, B-132, G-28, G-79
SR 2.11 RE 1 – Internal time synchronization	6.13.3.1		A-98, B-46, B-108, D-11, G-28, G-79
SR 2.11 RE 2 – Protection of time source integrity	6.13.3.2		G-28
SR 2.12 – Non-repudiation	6.14	SG.AU-16 Non-Repudiation	A-68, A-74, A-85, B-69, B-80, B-96, C-9, C-24, C-34, G-17, G-25, G-56
SR 2.12 RE 1 – Non-repudiation for all users	6.14.3.1		A-68, A-85, B-69, B-96, C-9, C-24, G-17, G-25, G-56
FR 3 – System integrity (SI)			
SR 3.1 – Communication integrity	7.3	SG.SC-8 Communication Integrity	A-38, A-85, A-101, B-95, B-111, C-9, G-17, G-22, G-23, G-39, G-43, G-56, G-71
SR 3.1 RE 1 – Cryptographic integrity protection	7.3.3.1		G-22, G-39, G-43, G-56

IEC 62443-3-3 versus NISTIR 7628 versus IEC TR 62351-12			
IEC 62443-3-3	**IEC 62443-3-3, Subclause**	**NISTIR 7628**	**IEC TR 62351-12**
SR 3.2 – Malicious code protection	7.4	SG.SI-3 Malicious Code and Spam Protection	G-70, G-90, G-91
SR 3.2 RE 1 – Malicious code protection on entry and exit points	7.4.3.1		G-90
SR 3.2 RE 2 – Central management and reporting for malicious code protection	7.4.3.2		G-90
SR 3.3 – Security functionality verification	7.5	SG.SI-6 Security Functionality Verification	A-10, A-11, A-16, A-49, A-59, A-61, A-77, A-84, A-85, A-87, A-88, A-124, A-132, A-133, A-134, B-1, B-3, B-4, B-38, B-42, B-50, B-52, B-53, B-59, B-64, B-83, B-95, B-97, B-98, B-116, B-121, B-124, B-131, B-143, B-144, B-144, C-8, C-9, C-11, C-13, G-19, G-21, G-22, G-41, G-52, G-53, G-60
SR 3.3 RE 1 – Automated mechanisms for security functionality verification	7.5.3.1		A-1, A-101, B-111
SR 3.3 RE 2 – Security functionality verification during normal operation	7.5.3.2		A-1, A-101, B-111
SR 3.4 – Software and information integrity	7.6	SG.SI-7 Software and Information Integrity	A-85, A-101, B-95, B-111, C-9, G-17, G-22, G-23, G-39, G-43, G-56, G-71
SR 3.4 RE 1 – Automated notification about integrity violations	7.6.3.1		A-97, B-45, B-107, G-22, G-28, G-67
SR 3.5 – Input validation	7.7	SG.SI-8 Information Input Validation	A-10, A-11, A-16, A-49, A-55, A-77, A-85, A-87, A-88, A-124, B-1, B-3, B-4, B-38, B-42, B-50, B-53, B-59, B-83, B-95, B-97, B-98, B-124, B-131, C-8, C-9, C-11, C-13, G-19, G-21, G-22, G-41, G-52, G-53, G-60
SR 3.6 – Deterministic output	7.8		A-97, B-107, D-2
SR 3.7 – Error handling	7.9	SG.SI-9 Error Handling	A-13, A-50, A-94, A-97, B-7, B-54, B-104, B-107, C-18
SR 3.8 – Session integrity	7.10		G-35, G-36, G-45, G-55, G-56, G-61
SR 3.8 RE 1 – Invalidation of session IDs after session termination	7.10.3.1		G-26, G-27, G-36, G-57, G-59
SR 3.8 RE 2 – Unique session ID generation	7.10.3.2		A-42, B-39
SR 3.8 RE 3 – Randomness of session IDs	7.10.3.3		*Not explicitly addressed*
SR 3.9 – Protection of audit information	7.11	SG.AU-9 Protection of Audit Information	A-98, A-99, A-100, A-103, B-36, B-46, B-79, B-108, B-109, B-110, B-122, B-137, C-37, G-15
SR 3.9 RE 1 – Audit records on write-once media	7.11.3.1		G-28
FR 4 – Data confidentiality (DC)			

IEC 62443-3-3 versus NISTIR 7628 versus IEC TR 62351-12			
IEC 62443-3-3	**IEC 62443-3-3, Subclause**	**NISTIR 7628**	**IEC TR 62351-12**
SR 4.1 – Information confidentiality	8.3	SG.SC-9 Communication Confidentiality	A-24, A-44, A-68, A-73, A-86, A-134, B-15, B-43, B-47, B-69, B-77, B-96, B-145, C-10, C-24, C-31, G-17, G-22, G-23, G-38, G-39, G-40, G-43, G-56
SR 4.1 RE 1 – Protection of confidentiality at rest or in transit via untrusted networks	8.3.3.1		A-93, B-103, C-6, C-17, G-102
SR 4.1 RE 2 – Protection of confidentiality across zone boundaries	8.3.3.2		G-102
SR 4.2 – Information persistence	8.4	SG.SC-4 Information Remnants	*Not explicitly addressed*
SR 4.2 RE 1 – Purging of shared memory resources	8.4.3.1		*Not explicitly addressed*
SR 4.3 – Use of cryptography	8.5	SG.SC-12 Use of Validated Cryptography	A-19, A-41, A-47, A-87, B-37, B-38, B-44, B-50, B-97, C-11, C-21, G-21, G-22, G-23, G-29, G-33, G-34, G-35, G-38, G-39, G-43, G-52, G-56, G-66,G-69, G-88, G-97
FR 5 – Restricted data flow (RDF)			
SR 5.1 – Network segmentation	9.3	SG.CM-7 Configuration for Least Functionality SG.SC-2 Communications Partitioning	A-79, A-80, A-81, A-90, B-41, B-85, B-91, B-100, C-15, G-72, G-84
SR 5.1 RE 1 – Physical network segmentation	9.3.3.1		A-82, A-90, B-41, B-88, B-100, C-15, G-72
SR 5.1 RE 2 – Independence from non-control system networks	9.3.3.2		A-90, B-41
SR 5.1 RE 3 – Logical and physical isolation of critical networks	9.3.3.3		A-82, A-90, B-18, B-41, B-87, C-5, C-7, C-8
SR 5.2 – Zone boundary protection	9.4	SG.SC-3 Security Function Isolation SG.SC-7 Boundary Protection	B-14, G-6, G-34
SR 5.2 RE 1 – Deny by default, allow by exception	9.4.3.1		A-90, A-91, A-92, A-94, A-120, A-121, A-122
SR 5.2 RE 2 – Island mode	9.4.3.2		A-90, A-91, A-92, A-94, B-104, B-135, C-18
SR 5.2 RE 3 – Fail close	9.4.3.3		A-90, A-91, A-92, A-94, B-104, B-135, C-18
SR 5.3 – General purpose person-to-person communication restrictions	9.5		*Not explicitly addressed*
SR 5.3 RE 1 – Prohibit all general purpose person- to-person communications	9.5.3.1		*Not explicitly addressed*
SR 5.4 – Application partitioning	9.6	SG.SC-29 Application Partitioning	G-54
FR 6 – Timely response to events (TRE)			
SR 6.1 – Audit log accessibility	10.3	SG.AU-1 Audit and Accountability Policy and Procedures	A-17, A-64, A-95, A-103, A-130, B-4, B-22, B-113, G-28

IEC 62443-3-3 versus NISTIR 7628 versus IEC TR 62351-12			
IEC 62443-3-3	**IEC 62443-3-3, Subclause**	**NISTIR 7628**	**IEC TR 62351-12**
SR 6.1 RE 1 – Programmatic access to audit logs	10.3.3.1		A-17, A-27, A-64, A-103, B-22, B-113, B-142, D-8,
SR 6.2 – Continuous monitoring	10.4	SG.CA-6 Continuous Monitoring	A-32, A-33, A-34, A-35, A-36, A-89, A-96, B-16, B-99, B-106, C-14, D-6, D-7, G-26, G-27
FR 7 – Resource availability (RA)			
SR 7.1 – Denial of service protection	11.3	SG.SC-5 Denial-of-Service Protection	A-31, A-32, A-33, A-34, A-35, A-36, A-54, B-58, D-15, G-17, G-24, G-75, G-77
SR 7.1 RE 1 – Manage communication loads	11.3.3.1		A-75, B-81, B-89, C-1, G-74, G-80, G-86
SR 7.1 RE 2 – Limit DoS effects to other systems or networks	11.3.3.2		G-80
SR 7.2 – Resource management	11.4	SG.SC-6 Resource Priority	A-75, B-81, B-89, C-1, D-22, G-28
SR 7.3 – Control system backup	11.5	SG.IR-10 Smart Grid Information System Backup	A-33, A-35, A-110, A-114, B-120, B-128
SR 7.3 RE 1 – Backup verification	11.5.3.1		A-33, A-35, A-110, A-114, B-120, B-128
SR 7.3 RE 2 – Backup automation	11.5.3.2		A-33, A-35, A-110, A-114, B-120, B-128
SR 7.4 – Control system recovery and reconstitution	11.6	SG.CP-10 Smart Grid Information System Recovery and Reconstitution	A-127, A-128, A-129, A-130, B-137, B-138, B-139, B-140, B-141, B-142, G-12
SR 7.5 – Emergency power	11.7	SG.PE-9 Emergency Power	A-35, A-36
SR 7.6 – Network and security configuration settings	11.8	SG.CM-6 Configuration Settings	A-39, A-43, A-56, A-114, A-116, A-119, A-128, B-23, B-60, B-128, B-130, B-141, G-4, G-17, G-22, G-24
SR 7.6 RE 1 – Machine-readable reporting of current security settings	11.8.3.1		B-23
SR 7.7 – Least functionality	11.9	SG.CM-7 Configuration for Least Functionality	A-90, B-41, B-100, C-15, G-72
SR 7.8 – Control system component inventory	11.10	SG.CM-8 Component Inventory	A-19, A-22, A-83, B-90, C-12, G-66, G-70

C.2 IEC TR 62351-12 cyber security items not mapped to all guidelines

Understandably, almost none of the IEC TR 62351-12 engineering strategy items can be mapped to the high level cyber security guideline documents, including those in Annex B which covers broader cyber security issues. In many cases, the cyber security items in IEC TR 62351-12 stretch the meanings of the guidelines they are associated with, but could be seen as at least partially covered by the guidelines. However, a few cyber security items in Clauses 7 to 9 do not have clear associations with IEC 62443-3-3 guidelines, but were covered in the NISTIR 7628 guidelines. In a few cases, neither guideline document included the requirement.

Table C.2 identifies some of the missing guideline areas, as identified in IEC TR 62351-12. It might be useful to see if the guidelines might be enhanced.

Table C.2 – IEC 62351-12 cyber security items not mapped to all guidelines

IEC TR 62351-12	NISTIR 7628	IEC 62443-3-3
A-23 The manufacturers of DER systems use penetration testing to ensure their systems are well-protected against cyber attacks B-13 The manufacturers of FDEMS use penetration testing to ensure their systems are well-protected	SG.CA-6 Continuous Monitoring SG.SA-11 Supply Chain Protection	None
A-25 The DER system is designed to permit only non-sensitive data to be provided to non-authenticated requests	SG.AC-14 Permitted Actions without Identification or Authentication	None
A-45 The integrator/installer provides instruction to DER owners on security requirements so they won't try to bypass security settings B-48 The integrator/installer provides instructions or training to FDEMS owners on security requirements so they won't try to bypass security settings	SG.AT-3 Security Training	None
A-46 Installers are trained appropriately to ensure that the recommended security settings are implemented. B-49 Installers are trained appropriately to ensure that the recommended security settings are implemented B-73 Users assigned to a security management role should understand instructions or take training on security requirements C-27 Users assigned to a security management role should understand instructions or take training on security requirements	SG.AT-3 Security Training	None
A-48 The integrator/installer certifies that they are supplying equipment from manufacturers who are certified as providing security-enabled equipment. B-51 The integrator/installer certifies that they are supplying equipment from manufacturers who are certified as providing security-enabled equipment.	SG.SA-11 Supply Chain Protection	None
A-104 Maintenance is permitted only by security-certified maintenance organizations. The security requirements for maintenance organizations (e.g. patched maintenance systems, up-to-date malware protection, security clearance for personnel etc.) are included in maintenance contracts. B-114 Maintenance is permitted only by security-certified maintenance organizations. The security requirements for maintenance organizations (e.g. patched maintenance systems, up-to-date malware protection, security clearance for personnel etc.) are included in maintenance contracts.	SG.MA-1 Smart Grid Information System Maintenance Policy and Procedures	None
A-106 Purchased equipment and updated DER systems are tested for its security capabilities, any holes in its security through security reviews, penetration tests and other methods, and the presence of any malware	SG.SA-11 Supply Chain Protection	None
A-111 Equipment is retested after maintenance for its security capabilities and the presence of any malware	SG.MA-3 Smart Grid Information System Maintenance	None
A-117 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 B-134 Upon detection of an attack or significant failure, the FDEMS issues commands to its DER systems to go to default output settings of reasonable or contractual limits, regardless of actual settings B-136 If the attack or failure is significantly affecting the FDEMS, shut down the FDEMS	SG.CP-10 Smart Grid Information System Recovery and Reconstitution	None

IEC TR 62351-12	NISTIR 7628	IEC 62443-3-3
A-126 Where available, Intrusion Detection Systems (IDS) notifies the "DER manager" of suspected intrusions B-133 Where available, Intrusion Detection Systems (IDS) notifies the "FDEMS manager" of suspected intrusions	SG.SI-4 Smart Grid Information System Monitoring Tools and Techniques	None
B-93 Communication protocols are well-established international standards with security	None	None

Annex D
(informative)

Glossary of terms

NOTE For the sake of transparency certain terms which appear in Clause 3, Terms and definitions, are provided here with slightly different definitions from different sources.

cyber-physical systems	hybrid networked cyber and engineered physical elements co-designed to create adaptive and predictive systems for enhanced performance [SOURCE: NIST presentation]
resilience	ability to recover from or adjust easily to misfortune or change [SOURCE: Merriam-Webster dictionary]
resilience	emergent property of an organization that can continue to carry out its mission in the presence of operational stress and disruption that does not exceed its limit NOTE The system shall be able to recover to its normal operating state once the disruption has ended. [SOURCE: CERT® Resilience Management Model: A Maturity Model for Managing Operational Resilience and the CERT Resilience Management Model pages on the CERT website (Caralli 2011, CERT 2012)]
threat	capabilities, intentions and attack methods of adversaries, or any circumstance or event, whether originating externally or internally, that has the potential to cause harm to information or a program or system or cause those to harm others [SOURCE: ISO/IEC 1st WD 21827:2006]
threat	any circumstance or event with the potential to adversely impact agency operations (including mission, functions, image, or reputation), agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service [SOURCE: NIST SP800-53]
vulnerability	flaw or weakness in the design or implementation of an information system (including the security procedures and security controls associated with the system) that could be intentionally or unintentionally exploited to adversely affect an organization's operations or assets through a loss of confidentiality, integrity, or availability [SOURCE: NIST SP800-53]

Bibliography

IEC 61850-7-420, *Communication networks and systems for power utility automation – Part 7-420: Basic communication structure – Distributed energy resources logical nodes*

IEC TR 61850-90-7, *Communication networks and systems for power utility automation – Part 90-7: Object models for power converters in distributed energy resources (DER) systems*

This page deliberately left blank

This page deliberately left blank

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email bsmusales@bsigroup.com.

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Copyright

All the data, software and documentation set out in all British Standards and other BSI publications are the property of and copyrighted by BSI, or some person or entity that owns copyright in the information used (such as the international standardization bodies) and has formally licensed such information to BSI for commercial publication and use. Except as permitted under the Copyright, Designs and Patents Act 1988 no extract may be reproduced, stored in a retrieval system or transmitted in any form or by any means – electronic, photocopying, recording or otherwise – without prior written permission from BSI. Details and advice can be obtained from the Copyright & Licensing Department.

Useful Contacts:

Customer Services
Tel: +44 845 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 845 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com