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

bsi.

AVA Documents
Document Sharing Hub

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.

© The British Standards Institution 2016.
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

Documents
Document Sharing Hub

Full document details: 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.

® Registered trademark of the International Electrotechnical Commission

Documents
Document Sharing Hub

Full document details: PD IEC/TR 62351-12:2016

CONTENTS

FOREWORD 6
INTRODUCTION 8
1 Scope 10
2 Normative references 10
3 Terms and definitions 11
4 Abbreviations and acronyms 12
5 DER architectures and DER cyber-physical concepts 13
5.1 Resiliency challenge for power systems with DER systems 13
5.2 Five-level DER hierarchical architecture 14
5.3 DER system interfaces 17
5.4 Resilience at different DER architectural levels 18
5.5 DER Systems as cyber-physical systems 19
5.5.1 Protecting cyber-physical DER systems 19
5.5.2 Cyber-physical threats 20
5.5.3 Resilience measures for cyber-physical systems 21
6 Threats, vulnerabilities, and impacts on power system resilience 23
6.1 Threats – engineering and cyber 23
6.1.1 Physical and electrical threats – mostly but not entirely inadvertent 23
6.1.2 Cyber threats – inadvertent and deliberate 23
6.2 Vulnerabilities – engineering and cyber vulnerabilities 26
6.2.1 General 26
6.2.2 Power system vulnerabilities and attacks 26
6.2.3 Cyber security vulnerabilities and attacks 28
6.3 Risk management and mitigation techniques 30
6.3.1 Risk handling 30
6.3.2 Risk mitigation categories 31
6.4 Impacts on power system resilience 33
6.4.1 Safety impacts 33
6.4.2 Power outage impacts 34
6.4.3 Power quality impacts 35
6.4.4 Financial impacts 35
6.4.5 Regulatory and legal impacts 36
6.4.6 Environmental impacts 36
6.4.7 Goodwill and other “soft” impacts 36
6.5 DER stakeholders' resilience responsibilities 36
6.6 Resilience Measures for DER systems to counter threats 37
6.6.1 General IT cyber security approach for DER systems 37
6.6.2 Resilience by engineering designs and operational strategies 38
7 Level 1 DER System resilience recommendations 38
7.1 General 38
7.2 Level 1 DER system: architecture 38
7.3 Level 1 DER system: vulnerabilities 40
7.3.1 General 40
7.3.2 Cyber vulnerabilities 40
7.3.3 Engineering design and development vulnerabilities 40

AVA Documents
Document Sharing Hub
Full document details: PD IEC/TR 62351-12:2016

7.3.4 Deployment and operational vulnerabilities 41
7.4 Level 1 DER system: impacts 41
7.5 Level 1 DER system: resilience recommendations 44
7.5.1 General 44
7.5.2 Manufacturer: DER system design for resilience recommendations 44
7.5.3 Integrator and installer: DER setup for meeting resilience recommendations 45
7.5.4 Testing personnel: resilient DER system interconnection testing recommendations 47
7.5.5 DER user: access recommendations 48
7.5.6 ICT designers: requirements for local DER communications 48
7.5.7 Security managers: alarming, logging, and reporting cyber security recommendations 50
7.5.8 Maintenance personnel: resilience recommendations for maintenance, updating and re-testing, systems 50
7.5.9 Recommended coping actions during an attack or failure 51
7.5.10 Recommended recovery and analysis actions after an attack or failure 52
8 Level 2: Facilities DER energy management (FDEMS) resilience recommendations 52
8.1 Level 2 FDEMS: architecture 52
8.2 Level 2 FDEMS: Vulnerabilities 54
8.3 Level 2 FDEMS: Impacts 54
8.4 Level 2 FDEMS: Resilience recommendations 56
8.4.1 General 56
8.4.2 Manufacturer: Design of FDEMS resilience recommendations 56
8.4.3 Integrators and installer: FDEMS implementation for meeting resilience recommendations 57
8.4.4 Testing personnel: Resilient FDEMS testing recommendations 60
8.4.5 FDEMS users: Access recommendations 60
8.4.6 FDEMS ICT designers: Resilience recommendations 61
8.4.7 Security managers: Alarming, logging, and reporting recommendations 63
8.4.8 Maintenance personnel: Resilience recommendations for maintenance, updating and re-testing, systems 63
8.4.9 Recommended coping actions during an attack or failure 64
8.4.10 Recommended recovery and analysis actions after an attack or failure 65
9 Level 3: Third parties: Retail energy provider or aggregators resilience recommendations 66
9.1 Level 3: Third parties: ICT architecture 66
9.2 Level 3: Third parties: ICT vulnerabilities 67
9.3 Level 3: Third parties: ICT impacts 68
9.4 Level 3: Third parties ICT: Resilience recommendations 69
9.4.1 Third party ICT designers: Resilience recommendations 69
9.4.2 ICT users: Access recommendations 71
10 Level 4: Distribution operations analysis resilience recommendations 72
10.1 Level 4 DSO analysis: Architecture 72
10.2 Level 4 DSO analysis: Vulnerabilities 73
10.3 Level 4 DSO analysis: Impacts 74
10.4 Level 4 DSO analysis: Resilience recommendations 76
10.4.1 Resilient design of distribution grid equipment with DER systems 76
10.4.2 Resilience through DSO grid operations with DER systems 76

AVA Documents
Document Sharing Hub
Full document details: PD IEC/TR 62351-12:2016

10.4.3 Resilience through power system analysis 77
10.4.4 Resilience by stakeholder training 78
Annex A (informative) NISTIR 7628 Smart Grid Catalog of Security Requirements 79
A.1 NISTIR 7628 families of security requirements 79
A.2 Detailed NISTIR 7626 Catalogue of Smart Grid Security Requirements 80
Annex B (informative) IT security guidelines 85
B.1 Overview of cyber security issues for DER systems 85
B.2 Security guidelines and policies across organizational boundaries 85
B.3 User and device authentication 87
B.4 Good practices for specifying and implementing cryptography 89
B.5 Cryptographic methods 90
B.6 Cryptography used for transport layer security on networks 91
B.7 Wireless cryptography 92
B.8 Key management using Public Key Cryptography 92
B.9 Multicast and group keys 94
B.10 Device and platform integrity 94
B.11 Resilient network configurations 94
B.12 Network and system management (NSM) 95
B.13 Some additional cyber security techniques 95
B.14 Security testing procedures 95
B.15 Security interoperability 96
Annex C (informative) Mapping between IEC 62443-3-3, NISTIR 7628, and IEC TR 62351-12 97
C.1 Mapping table 97
C.2 IEC TR 62351-12 cyber security items not mapped to all guidelines 103
Annex D (informative) Glossary of terms 106
Bibliography 107

Figure 1 – Smart grid resilience: intertwined IT cyber security and engineering strategies 9
Figure 2 – Smart Grid Architecture Model (SGAM) 15
Figure 3 – Five-level hierarchical DER system architecture 16
Figure 4 – Structure of use cases within the DER hierarchy 19
Figure 5 – Mitigations by engineering strategies and cyber security measures 21
Figure 6 – Security requirements, threats, and possible attacks 30
Figure 7 – Level 1: Autonomous DER systems at smaller customer and utility sites 39
Figure 8 – Level 2 FDEMS architecture 53
Figure 9 – DER third parties: Retail energy provider or aggregators architecture 67
Figure 10 – Distribution operations architecture 72

Table 1 – Examples of mitigations by engineering strategies and cyber security techniques 22
Table 2 – Engineering and cyber security data for managing the resilience of DER systems 22
Table 3 – Examples of mitigation categories for cyber-physical systems 32
Table 4 – Level 1 impact severities due to attacks and failures of autonomous DER systems 43

AVA Documents
Document Sharing Hub
Full document details: PD IEC/TR 62351-12:2016

Table 5 – Level 2 impact severities due to malicious attacks and failures of FDEMS.....55
Table 6 – Level 3 impact severities due to malicious attacks and failures of DER ICT.....69
Table 7 – Level 4 impact severities due to malicious attacks and failures of DMS or DERMS 75
Table A.1 – NIST Smart Grid Security Requirements Families 79
Table A.2 – Detailed NIST Catalogue of Smart Grid Security Requirements 80
Table C.1 – Mapping between IEC 62443-3-3, NISTIR 7628, and IEC TR 62351-12 98
Table C.2 – IEC 62351-12 cyber security items not mapped to all guidelines.....104

Documents
Document Sharing Hub
Full document details: PD IEC/TR 62351-12:2016

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.

Documents
Document Sharing Hub
Full document details: PD IEC/TR 62351-12:2016

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.

Documents
Document Sharing Hub

Full document details: PD IEC/TR 62351-12:2016

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.

Documents
Document Sharing Hub
Full document details: PD IEC/TR 62351-12:2016

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.

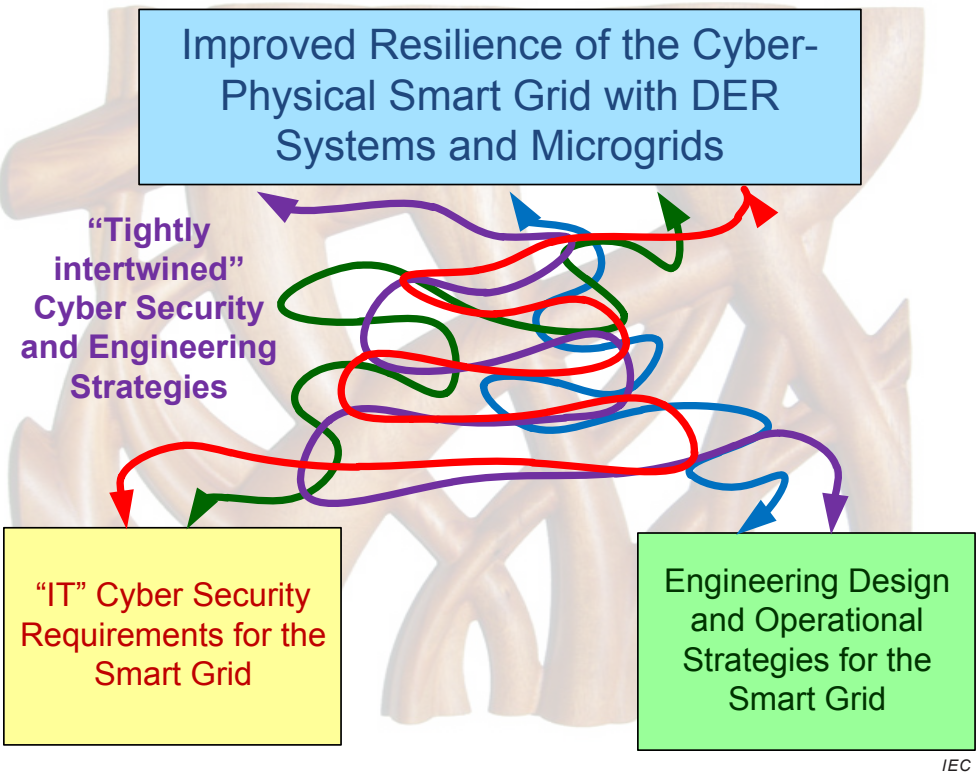

Figure 1 – Smart grid resilience: intertwined IT cyber security and engineering strategies

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.

Documents
Document Sharing Hub
Full document details: PD IEC/TR 62351-12:2016

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.

Documents
Document Sharing Hub
Full document details: PD IEC/TR 62351-12:2016

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]

Documents
Document Sharing Hub
Full document details: PD IEC/TR 62351-12:2016

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

Documents
Document Sharing Hub
Full document details: PD IEC/TR 62351-12:2016

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;

AVA Documents
Document Sharing Hub

- 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.

Documents
Document Sharing Hub
Full document details: PD IEC/TR 62351-12:2016

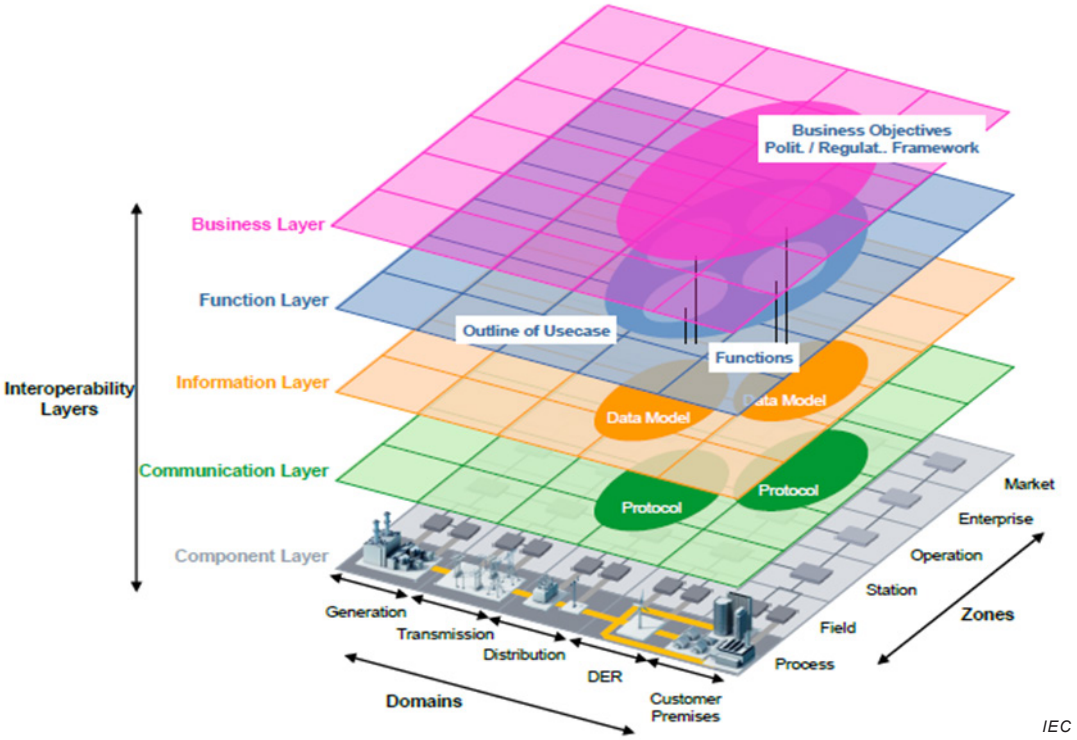

Figure 2 – Smart Grid Architecture Model (SGAM)

Documents
Document Sharing Hub
Full document details: PD IEC/TR 62351-12:2016

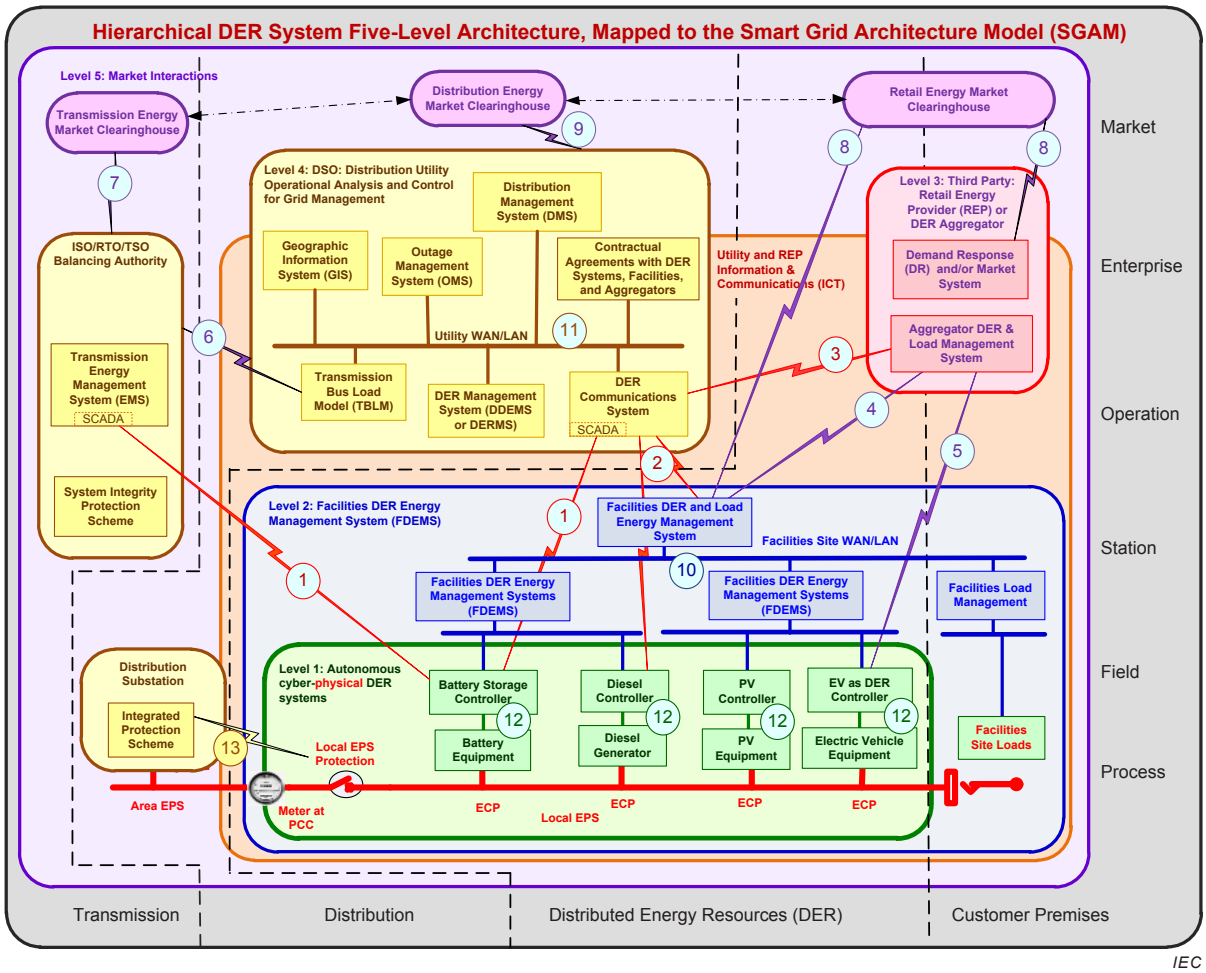

Figure 3 – Five-level hierarchical DER system architecture

- **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

AVA Documents
Document Sharing Hub
Full document details: PD IEC/TR 62351-12:2016

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

AVA Documents
Document Sharing Hub
Full document details: PD IEC/TR 62351-12:2016

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

AVA Documents
Document Sharing Hub

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.

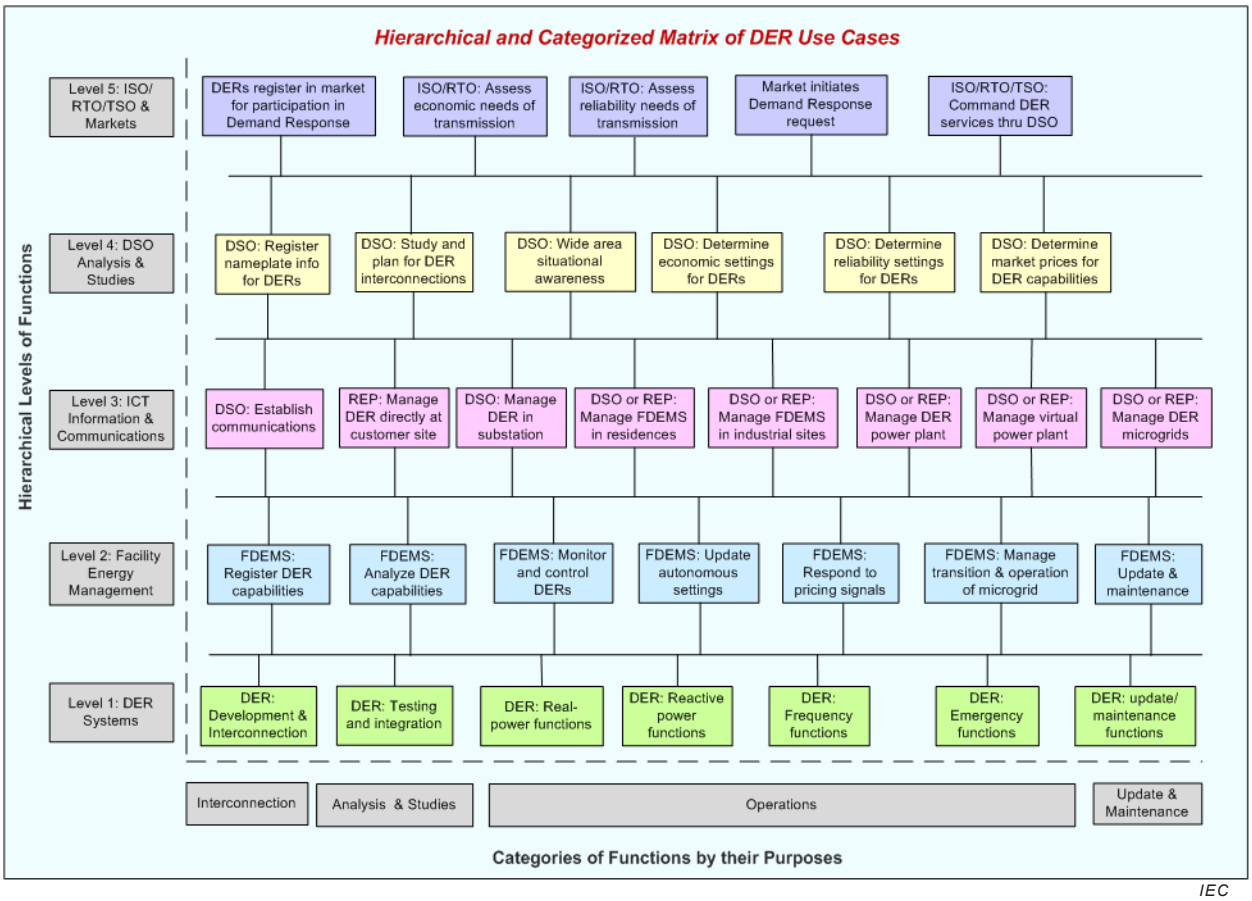

Figure 4 – Structure of use cases within the DER hierarchy

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.

Documents
Document Sharing Hub
Full document details: PD IEC/TR 62351-12:2016

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

Documents
Document Sharing Hub

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.

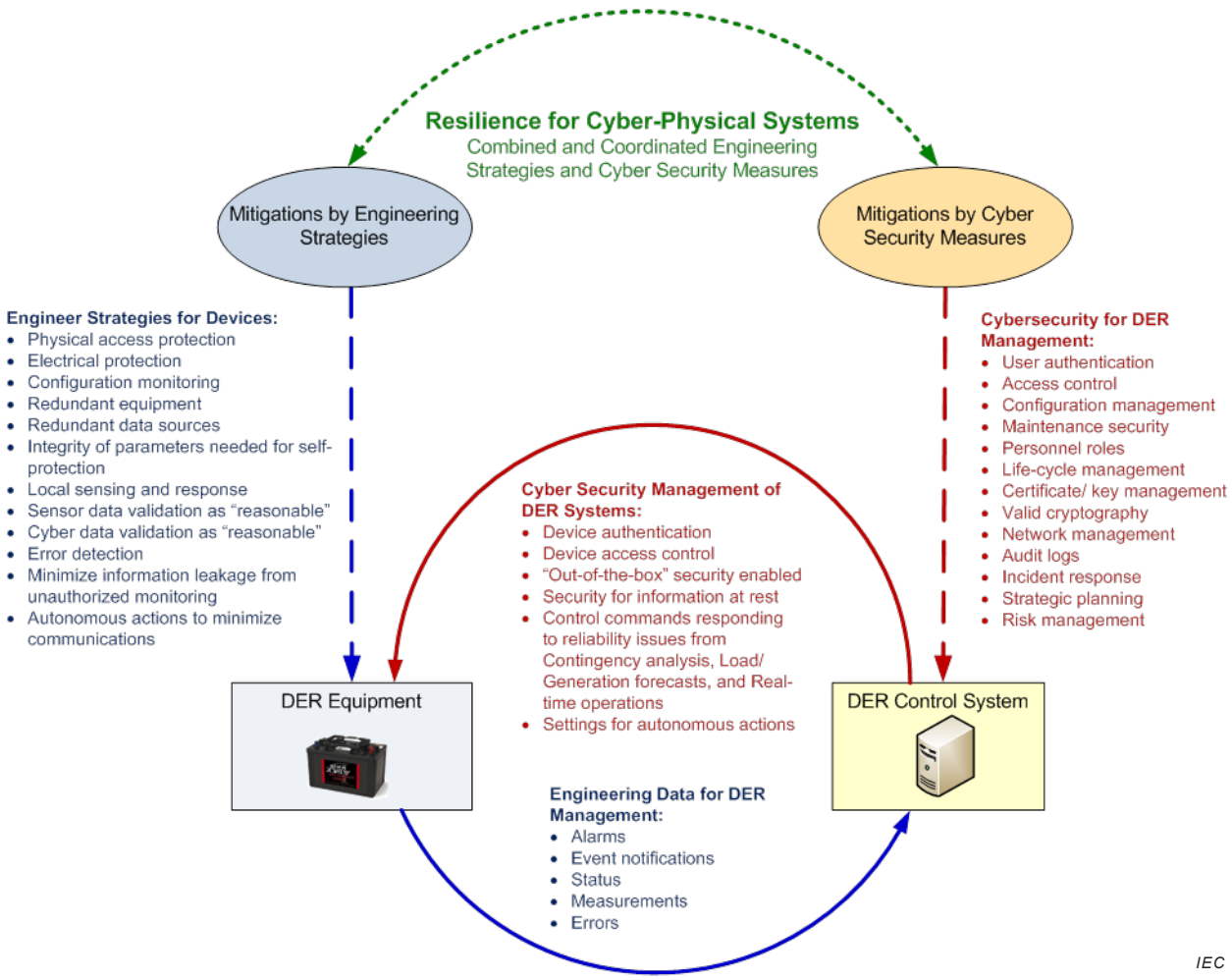

Figure 5 – Mitigations by engineering strategies and cyber security measures

Documents
Document Sharing Hub
Full document details: PD IEC/TR 62351-12:2016

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.	User identity and authentication
Electrical self-protection against cyber or physical attacks, such as “hardwired” limits, tripping off, disconnecting from grid, etc.	Role-based access control
System self protection through “secured” parameters that cannot be remotely changed	Access control management
Sensing and response to local conditions	Authorization
Sensor data validation as “reasonable”	Non-repudiation
Calculated data validation as “reasonable”	System configuration management
Error detection	Maintenance security
Alarms and events on physical changes	Personnel roles
Redundant equipment	Life-cycle management
Redundant data sources	Valid cryptography for authentication, confidentiality, and integrity
Redundant communication paths	Network management and control
Configuration validation and monitoring	Network configuration management
Securing the integrity of parameters that are needed for self-protection even from local access	Intrusion detection in networks and controllers
Autonomous actions that minimize the need for communications	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	Device authentication
Event notifications	Device access control
Status	Authorization
Measurements	“Out-of-the-box” security enabled
Errors	Security for information at rest
	Non-repudiation
	Valid cryptography for confidentiality and integrity
	Results from State Estimation to validate DER status
	Results from Contingency Analysis to manage DER systems
	Power-flow-based applications for situational awareness, such as Load/Generation Forecasts, Real-time Operations, Contingency Analysis, etc.
	Settings for autonomous actions

Documents
Document Sharing Hub
Full document details: PD IEC/TR 62351-12:2016

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.

Documents
Document Sharing Hub
Full document details: PD IEC/TR 62351-12:2016

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.

Documents
Document Sharing Hub
Full document details: PD IEC/TR 62351-12:2016

- 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

AVA Documents
Document Sharing Hub
Full document details: PD IEC/TR 62351-12:2016

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

AVA Documents
Document Sharing Hub

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

AVA Documents
Document Sharing Hub
Full document details: PD IEC/TR 62351-12:2016

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.

AVA Documents
Document Sharing Hub

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.

Documents
Document Sharing Hub
Full document details: PD IEC/TR 62351-12:2016

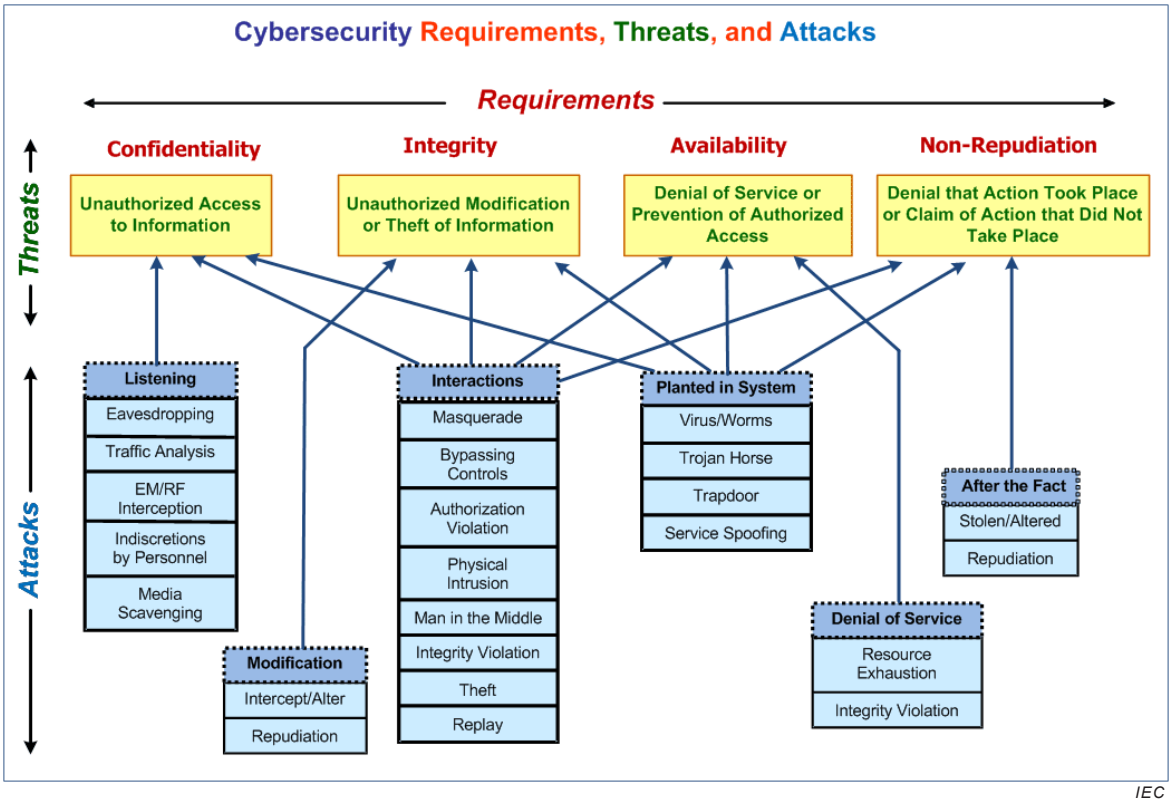

Figure 6 – Security requirements, threats, and possible attacks

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*.

Documents
Document Sharing Hub
Full document details: PD IEC/TR 62351-12:2016

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.

Documents
Document Sharing Hub
Full document details: PD IEC/TR 62351-12:2016

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

Documents
Document Sharing Hub
Full document details: PD IEC/TR 62351-12:2016