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



IEC TR 62351-12:2016-04(en)



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2016 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester. If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
info@iec.ch
www.iec.ch

About the IEC
The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications
The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

IEC Catalogue - webstore.iec.ch/catalogue
The stand-alone application for consulting the entire bibliographical information on IEC International Standards, Technical Specifications, Technical Reports and other documents. Available for PC, Mac OS, Android Tablets and iPad.

IEC publications search - www.iec.ch/searchpub
The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and also once a month by email.

Electropedia - www.electropedia.org
The world's leading online dictionary of electronic and electrical terms containing 20 000 terms and definitions in English and French, with equivalent terms in 15 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary
65 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

IEC Customer Service Centre - webstore.iec.ch/csc
If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: csc@iec.ch.

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

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

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

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

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

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.

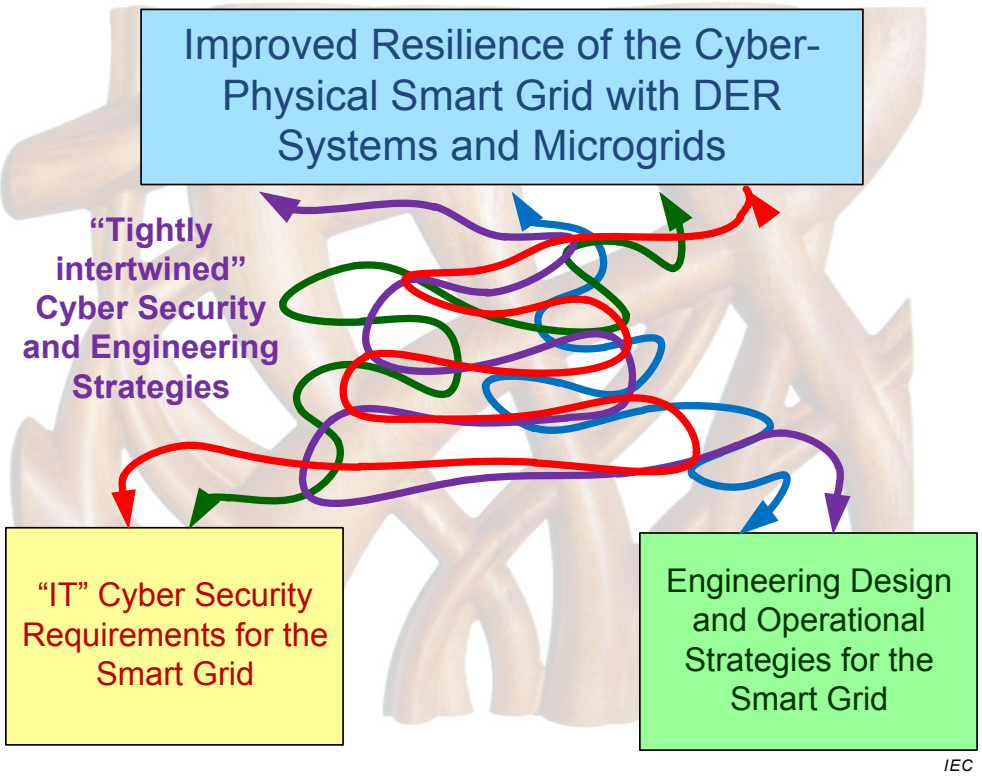


Figure 1 – Smart grid resilience: intertwined IT cyber security and engineering strategies

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