



IEEE Guide for Categorizing Security Needs for Protection-, Automation-, and Control-Related Data Files

IEEE Power and Energy Society

Developed by the
Power System Relaying and Control Committee

IEEE Std C37.249™-2024

STANDARDS

IEEE Guide for Categorizing Security Needs for Protection-, Automation-, and Control-Related Data Files

Developed by the

Power System Relaying and Control Committee
of the
IEEE Power and Energy Society

Approved 11 December 2024

IEEE SA Standards Board

Recognized as an American National Standard

Abstract: Security categorization is the first step in a security risk management framework because of its impact on all other steps, from the selection of security controls to apply based on the assessment to the level of effort required to assess the effectiveness of the security controls put in place. Information (data) at rest and information systems are covered by security categorization. The approach used in this guide applies only to data at rest. Types of information and information systems are considered by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-60 Vol. 1, Rev. 1 [B16]. Security categories—based on the magnitude of harm expected to result from compromises rather than on the results of an assessment that includes an attempt to determine the probability of compromise—are established by Federal Information Processing Standards (FIPS) 199 [B1]. These standards are aligned by the approach in this guide.

Keywords: automation files, control files, data at rest, IEEE C37.249, protection files, security categorization

The Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York, NY 10016-5997, USA

Copyright © 2025 by The Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 20 May 2025. Printed in the United States of America.

IEEE is a registered trademark in the U.S. Patent & Trademark Office, owned by The Institute of Electrical and Electronics Engineers, Incorporated.

PDF: ISBN 979-8-8557-1671-9 STD27615
Print: ISBN 979-8-8557-1672-6 STDPD27615

IEEE prohibits discrimination, harassment, and bullying.

For more information, visit <https://www.ieee.org/about/corporate/governance/p9-26.html>.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher.

Important Notices and Disclaimers Concerning IEEE Standards Documents

IEEE Standards documents are made available for use subject to important notices and legal disclaimers. These notices and disclaimers, or a reference to this page (<https://standards.ieee.org/ipr/disclaimers.html>), appear in all IEEE standards and may be found under the heading “Important Notices and Disclaimers Concerning IEEE Standards Documents.”

Notice and Disclaimer of Liability Concerning the Use of IEEE Standards Documents

IEEE Standards documents are developed within IEEE Societies and subcommittees of IEEE Standards Association (IEEE SA) Board of Governors. IEEE develops its standards through an accredited consensus development process, which brings together volunteers representing varied viewpoints and interests to achieve the final product. IEEE standards are documents developed by volunteers with scientific, academic, and industry-based expertise in technical working groups. Volunteers involved in technical working groups are not necessarily members of IEEE or IEEE SA and participate without compensation from IEEE. While IEEE administers the process and establishes rules to promote fairness in the consensus development process, IEEE does not independently evaluate, test, or verify the accuracy of any of the information or the soundness of any judgments contained in its standards.

IEEE makes no warranties or representations concerning its standards, and expressly disclaims all warranties, express or implied, concerning all standards, including but not limited to the warranties of merchantability, fitness for a particular purpose and non-infringement. IEEE Standards documents do not guarantee safety, security, health, or environmental protection, or compliance with law, or guarantee against interference with or from other devices or networks. In addition, IEEE does not warrant or represent that the use of the material contained in its standards is free from patent infringement. IEEE Standards documents are supplied “AS IS” and “WITH ALL FAULTS.”

Use of an IEEE standard is wholly voluntary. The existence of an IEEE standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard.

In publishing and making its standards available, IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity, nor is IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing any IEEE Standards document should rely upon their own independent judgment in the exercise of reasonable care in any given circumstances or, as appropriate, seek the advice of a competent professional in determining the appropriateness of a given IEEE standard.

IN NO EVENT SHALL IEEE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: THE NEED TO PROCURE SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE PUBLICATION, USE OF, OR RELIANCE UPON ANY STANDARD, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

Translations

The IEEE consensus balloting process involves the review of documents in English only. In the event that an IEEE standard is translated, only the English language version published by IEEE is the approved IEEE standard.

Use by artificial intelligence systems

In no event shall material in any IEEE Standards documents be used for the purpose of creating, training, enhancing, developing, maintaining, or contributing to any artificial intelligence systems without the express, written consent of IEEE SA in advance. “Artificial intelligence” refers to any software, application, or other system that uses artificial intelligence, machine learning, or similar technologies, to analyze, train, process, or generate content. Requests for consent can be submitted using the Contact Us form.

Official statements

A statement, written or oral, that is not processed in accordance with the IEEE SA Standards Board Operations Manual is not, and shall not be considered or inferred to be, the official position of IEEE or any of its committees and shall not be considered to be, or be relied upon as, a formal position of IEEE or IEEE SA. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that the presenter’s views should be considered the personal views of that individual rather than the formal position of IEEE, IEEE SA, the Standards Committee, or the Working Group. Statements made by volunteers may not represent the formal position of their employer(s) or affiliation(s). News releases about IEEE standards issued by entities other than IEEE SA should be considered the view of the entity issuing the release rather than the formal position of IEEE or IEEE SA.

Comments on standards

Comments for revision of IEEE Standards documents are welcome from any interested party, regardless of membership affiliation with IEEE or IEEE SA. However, **IEEE does not provide interpretations, consulting information, or advice pertaining to IEEE Standards documents.**

Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Since IEEE standards represent a consensus of concerned interests, it is important that any responses to comments and questions also receive the concurrence of a balance of interests. For this reason, IEEE and the members of its Societies and subcommittees of the IEEE SA Board of Governors are not able to provide an instant response to comments or questions, except in those cases where the matter has previously been addressed. For the same reason, IEEE does not respond to interpretation requests. Any person who would like to participate in evaluating comments or revisions to an IEEE standard is welcome to join the relevant IEEE SA working group. You can indicate interest in a working group using the Interests tab in the Manage Profile & Interests area of the [IEEE SA myProject system](#).¹ An IEEE Account is needed to access the application.

Comments on standards should be submitted using the [Contact Us](#) form.²

Laws and regulations

Users of IEEE Standards documents should consult all applicable laws and regulations. Compliance with the provisions of any IEEE Standards document does not constitute compliance to any applicable

¹ Available at: <https://development.standards.ieee.org/myproject-web/public/view.html#landing>.

² Available at: <https://standards.ieee.org/about/contact/>.

regulatory requirements. Implementers of the standard are responsible for observing or referring to the applicable regulatory requirements. IEEE does not, by the publication of its standards, intend to urge action that is not in compliance with applicable laws, and these documents may not be construed as doing so.

Data privacy

Users of IEEE Standards documents should evaluate the standards for considerations of data privacy and data ownership in the context of assessing and using the standards in compliance with applicable laws and regulations.

Copyrights

IEEE draft and approved standards are copyrighted by IEEE under U.S. and international copyright laws. They are made available by IEEE and are adopted for a wide variety of both public and private uses. These include both use by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of engineering practices and methods. By making these documents available for use and adoption by public authorities and private users, neither IEEE nor its licensors waive any rights in copyright to the documents.

Photocopies

Subject to payment of the appropriate licensing fees, IEEE will grant users a limited, non-exclusive license to photocopy portions of any individual standard for company or organizational internal use or individual, non-commercial use only. To arrange for payment of licensing fees, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; +1 978 750 8400; <https://www.copyright.com/>. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

Updating of IEEE Standards documents

Users of IEEE Standards documents should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of amendments, corrigenda, or errata. An official IEEE document at any point in time consists of the current edition of the document together with any amendments, corrigenda, or errata then in effect.

Every IEEE standard is subjected to review at least every 10 years. When a document is more than 10 years old and has not undergone a revision process, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE standard.

In order to determine whether a given document is the current edition and whether it has been amended through the issuance of amendments, corrigenda, or errata, visit [IEEE Xplore](#) or [contact IEEE](#).³ For more information about the IEEE SA or IEEE's standards development process, visit the IEEE SA Website.

Errata

Errata, if any, for all IEEE standards can be accessed on the [IEEE SA Website](#).⁴ Search for standard number and year of approval to access the web page of the published standard. Errata links are located

³ Available at: <https://ieeexplore.ieee.org/browse/standards/collection/ieee>.

⁴ Available at: <https://standards.ieee.org/standard/index.html>.

under the Additional Resources Details section. Errata are also available in [IEEE Xplore](#). Users are encouraged to periodically check for errata.

Patents

IEEE standards are developed in compliance with the [IEEE SA Patent Policy](#).⁵

Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken by the IEEE with respect to the existence or validity of any patent rights in connection therewith. If a patent holder or patent applicant has filed a statement of assurance via an Accepted Letter of Assurance, then the statement is listed on the IEEE SA Website at <https://standards.ieee.org/about/sasb/patcom/patents.html>. Letters of Assurance may indicate whether the Submitter is willing or unwilling to grant licenses under patent rights without compensation or under reasonable rates, with reasonable terms and conditions that are demonstrably free of any unfair discrimination to applicants desiring to obtain such licenses.

Essential Patent Claims may exist for which a Letter of Assurance has not been received. The IEEE is not responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patents Claims, or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of this standard are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from the IEEE Standards Association.

IMPORTANT NOTICE

Technologies, application of technologies, and recommended procedures in various industries evolve over time. The IEEE standards development process allows participants to review developments in industries, technologies, and practices, and to determine what, if any, updates should be made to the IEEE standard. During this evolution, the technologies and recommendations in IEEE standards may be implemented in ways not foreseen during the standard's development. IEEE standards development activities consider research and information presented to the standards development group in developing any safety recommendations. Other information about safety practices, changes in technology or technology implementation, or impact by peripheral systems also may be pertinent to safety considerations during implementation of the standard. Implementers and users of IEEE Standards documents are responsible for determining and complying with all appropriate safety, security, environmental, health, data privacy, and interference protection practices and all applicable laws and regulations.

⁵ Available at: <https://standards.ieee.org/about/sasb/patcom/materials.html>.

Participants

At the time this IEEE guide was completed, the H22 Working Group had the following membership:

Amir Makki, *Chair*
Cesar Calix, *Vice Chair*
Hugo Monterrubio, *Secretary*

David Busot
Mario Capuozzo
T. W. Cease
Kevin Easley
Didier Giarratano
Shane Haveron

Dennis Holstein
Anthony Johnson
Caitlin Martin
John Miller
Scott Mix
Craig Preuss

Dan Reckerd
Sam Sciacca
Charles Sufana
Dustin Tessier
Eric Thibodeau
Steve Turner

The following members of the individual Standards Association balloting group voted on this guide. Balloters may have voted for approval, disapproval, or abstention.

Galina Antonova
David Beach
Martin Best
Steven Bezner
Thomas Blair
James Bougie
Jon Brasher
Gustavo Brunello
Paul Cardinal
Diego Chiozzi
Ernest Duckworth
Thomas Dunmore II
Donald Dunn
Kenneth Fodero
James Formea
Carl Fredericks
Jean-Sebastien Gagnon
Rafael Garcia
Shubhanker Garg
Jalal Gohari
Roman Graf
Randy Hamilton
Werner Hoelzl
Gary Hoffman

Ali Hooshyar
Richard Hunt
Richard Jackson
Anthony Johnson
Piotr Karocki
John Kay
Vinoth Kumar
Mikhail Lagoda
Chung-Yiu Lam
Theo Laughner
An Le
Ting Li
Martine-Denise Long
Don Lukach
Bruce Mackie
Jeffrey McElray
Scott Mix
Navid Bayat Mokhtari
Adi Mulawarman
Rajesh Murthy
Cesar Negri
Dennis Neitzel
Arthur Neubauer
Dean Ouellette

Lorraine Padden
Bansi Patel
Michael Pinkston
Jeffrey Pond
Benito Ramos
R. K. Rannow
Charles Rogers
Daniel Sabin
Bartien Sayogo
Thomas Schossig
Ryan Stone
Charles Sufana
David Tepen
Eric Thibodeau
Michael Thompson
Eric Udren
Matthew Vacha
John Vergis
Quintin Verzosa
Nathan Wallace
Karl Weber
Philip B. Winston
Murty V. V. Yalla
Karl Zimmerman

When the IEEE SA Standards Board approved this guide on 11 December 2024, it had the following membership:

David J. Law, *Chair*
Jon Walter Rosdahl, *Vice Chair*
Gary Hoffman, *Past Chair*
Alpesh Shah, *Secretary*

Sara R. Biyabani
Ted Burse
Stephen Dukes
Doug Edwards
J. Travis Griffith
Guido R. Hiertz
Ronald W. Hotchkiss

Hao Hu
Yousef Kimiagar
Joseph L. Koepfinger*
Howard Li
Xiaohui Liu
John Haiying Lu
Kevin W. Lu
Hiroshi Mano

Paul Nikolich
Robby Robson
Lei Wang
F. Keith Waters
Sha Wei
Philip B. Winston
Don Wright

*Member Emeritus

Introduction

This introduction is not part of IEEE Std C37.249-2024, IEEE Guide for Categorizing Security Needs for Protection-, Automation-, and Control-Related Data Files.

Years ago, cyber security was not a big concern for protection-, automation-, and control-related data files because they did not exist for systems that were mostly electromechanical. If they were microprocessor-based, then dial-up and internet technologies were young and restrictive with minimal risk. Today, after incredible advances in communication and embedded systems, these systems are computer-based and internet technologies are making their way into protection, automation, and control systems. Cyber security is now a big concern for the files associated with protection, automation, and control systems. The collective efforts so far have mainly focused on managing physical and electronic access to protection, automation, and control equipment (data in motion issues) but have not specifically addressed access security for protection-, automation-, and control-related data files (data at rest issues). Such files may contain critical information including passwords, phone numbers, internet protocol (IP) addresses, settings, load and fault records, and other information that an electric power utility may designate as critical to the operation of protection, automation, and control systems. The need to secure such files is clear and especially so because the files are transmitted between protection, automation, and control equipment (e.g., protection relays, remote terminal units (RTU), human-machine interfaces (HMIs), Supervisory Control and Data Acquisition (SCADA) master stations, laptops) and exchanged between humans for analysis and maintenance purposes, increasing the risk that these files, whose information content can vary in its criticality, could be exposed to unauthorized personnel and present an unacceptable risk to an electric power utility. This guide presents an approach for categorizing the security needs for protection-, automation-, and control-related files. The approach aligns with NIST SP 800-60, Vol. 1, Rev. 1 [B16] and with FIPS 199 [B1], the latter establishes security categories based on the magnitude of harm expected to result from compromises rather than on the results of an assessment that includes an attempt to determine the probability of compromise.

Contents

1. Overview	12
1.1 General	12
1.2 Scope	12
1.3 Purpose	12
1.4 Word usage	12
2. Normative references	13
3. Definitions, acronyms, and abbreviations	13
3.1 Definitions	13
3.2 Acronyms and abbreviations	18
4. Security categorization of protection-, automation-, and control-related data files	19
4.1 General	19
4.2 Security categories and objectives	20
4.3 Assessment of potential impact	20
5. Security categorization process	21
5.1 General	21
5.2 Step 1: Identify information types	21
5.3 Step 2: Select provisional impact levels	22
5.4 Step 3: Review provisional impact levels and adjust/finalize information type impact levels	25
5.5 Step 4: Assign security category	26
5.6 Step 5: Document the security categorization process	30
5.7 Step 6: Follow the EPU's process for reviewing the categorization	30
6. Protection-, automation-, and control-related information types	30
6.1 General	30
6.2 Address information type	30
6.3 Authentication credential information type	30
6.4 Enable/disable selection information type	31
6.5 Environmental rating information type	31
6.6 Firmware information type	31
6.7 Identification information type	31
6.8 Input information type	32
6.9 Installation information type	32
6.10 Interconnection information type	32
6.11 Layout information type	32
6.12 Location information type	32
6.13 Logic information type	33
6.14 Maintenance information type	33
6.15 Manufacturer information type	33
6.16 Measurement information type	33
6.17 Model number information type	34
6.18 Operation information type	34
6.19 Output information type	34
6.20 Logical port information type	34
6.21 Program information type	35
6.22 Protocol information type	35
6.23 Protection setting information type	35
6.24 Rating information type	35
6.25 Seasonal rating information type	36
6.26 Test parameter information type	36

6.27 Test result information type	36
6.28 Test setup information type	36
6.29 Threshold information type	36
6.30 Troubleshooting information type	37
6.31 User name information type	37
7. Example protection, automation, and control file evaluations.....	37
7.1 General	37
7.2 Drawings.....	38
7.3 Manuals	41
7.4 Transmission and distribution system operation procedures	42
7.5 Black start procedures.....	44
7.6 Post-disaster recovery procedures	45
7.7 Inventory and spare lists	46
7.8 Equipment ratings	49
7.9 Environmental ratings.....	50
7.10 Seasonal ratings	51
7.11 Settings	52
7.12 Measurements	54
7.13 Addressing	56
7.14 Access logs	57
7.15 Authentication credentials	58
7.16 Test report file type.....	59
7.17 Maintenance schedules	61
7.18 Programs	63
Annex A (informative) Bibliography	64

IEEE Guide for Categorizing Security Needs for Protection-, Automation-, and Control-Related Data Files

1. Overview

1.1 General

This guide identifies the various types of protection-, automation-, and control-related data files categorized based on the risk of disclosure or compromise to help guide both electric utilities and standards development bodies to enact appropriate security measures based on the categorization of each file type. Such enactment will help guide the proper balance between security and functionality as related to maintenance and analysis of protection and automation-related data files.

1.2 Scope

This guide identifies and categorizes commonly used protection-, automation-, and control-related data files based on content, use, and risk of disclosure or compromise. Protection-, automation-, and control-related data files include, but are not limited to, files used for configuration, management, and analysis of protection, automation, and control systems.

1.3 Purpose

This guide adds granularity to security practices to precisely categorize security needs without impeding the use or access to protection-, automation-, and control-related data files.

1.4 Word usage

The word *shall* indicates mandatory requirements strictly to be followed in order to conform to the standard and from which no deviation is permitted (*shall* equals *is required to*).^{6, 7}

The word *should* indicates that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others; or that a certain course of action is preferred but not necessarily required (*should* equals *is recommended that*).

⁶ The use of the word *must* is deprecated and cannot be used when stating mandatory requirements; *must* is used only to describe unavoidable situations.

⁷ The use of *will* is deprecated and cannot be used when stating mandatory requirements; *will* is only used in statements of fact.

The word *may* is used to indicate a course of action permissible within the limits of the standard (*may* equals *is permitted to*).

The word *can* is used for statements of possibility and capability, whether material, physical, or causal (*can* equals *is able to*).

2. Normative references

There are no normative references in this guide.

3. Definitions, acronyms, and abbreviations

3.1 Definitions

For the purposes of this document, the following terms and definitions apply. The *IEEE Standards Dictionary Online* should be consulted for terms not defined in this clause.⁸

availability, loss of: The disruption of access to, or use of, the information. (This definition is derived from NIST SP 800-60, Vol. 1, Rev. 1 [B16].)

availability: A property that information is where the user needs it, when the user needs it, and how the user needs it. (This definition is derived from NIST IR 7628 [B14].)

black start procedures: Written procedures that provide the process of restoring an electric power generation plant or any part of an electric transmission or distribution grid to operation without relying on an external source of power. Normally, the station generators provide electric power used within the plant. If all the main generators are offline, then the high-voltage grid provides station service power through the transmission lines. This off-site power source is not available during a wide-area outage. Therefore, a black start is required in the absence of grid power. Generating plants using steam turbines (e.g., fossil fuel and nuclear) require station service power up to 10% of their total capacity. For example, bring on-line boiler feed water pumps, boiler forced draft combustion air blowers, and fuel preparation. It is uneconomical to provide such a large standby capacity at each station, so black start power is only provided over the electrical transmission network at specific power stations. Hydroelectric power plants are often the black start sources since these stations need very little initial power to start and can put a large block of power online very quickly to then start up large steam turbines at fossil-fueled and nuclear stations. These procedures may identify the characteristics of a black start resource such as its name, type of unit, location, and capacity (in megawatt and megavar).

business areas: Separation of electric power utility (EPU) operations into high-level categories relating to the purpose of the EPU, the mechanisms the EPU uses to achieve its purposes, the support functions necessary to conduct EPU operations, and resource management functions that support all areas of the EPU's business. *Business areas* are subdivided into *areas of operation* or *lines of business*. (This definition is derived from NIST SP 800-60, Vol. 1, Rev. 1 [B16].)

communication diagram: Also known as a *telecommunications diagram*, *integration one-line diagram*, *block diagram*, and *local area network (LAN) architecture diagram*. These diagrams typically show detailed operating requirements for the telecommunication technology in use, i.e., power line carrier, optical fiber cable, telephone, microwave, etc. Other communication diagrams typically show the interconnection of components and how they communicate with each other, sometimes without regard to the physical locations of the components. Details typically include specific port numbers of devices to which connections are made. (This definition is derived from IEEE PES-TR47 [B4].)

⁸ *IEEE Standards Dictionary Online* is available at: <http://dictionary.ieee.org>. An IEEE Account is required for access to the dictionary, and one can be created at no charge on the dictionary sign-in page.

confidentiality, loss of: The unauthorized disclosure of information. (This definition is derived from NIST SP 800-60, Vol. 1, Rev. 1 [B16].)

confidentiality: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes. (This definition is derived from NIST IR 7628 [B13].)

drawings; ac schematic: Drawings that typically show detailed schematic connections between the instrument transformers and the protection, automation, and control system components using a single line for each phase. Also known as an *ac three-line diagram*, *three-line connection diagram*, *current and potential diagrams*, and *elementary wiring diagrams*. (This definition is derived from IEEE PES-TR47 [B4].)

drawings; dc schematic: Drawings that typically show the interconnection of components and how the components function in the control circuit without regard to the physical locations of the components. Also known as *elementary wiring diagrams*. (This definition is derived from IEEE PES-TR47 [B4].)

equipment arrangement drawings: Drawings for equipment (e.g., for transformers, circuit breakers, bus structures, generating station equipment, reclosers, switches) that typically show how a specific piece of equipment is arranged for installation, including dimensions, views (e.g., top view, [which is like a plot plan], side views), and interfaces between discrete components of the equipment being shown.

high impact (H): Severe or catastrophic effect on primary functionality, asset damage, financial loss, or harm to the public or electric power utility (EPU) personnel (life-threatening or severe injuries).

high-water mark: This concept determines that the security impact level for a file will generally be the highest impact level for the security objectives (confidentiality, integrity, and availability) associated with the aggregate of system information types.

information: An instance of an information type, such as a file that is stored.

information type: A specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by specific regulation (e.g., local, state, regional, or national legislative bodies) by an electric power utility (EPU) through an EPU executive order, directive, policy, or regulation. (Refer to NIST SP 800-60, Vol. 1, Rev. 1 [B16].)

information type, address: Describes a unique identifier of a device in the use of a protocol (e.g., internet protocol [IP] address) as deployed by the electric power utility (EPU).

information type, authentication credential: Describes the factor(s) used to ascertain the identity of a user or system. In multi-factor authentication, two or more factors are used to authenticate the user/system, e.g., something possessed or known by the user/system (e.g., a passphrase or password), something the user/system has (e.g., a token), or something that the user/system is (e.g., biometrics such as a fingerprint). These factors are called *credentials*.

information type, enable/disable selection: Describes whether a configuration setting is set to disable or enable (e.g., reclosing can be selected as enable or disable).

information type, environmental rating: Describes information on how equipment is rated to withstand certain adverse environmental conditions, such as moisture and temperature; describe how the equipment impacts the environment, such as drainage, noise, road traffic, site disturbance, historical impact, shoreline impact, flood zone impact, wetland impact, zoning, lighting, etc.

information type, firmware: Describes the version of firmware running in equipment or a device. Refer to IEEE Std C37.233™ [B8] for a discussion of the characterization of firmware. The firmware is a string of characters that is typically an alpha-numeric designation assigned by the manufacturer.

information type, identification: Describes how a piece of equipment, component, device, etc. is identified (typically in a unique manner across a location or system) so it can be installed, operated, maintained, and removed. May also be called a name, tag, or label.

information type, input: Typically contained within a configuration file that designates an input to a device, e.g., digital input, ac input, mA input, etc. Other characteristics of the input may also be included in this information type, such as the input's description.

information type, installation: Describes how to install a piece of equipment, component, device, etc. so that it may be operated and maintained per the manufacturer's requirements.

information type, interconnection: Describes how different components, equipment, devices, etc. are connected together into an interconnected system of power, communication, etc.

information type, layout: Describes the spatial relationship between different pieces of equipment, component, device, etc. so that they may be installed, operated, maintained, and removed.

information type, location: Describes via graphical plot plan or text the geospatial relationship between major facilities that may or may not include a mailing address or other means to find the location using a map or geo-positioning services (e.g., longitude and latitude).

information type, logic: Describes in a non-spatial, abstract diagram or equation. This may include a schematic drawing of the logical relationships of different kinds of operations (e.g., and gates, or gates, mathematical operations). It may also include graphical representation of formal logic that can also be shown in an equation. It may show a flow chart of hardware circuits or program logic.

information type, maintenance: Describes how to maintain a piece of equipment, component, device, etc. so that it may be maintained per the manufacturer's requirements so that it successfully performs its intended use.

information type, manufacturer: Describes who or what entity manufactured a device, piece of equipment, or other component.

information type, measurement: May include event data (fault, disturbance, sequence of events, etc.) and load records (peaks, forecasting, planning, etc.) that are invaluable in analyzing electrical system problems, system operations, and planning for future enhancements to the system.

information type, mission-based: Information types specific to individual departments and agencies or to specific sets of departments and agencies. This definition is derived from NIST SP 800-60, Vol. 1, Rev. 1 [B16].

information type, model number: Describes a manufacturer's model number for a piece of equipment, component, device, etc.

information type, operation: Describes how to operate a piece of equipment, component, device, etc. so that it may be operated per the manufacturer's requirements.

information type, output: Typically contained within a configuration file that designates an output from a device, e.g., digital output, ac output, mA output, etc. Other characteristics of the output may also be included in this information type, such as the output's description.

information type, port: Describes a physical or logical communication port, its connector type, speed of the connection, etc. and typically identifies a unique label or number unique to a piece of equipment, component, device, etc.

information type, program: Describes the installation files used to install the program onto a computer, equipment, device, or system; programs used to create configuration or setting files for equipment or devices; diagnostic tools used to monitor and troubleshoot equipment or devices; intelligent electronic device (IED) executable firmware that is directly loaded onto equipment or device, which is different than the firmware information type.

information type, protocol: Describes a communication protocol in use, such as Modbus, DNP3 (IEEE Std 1815™ [B6], IEC 61850 [B3]) such as Generic Object Oriented System Event (GOOSE) and Manufacturing Message Specification (MMS) and Sampled Values, Simple Network Management Protocol (SNMP), Secure Hyper Text Transfer Protocol (HTTPS), etc.

information type, protection setting: Describes information on how a protection function, such as those defined in IEEE Std C37.2™ [B7], are defined in the device to accomplish the protection function. This information type may summarize multiple protection functions found in IEEE Std C37.2.

information type, rating: Describes information on how equipment is rated under various conditions, e.g., normal operation, emergency operation, etc. Also refer to more specific rating information types, such as environmental rating information type.

information type, seasonal rating: Describes operating characteristic of a piece of equipment based upon changes in the weather (e.g., temperature, humidity, etc.) based upon season or seasons. Multiple seasonal ratings may be summarized in one seasonal rating information type, e.g., winter seasonal ratings and summer seasonal ratings described as a singular seasonal rating information type.

information type, test parameter: Describes information on how a particular function of a piece of equipment (e.g., a protection relay) is tested, typically a value or magnitude of a quantity (e.g., volts, amps) at some duration.

information type, test result: Describes how a particular function of a piece of equipment (e.g., a protection relay) was tested and whether the test was successful or not. Other information may be included, such as the reason(s) for test failure and actions taken as a result of that failure.

information type, test setup: Describes how a particular function of a piece of equipment (e.g., a protection relay) will be tested.

information type, threshold: Describes a configuration setting that triggers a specified operation when a condition operates at, above, or below the specified value.

information type, troubleshooting: Describes how to troubleshoot a piece of equipment, component, device, etc. so that it may be operated and maintained per the manufacturer's requirements.

information type, user name: Describes the defined names of users with access to a device, file, system, etc. The user name information type may be general (e.g., "admin", "administrator", "operations", etc.), specific to a user's given name, derived from a user's given name, an assigned alphanumeric character string, etc. User names, within a domain (A distinct subset of the internet with addresses sharing a common suffix) may be group-based (e.g. a group of users make use of the same user name) or individual-based. May also be called an account name, User ID, etc.

integrity: A property whereby data has not been altered in an unauthorized manner since it was created, transmitted or stored. (This definition is derived from NIST IR 7628 [B14].)

intended use: The use of a device, over its full range of functions (such as those defined in IEEE C37.2), in accordance with the instructions provided by the manufacturer, including instructions on operating position and orientation.

interconnection wiring diagrams: Diagrams that typically show the wiring connections between control panels provided by one manufacturer and other panels or equipment provided by another manufacturer. (This definition is derived from IEEE PES-TR47 [B4].)

lines of business: Describes the Electric Power Utility's (EPU's) purpose in functional terms or describe the support functions that the EPU conducts in order to effectively deliver its services. "Lines of business" relating to the EPU's purpose and the mechanisms the government uses to achieve its purposes tend to be mission-based. "Lines of business" relating to support functions and resource management functions that are necessary to conduct EPU operations tend to be common to most EPUs. (This definition is derived from NIST SP 800-60, Vol. 1, Rev. 1 [B16].)

logic diagrams: Drawings that typically show the control logic programmed into protection, automation and control devices using logic symbols (e.g., AND gates, OR gates) to show the Boolean logic being performed. These diagrams typically show in a graphical way how inputs are processed (e.g., delay timers and level comparisons) to generate outputs. Logical outputs may be combined with the status of other logic for further processing, get communicated to other devices over communication circuits, or assert physical output contacts that cause some action in the control circuit. (This definition is derived from IEEE PES-TR47 [B4].)

low impact (L): Noticeable loss of functionality, minor asset damage, financial loss, or harm to the public or EPU personnel.

moderate impact (M): Significant degradation of primary functionality, asset damage, financial loss, or harm to individuals (non-life threatening).

panel layout diagrams: Drawings that typically show the physical locations of components on one or more panels, usually to scale, where all items are uniquely identified so that each device can be found in the schematics and for the purpose of fabrication. Also known as panel arrangement diagrams, front views, and electrical arrangement diagrams. (This definition is derived from IEEE PES-TR47 [B4].)

personally identifiable information (PII): Any information about an individual maintained by someone else, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. (This definition is derived from NIST SP 800-122 [B18].)

provisional security impact level: The initial or conditional impact determinations made until all considerations are fully reviewed, analyzed, and accepted in the subsequent categorization steps by appropriate officials of the electric power utility. (This definition is derived from NIST SP 800-60, Vol. 1, Rev. 1 [B16].)

post-disaster recovery procedures: Procedures that describe philosophies and procedures used to implement system restoration of natural or other disasters.

remedial action scheme (RAS): A protection relay scheme designed to detect predefined abnormal system conditions and initiate automatic corrective action that will result in acceptable system performance. They are designed to be highly reliable relaying schemes. They are used to help maintain system stability, acceptable voltages and equipment loading, often by initiating one or more of the following actions: reducing generation, modifying system configurations, and or inserting equipment that serves to correct an unacceptable system condition. For example, they are often used to allow generators to operate at full output even under single contingency outages that would otherwise result in curtailment of generation in preparation of the next contingency event. Also known as special protection scheme (SPS) and system integrity protection scheme (SIPS). Under-voltage and under-frequency load shedding (and out of step) schemes are not included in the Glossary of Terms used in NERC Reliability Standards definition of an SPS. (Refer to NERC, Glossary [B12], and IEEE PSRC [B5].)

security category: The characterization of information based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information would have on an electric power utility. (This definition is derived from NIST SP 800-60, Vol. 1, Rev. 1 [B16].)

security objective: Confidentiality, integrity, and availability, with no implied order of importance. (This definition is derived from NIST SP 800-60, Vol. 1, Rev. 1 [B16].)

single-line diagram: Shows a simplified schematic of the overall protection, automation and control schemes with connections and interactions between power system apparatus and protection, automation and control system components using a single line for all three phases. Also known as meter and relay single-line or one-line diagram. (This definition is derived from IEEE PES-TR47 [B4].)

sub-function: The basic operations employed by an Electric Power Utility (EPU) to provide the system services within each area of operations or line of business in the EPU.

System Configuration Language (SCL): IEC 61850 [B3] standard for substation automation specifies a standardized Substation Configuration Language (SCL) to transfer device descriptions and communication parameters among different vendors/manufacturers.

transmission and distribution system operation procedures: Procedures that typically contain critical procedures for grid operation (e.g., tagging, switching, and clearance procedures). These procedures may also include work practices that support compliance with safety regulations, define boundaries between systems (transmission and distribution), classify worker qualifications, etc. In many cases these procedures are restricted to inside of the utility operating environments.

wiring diagrams: Drawings that typically show the point-to-point, detailed connections between terminal blocks located on the panels and protection, automation and control devices as shown on associated schematic drawings. Wiring diagrams match the layout of the components on the panel as if looking at the panel from the side where the wiring takes place (e.g., back view if wired from the back). Also known as panel wiring diagrams and control wiring diagrams. (This definition is derived from IEEE PES-TR47 [B4].)

3.2 Acronyms and abbreviations

A	availability (refer to 3.1)
C	confidentiality (refer to 3.1)
CIP	critical infrastructure protection
DNP3	distributed network protocol
EPU	electric power utility
FIPS	Federal Information Processing Standards
FTP	file transfer protocol
GOOSE	Generic Object Oriented System Event
HTTP	Hyper Text Transfer Protocol
HTTPS	Secure Hyper Text Transfer Protocol
GSU	generator step-up

H	high impact (refer to 3.1)
HMI	human-machine interface
I	integrity (refer to 3.1)
IP	internet protocol
IED	intelligent electronic device
L	low impact (refer to 3.1)
OLTC	on-load tap changer
M	moderate impact (refer to 3.1)
MSDS	Material safety data sheet
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
PII	personally identifiable information
RTU	remote terminal unit
SC	security category
SCADA	Supervisory Control and Data Acquisition
SCL	System Configuration description Language
SF ₆	sulfur-hexafluoride
SNMP	Simple Network Management Protocol
SP	Special Publication
XML	Extensible Markup Language File
MMS	Manufacturing Message Specification

4. Security categorization of protection-, automation-, and control-related data files

4.1 General

This guide provides electric power utilities (EPUs) claiming conformance or compliance with this guide a process that includes:

- a) Definitions of the security categories⁹ and security objectives (4.2).

⁹ FIPS 199 establishes security categories based on the expected magnitude of harm to result from compromise rather than on the assessment result that includes an attempt to determine the probability of compromise.