IEEE SA
STANDARDS ASSOCIATION

STANDARDS

IEEE Standard for Intelligent Electronic Devices Cybersecurity Capabilities

IEEE Power and Energy Society

Developed by the
Power System Communications and Cybersecurity Committee

IEEE Std 1686™-2022
(Revision of IEEE Std 1686-2013)

IEEE

IEEE Std 1686™-2022
(Revision of IEEE Std 1686-2013)

IEEE Standard for Intelligent Electronic Devices Cybersecurity Capabilities

Developed by the

Power System Communications and Cybersecurity Committee
of the
IEEE Power and Energy Society

Approved 8 November 2022

IEEE SA Standards Board

Abstract: The functions and features to be provided in intelligent electronic devices (IEDs) to accommodate cybersecurity programs are defined in this standard. Security regarding access, operation, configuration, firmware revision, and data retrieval from an IED are addressed. Confidentiality, integrity, and availability of external interfaces of the IED are also addressed.

Keywords: CIP, critical infrastructure protection, cyber, IED, IEEE 1686™, intelligent electronic device, security, substation

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

PDF: ISBN 978-1-5044-9374-1 STD25909
Print: ISBN 978-1-5044-9375-8 STDPD25909

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 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 the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE SA) Standards Board. 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 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 this standard, including but not limited to the warranties of merchantability, fitness for a particular purpose and non-infringement. 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 his or her 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 development process involves the review of documents in English only. In the event that an IEEE standard is translated, only the English version published by IEEE is the approved IEEE standard.

Official statements

A statement, written or oral, that is not processed in accordance with the IEEE SA Standards Board Operations Manual 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, nor be relied upon as, a formal position of IEEE. 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.

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 Standards Coordinating Committees 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 in revisions to an IEEE standard is welcome to join the relevant IEEE 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 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.

[1] Available at: https://development.standards.ieee.org/myproject-web/public/view.html#landing.
[2] Available at: https://standards.ieee.org/content/ieee-standards/en/about/contact/index.html.

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 US 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, IEEE does not 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 under the Additional Resources Details section. Errata are also available in IEEE Xplore. Users are encouraged to periodically check for errata.

[3] Available at: https://ieeexplore.ieee.org/browse/standards/collection/ieee.
[4] Available at: https://standards.ieee.org/standard/index.html.

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

IEEE Standards do not guarantee or ensure safety, security, health, or environmental protection, or ensure against interference with or from other devices or networks. 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, 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 standard was completed, the PSCC S1 Working Group had the following membership:

Marc Lacroix, *Chair*
Éric Thibodeau, *Vice Chair*

Jay Anderson
Arijit Kumar Bose
Mike Dood
Herb Falk
James Formea
Steffen Fries
Didier Giarratano
Shane Haveron
Dennis Holstein
Mario Jardim
Anthony Johnson
Steven Kunsman
Jason Lombardo
Johan Malmstrom
Steve Mark
Aaron Martin
Ryan Newell
Craig Preuss
Harsh Vardhan
Nathan Wallace

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

Jay Anderson
Michael Basler
Navid Bayat Mokhtari
Philip E. Beecher
Steven Bezner
Jens Boemer
James Bougie
Jon Brasher
Gustavo Brunello
Paul Cardinal
Sean Carr
Suresh Channarasappa
Diego Chiozzi
Frances Cleveland
Mario Roberto da Silva Jardim
Ryan Davidson
Mamadou Diong
Michael Dood
Kenneth Fodero
James Formea
Carl Fredericks
Fredric Friend
Jean-Sebastien Gagnon
Shubhanker Garg
George Gela
Didier Giarratano
Jalal Gohari
Roman Graf
Randy Hamilton
Werner Hoelzl
Gary Hoffman
Ali Hooshyar
Yi Hu
Richard Hunt
C. Huntley
Dmitry Ishchenko
Richard Jackson
Anthony Johnson
Piotr Karocki
John Kay
Marc Lacroix
Chung-Yiu Lam
Ronald Landheer-Cieslak
Ting Li
Bruce Mackie
Jeffrey McElray
Scott Mix
Sepehr Mogharei
Adi Mulawarman
Jerry Murphy
Rajesh Murthy
Bruce Muschlitz
Gayle Nelms
Arthur Neubauer
Joe Nims
Sivaraman P
Lorraine Padden
Craig Palmer
Bansi Patel
Howard Penrose
Jeffrey Pond
Benito Ramos
Charles Rogers
Thomas Rudolph
Daniel Sabin
Bartien Sayogo
Thomas Schossig
Wayne Stec
Eugene Stoudenmire
Walter Struppler
Charles Sufana
David Tepen
Michael Thesing
Eric Thibodeau
Michael Thompson
Matthew Vacha
James Van De Ligt
Benton Vandiver
Harsh Vardhan
John Vergis
Quintin Verzosa
Nathan Wallace
Keith Waters
Karl Weber
Donald Wengerter
Kenneth White
Jeffrey Wischkaemper
Murty V. V. Yalla
Xiaokang Yin
Francisc Zavoda

When the IEEE SA Standards Board approved this standard on 8 November 2022, it had the following membership:

David J. Law, *Chair*
Ted Burse, *Vice Chair*
Gary Hoffman, *Past Chair*
Konstantinos Karachalios, *Secretary*

Edward A. Addy
Ramy Ahmed Fathy
J. Travis Griffith
Guido R. Hiertz
Yousef Kimiagar
Joseph L. Koepfinger*
Thomas Koshy
John D. Kulick
Johnny Daozhuang Lin
Kevin Lu
Daleep C. Mohla
Andrew Myles
Damir Novosel
Annette D. Reilly
Robby Robson
Jon Walter Rosdahl
Mark Siira
Dorothy V. Stanley
Lei Wang
F. Keith Waters
Karl Weber
Sha Wei
Philip B. Winston
Daidi Zhong

*Member Emeritus

Introduction

This introduction is not part of IEEE Std 1686-2022, IEEE Standard for Intelligent Electronic Devices Cybersecurity Capabilities.

Cybersecurity programs developed by utilities are highly dependent on the functionality and capabilities of intelligent electronic devices (IEDs) regarding cybersecurity. This standard provides utilities that develop such programs the ability and help to procure, install, and commission IEDs that do not compromise their programs. This standard also provides the required suite of functions and capabilities to the various manufacturers that will be required to incorporate these features in their product line for customers that cite this standard.

Since the publication of the first IEEE Std 1686 edition, protection, automation, and control systems became more complex. In some cases, IEDs are increasingly relying on local area networks (LANs) or wide area networks (WANs). Consequently, these large systems became more exposed to cyber threats and new cybersecurity measures had to be adopted. At the same time, cybersecurity technologies were improved to allow a better robustness against attacks and improve management of large systems.

This revision of IEEE Std 1686 introduces new requirements for cybersecurity management. In addition, Clause 5 has been restructured to harmonize with the NIST Cybersecurity Framework and the requirements are now grouped into the following six themes:

— Identification and authentication

— Authorization and access

— Data integrity

— Data confidentiality

— Response to security events

— Resiliency

Table 1 shows the equivalence between IEEE Std 1686-2013 requirements and those in the present edition.

Table 1—IEEE Std 1686-2013 equivalence

IEEE Std 1686-2013 subclause number	IEEE Std 1686-2013 subclause title	Comment
5.1	Electronic access control	
5.1.2	Password defeat mechanisms	Now in 5.1.2.4
5.1.3	Number of individual users	Now in 5.1.2.5
5.1.4	Password construction	Now in 5.1.2.2
5.1.5	IED access control	Now in 5.2
5.1.5.1	Authorization levels by password	Now in 5.2.2
5.1.5.2	Authorization using role-based access control (RBAC)	Now in 5.2.2
5.1.6	IED main security functions	Now in 5.2.3
5.1.7	Password display	Now in 5.1.2.2
5.1.8	Access timeout	Now in 5.1.2.3
5.2	Audit trail	Renamed IED response to cybersecurity events (5.5)
5.2.2	Storage capability	Now in 5.5.2
5.2.3	Storage record	Now in 5.5.2
5.2.4	Audit trail event types	Now in 5.5.3
5.3	Supervisory monitoring and control	The requirements for alarms and events recording and reporting are now in 5.5
5.3.2	Events	Now in 5.5.3.1
5.3.3	Alarms	Now in 5.5.3.2
5.3.4	Alarm point change detect	Now in 5.5, which describes reporting to SCADA or other security management systems.
5.3.5	Event and alarm grouping	Since this standard supports different reporting mechanisms, this requirement is not included in this edition. Grouping function is performed by the chosen reporting protocol.
5.3.6	Supervisory permissive control	This requirement is not included in this edition. The proposed approach in this subclause is not secure by today's standard.
5.4	IED cybersecurity features	Now in 5.3 and 5.4
5.4.1	IED functionality compromise	Now in 5.6
5.4.2	Specific cryptographic features	Now in 5.3 and 5.4
5.4.3	Cryptographic techniques	Now in 5.3 and 5.4
5.4.4	Encrypting serial communications	Now in 5.4.2
5.4.5	Protocol-specific security features	Now in 5.6
5.5	IED configuration software	Now in 5.1, 5.2, 5.3, and 5.4
5.5.1	Authentication	Now in 5.1, 5.2, 5.3, and 5.4
5.5.2	Digital signature	Now in 5.1, 5.2, 5.3, and 5.4
5.5.3	ID/password control	Now in 5.1
5.5.4	ID/password-controlled features	Now in 5.1
5.5.4.1	View configuration data	Now in 5.4
5.5.4.2	Change configuration data	Now in 5.4
5.6	Communications port access	Now in 5.6.2
5.7	Firmware quality control	Now in 5.7

In this revision of the standard, the word *conformance* replaces *compliance*. *Conformance* is the fact of following rules or standards (per the *Oxford English Dictionary*). *Compliance* applies to law and regulation.

Annex B presents the IED's capabilities for certificate management. At the time of P1686 draft preparation, the working group felt it was too early to make these capabilities mandatory and that we need to gain more experience on this topic. It is expected that they will become mandatory in the next revision.

This revision of IEEE Std 1686 also introduces Annex C, which describes IED lifecycles. While this annex is informative, it gives the reader some insight on cybersecurity requirements to fully support cybersecurity measures during the entire life of the IED.

Contents

IEEE Standard for Intelligent Electronic Devices Cybersecurity Capabilities

1. Overview

1.1 Scope

The standard defines the functions and features to be provided in IEDs to accommodate cybersecurity programs. The standard addresses security regarding the access, operation, configuration, firmware revision, and data retrieval from an IED. Confidentiality, integrity, and availability of external interfaces of the IED are also addressed.

1.2 Purpose

The standard defines the functions and features to be provided in IEDs to support cybersecurity programs. Specifically, the standard states what safeguards, audit mechanisms, and alarm indications shall be provided by the vendor of the IED regarding the capabilities associated with access, operation, configuration, firmware revision, and data retrieval from an IED. The standard also allows the user to define a security program around these features tailored to the specific requirements of that security program; if an IED does not meet this standard, whether the requirements are tailored or not, this can identify the need for other defensive measures (technical and/or procedural) to be taken. This standard also defines explicit measures to help ensure authenticity, integrity, and confidentiality of data at rest and in transit.

1.3 Reason

Cybersecurity is one of the major concerns for the industry and utilities have to implement a security program to protect digital assets, including protection and control systems, that follows appropriate best practices from the information technology (IT) industry, such as NIST SP 800-53 [B10],[6] and additional industrial control system cybersecurity standards such as NIST 800-82 [B13] and the IEC 62443 suite of standards. The IEC 62351 suite of standards also defines the cybersecurity requirements for implementing security technologies in the power system operational environment. The rationale is to protect the bulk power delivery system from compromise and guard utilities against reputational damage, loss of revenue, and potential litigation caused by customer interruption from security breaches. The industry must also follow the rules prescribed by reliability organizations such as North American Electric Reliability

[6] Numbers in brackets refer to bibliographic references in Annex D.

Corporation (NERC) in North America or Directive on security of network and information systems (the NIS directives) adopted by the European Union. These organizations define a series of cybersecurity standards for critical infrastructure protection (CIP) which, depending on the CIP program at a utility, may drive requirements for cybersecurity features in some IEDs. Stakeholders that might be interested in this standard are as follows:

- Utilities/users who can specify that IEDs meet this standard to be consistent with their cybersecurity programs.
- Vendors/system integrators who will have a clear understanding of the functions and features that must be present in their product offerings.
- Regulatory agencies and governments who have a vested interest in critical infrastructure protection program effectiveness.
- Conformity assessment bodies and test labs.

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*).[7, 8]

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*).

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

The following referenced documents are indispensable for the application of this document (i.e., they must be understood and used, so each referenced document is cited in text and its relationship to this document is explained). For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments or corrigenda) applies.

IEEE Std C37.231™-2006, IEEE Recommended Practice for Microprocessor-Based Protection Equipment Firmware Control.[9, 10]

[7] The use of the word *must* is deprecated and cannot be used when stating mandatory requirements; *must* is used only to describe unavoidable situations.
[8] The use of *will* is deprecated and cannot be used when stating mandatory requirements; *will* is only used in statements of fact.
[9] The IEEE standards or products referred to in Clause 2 are trademarks of The Institute of Electrical and Electronics Engineers, Inc.
[10] IEEE publications are available from The Institute of Electrical and Electronics Engineers (https://standards.ieee.org/).

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.[11]

cyber security: Measures related to the informational security of an intelligent electronic device (IED).

cybersecurity: Measures related to the informational and physical security of an intelligent electronic device (IED).

intelligent electronic device (IED): A physical device or virtual device (vIED) having processing capacity with the capability of receiving or sending data/control from or to an external source, including computer-based systems and physical or virtual devices. In the scope of this standard, IEDs perform protection, metering, monitoring, automation, control, and/or communication functions for electric power management.

memorized secret: A type of authenticator composed of a character string intended to be memorized or memorable by the subscriber, permitting the subscriber to demonstrate *something they know* as part of an authentication process. (NIST SP 800-63-3 [B11])

3.2 Acronyms and abbreviations

CA	certificate authority
CIP	critical infrastructure protection
ID	identification
IED	intelligent electronic device
IT	information technology
JTAG	joint test action group
LAN	local area network
NERC	North American Electric Reliability Corporation
RBAC	role-based access control
SCADA	supervisory control and data acquisition
TOC	table of conformance
USB	universal serial bus
vIED	virtual intelligent electronic device
WAN	wide area network

[11] *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.

4. Use of this standard

4.1 General

The purpose of this standard is to establish a baseline of security requirements and features to be provided in intelligent electronic devices (IEDs) associated with the electric grid. The use of this standard during the lifecycle of the IED, including the procurement and testing of IEDs, may help ensure that a cybersecurity program that requires specific conformance to IEEE Std 1686 table of conformance (TOC) features is not compromised by the lack of a required feature or an operation in an unintended manner when new IEDs are installed. For users who make this standard an integral part of their IED cybersecurity posture, successful cybersecurity of IEDs is a combination of awareness training, technology, administrative procedures, documentation, monitoring, and diligent enforcement.

CAUTION

Adherence to this standard alone does not ensure adequate cybersecurity. Successful cybersecurity of IEDs is a combination of awareness training technology, engineering, administrative procedures, documentation, monitoring, and diligent enforcement.

IED cybersecurity technical control solutions need to be augmented with the following:

- Risk analysis to identify the potential threats and their impacts
- System-level analysis to mitigate the risks identified during the risk analysis
- Control and monitoring of physical access to the secure perimeter housing the IED
- Control and monitoring of network access to the secure perimeter housing the IED
- IED access control administration (e.g., memorized secrets, certificates)
- Control of sensitive IED documents (e.g., technical manuals, drawings)
- Real-time monitoring of IED conditions and alarming
- Security awareness training of utility personnel
- Security plans and procedures for non-utility personnel (e.g., system integrators, panel suppliers, contract maintenance suppliers)

Application of this standard can be tailored to determine the scope of IED capabilities applicable to the targeted cybersecurity program. This standard provides a set of features, functions, and practices for IEDs that are deemed to require security for electronic access (local or remote), data integrity, availability, confidentiality, and support for cybersecurity audit.

A cybersecurity program can use this standard to assess how new or existing IEDs meet the significant security issues addressed in this standard. The fact that a new or existing IED does not meet this standard does not imply that an effective cybersecurity program is not capable of securing the IED per a particular cybersecurity program’s requirement. In this case, this standard will help users identify what features a separate system should have to improve the security capabilities of an IED.

4.2 Applicability

This standard can be applied to any IED for which the user requires security, accountability, and audit ability in the installation, commissioning, configuration, operation, and maintenance of the IED.

Users of this standard should follow a risk-based approach to assess their specific situation and choose the devices to which the standard should apply in their particular case.[12] Issues affecting this choice include, but are not limited to, the following:

- IED classification (critical/non-critical infrastructure)
- User cybersecurity plan and procedures
- Communication and local area network (LAN)/wide area network (WAN) facilities
- Protection and control system architecture

4.3 Implementing IED security

The secure integration of an IED into a power system requires application of both technologies (cybersecurity capabilities provided by the IED) and procedures (to handle the specific features). This standard defines the cybersecurity capabilities to be provided in IEDs to accommodate cybersecurity programs. It is recognized, however, that in some cases, the capabilities may be tailored to meet a user's specific situation.

When an IED partially conforms with the applicable clauses of this standard, compensating measures can be applied to allow its deployment in a secure manner. These compensating measures can be a combination of engineering and cyber technologies (features provided by the IED) and procedures (to handle the specific features).

4.4 Proper use of this standard

4.4.1 IEEE Std 1686 requirements

The proper use of this standard requires the following:

- Proper citation of the standard
- Table of conformance (TOC) to the standard

4.4.2 Proper citation

The proper citation of this standard in a procurement document is as follows:

> The IED shall meet or exceed the requirements established in IEEE Std 1686™-2022, IEEE Standard for Intelligent Electronic Devices Cybersecurity Capabilities, as listed in the TOC.

[12] Standards ISO/IEC 27005 [B7], ISO 31000 [B5], and NIST SP800-39 [B9] describe guidelines for security risk management.

Modifications to the standard by the user to meet specific circumstances or requirements are permissible, so long as they are clearly identified in supporting documentation that accompanies the specification as part of a procurement process. When this is desired, it may be stipulated in a citation as in the following examples:

> The IED shall meet or exceed the requirements established in IEEE Std 1686™-2022, IEEE Standard for Intelligent Electronic Device Cybersecurity Capabilities, except as noted below:
>
> **5.1.2.5:** The minimum number of supported users shall be 20 (user desires a greater number of supported users than provided by the standard).
>
> **5.5.2 e):** The minimum number of records in the event and alarm buffer shall be 512 (user desires to fix the length of the buffer to meet system-level requirements).

Users are strongly discouraged against making generic statements such as “IED shall meet all applicable clauses and subclauses of IEEE Std 1686.” Such statements create the potential for differing assessments by the user and the manufacturer/integrator as to what is applicable.

4.4.3 Table of conformance (TOC)

Manufacturers claiming conformance with this standard shall be required to provide a TOC. The TOC shall list every subclause of Clause 5 of this standard on a separate line. For each subclause, the manufacturer shall then indicate the level of conformance for the product in question. The following responses shall be used:

- Acknowledge: Used as a placeholder when no requirement is presented in the subclause
- Exception: Product fails to meet one or more of the stated requirements of the subclause
- Conform: Product fully meets the stated requirements of the subclause
- Exceed: Product exceeds one or more of the stated requirements of the subclause

A column for comments and explanations may be included to provide additional information the manufacturer deems useful for clarification of the response.

Annex A shows an example of a TOC.

5. IED cybersecurity capabilities

5.1 IED identification and authentication control

5.1.1 Purpose

The purpose of this clause is to enforce the IED capabilities to identify, authenticate, and assign to a role all users on all interfaces capable of user access. Each role, either defined locally or remotely, shall have specific privileges associated with it. All user attempts to perform actions shall be validated against these privileges (refer to 5.2).

Memorized secret–based access can be used for IED remote or local access. Memorized secret–based access enforces policies such as rules for memorized secret renewal, and the IED typically validates basic rules such as memorized secret complexity, reuse of memorized secret, etc.

5.1.2 Requirements

5.1.2.1 Memorized secret–based access

Memorized secret–based access requirements are as follows:

a) The IED shall provide the capability to uniquely identify and authenticate users on all interfaces capable of user access. This capability shall enforce identification and authentication to support the segregation of duties and least privilege.

b) The IED shall provide the capability to support local or centralized user management.

c) For IEDs that utilize local memorized secret–based authentication, the IED shall provide the capability to enforce configurable memorized secret strength specified in 5.1.2.2.[13]

5.1.2.2 Memorized secret construction

User-created memorized secrets shall follow the following requirements:[14]

a) At least twelve characters shall be used, and the memorized secret shall be case-sensitive.

b) The IED should permit memorized secrets at least 64 characters in length.

c) All printing ASCII characters (including space) shall be supported.

d) Memorized secret checking: IED shall compare the prospective secrets against a configurable list of disallowed memorized secrets.

e) Truncation of the memorized secret shall not be performed when processed.

f) Memorized secret hints and knowledge-based authentication shall not be allowed (e.g., “What was the name of your first boss?”).

g) The IED shall offer the option to display the memorized secret in clear text (no dot or asterisk) until it is entered.

h) Any attempt to create a memorized secret that violates these rules shall be captured at the time of attempted creation and the user shall be notified and prompted to choose another memorized secret that conforms to the rules.

i) The IED may support manual or automatic expiration of memorized secrets, but the default setting shall be for no expiration.

[13] In the case of centralized user management, the memorized secret policy is enforced by the centralized system.
[14] These requirements are based on NIST SP 800-63B (section 5.1.1) [B12]. New NIST requirements recommend increased length over complexity.

j) User-created memorized secrets may support Unicode (ISO/IEC 10646 [B6]) characters provided that the length of the memorized secret is calculated on the number of code points.

k) Multiple consecutive space characters in user-created memorized secrets may be disallowed and the IED may replace this occurrence by single space provided that the length of the resulting secret is not less than the number of characters specified in 5.1.2.2 a).

5.1.2.3 Log in management policy enforcement

When an IED provides an authentication capability, the IED shall provide the capability to:

a) Enforce a limit of a configurable number of consecutive invalid access attempts by the same user (human, software process, or device) during a configurable time period.

b) If the limit described in 5.1.2.3 a) is exceeded, access shall be denied for a configurable period of time or until unlocked by an authorized user.

5.1.2.4 Memorized secret defeat mechanisms

The IED shall have no mechanism whereby the user-created ID/memorized secret control can be defeated or circumvented, unless all such means are disclosed to the implementing entity. This includes, but is not limited to, the following mechanisms and techniques:

— Embedded master memorized secret

— Hardware bypass of memorized secrets, such as jumpers and switch settings or internal commmunication access (e.g., joint test action group [JTAG], on-board universal serial bus [USB], etc.)

— Memorized secret reset function

— Complete device setting reset

5.1.2.5 Number of individual users

The IED shall support a minimum of 10 individual user accounts. Each account shall be assigned a unique user ID.

5.2 IED authorization and access control

5.2.1 Purpose

The purpose of this clause is to enforce the assigned privileges of an authenticated user to perform the requested action on the IED and monitor the use of these privileges.

5.2.2 Requirements

IED authorization and access control requirements are as follows:

a) The IED shall provide an authorization enforcement mechanism for all authenticated users based on their assigned responsibilities and least privilege.

b) For IEDs supporting a configuration file, the IED shall provide the capability to check that the file originates from a trusted source (e.g., by verifying a digital signature or a checksum).

c) For IEDs supporting least privilege mechanisms, the IED shall support role-based access control (RBAC) following capabilities:[15]

   1) The IED shall support at least four user-defined roles.

   2) The IED shall support any combination of functions listed in 5.2.3 a) through 5.2.3 g) for each role.

   3) The IED shall assign a role to each user/memorized secret combination, thereby conveying the permissions of that role to the user upon log in.

d) If an IED supports local or remote sessions, the IED shall provide the capability to terminate sessions that are idle or for which the authentication is no longer valid (e.g., timeout, inactivity, expired authentication).

e) The IED shall provide the capability to record all user actions and accesses.

5.2.3 IED main security functions

The IED main security functions include the following:

a) *View data* refers to the ability to view operational data (voltage, current, power, energy, status, alarms, etc.) of the IED that are not intended to be available in the general information display.

b) *View configuration settings* refer to the ability to view configuration settings of the IED, such as scaling, communications addressing, programmable logic routines, and the firmware version numbers.

c) *Force values* refer to the ability to manually override real data with manually inputted data and/or the ability to cause a control-output operation to occur.

d) *Configuration change* refers to the ability to download and upload configuration files to the unit and/or effect changes to the existing configuration.

e) *Firmware change* refers to the ability to load new firmware that does not require a corresponding hardware change.

f) *ID/password or RBAC management* refers to the ability to create, delete, or modify user IDs, passwords, roles and/or passwords, and role authorization levels.

g) *Audit trail* refers to the ability to view and download the audit trail.

[15] For a more complete RBAC implementation, refer to IEC 62351-8 [B1].

5.3 IED data integrity

5.3.1 Purpose

The purpose of this clause is to support the integrity of information on communication channels and in data at rest to prevent unauthorized modifications or errors.

5.3.2 Requirements

IED data integrity requirements are as follows:

a) The IED shall support the secure variant of the communication protocol to ensure data integrity for data in transit.

b) The IED shall provide the capability to ensure, with reasonable certainty, that data has been received from an authorized source and has not been altered.

c) The IED shall provide the capability to reject any message or setting that does not conform to the syntax and value types specified for data received on a specified interface.

d) The IED shall protect data at rest from unauthorized access, modification, and deletion.

e) The IED shall support the ability to be updated (as an example, but not limited to, firmware, patch, configuration, and settings) once installed by an authorized user only.

f) The IED shall validate the authenticity and integrity of any update prior to installation.

5.4 IED data confidentiality

5.4.1 Purpose

The purpose of this clause is to support the confidentiality of sensitive information on communication channels and in data at rest to prevent unauthorized disclosure.

5.4.2 Requirements

IED data confidentiality requirements are as follows:

a) The IED shall provide the capability to protect the confidentiality of information at rest for which explicit read authorization is supported.

b) The IED shall provide the capability to protect the confidentiality of sensitive information in transit.

c) The IED shall provide the capability to erase all information from the IED to be released from active service and/or decommissioned, except for the audit trail. Erasure of audit trail data is permitted but not required. The manufacturer shall disclose the audit trail erasure capability in the TOC.

5.5 IED response to cybersecurity events

5.5.1 Purpose

The purpose of this clause is to respond to security violations by notifying the proper authorities, reporting needed evidence of the violation, and taking timely corrective action when incidents are discovered. The IEDs could report security-related activities through standard SCADA communication protocols (e.g., IEEE 1815™, IEC 61850). The IED could also report events and alarms through standard IT management protocol such as Simple Network Management Protocol (SNMP) (RFC 1157 [B14]) or Syslog (RFC 3164 [B15]).

Events are defined as activities that can be expected to occur in the routine use and maintenance of the IED.

Alarms are defined as activities that may indicate unauthorized or invalid events. For example, an alarm can be raised if consecutive unsuccessful log in attempts reached a defined threshold.

5.5.2 Requirements

IED response to cybersecurity events requirements are as follows:

a) The IED shall have the capability to generate and store cybersecurity internal alarms and events described in 5.5.3.

b) The IED shall provide the capability to detect and limit the recording of repeated events or alarms to avoid intentional audit trail rollover.

c) The IED shall record the following information for each internal alarm and event committed to the audit trail.

   1) Event record number: The automatically generated sequential number for the event
   2) Time and date: Time and date of the event including year, month, day, hour, minute, and second
   3) User identification: The user ID associated with the event
   4) Event type: Defined in 5.5.3

d) The IED shall protect the audit trail against modification or deletion.

e) The IED shall store at least 2048 cybersecurity events before overwriting the oldest event with the newest event.

f) The IED shall provide mechanisms to prevent a failure of the IED when it reaches or exceeds the events storage capacity.

g) The IED shall have the capability to map internal cybersecurity alarms and events to industry standard communication protocols (e.g., an alarm status point in DNP3).

h) The IED shall provide the capability for authorized users to access the audit trail on a read-only basis.

i) The IED shall provide the capability of reporting any failures in the integrity of:

   1) Hardware

   2) Firmware/software

   3) Configuration

   4) Operating system

5.5.3 Events and alarms definition

5.5.3.1 Events

If implemented, the following events shall cause an entry into the audit trail:

a) Log in: Successful log in (locally or remotely) of a user to the device.

b) Manual log out: User-initiated log out.

c) Timed log out: Log out of user after a predefined period of inactivity elapses.

d) Value forcing: Action of a logged-in user that overrides real data with manual entry and/or causes a control operation.

e) Configuration access: Downloading of a configuration file from the IED to an external device or memory location (e.g., computer, memory stick, compact disc).

f) Configuration change: The uploading of a new configuration file to the IED or keystroke entry of new configuration parameters that causes a change in IED configuration.

g) Firmware change: Writing new firmware to persistent (permanent) memory.

h) ID/memorized secret creation or modification: Creation of new ID/memorized secret or modification of ID/memorized secret or RBAC levels of authorization.

i) ID/memorized secret deletion: Deletion of a user ID/memorized secret.

j) Audit trail access: User access of audit trail for viewing or audit trail download to an external device or memory location (e.g., computer, memory stick, compact disc).

k) Time/date change: User request to change time and date.

l) Alarm incident: The occurrence of an alarm incident as defined in 5.5.3.2.

m) Failed connection authentication (invalid security certificate, invalid pre-shared key, etc.).

n) Privilege violation: Attempt to perform a security function (defined in 5.2.3) not authorized in the user's role.

5.5.3.2 Alarms

The following incidents shall cause a unique alarm occurrence:

a) Unsuccessful log in attempt: Incorrect memorized secret entries [see 5.1.2.3 a)] in succession during a single log in attempt. Successive failed log in attempts after three shall generate a single entry into the alarm buffer listing the time of the last attempt and the total number of log in attempts that have occurred in succession.

b) Reboot: The rebooting or restarting of the IED by means of removing power or using a device resident rebooting mechanism such as a reset button, power-up sequence, or access software feature.

c) Invalid configuration or firmware: The detection by the IED of a configuration or firmware that does not contain the proper credentials that identify the configuration or firmware as valid.

d) Unauthorized configuration or firmware: The detection by the IED of a configuration or firmware download or install to the IED that does not contain the proper credentials that identify the configuration or firmware as authorized.

e) Time signal out of tolerance: The IED shall validate time synchronization messages received through protocol or dedicated time synchronization channels and raise an alarm if the received time differs from the IED's internal/local clock plus/minus a defined range.

f) Invalid field hardware changes: The IED shall validate user-performable (as identified by the manufacturer) field hardware changes and alarm if the field hardware change is performed improperly (i.e., wrong I/O board inserted in a designated I/O slot).

g) Tampering attempt: The IED shall log hardware tampering attempts.

5.6 IED resilience

5.6.1 Purpose

The purpose of this clause is to support the availability of IEDs against the degradation or denial of essential services.

5.6.2 Requirements

IED resilience requirements are as follows:

a) The IED shall provide the capability to maintain essential functions when operating in a degraded mode.

b) The IED shall provide the capability to recover to a known secure state after a power failure.

c) The IED shall provide the capability to detect tampering attempts; see 5.5.3.2 g).

d) The IED shall provide the capability to specifically disable unused functions, ports, protocols, and/or services.

e) The IED shall apply input validation and sanitization to all data inputs from external sources.

5.7 Firmware quality assurance

Firmware quality assurance should follow the guidelines set forth in IEEE Std C37.231™.

5.8 Documentation

5.8.1 Requirements

Documentation is important for cybersecurity (hardware and software) management and assessment. Documentation shall include the following:

a) Cybersecurity (hardware and software) hardening[16] of the device

b) Secure decommissioning

5.8.2 Recommendations

The manufacturer should also provide the minimum information that allows the operator to be able to evaluate an IED's cybersecurity posture such as:

— Operating system including the version number

— List of third-party software libraries and executables plus version number

— List of open-source libraries plus version number

[16] Hardening is the ability to limit IED features to reduce its vulnerability surface.

Annex A

(informative)

Table of conformance (TOC)

Table A.1 must be completed to indicate the intelligent electronic device (IED) conformance to IEEE Std 1686™-2022, except for status and comment cells that are shaded.

Table A.1—Example TOC

Clause/ subclause number	Clause/subclause title	Status	Comment
5	IED cybersecurity capabilities		
5.1	IED identification and authentication control		
5.1.1	Purpose		
5.1.2	Requirements		
5.1.2.1	Memorized secret–based access		
5.1.2.1 a)	Capability to identify and authenticate all human users on all interfaces		
5.1.2.1 b)	Capability to support local or centralized user management		
5.1.2.1 c)	Capability to enforce configurable memorized secret as defined in 5.1.2.2		
5.1.2.2	Capability of supporting memorized secret construction		
5.1.2.2 a)	Support at least 12 case-sensitive characters		
5.1.2.2 b)	Support 64 characters memorized secret		
5.1.2.2 c)	Support all printing ASCII characters		
5.1.2.2 d)	Support memorized secret checking		
5.1.2.2 e)	Support integrity of memorized secret (no truncation)		
5.1.2.2 f)	Avoid the use of memorized secret hints		
5.1.2.2 g)	Support displaying of memorized secret		
5.1.2.2 h)	Memorized secret rules violation check at the time of creation		
5.1.2.2 i)	Memorized secret expiration is allowed (default setting: no expiration) (optional)		
5.1.2.2 j)	Support Unicode characters (optional)		
5.1.2.2 k)	Support multiple consecutive spaces replacement (optional)		
5.1.2.3	Log in management policy enforcement		
5.1.2.3 a)	Capability of limiting a configurable number of consecutive invalid access attempts		
5.1.2.3 b)	Capability for denying access for a configurable period of time when this invalid access limit has been reached		
5.1.2.4	Capability of memorized secret defeat mechanism		
5.1.2.5	Capability of supporting at least 10 users accounts		
5.2	IED authorization and access control		
5.2.1	Purpose		
5.2.2	Requirements		
5.2.2 a)	Provide authorization enforcement mechanism		
5.2.2 b)	Capability of validating file source and signature		
5.2.2 c)	Capability to support RBAC		
5.2.2 c) 1)	Support at least four roles		
5.2.2 c) 2)	Support combination of functions listed in 5.2.3		
5.2.2 c) 3)	Assign a role to each user/memorized secret combination		

Clause/ subclause number	Clause/subclause title	Status	Comment
5.2.2 d)	Capability to terminate a session based on some conditions		
5.2.2 e)	Capability to log (or record) all users actions and accesses		
5.2.3	IED main security functions		
5.2.3 a)	View operational data		
5.2.3 b)	View configuration setting		
5.2.3	IED main security functions		
5.2.3 d)	Modify configuration setting		
5.2.3 e)	Modify firmware		
5.2.3 f)	Create/modify/delete user IDs		
5.2.3 g)	View/download audit trail		
5.3	IED data integrity		
5.3.1	Purpose		
5.3.2	Requirements		
5.3.2 a)	Support secure variant of communication protocols to ensure integrity of data in transit		
5.3.2 b)	Capability to authenticate and validate received data		
5.3.2 c)	Capability of rejecting a message or setting that does not conform to the syntax and value type		
5.3.2 d)	Capability of protecting data at rest from unauthorized access modification or deletion		
5.3.2 e)	Provide the capability to be updated		
5.3.2 f)	Capability of validating the authenticity and integrity of any update prior to install		
5.4	IED data confidentiality		
5.4.1	Purpose		
5.4.2	Requirements		
5.4.2 a)	Provide the capability to protect the confidentiality of data at rest		
5.4.2 b)	Provide the capability to protect the confidentiality of data in transit		
5.4.2 c)	Capability to erase all internal data (except for audit trail)		
5.5	IED response to security events		
5.5.1	Purpose		
5.5.2	Requirements		
5.5.2 a)	Capability to generate and store security events and alarms		
5.5.2 b)	Capability to detect and limit repeated events or alarms		
5.5.2 c) 1)	Shall record event number		
5.5.2 c) 2)	Shall record time and date		
5.5.2 c) 3)	Shall record user identification		
5.5.2 c) 4)	Shall record event or alarm type		
5.5.2 d)	Protection against modification or deletion		
5.5.2 e)	Capability to store at least 2048 events		
5.5.2 f)	Capability to prevent a failure when the events storage capacity is exceeded		
5.5.2 g)	Capability to map internal security alarms and events to industry standard communication protocols		
5.5.2 h)	Capability for authorized users to access audit trail		
5.5.2 i) 1)	Capability of reporting failures in hardware		
5.5.2 i) 2)	Capability of reporting failures in firmware/software		
5.5.2 i) 3)	Capability of reporting failures in configuration		
5.5.2 i) 4)	Capability of reporting failures in operating system		
5.5.3	Events and alarms definition		
5.5.3.1	Events		
5.5.3.1 a)	Successful log in		
5.5.3.1 b)	User-initiated log out		

Clause/ subclause number	Clause/subclause title	Status	Comment
5.5.3.1 c)	Timed log out		
5.5.3.1 d)	Value forcing		
5.5.3.1 e)	Configuration access		
5.5.3.1 f)	Configuration change		
5.5.3.1 g)	Firmware change		
5.5.3.1 h)	ID/memorized secret creation or modification		
5.5.3.1 i)	ID/memorized secret deletion		
5.5.3.1 j)	Audit trail access		
5.5.3.1 k)	Time/date change		
5.5.3.1 l)	Alarm incident		
5.5.3.1 m)	Failed connection		
5.5.3.1 n)	Privilege violation		
5.5.3.2	Alarms		
5.5.3.2 a)	Unsuccessful log in attempt		
5.5.3.2 b)	Reboot		
5.5.3.2 c)	Invalid configuration or firmware update		
5.5.3.2 d)	Unauthorized configuration or firmware update		
5.5.3.2 e)	Time signal out of tolerance		
5.5.3.2 f)	Invalid field hardware changes		
5.5.3.2 g)	Tampering attempt		
5.6	IED resiliency		
5.6.1	Purpose		
5.6.2	Requirements		
5.6.2 a)	Capability to maintain essential functions when operating in a degraded mode		
5.6.2 b)	Capability of restoring to a known state after a power failure		
5.6.2 c)	Capability to detect and report tampering attempts		
5.6.2 d)	Capability to specifically disable unused functions, ports, protocols, and/or services		
5.6.2 e)	Validate and sanitize all data from external sources		
5.7	Capability to support firmware quality assurance		
5.8	Documentation requirements		
5.8.1 a)	Documentation shall cover procedures for cybersecurity hardening of the device		
5.8.1 b)	Documentation shall cover procedures for cybersecurity secure decommissioning		
5.8.2	Recommendations (optional): The manufacturer should also provide minimum information related to: — Operating system including the version number — List of third-party software libraries and executables plus version number — List of open-source libraries plus version number		

Annex B

(informative)

Certificate-based access[17]

B.1 Purpose

Certificate-based access is used if the intelligent electronic device (IED) communicates with other components on a network. When certificate-based access is used, key and certificate management are typically supported at the system level and the IED has the capabilities of accepting and validating certificates.

B.2 IED capabilities

The IED should provide the capability to identify itself and authenticate with other IEDs and other protocol-compatible devices such as authentication servers.

If the IED uses certificates for authentication, the following capabilities are required:

a) For certificate-based access control, the IED should:
   1) Verify the certificate (including validity period, revocation state, and certificate chain)

b) IED certificate management should support:
   1) Automated or manual certificate initial configuration (certificate bootstrapping)
   2) Certificate renewal (automated)
   3) Certificate deletion (during decommissioning of IED)
   4) Fetching certificate revocation information

c) IED configuration should implement:
   1) Certificate initial configuration (either automated or manual certificate management)
   2) Automated certificate management using certificate authority
   3) Manually defined certificates (for manual certificate management)
   4) Certificate renewal period (depending on certificate validity period)
   5) Trust anchors (accepted root certificate authority [CA] certificates)
   6) Interfaces on which certificates are used (e.g., protocol specific)

d) The IED should support a local authentication mechanism for emergency situations

[17] IEC 62351-9 [B2] specifies detailed implementations for key/certificate management.

B.3 Certificates events and alarms

If certificate-based access is implemented, the following events and alarms should be supported:

Events:

a) Successful and unsuccessful renewal of certificates

b) Successful and unsuccessful certificate enrolment

Alarms:

c) Expired certificate

d) Failure of certificate validation

e) Revocation of any certificates owned/used by the IED

f) Certificate chain validation error

g) Certificate revocation information is missing or obsoleted

Table B.1—Table of conformance (TOC) for certificate-based management

Clause/ subclause number	Clause/subclause title	Status	Comment
B.2	Certificate-based access		
B.2 a) 1)	Capability of verifying certificates		
B.2 b) 1)	Capability of initial certificate configuration		
B.2 b) 2)	Capability of certificate renewal		
B.2 b) 3)	Capability of certificate deletion		
B.2 b) 4)	Capability of fetching certificate revocation information		
B.2 c) 1)	Configuration to support initial certificate configuration		
B.2 c) 2)	Configuration to support automated certificate management		
B.2 c) 3)	Configuration to support manually defined certificates		
B.2 c) 4)	Configuration to define certificate renewal period		
B.2 c) 5)	Configuration to define trust anchors		
B.2 c) 6)	Configuration to define certificate use on different interfaces		
B.2 d)	Capability to support local authentication mechanism in case of emergency		
B.3 a)	Successful and unsuccessful renewal of certificates		
B.3 b)	Certificate chain		
B.3 c)	Expired certificate		
B.3 d)	Failure of certificate validation		
B.3 e)	Revocation of any certificates owned/used by the IED		
B.3 f)	Certificate chain validation error		
B.3 g)	Certificate revocation information is missing or obsoleted		

Annex C

(informative)

Intelligent electronic device (IED) secure product lifecycle guidelines

A secure product will pass through several relevant steps during its lifecycle as shown in Figure C.1. This annex aims to produce guidelines that will help the user/owner of those products to have a higher level of confidence in its conception and enough documentation for its day-to-day operation and maintenance. These guidelines are product oriented and should be added, when applicable, to system cybersecurity documentation.

Since many of the guidelines listed in this annex are outside the scope of this standard, each of them is marked by either “informative” or by the IEEE 1686 Clause 5 corresponding requirement.

Figure C.1—Product lifecycle

C.1 Secure development

C.1.1 Product development environment check

A general product development/maintenance process should be documented and enforced that is consistent and integrated with commonly accepted product development processes that include, but are not limited to the following:

a) Repeatable testing verification and validation process—informative

b) Review and approval of all development process records—informative

c) That the personnel are authorized, trained, and qualified to develop the IED—informative

d) That during the development, the integrity of the files is verified (origin and integrity)—IEEE Std 1686 5.3.2, items d) and f)

e) That a process is in place to transfer any sensitive information into the IED (e.g., keys)—IEEE Std 1686 5.4.2, items a) and b)

f) That a process should be employed to identify and manage the security risks of all externally provided components used within the IED (this includes the hardware, software, firmware, and operating system)—IEEE Std 1686 5.6.2, items a), b), c), d), and e)

g) Development environments are secure—informative

h) That a process is in place to ensure IED is free from known malicious code and malware—informative

i) Secure delivery, including tamper-evident packaging of physical devices and checksum/hash for software/firmware—informative

j) The manufacturer should test the IED for the following:

1) Known and common vulnerability testing—informative
2) Malware testing—informative
3) Malformed input testing—informative
4) Structured penetration testing—informative
5) Software weakness analysis—informative

C.2 Engineering and maintenance

C.2.1 Engineering

The client should:

a) Perform a risk and impact analysis of the future system product—informative

b) Identify the risks caused by the new IED—informative

c) Design the system to mitigate, assume, or transfer the risk—informative

d) Define the policies for security management and audit—informative

e) List the IED cybersecurity requirements—IEEE Std 1686

C.2.2 Installing and commissioning

A process is employed to create product user documentation that includes guidelines for hardening the product when installing and maintaining the product. The guidelines include, but are not limited to, instructions, rationales, and recommendations for the integration of the product, configuration and use of security options/capabilities, and the tools.

a) The client and the manufacturer/integrator validate that all the cybersecurity requirements [C.2.1 item e)] are included in the IED—IEEE Std 1686.
b) The client and manufacturer should complete functional testing with field equipment, interfaces, and central management systems (e.g., logging and authentication)—informative.
c) The client validates the documentation provided by the manufacturer/integrator—IEEE Std 1686 5.8.
d) The client validates the manufacturer's software support and update process—informative.

C.2.3 Maintenance and support (manufacturer/integrator)

The manufacturer/integrator:

a) Should implement a change management system—informative
b) Should analyze and compile the client's issues and questions—informative
c) Should verify if a published cybersecurity vulnerability affects any of the externally provided software components contained in the IED—informative
d) Should correct any problem found in the internal or external software module—informative

e) Should inform the client of any cybersecurity risks—informative

f) Should document and distribute patches and software updates including vendor signature—IEEE Std 1686 5.3.2 items a), b), and c)

C.2.4 Maintenance and operation (client)

The client:

a) Should support a change management system—informative

b) Should test any software/firmware patch or update received from the manufacturer—informative

c) Should update IED software using manufacturer and client signatures—informative

d) Should audit IED performances and tampering—IEEE Std 1686 5.6.2

e) Should analyze and record IED cybersecurity events—IEEE Std 1686 5.5.2

C.2.5 Security update

A process should be used to ensure that the documentation related to product security updates is made available to the users. Required information includes the product version number, the instructions on how to apply the update and a description of any impacts that applying the patch to the product can have, including IED reboot.

The client should validate and plan the deployment of the update depending on the severity of the potential risks.

C.3 Decommissioning

C.3.1 Decommissioning, recycling, and disposal (client)

A process should be employed to create product user documentation that includes guidelines for removing the product from use. The guidelines include, but are not limited to, instructions and recommendations for the following:

a) Removing the product from its intended environment—informative

b) Removing references and configuration data stored within the environment—IEEE Std 1686 5.4.2, item c)

The client should develop a policy describing the following:

a) Secure disposal of the product to prevent potential disclosure of data contained in the product that could not be removed as described in IEEE Std 1686 5.4.2, item c)—informative

Annex D

(informative)

Bibliography

Bibliographical references are resources that provide additional or helpful material but do not need to be understood or used to implement this standard. Reference to these resources is made for informational use only.

[B1] IEC 62351-8, Power systems management and associated information exchange—Data and communications security—Part 8: Role-based access control for power system management.[18]

[B2] IEC 62351-9, Cyber security key management for power system equipment.

[B3] IEC 62443-4-1, Security for industrial automation and control systems—Part 4-1: Secure product development lifecycle requirements.

[B4] IEC 62443-4-2, Security for industrial automation and control systems—Part 4-2: Technical security requirements for IACS components.

[B5] ISO 31000:2010, Risk management—Guidelines.[19]

[B6] ISO/IEC 10646, Information technology—Universal Coded Character Set (UCS).

[B7] ISO/IEC 27005:2018, Information technology—Security techniques—Information security risk management.

[B8] NERC Cybersecurity Standards CIP-002 to CIP-009.[20]

[B9] NIST SP 800-39, Managing Information Security Risk—Organization, Mission, and Information System View.[21]

[B10] NIST SP 800-53, Security and Privacy Controls for Information Systems and Organizations.

[B11] NIST SP 800-63-3, Digital Identity Guidelines.

[B12] NIST SP 800-63B, Digital Identity Guidelines: Authentication and Lifecycle Management.

[B13] NIST SP 800-82 rev. 2, Guide to Industrial Control Systems (ICS) Security.

[B14] RFC 1157, A simple network management protocol.[22]

[B15] RFC 3164, The BSD syslog protocol.

[18] IEC publications are available from the International Electrotechnical Commission (https://www.iec.ch) and the American National Standards Institute (https://www.ansi.org/).
[19] ISO publications are available from the International Organization for Standardization (https://www.iso.org/) and the American National Standards Institute (https://www.ansi.org/).
[20] NERC publications are available from the North American Electric Reliability Corporation (https: www.nerc.com/).
[21] NIST publications are available from the National Institute of Standards and Technology (https://www.nist.gov/).
[22] Internet Requests for Comments (RFCs) are available on the World Wide Web at the following ftp site: venera.isi.edu; logon: anonymous; password: user's e-mail address; directory: in-inotes.

IEEE SA
STANDARDS ASSOCIATION

RAISING THE WORLD'S STANDARDS

Connect with us on:

Twitter: twitter.com/ieeesa
Facebook: facebook.com/ieeesa
LinkedIn: linkedin.com/groups/1791118
Beyond Standards blog: beyondstandards.ieee.org
YouTube: youtube.com/ieeesa

standards.ieee.org
Phone: +1 732 981 0060

IEEE