

STN	Zdravotnícka informatika Interoperabilita prístroja Časť 40102: Základ Kybernetická bezpečnosť Možnosti zmierňovania (ISO/IEEE 11073-40102: 2022)	STN EN ISO/IEEE 11073-40102 84 8038
------------	--	---

Health informatics - Device interoperability - Part 40102: Foundational - Cybersecurity - Capabilities for mitigation (ISO/IEEE 11073-40102:2022)

Táto norma obsahuje anglickú verziu európskej normy.
This standard includes the English version of the European Standard.

Táto norma bola oznámená vo Vestníku ÚNMS SR č. 06/22

Obsahuje: EN ISO/IEEE 11073-40102:2022, ISO/IEEE 11073-40102:2022

EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

**EN ISO/IEEE 11073-
40102**

March 2022

ICS 35.240.80

English Version

**Health informatics - Device interoperability - Part 40102:
Foundational - Cybersecurity - Capabilities for mitigation
(ISO/IEEE 11073-40102:2022)**

Informatique de santé - Interopérabilité des dispositifs
- Partie 40102: Fondamentaux - Cybersécurité -
Capacités d'atténuation (ISO/IEEE 11073-40102:2022)

Medizinische Informatik - Geräteinteroperabilität - Teil
40102: Grundlagen - Cybersicherheit - Möglichkeiten
zur Schadensbegrenzung (ISO/IEEE 11073-
40102:2022)

This European Standard was approved by CEN on 13 March 2022.

CEN members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.



EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

EN ISO/IEEE 11073-40102:2022 (E)

Contents	Page
European foreword.....	3

European foreword

This document (EN ISO/IEEE 11073-40102:2022) has been prepared by Technical Committee ISO/TC 215 "Health informatics" in collaboration with Technical Committee CEN/TC 251 "Health informatics" the secretariat of which is held by NEN.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by September 2022, and conflicting national standards shall be withdrawn at the latest by September 2022.

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

Any feedback and questions on this document should be directed to the users' national standards body/national committee. A complete listing of these bodies can be found on the CEN website.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

Endorsement notice

The text of ISO/IEEE 11073-40102:2022 has been approved by CEN as EN ISO/IEEE 11073-40102:2022 without any modification.

INTERNATIONAL ISO/IEEE STANDARD 11073-40102

First edition
2022-03

Health informatics — Device interoperability —

Part 40102: Foundational — Cybersecurity — Capabilities for mitigation

Informatique de santé — Interopérabilité des dispositifs —

*Partie 40102: Fondamentaux — Cybersécurité — Capacités
d'atténuation*



IEEE

Reference number
ISO/IEEE 11073-40102:2022(E)

© IEEE 2021

ISO/IEEE 11073-40102:2022(E)**COPYRIGHT PROTECTED DOCUMENT**

© IEEE 2021

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from IEEE at the address below.

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

Email: stds.ipr@ieee.org
Website: www.ieee.org

Published in Switzerland

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted (see www.iso.org/directives).

IEEE Standards documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE-SA) Standards Board. The IEEE develops its standards through a consensus development process, approved by the American National Standards Institute, which brings together volunteers representing varied viewpoints and interests to achieve the final product. Volunteers are not necessarily members of the Institute and serve without compensation. While the IEEE administers the process and establishes rules to promote fairness in the consensus development process, the IEEE does not independently evaluate, test, or verify the accuracy of any of the information contained in its standards.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

ISO/IEEE 11073-40102 was prepared by the IEEE 11073 Standards Committee of the IEEE Engineering in Medicine and Biology Society (as IEEE Std 11073-40102-2020) and drafted in accordance with its editorial rules. It was adopted, under the “fast-track procedure” defined in the Partner Standards Development Organization cooperation agreement between ISO and IEEE, by Technical Committee ISO/TC 215, *Health informatics*.

A list of all parts in the ISO/IEEE 11073 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

IEEE Std 11073-40102™-2020

Health informatics—Device interoperability

Part 40102: Foundational—Cybersecurity— Capabilities for mitigation

Developed by the

IEEE 11073 Standards Committee
of the
IEEE Engineering in Medicine and Biology Society

Approved 24 September 2020

IEEE SA Standards Board

Abstract: For Personal Health Devices (PHDs) and Point-of-Care Devices (PoCDs), a security baseline of application layer cybersecurity mitigation techniques is defined by this standard for certain use cases or for times when certain criteria are met. The mitigation techniques are based on an extended confidentiality, integrity, and availability (CIA) triad and are described generally to allow manufacturers to determine the most appropriate algorithms and implementations. A scalable information security toolbox appropriate for PHD/PoCD interfaces is specified that fulfills the intersection of requirements and recommendations from the National Institute of Standards and Technology (NIST) and the European Network and Information Security Agency (ENISA). A mapping of this standard to the NIST cybersecurity framework; IEC TR 80001-2-2; and the Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege (STRIDE) classification scheme is defined.

Keywords: cybersecurity, IEEE 11073-40102™, medical device communication, mitigation techniques, Personal Health Devices, Point-of-Care Devices

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

Copyright © 2021 by The Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 8 January 2021. 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 978-1-5044-7088-9 STD24424
Print: ISBN 978-1-5044-7089-6 STDPD24424

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 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](#). An IEEE Account is needed to access the application.

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

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.

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](#). 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](#). 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.

Patents

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

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.

Participants

At the time this standard was submitted to the IEEE SA Standards Board for approval, the Public Health Device Working Group had the following membership:

Daidi Zhong, *Chair*
Michael Kirwan and Christoph Fischer, *Vice Chairs*

Karsten Aalders	Cory Condek	Shu Han
Charles R. Abbruscato	Todd H. Cooper	Nathaniel Hamming
Nabil Abujbara	David Cornejo	Rickey L. Hampton
Maher Abuzaid	Douglas Coup	Sten Hanke
James Agnew	Nigel Cox	Aki Harma
Manfred Aigner	Hans Crommenacker	Jordan Hartmann
Jorge Alberola	Tomio Crosley	Kai Hassing
David Aparisi	Allen Curtis	Avi Hauser
Lawrence Arne	Jesús Daniel Trigo	Wolfgang Heck
Diego B. Arquillo	David Davenport	Nathaniel Heintzman
Serafin Arroyo	Russell Davis	Charles Henderson
Muhammad Asim	Sushil K. Deka	Jun-Ho Her
Kit August	Ciro de la Vega	Helen B. Hernandez
Doug Baird	Pedro de-las-Heras-Quiros	Timothy L. Hirou
David Baker	Jim Dello Stritto	Allen Hobbs
Anindya Bakshi	Kent Dicks	Alex Holland
Abira Balanadarasan	Hyoungdo Do	Arto Holopainen
Ananth Balasubramanian	Jonathan Dougherty	Kris Holtzclaw
Sunlee Bang	Xiaolian Duan	Robert Hoy
M. Jonathan Barkley	Sourav Dutta	Anne Huang
Gilberto Barrón	Jakob Ehrensvar	Zhiyong Huang
David Bean	Fredrik Einberg	Ron Huby
John Bell	Javier Escayola Calvo	David Hughes
Olivia Bellamou-Huet	Mark Estes	Robert D. Hughes
Rudy Belliardi	Leonardo Estevez	Jiyoung Huh
Daniel Bernstein	Bosco T. Fernandes	Hugh Hunter
George A. Bertos	Morten Flintrup	Philip O. Isaacson
Chris Biernacki	Joseph W. Forler	Atsushi Ito
Ola Björnsne	Russell Foster	Michael Jaffe
Thomas Blackadar	Eric Freudenthal	Praduman Jain
Thomas Bluethner	Matthias Frohner	Hu Jin
Douglas P. Bogia	Ken Fuchs	Danny Jochelson
Xavier Boniface	Jing Gao	Akiyoshi Kabe
Shannon Boucousis	Marcus Garbe	Steve Kahle
Julius Broma	John Garguilo	Tomio Kamioka
Lyle G. Bullock, Jr.	Liang Ge	James J. Kang
Bernard Burg	Rick Geimer	Kei Kariya
Chris Burns	Igor Gejdos	Andy Kaschl
Jeremy Byford-Rew	Ferenc Gerbovics	Junzo Kashiara
Satya Calloji	Alan Godfrey	Colin Kennedy
Carole C. Carey	Nicolae Goga	Ralph Kent
Craig Carlson	Julian Goldman	Laurie M. Kermes
Santiago Carot-Nemesio	Raul Gonzalez Gomez	Ahmad Kheirandish
Randy W. Carroll	Chris Gough	Junhyung Kim
Seungchul Chae	Channa Gowda	Minho Kim
Peggy Chien	Charles M. Gropper	Min-Joon Kim
David Chiu	Amit Gupta	Taekon Kim
Jinyong Choi	Jeff Guttmacher	Tetsuya Kimura
Chia-Chin Chong	Rasmus Haahr	Alfred Kloos
Saeed A. Choudhary	Christian Habermann	Jeongmee Koh
Jinhan Chung	Michael Hagerty	Jean-Marc Koller
John A. Cogan	Jerry Hahn	John Koon
John T. Collins	Robert Hall	Patty Krantz

Raymond Krasinski	Carl Pantiskas	Raymond A. Strickland
Alexander Kraus	Harry P. Pappas	Chandrasekaran Subramaniam
Ramesh Krishna	Hanna Park	Hermann Suominen
Geoffrey Kruse	Jong-Tae Park	Lee Surprenant
Falko Kuester	Myungeun Park	Ravi Swami
Rafael Lajara	Soojun Park	Ray Sweidan
Pierre Landau	Phillip E. Pash	Na Tang
Jaechul Lee	TongBi Pei	Haruyuyki Tatsumi
JongMuk Lee	Soren Petersen	Isabel Tejero
Kyong Ho Lee	James Petisce	Tom Thompson
Rami Lee	Peter Piction	Jonas Tirén
Sungkee Lee	Michael Pliskin	Janet Traub
Woojae Lee	Varshney Prabodh	Gary Tschautscher
Qiong Li	Jeff Price	Masato Tsuchid
Xiangchen Li	Harald Prinzhorn	Ken Tubman
Zhuofang Li	Harry Qiu	Akib Uddin
Patrick Lichter	Tanzilur Rahman	Sunil Unadkat
Jisoon Lim	Phillip Raymond	Fabio Urbani
Joon-Ho Lim	Terrie Reed	Philipp Urbauer
Xiaoming Liu	Barry Reinhold	Laura Vanzago
Wei-Jung Lo	Brian Reinhold	Alpo Värri
Charles Lowe	Melvin I. Reynolds	Andrei Vasilateanu
Don Ludolph	John G. Rhoads	Dalimar Velez
Christian Luszick	Jeffrey S. Robbins	Martha Veleziz
Bob MacWilliams	Chris Roberts	Rudi Voon
Srikkanth Madhurbotheswaran	Stefan Robert	Barry Vornbrock
Miriam L. Makhoul	Scott M. Robertson	Isobel Walker
Romain Marmot	Timothy Robertson	David Wang
Sandra Martinez	David Rosales	Linling Wang
Miguel Martínez de	Bill Saltzstein	Jerry P. Wang
Espronceda Cámara	Giovanna Sannino	Yao Wang
Peter Mayhew	Jose A. Santos-Cadenas	Yi Wang
Jim McCain	Stefan Sauermann	Steve Warren
László Meleg	John Sawyer	Fujio Watanabe
Alexander Mense	Alois Schloegl	Toru Watsuji
Behnaz Minaei	Paul S. Schluter	David Weissman
Jinsei Miyazaki	Mark G. Schnell	Kathleen Wible
Erik Moll	Richard A. Schrenker	Paul Williamson
Darr Moore	Antonio Scorpiniti	Jan Wittenber
Chris Morel	KwangSeok Seo	Jia-Rong Wu
Robert Moskowitz	Riccardo Serafin	Will Wykeham
Carsten Mueglitz	Sid Shaw	Ariton Xhafa
Soundharya Nagasubramanian	Frank Shen	Ricky Yang
Alex Neefus	Min Shih	Melanie S. Yeung
Trong-Nghia Nguyen-Dobinsky	Mazen Shihabi	Qiang Yin
Michael E. Nidd	Redmond Shouldice	Done-Sik Yoo
Jim Niswander	Sternly K. Simon	Zhi Yu
Hiroaki Niwamoto	Marjorie Skubic	Jianchao Zeng
Thomas Norgall	Robert Smith	Jason Zhang
Yoshiteru Nozoe	Ivan Soh	Jie Zhao
Abraham Ofek	Motoki Sone	Thomas Zhao
Brett Olive	Emily Sopensky	Yuanhong Zhong
Begonya Ota	Rajagopalan Srinivasan	Qing Zhou
Marco Paleari	Nicholas Steblay	Miha Zoubek
Bud Panjwani	Lars Steubesand	Szymon Zyskoter
	John (Ivo) Stivorc	

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

Robert Aiello
Johann Amsenga
Bjoern Andersen
Pradeep Balachandran
Demetrio Bucaneg, Jr.
Lyle G. Bullock, Jr.
Craig Carlson
Juan Carreon
Pin Chang
Malcolm Clarke
Christoph Fischer

David Fuschi
Randall Groves
Robert Heile
Werner Hoelzl
Raj Jain
Martin Kasparick
Stuart Kerry
Yongbum Kim
Raymond Krasinski
Javier Luiso
H. Moll
Nick S. A. Nikjoo

Bansi Patel
Beth Pumo
Stefan Schlichting
Thomas Starai
Mark-Rene Uchida
John Vergis
J. Wiley
Yu Yuan
Oren Yuen
Janusz Zalewski
Daidi Zhong

When the IEEE SA Standards Board approved this standard on 24 September 2020, it had the following membership:

Gary Hoffman, *Chair*
Jon Walter Rosdahl, *Vice Chair*
John D. Kulick, *Past Chair*
Konstantinos Karachalios, *Secretary*

Ted Burse
Doug Edwards
J. Travis Griffith
Grace Gu
Guido R. Hiertz
Joseph L. Koepfinger*

David J. Law
Howard Li
Dong Liu
Kevin Lu
Paul Nikolich
Damir Novosel
Dorothy Stanley

Mehmet Ulema
Lei Wang
Sha Wei
Philip B. Winston
Daidi Zhong
Jingyi Zhou

*Member Emeritus

Introduction

This introduction is not part of IEEE Std 11073-40102-2020, Health informatics—Device interoperability—Part 40102: Foundational—Cybersecurity—Capabilities for mitigation.

Users of Personal Health Devices (PHDs) and Point-of-Care Devices (PoCDs) have implicit expectations on convenience, connectivity, accessibility, and security of data. For example, they expect to connect PHDs/PoCDs to their mobile devices and dashboards, view the data in the cloud, and easily share the information with clinicians or care providers. In some cases, the users themselves are taking action to build connections between PHDs/PoCDs, mobile devices, and the cloud to create the desired system. While many manufacturers are working on solving PHD/PoCD connectivity challenges with proprietary solutions, no standardized approach exists to provide secure plug-and-play interoperability.

The ISO/IEEE 11073 PHDs/PoCDs family of standards, Bluetooth Special Interest Group profiles and services specifications, and the Continua Design Guidelines (PCHAlliance [B20]) were developed to specifically address plug-and-play interoperability of PHDs/PoCDs (e.g., physical activity monitor, physiological monitor, pulse oximeter, sleep apnoea breathing therapy equipment, ventilator, insulin delivery device, infusion pump, continuous glucose monitor). In this context, the following terms have specific meanings:

- *Interoperability* is the ability of client components to communicate and share data with service components in an unambiguous and predictable manner as well as to understand and use the information that is exchanged (PCHAlliance [B20]).
- *Plug and play* are all the user has to do to make a connection—the systems automatically detect, configure, and communicate without any other human interaction (ISO/IEEE 11073-10201 [B13]).¹

Within the context of *secure* plug-and-play interoperability, cybersecurity is the process and capability of preventing unauthorized access or modification, misuse, denial of use, or the unauthorized use of information that is stored on, accessed from, or transferred to and from a PHD/PoCD. This standard describes the capability part of cybersecurity for transport-independent applications and information profiles of PHDs/PoCDs. These profiles define data exchange, data representation, and terminology for communication between agents (e.g., pulse oximeters, sleep apnoea breathing therapy equipment) and connected devices (e.g., health appliances, set top boxes, cell phones, personal computers, monitoring cockpits, critical care dashboards).

For PHDs/PoCDs, this standard defines a security baseline of application layer cybersecurity mitigation techniques for certain use cases or for times when certain criteria are met. This standard provides a scalable information security toolbox appropriate for PHD/PoCD interfaces, which fulfills the intersection of requirements and recommendations from the National Institute of Standards and Technology (NIST) and the European Network and Information Security Agency (ENISA). This standard maps to the NIST cybersecurity framework [B15]; IEC TR 80001-2-2 [B8]; and the Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege (STRIDE) classification scheme. The mitigation techniques are based on an extended confidentiality, integrity, and availability (CIA) triad and are described generally to allow manufacturers to determine the most appropriate algorithms and implementations.

¹ The numbers in brackets correspond to the numbers of the bibliography in Annex A.

Contents

1. Overview	11
1.1 General	11
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	13
4. Information security	14
4.1 General	14
4.2 Confidentiality	14
4.3 Integrity	14
4.4 Availability	14
4.5 Non-repudiation.....	15
5. Security with safety and usability.....	15
5.1 High-level view	15
5.2 Safety relationships.....	15
5.3 Usability relationships	16
6. Mitigation	16
6.1 General	16
6.2 Software security updates	17
6.3 Secure design principles	17
6.4 Secure by design and secure by default principles	18
6.5 Privacy by design and privacy by default principles	18
6.6 Ensure robust interface design.....	19
6.7 Limit access to trusted users only	19
6.8 Ensure trusted content.....	19
6.9 Mapping of mitigation categories, security capabilities, mitigation techniques, and design principles	19
7. Information security controls.....	22
8. Information security toolbox	23
8.1 General	23
8.2 Nonce.....	24
8.3 Encryption	24
8.4 Message authentication code	24
8.5 Key exchange	25
8.6 Key derivation function	26
8.7 Audit trail.....	26
Annex A (informative) Bibliography	27
Annex B (informative) Test vectors	29
B.1 General.....	29
B.2 NIST AES-GCM test vector	29
B.3 NIST AES-GMAC test vector	29
B.4 NIST ECDH test vectors.....	30

Health informatics—Device interoperability

Part 40102: Foundational—Cybersecurity— Capabilities for mitigation

1. Overview

1.1 General

Many Personal Health Devices (PHDs) and Point-of-Care Devices (PoCDs) provide vital support for people living with chronic disease or experiencing a life-threatening medical event. Cybersecurity attacks on vulnerable devices may lead to the alteration of prescribed therapy (e.g., sleep apnoea breathing therapy, insulin therapy) or to information disclosure that results in insurance or identity fraud or in direct or indirect patient harm. Companies subject to a successful cybersecurity attack may suffer financial harm and a negative reputation.

Manufacturers of PHDs/PoCDs may be required to support application layer end-to-end information security. PHD/PoCD data exchange may be conducted over an untrusted transport. Also, a requirement may exist for multiple access control levels (e.g., restricted read access, restricted write access, full read access, full write access, full control access). Most PHDs/PoCDs have limited resources (e.g., processing power, memory, energy). Current standardized PHD/PoCD data exchange assumes the exchange is secured by other means, such as secure transport channel. This assumption requires that manufacturers define solutions by, for example, extensions or using mechanisms on the transport layer. Such solutions limit the usage of PHD/PoCD data exchange standards and restricts interoperability.

This standard is based on the PHD Cybersecurity Standards Roadmap findings (IEEE white paper [B10]) and defines a security baseline of application layer cybersecurity mitigation techniques for PHD/PoCD interfaces.² The mitigation techniques address an extended confidentiality, integrity, and availability (CIA) triad and allow manufacturers to implement the most appropriate algorithms. The mitigation techniques are not dependent on a specific risk management process. Instead they are applicable to any approach, including the vulnerability assessment described in IEEE Std 11073-40101™ [B9]. In Figure 1, IEEE Std 11073-40101 is depicted by the top row, and this standard is depicted by the bottom row.

² The numbers in brackets correspond to the numbers in the bibliography in Annex A.

IEEE Std 11073-40102-2020
 Health informatics—Device interoperability
 Part 40102: Foundational—Cybersecurity—Capabilities for mitigation

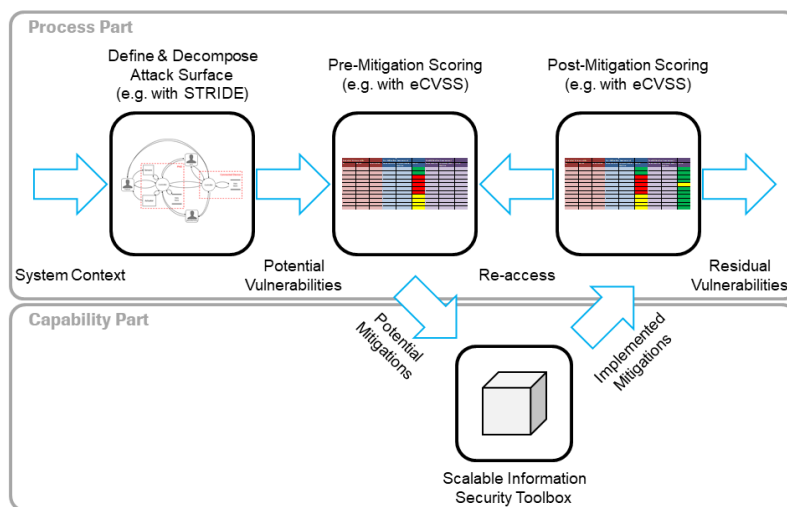


Figure 1—Vulnerability assessment workflow

1.2 Scope

Within the context of secure plug-and-play interoperability, cybersecurity is the process and capability of preventing unauthorized access or modification, misuse, denial of use, or the unauthorized use of information that is stored on, accessed from, or transferred to and from a PHD/PoCD. The capability part of cybersecurity is information security controls related to both digital data and the relationships to safety and usability.

For PHDs/PoCDs, this standard defines a security baseline of application layer cybersecurity mitigation techniques for certain use cases or for times when certain criteria are met. This standard provides a scalable information security toolbox appropriate for PHD/PoCD interfaces, which fulfills the intersection of requirements and recommendations from National Institute of Standards and Technology (NIST) and the European Network and Information Security Agency (ENISA). This standard maps to the NIST cybersecurity framework [B15]; IEC TR 80001-2-2 [B8]; and the Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege (STRIDE) classification scheme. The mitigation techniques are based on the extended CIA triad (Clause 4) and are described generally to allow manufacturers to determine the most appropriate algorithms and implementations.

1.3 Purpose

The purpose of this document is to build a common approach to cybersecurity mitigation on PHD/PoCD interfaces and define a scalable information security toolbox appropriate for the PHD/PoCD data exchange standards.

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*).^{3,4}

³ The use of the word *must* is deprecated and cannot be used when stating mandatory requirements; *must* is used only to describe unavoidable situations.

⁴ The use of *will* is deprecated and cannot be used when stating mandatory requirements; *will* is used only in statements of fact.

IEEE Std 11073-40102-2020
Health informatics—Device interoperability
Part 40102: Foundational—Cybersecurity—Capabilities for mitigation

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; therefore, 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.

NIST FIPS Publication 197, Advanced Encryption Standard (AES).
(<https://csrc.nist.gov/publications/detail/fips/197/final>)

NIST SP 800-38D, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC. (<https://csrc.nist.gov/publications/detail/sp/800-38d/final>)

See Annex A for all informative material referenced by this standard.

koniec náhľadu – text ďalej pokračuje v platenej verzii STN