INTERNATIONAL STANDARD **ISO/IEEE 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

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

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.

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

PDF: ISBN 978-1-5044-7088-9 STD24424
Print: ISBN 978-1-5044-7089-6 STDPD24424

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

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

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

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.

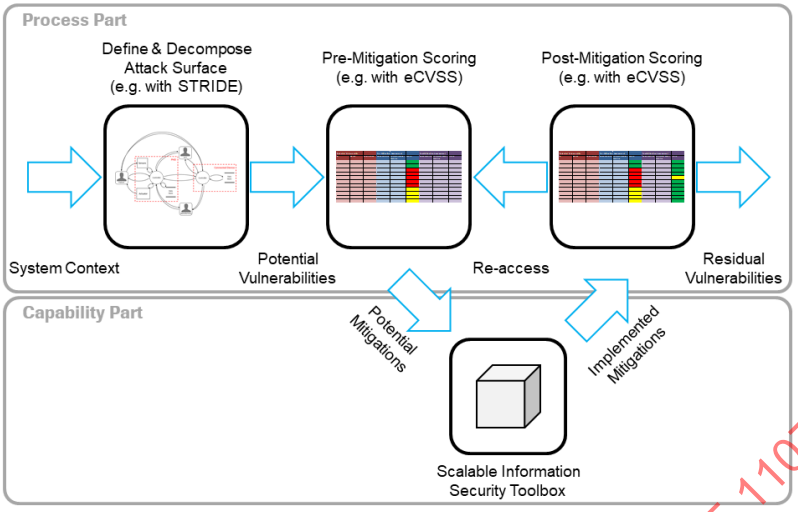

Figure 1—Vulnerability assessment workflow

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.

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.

3. Definitions, acronyms, and abbreviations

3.1 Definitions

For the purposes of this document, the terms and definitions provided in the PHD Cybersecurity Standards Roadmap (IEEE white paper [B10]) apply. The *IEEE Standards Dictionary Online* should be consulted for terms not defined there.[5]

3.2 Acronyms and abbreviations

AES	Advanced Encryption Standard
AES-GCM	Advanced Encryption Standard–Galois/Counter Mode
AES-GMAC	Advanced Encryption Standard–Galois Message Authentication Code
CIA	confidentiality, integrity, and availability
ECDH	Elliptic Curve Diffie–Hellman
ENISA	European Network and Information Security Agency
HCP	Health Care Provider
MAC	message authentication code
NIST	National Institute of Standards and Technology
PHD	Personal Health Device
PoCD	Point-of-Care Device
STRIDE	Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privileges

[5] *IEEE Standards Dictionary Online* is available at https://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. Information security

4.1 General

Within the context of PHD/PoCD interfaces, security is most frequently used in reference to information security. It describes characteristics of information-processing and information-storing systems, which maximize confidentiality (see 4.2), integrity (see 4.3), and availability (see 4.4). These three core principles of information security are called the *CIA triad*. Information security helps protect from dangers and/or threats, avoid damage, and minimize risks. The *extended CIA triad* additionally includes non-repudiation (see 4.5) as a principle.

4.2 Confidentiality

Confidentiality has been defined by the International Organization for Standardization in ISO/IEC 27002 [B12] as "ensuring that information is accessible only to those authorized to have access." Minimizing disclosure of information to unauthorized individuals or systems is one cornerstone of information security. A confidentiality breach might take many forms, even if no information technology is involved, e.g., eavesdropping on conversations of others, looking over the shoulder to read information, looking into secret documents, injecting a computer virus, or using a Trojan horse that sends information to another person. In the context of PHD/PoCD, a confidentiality breach primarily means eavesdropping on information somewhere between the source (e.g., sensor) and the receiver (e.g., personal computer, physician's computer, hospital server) or unauthorized access to stored information. To enforce confidentiality, the information could be encrypted during transmission (i.e., data in transit) and storage (i.e., data at rest) as well as requiring authentication and/or authorization within the request before transmission.

Privacy is an important part of confidentiality, especially when it comes to protected health information (PHI). PHI is defined as individually identifiable health information transmitted or maintained by a covered entity or its business associates in any form or medium (45CFR160.103 [B1]). The U.S. Health Insurance Portability and Accountability Act (HIPAA) limits the circumstances in which an individual's PHI may be used or disclosed by covered entities (HHS [B7]). Similarly, the EU General Data Protection Regulation states that personal data shall be processed lawfully, fairly, and in a transparent manner; collected for specified, explicit, and legitimate purposes; and kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed (Official Journal of the EU [B19]).

4.3 Integrity

In information security, integrity (also known as authenticity) means that data is not modified or deleted without authorization. Integrity is violated when information is changed by a user that is not authorized to do so. A security breach related to integrity might occur directly on the devices (e.g., because of a virus) and on the way from information source to receiver.

Authentication technologies help ensure that the original data is not altered or deleted during the transfer. They also provide technological means to check if the data came from the right sender and not from a sender that only pretends to be the sender. This is achieved, for example, through electronic signatures and certificates.

4.4 Availability

Information security availability means the information is available when it is needed by authorized users. The computing systems (physical and digital) used to store and process the information, the security controls used to protect it, and the communication channels used to access it have to be functioning correctly and reliably.

4.5 Non-repudiation

Non-repudiation means an undeniable and immutable account about where the received information originates, where it is going, who is requesting it, and who is providing it, in such a way that no entity can deny what its contribution was to the overall activity. Non-repudiation can be achieved through electronic signatures and audit trails.

5. Security with safety and usability

5.1 High-level view

Safety and usability play key roles as part of risk management and information security. Risk management views the PHD/PoCD holistically by considering the PHD/PoCD, users, intended use, interfaces, applied security, and environment to identify, describe, and reduce risks of the system (IEEE Std 11073-40101 [B9]). When viewing the PHD/PoCD as a black box, the relationship between the PHD/PoCD, security, safety, and usability is depicted in Figure 2 and is as follows: security is keeping what's inside the box secure, safety is keeping what's outside the box safe, and usability helps ensure interaction with what's inside the box is as intended and meets user needs.

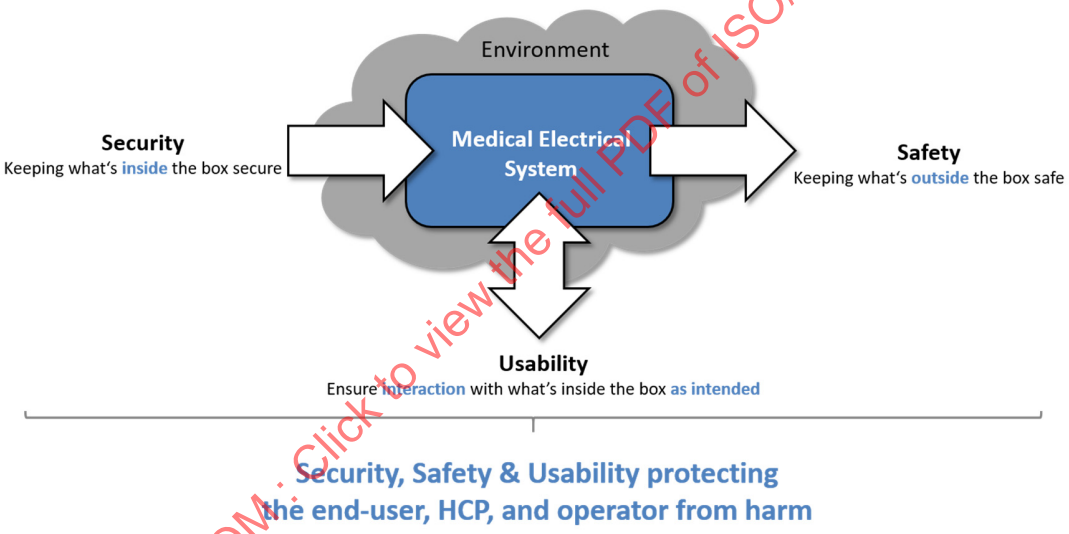

Figure 2—Security, safety, and usability relationship

5.2 Safety relationships

An utmost concern in the design of a PHD/PoCD is safety during intended use. Safety is determined by avoiding potential harm to relevant stakeholders [including, but not limited to, the end-user, Health Care Provider (HCP), or operator] and their environment. Regulatory authorities approve the sale and distribution of regulated PHDs/PoCDs, in part, based on evidence that the benefit of the PHD/PoCD outweighs the risks to safety. A PHD/PoCD should be designed and manufactured to be reasonably safe. The manufacturer takes reasonable measures to identity the risks inherent in the device. If the risks can be eliminated, the manufacturer should eliminate them. If the risks cannot be eliminated, the manufacturer should reduce the risks as much as possible and provide for protection appropriate to those risks (e.g., alarms, labeling, documentation). See IEEE Std 11073-40101 [B9] for additional details.

It is important to distinguish safety and information security. Both are of great importance in PHD/PoCD design and intended use, and while these terms may be coupled, they are distinct (see 5.1). Safety is the

protection of the end-user and the environment from hazardous conditions caused by or related to the system. Information security is the protection of the system from influence of an end-user and the environment to help ensure confidentiality, integrity, and availability. However, in order to maintain safety, security should also be maximized.

5.3 Usability relationships

A PHD/PoCD is intended to focus on the needs of end-users to improve their quality of life and should be designed to ease their day-to-day burden. Usability plays a valuable role in the design of a PHD/PoCD. A PHD/PoCD user interface that establishes effective and efficient end-user learning and satisfaction is considered highly usable (ISO 9241-210 [B11]). As an example, some end-users might be physically handicapped or visually impaired; thus the system must conform to accessibility guidelines. The usability of a PHD/PoCD may also target care providers or HCPs. An HCP user interface that provides a clear and concise summary of measured vitals at a critical moment could be lifesaving. Specific disciplines of an HCP (e.g., nurse, dietitian, occupational therapist) generally focus on a very particular part of the data. Personalized interfaces and menus can greatly improve usability. Conducting usability studies with representative target groups during the design phase of a PHD/PoCD can maximize consistent positive end-user and HCP engagement.

Usability is a tool that can identify the risk associated with using the PHD/PoCD. However, it is very difficult to determine the use errors until the PHD/PoCD use is simulated and observed. Usability studies can be conducted to assess intended use cases and determine if there is any risk, for example, of harm to users and their environment or impediment to the prescribed therapy. Controls can be added to the PHD/PoCD to mitigate these potential risks such that they are eliminated or reduced to the extent possible. Regulatory bodies consider usability testing a valuable component of product development and recommend that manufacturers consider usability testing of a PHD/PoCD as part of a robust design control system (FDA “Human Factors” [B4]).

Usability is also of importance from an information security point of view. Experience shows that a weak point in security is typically human misuse or human limitation. For example, users may continuously forget to log off when they have completed their tasks and, as a consequence, leave the system open for attack from impersonation of an authorized user. By understanding the workflow of the system and behaviors of users, such attacks could be blocked. The system should defend itself from potential attacks by understanding the user workflow and making users aware when potential security risks exist.

However, there is typically a trade-off between increased security or reduced risk and usability. Often controls included in a PHD/PoCD to mitigate specific information security vulnerabilities or to reduce identified unacceptable risk can reduce the usability of the PHD/PoCD. As such, either the end-user engagement or the prescribed therapy suffers as the cost of a more secure PHD/PoCD. Manufacturers should carefully consider the benefits of including information security controls and should not unreasonably hinder end-user or HCP access to PHD/PoCD data or its intended use.

6. Mitigation

6.1 General

In the context of PHD/PoCD cybersecurity, mitigation is the act of introducing security controls into a device or system to prevent an attack or reduce the impact of an attack. Failure to maintain PHD/PoCD cybersecurity can result in compromised device functionality or loss of data (medical or personal)—in other words, availability, loss of integrity, or exposure of other connected devices or networks to security threats. Such failures in turn may result in patient illness, injury, or death.

Security controls should be included in the design of the PHD/PoCD before it is shipped but, as is often the case, vulnerabilities are discovered in hardware, software, and communication protocols after a product is released. Rigorous design and testing are still an imperfect process, and system features are sometimes expanded to include use models that were not part of the initial system design and analysis process. There is a need to provide security updates to mitigate newly discovered vulnerabilities.

System vulnerabilities identify the areas subject to potential threats and determine both the need for and type of mitigation. Specific frameworks used to decompose a system and quantify vulnerabilities are designed to identify threats based on common security properties. Generally, the protection of these common security properties uses general mitigation techniques, which are then realized by specific security controls.

6.2 Software security updates

Maintaining a robust software lifecycle process includes monitoring software and hardware components of the PHD/PoCD for vulnerabilities throughout the expected lifetime of the device. This monitoring includes software of unknown provenance (SOUP) or off-the-shelf (OTS) components. While discoveries of vulnerabilities within a hardware component may require recalls or replacement of the PHD/PoCD, a newly discovered vulnerability within a software component may be able to be mitigated with a software security update. Of the many considerations, it is important to assess the following:

- Discoverability, exploitability, and reproducibility of the vulnerability
- Security of the update deployment mechanism
- Trade-off between cost of deployment versus disposal or replacement of the device
- Manner in which to disclose a vulnerability and inform the end-user

The deployment of a software security update should be made as quickly as possible and ideally prior to any exploitation. As such, the PHD/PoCD should be designed to anticipate the need for updates to address future vulnerabilities and to facilitate the rapid verification, validation, and testing of these updates (FDA “Premarket” [B5]).

Threat modeling is important in understanding and assessing the discoverability, exploitability and reproducibility of a vulnerability and potential for end-user harm. Threat modeling can also be used in determining whether a proposed or implemented remediation can reasonably control the risk of end-user harm due to a vulnerability (FDA “Postmarket” [B6]).

When deploying the software security update, the mechanisms need to be secure, for example, to protect against man-in-the-middle attacks. Cryptographic signatures help secure and authenticate updates and prevent unauthorized access to the device. Integrity checks of the update prior to installation or execution help ensure that the update has not been altered. The security of the transfer of the update from end to end (e.g., the manufacturer to the device) must also be considered.

6.3 Secure design principles

The hostile environment that can result from a connected PHD/PoCD requires the development of design principles to produce robust systems. Manufacturers are responsible for PHD/PoCD cybersecurity and maintaining the intended device functionality and safety throughout the PHD/PoCD’s service life. Thus, manufacturers should address cybersecurity during the design and development of the PHD/PoCD, as well as over the course of the PHD/PoCD’s service life, to identify more robust and efficient mitigation of end-user risks. More robust and efficient mitigations can be achieved by establishing design principles related to cybersecurity to address the following (FDA “Premarket” [B5]):

- Identification of assets, threats, and vulnerabilities
- Assessment of the impact of threats and vulnerabilities on device functionality and end-users
- Assessment of the likelihood of a threat and of a vulnerability being exploited

— Determination of risk levels and suitable mitigation strategies
— Assessment of residual risk and risk acceptance criteria

6.4 Secure by design and secure by default principles

Secure by design means that the software has been designed from the ground up to be secure. Under Secure by Design principles, manufacturers may assume the existence of malicious activities and take care to minimize the impact when an attempt is made to exploit a system.

Secure by default is the concept of designing the system so that it operates by default with a minimal required set of functionalities with a secure configuration.

Secure by design and secure by default include, but are not limited to, the following:

— **Least privileges:** All components and users operate with the fewest possible permissions.
— **Defense in depth:** Design does not rely on a single threat mitigation solution alone for protection; rather, layers of protection are implemented.
— **Secure default settings:** Based on the known attack surfaces for the system, the design minimizes the attack surfaces in the default configuration.
— **Avoidance of insecure operating system changes:** Applications do not make or require any default changes to the operating system or security settings that reduce security for the host computer without consideration of possible risks.
— **Services off by default:** The services off by default allows that, if a feature of a system is rarely used, that feature is deactivated by default.

6.5 Privacy by design and privacy by default principles

Privacy by design means that privacy and data protection are embedded throughout the entire system lifecycle, from the early design stage to deployment, use, and ultimate disposal. This concept includes, but is not limited to, the following:

— **Provide notice of privacy practices to users:** Provide appropriate notice to users about data that is collected, stored, or shared so that users can make informed decisions about how their personal information is used and disclosed.
— **Do not store secrets:** Collect the minimum amount of data that is required for a particular purpose and use the least sensitive form of that data.
— **Protect secrets and secret data; de-identification:** Encrypt sensitive data at rest and in transfer, limit access to stored data, and verify that data usage complies with the system's intended use. If encryption is not possible, anonymize patient data (e.g., log and trace files).

Privacy by default means that privacy and data protection are embedded as default configuration settings in a system. This concept includes, but is not limited to, the following:

— **Least privileges:** Ship with secure default privacy settings, and prevent unauthorized access through technical controls.
— **Do not store secrets:** Process and store only minimum necessary data. Retain data for the shortest possible time.
— **Protect secrets and secret data:** Protect any sensitive data at rest and in transit with access controls and encryption.

6.6 Ensure robust interface design

To *ensure robust interface design* means that the system maintains the ability to function as intended in a hostile operating context. This concept includes, but is not limited to, the following:

- **Input validation; input sanitization:** Protect the system from input tampering such as through fuzzing, Structured Query Language (SQL) injection, or a malicious security digital (SD) card.
- **Message authentication code; encryption:** Require all wireless communication interfaces to be robust against the occurrence of eavesdropping, injection, and replay attacks.
- **Protect secrets and secret data:** Employ protection of technical secrets by keeping safe any objects that are used to secure data through such mechanisms as encryption keys, passwords, and tokens.

6.7 Limit access to trusted users only

Limit access to trusted users only means the system requires authentication and restricts requests to authorized functions. This concept includes, but is not limited to, the following:

- **Authentication:** Limit access to devices through the authentication of users (e.g., user identity and password, smartcard, biometric). Use appropriate authentication (e.g., multi-factor authentication to permit privileged device access to system administrators, service technicians, and maintenance personnel). Require authentication or other appropriate controls before permitting software or firmware updates, including those affecting the operating system, applications, and anti-malware.
- **Quality of service:** Use automatic timed methods to terminate sessions within the system where appropriate for the use environment.
- **Authorization; least privileges:** Where appropriate, employ a layered authorization model by differentiating privileges based on the user role (e.g., caregiver, system administrator) or device role.
- **Do not store secrets; protect secrets and secret data:** Strengthen password protection by avoiding "hardcoded" password or common words (i.e., passwords that are the same for each device, difficult to change, and vulnerable to public disclosure) and limit public access to passwords used for privileged device access.
- **Physical tamper resistant; physical tamper evidence:** Where appropriate, provide physical locks on devices and their communication ports to minimize tampering.

6.8 Ensure trusted content

To *ensure trusted content* means the system employs security measures to determine the integrity and source of the content it provides to the user. This concept includes, but is not limited to, the following:

- **Message authentication code; authentication; digital signature:** Restrict software or firmware updates to authenticated code. One authentication method manufacturers may consider is code signature verification.
- **Systematic procedures; authorization:** Use systematic procedures for authorized users to download version-identifiable software and firmware from the manufacturer.
- **Encryption; message authentication code; digital signature:** Utilize secure data transfer to and from the device, and when appropriate, use methods for encryption.

6.9 Mapping of mitigation categories, security capabilities, mitigation techniques, and design principles

Each security property has primary mitigation techniques to address the vulnerabilities that could be identified by a risk management process. Table 1 provides a list of mitigations grouped into the following categories defined by the NIST cybersecurity framework [B15]:

- **Identify:** Process of recognizing the attributes that identify the object. Within the NIST cybersecurity framework, the identify category is intended to limit access to trusted users only and help ensure integrity of trusted content.
- **Protect:** The ability to limit or contain the impact of a potential cybersecurity event.
  - **Prevent:** Measures that avoid or preclude a cybersecurity event.
  - **Limit:** Measures intended to reduce the impact of a cybersecurity event.
- **Detect:** Security controls intended to detect a cybersecurity event.
- **Respond:** Appropriate activities to execute regarding a detected cybersecurity event.
- **Recover:** Appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

Also provided in Table 1 is a mapping to IEC TR 80001-2-2 [B8] security capabilities. The security capabilities are broad categories of technical, administrative, or organizational controls to manage risks to confidentiality, integrity, availability, and accountability of data and systems. The capabilities are intended to support health delivery organizations, PHD/PoCD manufacturers, and information technology vendors. Among the 19 security capabilities described in IEC TR 80001-2-2, the “Third-party components in product lifecycle roadmap” is not mapped in Table 1 since it is not related to the interfaces to and from the PHD/PoCD.

Finally, Table 1 provides mapping to STRIDE categories to provide alignment with IEEE Std 11073-40101 [B9]. STRIDE is a classification scheme, useful for system decomposition, for characterizing identified threats according to the kinds of exploit that are used by the attacker. The STRIDE acronym is formed from the first letter of each of the following threat categories: **S**poofing, **T**ampering, **R**epudiation, **I**nformation Disclosure, **D**enial of Service, and **E**levation of Privilege.

Using this mapping, moderate- and high-risk vulnerabilities for each STRIDE category are mitigated by one or more of the mapped mitigation techniques. The mitigation technique is investigated to help ensure it will address the vulnerability identified based on the PHD/PoCD use case or intended function. Mitigation techniques were selected such that they may be scalable from the less complex PHD/PoCD to the most complex PHD/PoCD. In the cases where multiple mitigation techniques can address the moderate- and/or high-risk vulnerabilities, effort is made to reduce the mitigation to a single technique.

While end-user signalization is not a core mitigation identified as part of this work, instead a last mode of defense, it should be noted that scoring systems may weight user awareness heavily. While this standard agrees that end-user signalization is a power mitigation, the focus is on secure data exchange. However, manufacturers should evaluate the effective use of increasing user awareness to further reduce vulnerabilities to an acceptable risk level.

Table 1—Mitigation categories, security capabilities, mitigation techniques, and design principles

Mitigation category (based on NIST cybersecurity framework [B15])			Security capability (based on IEC TR 80001-2-2 [B8])	Mitigation technique and design principle	S	T	R	I	D	E
Identify			Node authentication Personal authentication	Authentication	X				X	
				Digital signatures	X	X	X			
Protect	Prevent		Authorization Health data de-identification Health data storage and confidentiality Health data integrity and authenticity Physical locks on device Automatic logoff Configuration of security features	Authorization		X		X	X	X
				De-identification				X		
				Do not store secrets	X	X		X		X
				Encryption				X		
				Filtering					X	
				Message authorization code		X				
				Physical tamper resistant		X		X		
				Protect secrets and secret data	X	X		X		X
		Limit	Software application hardening Security guidelines	Input sanitization		X		X		
				Input validation		X				
				Quality of service					X	
				Least privileges						X
				Throttling					X	
Detect			Audit Physical locks on device	Audit trail			X			
				Physical tamper evidence		X		X		
Respond			Malware detection and protection emergency access	End-user signalization	X	X		X	X	X
				Invalidate compromised security	X	X	X	X	X	X
Recover			Data backup and disaster recovery cybersecurity product updates	Re-establish security	X	X	X	X	X	X

7. Information security controls

The identification of cybersecurity vulnerabilities and estimation of risk can be done according to IEEE Std 11073-40101 [B9] or any equivalent approach. This standard considers generic information security controls based on the mitigation technique to help ensure the security control addresses the vulnerability. Where appropriate, specific methods or algorithms are listed in Clause 8 to enable interoperability. The risk management process will evaluate any residual risk after security controls are applied and determine if any additional security controls are required to further reduce the risk to an acceptable level.

The mitigation techniques presented in Table 1 shall be applied to the vulnerabilities identified through the risk management process as security controls. Only mitigation techniques that address a specific vulnerability should be included as security controls. As well, security controls are needed to mitigate only moderate- and high-risk vulnerabilities. The mitigation techniques can be further reduced to those most applicable to selected PHD/PoCD interfaces. Note that while *physical tamper resistant* and *physical tamper evidence* are useful security controls, they are considered out of scope as this standard aims to provide a scalable information security toolbox appropriate for PHD/PoCD interfaces. Also note that some mitigation techniques are intended as an implementation robustness control (e.g., *input sanitization*, *input validation*) and not necessarily applicable to PHD/PoCD interfaces or enforceable by communication standards.

Table 2 presents prioritized mitigation techniques for security controls on PHD/PoCD interfaces. All mitigation techniques have merit; however, some were deemed to be applicable for any type of PHD/PoCD interface where moderate- or high-risk vulnerabilities were identified (IEEE white paper [B10]). Mitigation techniques marked as mandatory (M) are included if a high-risk vulnerability was identified and should be considered to mitigate moderate-risk vulnerabilities. For example, the STRIDE category of Spoofing identified a high-risk vulnerability; thus the mitigation technique *authentication* is required. Mitigation techniques marked as conditional (C) are included if a high-risk vulnerability was identified and if a specific condition or requirement exists and should be considered to mitigate moderate-risk vulnerabilities. All mitigation techniques without either a M or C (—) should still be considered for appropriate PHD/PoCD interfaces and included based on the identified vulnerabilities, use case, or intended function. Inclusion of any security controls on a PHD/PoCD interface based on a mitigation technique requires reassessment of all moderate- and high-risk vulnerabilities identified on that interface to determine that any residual risk has been reduced at an acceptable level.

Table 2—Minimum mitigation techniques

Mitigation technique	Qualifiers[a]
Authentication	M
Digital signature	C
Authorization	M
De-identification	C
Do not store secrets	—
Encryption	C
Filtering	—
Message authentication code	C
Physical tamper resistant	—
Protect secrets and secret data	—
Input sanitization	—
Input validation	—
Quality of service	—

Table 2—Minimum mitigation techniques *(continued)*

Mitigation technique	Qualifiers[a]
Least privileges	C
Throttling	—
Audit trail	C
Physical tamper evidence	—
End-user signalization	C
Invalidate compromised security	—
Re-establish security	—

[a] M = mandatory; C = conditional.

The criteria of conditional mitigation techniques are as follows:

- **Digital signature:**
  - If the manufacturer requires identity attached to the data exchange, a digital signature is mandatory.
  - If an audit trail is mandatory and the manufacturer wants an audit trail protected against repudiation and tampering, digital signatures are mandatory.
- **De-identification:**
  - If any personal information is included in the data exchange, de-identification is mandatory, such that the personal information is protected from passive listeners accessing this information. Inclusion of personal information into the data exchange should be avoided when not necessary.
- **Encryption:**
  - If the data itself or the data exchange is intended to be confidential, encryption is mandatory.
- **Message authentication code:**
  - If the integrity and/or authentication of the data exchange is required, a message authentication code (MAC) is mandatory.
- **Least privileges:**
  - When the device has an intended use case that includes multiple authorization levels, running with least privileges is mandatory.
- **Audit trail:**
  - When the PHD/PoCD has an intended use case where it participates in a data exchange of significant risk with a connected device, an audit trail is mandatory.
- **End-user signalization:**
  - End-user signalization is a conditional mitigation and limited to the last mode of defense in cases where other mitigation techniques cannot address a moderate- or high-risk vulnerability.
  - Even then, end-user signalization should be limited to only critical functions/values that can produce adverse events.

8. Information security toolbox

8.1 General

The information security toolbox is intended to provide industry-proven information security controls to support application layer end-to-end information security and protect from common threats. Specific methods or algorithms are listed in this clause to enable interoperability. They fulfill the intersection of requirements and recommendations from NIST and ENISA.