

# INTERNATIONAL ISO/IEEE STANDARD 11073-40101

First edition  
2022-03

---

---

## Health informatics — Device interoperability —

### Part 40101: Foundational — Cybersecurity — Processes for vulnerability assessment

*Informatique de santé — Interopérabilité des dispositifs —*

*Partie 40101: Fondamentaux — Cybersécurité — Processus pour  
l'évaluation de la vulnérabilité*

ISO/IEEE 11073-40101:2022

<https://standards.iteh.ai/catalog/standards/sist/e3e2b4fd-5a69-4611-87df-d938323a31b/iso-ieee-11073-40101-2022>



Reference number  
ISO/IEEE 11073-40101:2022(E)

© IEEE 2021

iTeh STANDARD PREVIEW  
(standards.iteh.ai)

ISO/IEEE 11073-40101:2022

<https://standards.iteh.ai/catalog/standards/sist/e3e2b4fd-5a69-4611-87df-d93832f3a31b/iso-ieee-11073-40101-2022>



**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](mailto:stds.ipr@ieee.org)  
Website: [www.ieee.org](http://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](http://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](http://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](http://www.iso.org/iso/foreword.html).

ISO/IEEE 11073-40101 was prepared by the IEEE 11073 Standards Committee of the IEEE Engineering in Medicine and Biology Society (as IEEE Std 11073-40101-2020) 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](http://www.iso.org/members.html).



## Health informatics—Device interoperability

# Part 40101: Foundational—Cybersecurity— Processes for vulnerability assessment

Developed by the

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

Approved 24 September 2020

**IEEE SA Standards Board** [ISO/IEEE 11073-40101:2022](https://standards.ieee.org/standard/11073-40101-2020.html)

<https://standards.ieee.org/standard/11073-40101-2020.html>  
<https://standards.ieee.org/standard/11073-40101-2020.html>

**Abstract:** For Personal Health Devices (PHDs) and Point-of-Care Devices (PoCDs), an iterative, systematic, scalable, and auditable approach to identification of cybersecurity vulnerabilities and estimation of risk is defined by this standard. The standard presents one approach to iterative vulnerability assessment that uses the Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege (STRIDE) classification scheme and the embedded Common Vulnerability Scoring System (eCVSS). The assessment includes system context, system decomposition, pre-mitigation scoring, mitigation, and post-mitigation scoring and iterates until the remaining vulnerabilities are reduced to an acceptable level of risk.

**Keywords:** cybersecurity, embedded Common Vulnerability Scoring System, IEEE 11073-40101™, medical device communication, Personal Health Devices, Point-of-Care Devices, STRIDE, vulnerability assessment

## iTeh STANDARD PREVIEW (standards.iteh.ai)

ISO/IEEE 11073-40101:2022

<https://standards.iteh.ai/catalog/standards/sist/e3e2b4fd-5a69-4611-87df-d93832f3a31b/iso-ieee-11073-40101-2022>

---

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.

Microsoft and Excel are registered trademarks of Microsoft Corporation in the United States and/or other countries.

Open Web Application Security Project and OWASP are registered trademarks of the OWASP Foundation, Inc.

PDF: ISBN 978-1-5044-7086-5 STD24423  
Print: ISBN 978-1-5044-7087-2 STDPD24423

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

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

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

Robert Aiello	Randall Groves	Bansi Patel
Johann Amsenga	Robert Heile	Dalibor Pokrajac
Bjoern Andersen	Werner Hoelzl	Beth Pumo
Pradeep Balachandran	Raj Jain	Stefan Schlichting
Demetrio Bucaneg, Jr.	Martin Kasparick	Thomas Starai
Lyle G. Bullock, Jr.	Stuart Kerry	Mark-Rene Uchida
Craig Carlson	Edmund Kienast	John Vergis
Juan Carreon	Yongbum Kim	J. Wiley
Pin Chang	Raymond Krasinski	Yu Yuan
Malcolm Clarke	Javier Luiso	Oren Yuen
Christoph Fischer	H. Moll	Janusz Zalewski
David Fuschi	Nick S. A. Nikjoo	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	David J. Law	Mehmet Ulema
Doug Edwards	Howard Li	Lei Wang
J. Travis Griffith	Dong Liu	Sha Wei
Grace Gu	Kevin Lu	Philip B. Winston
Guido R. Hiertz	Paul Nikolich	Daidi Zhong
Joseph L. Koepfinger*	Damir Novosel	Jingyi Zhou
	Dorothy Stanley	

<https://standards.iteh.ai/catalog/standards/sist/e3e2b4fd-5a69-4611-87df-d93832f3a31b/iso-ieee-11073-40101-2022>

\*Member Emeritus

## Introduction

This introduction is not part of IEEE Std 11073-40101-2020, Health informatics—Device interoperability—Part 40101: Foundational—Cybersecurity—Processes for vulnerability assessment.

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 [B7]) 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 [B7]).
- *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 [B5]).<sup>1</sup>

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 process 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 an iterative, systematic, scalable, and auditable approach to identification of cybersecurity vulnerabilities and estimation of risk. This standard presents one approach to iterative vulnerability assessment that uses the Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege (STRIDE) classification scheme and the embedded Common Vulnerability Scoring System (eCVSS). The assessment includes system context, system decomposition, pre-mitigation scoring, mitigation, and post-mitigation scoring and iterates until the remaining vulnerabilities are reduced to an acceptable level of risk.

<sup>1</sup> 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. Definitions, acronyms, and abbreviations .....	13
2.1 Definitions .....	13
2.2 Acronyms and abbreviations .....	13
3. Risk management .....	13
4. Software of unknown provenance .....	14
5. Multi-component system vulnerability assessment .....	14
6. Threat modeling.....	14
6.1 General .....	14
6.2 Data flow diagram .....	15
6.3 STRIDE classification scheme .....	15
7. Scoring system .....	15
7.1 General .....	15
7.2 CVSS .....	15
7.3 eCVSS .....	16
8. Process for vulnerability assessment .....	17
8.1 Iterative vulnerability assessment .....	17
8.2 System context.....	17
8.3 System decomposition .....	20
8.4 Scoring.....	22
8.5 Mitigation .....	24
8.6 Iteration.....	24
Annex A (informative) Bibliography .....	25
Annex B (informative) STRIDE.....	26
Annex C (informative) embedded Common Vulnerability Scoring System .....	30
C.1 Overview.....	30
C.2 Scoring equations in pseudo code.....	35
C.3 Test vectors .....	36
Annex D (informative) Microsoft TMT2Excel Macro.....	37
Annex E (informative) Example insulin delivery device vulnerability assessment.....	40
E.1 General.....	40
E.2 System context .....	40
E.3 Threat model .....	41
E.4 Pre- and post-mitigation vulnerability assessment scores .....	42

## Health informatics—Device interoperability

# Part 40101: Foundational—Cybersecurity— Processes for vulnerability assessment

## 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 regulated PHDs/PoCDs are required to address cybersecurity vulnerabilities through a detailed risk analysis of use cases specific to the device. Of the various approaches to vulnerability assessment, some are not repeatable, scalable, systematic, and auditable. Both manufacturers and regulatory bodies may benefit from a common approach to vulnerability assessment based on threat modeling capable of analyzing PHDs/PoCDs across domains and described in a trusted open consensus standard. Likewise, patients, providers, and payers benefit from consistent and sufficient information provided in PHD/PoCD labeling.

This standard is based on the PHD Cybersecurity Standards Roadmap findings (IEEE white paper [B4]) and presents a repeatable, scalable, systematic, and auditable approach to vulnerability assessment.<sup>2</sup> While a specific approach is provided, any comparable approach is appropriate and will be compatible with the mitigations found in IEEE Std 11073-40102™ [B3]. In Figure 1, this standard is depicted by the top row, and IEEE Std 11073-40102 is depicted by the bottom row.

<sup>2</sup> The numbers in brackets correspond to the numbers of the bibliography in Annex A.