NORME INTERNATIONALE

ISO/IEEE 11073-40101

Première édition
2022-03

Informatique de santé — Interopérabilité des dispositifs —

Partie 40101 :

Fondamentaux — Cybersécurité — Processus pour l'évaluation de la vulnérabilité

Health informatics — Device interoperability — Part 40101: Foundational — Cybersecurity — Processes for vulnerability assessment

~~Numéro de référence ISO/IEEE 11073-~~

Numéro de référence
ISO/IEEE 11073-40101:2022(F)

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

E-mail : stds.ipr@ieee.org
Site Web : www.ieee.org

Publié en Suisse

Avant-propos

L'ISO (Organisation internationale de normalisation) est une fédération mondiale d'organismes nationaux de normalisation (comités membres de l'ISO). L'élaboration des Normes internationales est en général confiée aux comités techniques de l'ISO. Chaque comité membre intéressé par une étude a le droit de faire partie du comité technique créé à cet effet. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO participent également aux travaux. L'ISO collabore étroitement avec la Commission électrotechnique internationale (IEC) en ce qui concerne la normalisation électrotechnique.

Les procédures utilisées pour élaborer le présent document et celles destinées à sa mise à jour sont décrites dans les Directives ISO/IEC, Partie 1. Il convient, en particulier de prendre note des différents critères d'approbation requis pour les différents types de documents ISO (voir www.iso.org/directives).

Les documents normatifs de l'IEEE sont développés au sein des sociétés de l'IEEE et des Comités de Coordination des Normes du Conseil des Normes de l'Association des normes IEEE (IEEE-SA). L'IEEE développe ses normes par le biais d'un processus de développement de consensus, approuvé par l'Institut national américain de normalisation, qui rassemble des volontaires représentant divers points de vue et divers intérêts pour parvenir au produit final. Les volontaires ne sont pas nécessairement des membres de l'Institut et aucune compensation ne leur est attribuée pour leur participation. Bien que l'IEEE administre le processus et établisse des règles pour favoriser l'équité au cours du processus de développement du consensus, l'IEEE n'évalue pas, ne teste pas ou ne vérifie pas de manière indépendante l'exactitude des informations contenues dans ses normes.

L'attention est attirée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. L'ISO ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et averti de leur existence. Les détails concernant les références aux droits de propriété intellectuelle ou autres droits analogues identifiés lors de l'élaboration du document sont indiqués dans l'Introduction et/ou dans la liste des déclarations de brevets reçues par l'ISO (voir www.iso.org/brevets).

Les appellations commerciales éventuellement mentionnées dans le présent document sont données pour information, par souci de commodité, à l'intention des utilisateurs et ne sauraient constituer un engagement.

Pour une explication de la nature volontaire des normes, la signification des termes et expressions spécifiques de l'ISO liés à l'évaluation de la conformité, ou pour toute information au sujet de l'adhésion de l'ISO aux principes de l'Organisation mondiale du commerce (OMC) concernant les obstacles techniques au commerce (OTC), voir le lien suivant : www.iso.org/iso/fr/avant-propos.

L'ISO/IEEE 11073-40101 a été élaborée par le Comité des normes IEEE 11073 de la Société d'Ingénierie en Médecine et Biologie de l'IEEE (en tant que norme IEEE 11073-40101-2020) et rédigée conformément aux règles de rédaction de celui-ci. Elle a été adoptée dans le cadre de la « procédure rapide » définie par l'accord de coopération entre les Organisations Partenaires de Développement de Normes que sont l'ISO et l'IEEE, par le comité technique ISO/TC 215, *Informatique de santé*.

Une liste de toutes les parties de la série ISO/IEEE 11073 peut être consultée sur le site web de l'ISO.

Il convient que l'utilisateur adresse tout retour d'information ou toute question concernant le présent document à l'organisme national de normalisation de son pays. Une liste exhaustive desdits organismes se trouve à l'adresse www.iso.org/fr/members.html.

Informatique de santé — Interopérabilité des dispositifs

Fondamentaux — Cybersécurité — Processus pour l'évaluation de la vulnérabilité

Développée par le

Comité des normes IEEE 11073
de la
Société d'Ingénierie en Médecine et Biologie de l'IEEE

Approuvée le 24 septembre 2020

Conseil des Normes IEEE SA

Résumé : Pour les dispositifs de santé personnels (PHD) et les dispositifs sur les sites de soins (PoCD), la présente norme définit une approche itérative, systématique, évolutive et auditable de l'identification des vulnérabilités en matière de cybersécurité et l'estimation des risques. La norme présente une approche de l'évaluation itérative des vulnérabilités qui utilise le schéma de classification STRIDE (usurpation d'identité, falsification, répudiation, divulgation d'informations, déni de service, élévation du privilège) et le Système d'évaluation des vulnérabilités courantes intégré (eCVSS). L'évaluation comprend le contexte du système, la décomposition du système, la notation avant atténuation, l'atténuation et la notation après atténuation et se répète jusqu'à ce que les vulnérabilités restantes soient réduites à un niveau de risque acceptable.

Mots-clés : cybersécurité, Système d'évaluation des vulnérabilités courantes intégré, IEEE 11073-40101™, communication entre dispositifs médicaux, dispositifs de santé personnels, dispositifs sur les sites de soins, STRIDE, évaluation de la vulnérabilité

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

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

Notes et rejets de responsabilité importants concernant les documents normatifs de l'IEEE

Les documents normatifs de l'IEEE sont mis à disposition pour utilisation sous réserve de notes importantes et de rejets de responsabilité légale. Ces notes et rejets de responsabilité, ou la référence à cette page (https://standards.ieee.org/ipr/disclaimers.html), apparaissent dans toutes les normes et peuvent être trouvés sous le titre « Notes importantes et rejets de responsabilité concernant les documents normatifs de l'IEEE ».

Note et rejet de responsabilité concernant l'utilisation des documents de l'IEEE

Les documents normatifs de l'IEEE sont développés au sein des sociétés de l'IEEE et des Comités de Coordination des Normes du Conseil des Normes de l'Association des normes IEEE (IEEE-SA). L'IEEE développe ses normes par le biais d'un processus de développement de consensus accrédité qui rassemble des volontaires représentant divers points de vue et divers intérêts pour parvenir au produit final. Les normes IEEE sont des documents conçus par des volontaires dans le cadre de groupes de travail techniques avec une expertise scientifique, universitaire et technique du secteur d'activité concerné. Les volontaires ne sont pas nécessairement des membres de l'IEEE ou de l'IEEE-SA et aucune compensation ne leur est attribuée pour leur participation. Bien que l'IEEE administre le processus et établisse des règles pour favoriser l'équité au cours du processus de développement du consensus, l'IEEE n'évalue pas, ne soumet pas à essai ou ne vérifie pas de manière indépendante l'exactitude des informations, ni le bien-fondé de toutes les appréciations contenues dans ses normes.

L'IEEE ne donne aucune garantie ou représentation concernant ses normes, et rejette expressément toute garantie, qu'elle soit explicite ou implicite, concernant la présente norme, y compris, sans toutefois s'y limiter, les garanties de qualité marchande, d'adéquation à un usage particulier et d'absence de violation de droits de la propriété intellectuelle. En outre, l'IEEE ne garantit ni ne déclare que l'utilisation du matériel contenu dans ses normes est exempte de toute violation de brevet. Les documents normatifs de l'IEEE sont fournis « EN L'ÉTAT » et « AVEC TOUS LEURS DÉFAUTS ».

L'utilisation d'une norme IEEE est totalement volontaire. L'existence d'une norme IEEE n'implique pas qu'il n'y ait pas d'autres manières de produire, de soumettre à essai, de mesurer, d'acheter, de commercialiser ou de fournir d'autres biens et services qui se rapportent au domaine d'application de la norme IEEE. En outre, le point de vue exprimé à l'instant où une norme est approuvée et émise, est soumis aux changements induits par les développements techniques et les commentaires reçus des utilisateurs de la norme

En publiant ses normes et en les rendant disponibles, l'IEEE ne suggère pas, ni ne fournit de services professionnels ou autres à une personne ou une entité quelconque, ou en son nom. L'IEEE ne s'engage pas non plus à assumer une quelconque responsabilité de toute autre personne ou entité envers une autre. Il est recommandé à toute personne utilisant un document normatif de l'IEEE de se fier à son propre jugement indépendant dans l'exercice d'une diligence raisonnable dans toutes les circonstances données ou, le cas échéant, de demander conseil à un professionnel compétent pour déterminer la pertinence d'une norme IEEE donnée.

EN AUCUN CAS l'IEEE NE DOIT ÊTRE TENUE RESPONSABLE DE QUELCONQUES DOMMAGES DIRECTS, INDIRECTS, INCIDENTS, SPÉCIAUX, EXEMPLAIRES OU CONSÉCUTIFS (Y COMPRIS, MAIS NON LIMITÉ À : BESOIN DE SE PROCURER DES BIENS OU SERVICES DE REMPLACEMENT ; PERTE D'UTILISATION, DE DONNÉES OU DE PROFITS ; OU INTERRUPTION D'ACTIVITÉ), QUELLE QU'EN SOIT LA CAUSE ET QUELLE QUE SOIT LA THÉORIE DE LA RESPONSABILITÉ, QUE CE SOIT DANS LE CADRE D'UN CONTRAT, D'UNE RESPONSABILITÉ STRICTE OU D'UN DÉLIT (Y COMPRIS LA NÉGLIGENCE OU AUTRE), RÉSULTANT DE QUELQUE MANIÈRE QUE CE SOIT DE LA PUBLICATION, DE L'UTILISATION D'UNE NORME OU DE LA CONFIANCE ACCORDÉE À UNE NORME, MÊME EN CAS DE NOTIFICATION DE LA POSSIBILITÉ DE TELS DOMMAGES, ET INDÉPENDAMMENT DU FAIT QUE LE PRÉJUDICE ÉTAIT PRÉVISIBLE OU NON.

Traductions

Le processus de développement du consensus de l'IEEE implique l'examen de documents en anglais uniquement. Si une norme de l'IEEE est traduite, il convient que la seule la version anglaise publiée par l'IEEE soit la norme IEEE approuvée.

Déclarations officielles

Une déclaration, écrite ou orale, qui n'est pas traitée conformément au manuel des opérations du Conseil des Normes IEEE-SA, ne doit pas être considérée ou interprétée comme étant la position officielle de l'IEEE ou de l'un quelconque de ses comités et ne doit pas être considérée comme une position formelle de l'IEEE, ni être invoquée comme telle. Lors de conférences, de symposiums, de séminaires ou de cours de formation, une personne présentant des informations sur les normes de l'IEEE doit indiquer clairement qu'il convient que les opinions du présentateur soient considérées comme les opinions personnelles de cet individu et non comme la position officielle de l'IEEE, de l'IEEE-SA, du Comité de normalisation ou du Groupe de travail.

Commentaires relatifs aux normes

Toute partie intéressée, qu'elle soit ou non membre de l'IEEE ou de l'IEEE-SA, est invitée à émettre des commentaires en vue de la révision des documents normatifs de l'IEEE. Toutefois, l'**IEEE ne fournit pas d'interprétation, d'informations de consulting ou de conseils relatifs aux documents normatifs de l'IEEE.**

Il convient que les suggestions de modification à apporter aux documents se présentent sous la forme d'une proposition de modification du texte, accompagnée des commentaires d'appui appropriés. Comme les normes de l'IEEE représentent un consensus des intérêts concernés, il est important que toute réponse à des commentaires et questions reçoive également l'attention d'intérêts équilibrés. Pour cette raison, l'IEEE et les membres de ses sociétés et de ses Comités de Coordination des Normes ne peuvent pas fournir une réponse instantanée aux commentaires ou questions, excepté dans les cas où le sujet aurait été traité précédemment. Pour la même raison, l'IEEE ne répond pas aux demandes d'interprétation. Toute personne désireuse de participer à l'évaluation de commentaires ou de révisions d'une norme de l'IEEE est invitée à se joindre au groupe de travail approprié de l'IEEE. Vous pouvez manifester votre intérêt pour un groupe de travail dans l'onglet *Interests* de la zone *Manage Profile & Interests* de IEEE SA myProject system. Un compte IEEE est nécessaire pour accéder à l'application.

Il est recommandé d'adresser les commentaires sur les normes à l'aide du formulaire Contact Us

Lois et règlements

Il est recommandé aux utilisateurs des documents normatifs de l'IEEE de consulter toutes les lois et tous les règlements applicables. L'observance des dispositions d'un document normatif de l'IEEE, quel qu'il soit, ne vaut pas respect des exigences réglementaires applicables. Il incombe aux personnes ou organismes mettant en œuvre la norme d'observer les exigences réglementaires applicables ou d'y faire référence. L'IEEE n'a pas l'intention, du fait de la publication de ses normes, d'inciter à une action qui ne serait pas conforme aux lois applicables, et ces documents ne peuvent pas être interprétés comme le faisant.

Protection des données

Il convient que les utilisateurs des documents normatifs de l'IEEE évaluent les normes pour prendre en compte la protection et la propriété des données dans le contexte de l'évaluation et de l'utilisation des normes en conformité avec les lois et réglementations applicables.

Copyrights

Photocopies

Mise à jour de documents normatifs de l'IEEE

Il convient que les utilisateurs des documents normatifs de l'IEEE soient informés du fait que ces documents peuvent être remplacés à tout moment par la publication de nouvelles éditions ou peuvent être amendés de temps à autre par le biais de l'émission d'amendements, de correctifs ou d'errata. Un document IEEE officiel, à un instant quelconque, est constitué de l'édition actuelle du document accompagnée de tous les amendements, correctifs ou errata alors en vigueur.

Chaque Norme IEEE est soumise à un examen au moins tous les dix ans. Lorsqu'un document a plus de dix ans et qu'il n'a pas fait l'objet d'une révision, il est raisonnable de conclure que son contenu, bien qu'il ait encore une certaine valeur, ne reflète pas totalement l'état actuel de la technique. Les utilisateurs sont invités à s'assurer qu'ils disposent de la dernière édition des normes IEEE.

Pour déterminer si un document donné est l'édition actuelle et s'il a été amendé par le biais de l'émission d'amendements, de correctifs ou d'errata, il convient de visiter le site web IEEE Xplore à l'adresse IEEE Xplore ou contact IEEE. Pour plus d'informations sur l'IEEE Standards Association ou le processus de développement des normes IEEE, visiter le site web de l'IEEE SA.

Errata

Le cas échéant, les errata de toutes les normes IEEE sont accessibles sur le site Web de l'IEEE-SA (IEEE SA Website). Rechercher un numéro de norme et l'année d'approbation pour accéder à la page Web de la norme publiée. Les liens vers les errata se trouvent dans le paragraphe « Additional Resources Details ». Les errata sont également disponibles sur IEEE Xplore. Les utilisateurs sont encouragés à faire des vérifications régulières des errata.

Brevets

Les normes IEEE sont développées en conformité avec l'IEEE SA Patent Policy.

L'attention est attirée sur la possibilité que la mise en œuvre de la présente norme puisse requérir l'utilisation d'un objet couvert par des droits de propriété intellectuelle ou des droits analogues. Du fait de la publication de la présente norme, aucune position n'est adoptée par l'IEEE en ce qui concerne l'existence ou la validité de tout droit de propriété intellectuelle ou droit analogue en rapport avec celle-ci. Si le détenteur d'un brevet ou le demandeur d'un brevet a déposé une déclaration d'assurance par le biais d'une lettre d'assurance acceptée, alors la déclaration est incluse sur le site web de l'IEEE SA à l'adresse https://standards.ieee.org/about/sasb/patcom/patents.html. Les lettres d'assurance peuvent indiquer si le déposant accepte ou non d'accorder des licences dans le cadre de ces droits sans compensation ou avec des redevances raisonnables, avec des termes et conditions raisonnables dont il peut être démontré qu'elles sont exemptes de toute discrimination inéquitable pour les demandeurs désirant obtenir de telles licences.

D'autres revendications essentielles de brevets peuvent exister, pour lesquelles une déclaration d'assurance n'a pas été reçue. Il n'incombe pas à l'IEEE d'identifier les Essential Patent Claims (Revendications Essentielles de Brevets) pour lesquelles une licence peut être requise, de mener des enquêtes portant sur la validité légale ou la portée des revendications de brevet ou de déterminer si des termes ou conditions d'attribution de licence fournis en rapport avec la soumission d'une lettre d'assurance, s'il y en a, ou dans des accords d'attribution de licence quelconques sont raisonnables ou non discriminatoires. Les utilisateurs de la présente norme sont expressément avisés que la détermination de la validité de tout droit de brevet et le risque de violation de ces droits leur incombent entièrement. Des informations supplémentaires peuvent être obtenues auprès de l'Association des normes IEEE.

NOTE IMPORTANTE

Les normes IEEE ne garantissent ou n'assurent pas la sécurité, la sûreté, la santé ou la protection de l'environnement, ni n'assurent une protection contre toute interférence avec ou provenant d'autres dispositifs ou réseaux. Les activités de développement des normes IEEE prennent en compte la recherche et les informations présentées au groupe de développement des normes lors du développement de toute recommandation de sécurité. Les autres informations sur les pratiques relatives à la sécurité, aux modification de technologie ou mise en œuvre de technologie, ou aux impacts des systèmes périphériques, peuvent également être pertinentes pour les considérations de sécurité pendant la mise en œuvre de la norme. Il incombe aux personnes appliquant des documents normatifs de l'IEEE et à leurs utilisateurs de déterminer toutes les pratiques appropriées de protection concernant la sécurité, la sûreté, l'environnement, la santé et les interférences, ainsi que toutes les lois et réglementations applicables, et de s'y conformer.

Participants

Au moment où la présente norme a été soumise au Conseil des Normes IEEE SA pour approbation, le Groupe de travail Public Health Device comprenait les membres suivants :

Daidi Zhong, *Président*
Michael Kirwan et **Christoph Fischer**, *Vice-présidents*

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

La présente norme a été votée par les membres suivants du groupe de vote individuel. Les choix offerts aux votants étaient les suivants : approbation, désaccord ou 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
Edmund Kienast
Yongbum Kim
Raymond Krasinski
Javier Luiso
H. Moll
Nick S. A. Nikjoo
Bansi Patel
Dalibor Pokrajac
Beth Pumo
Stefan Schlichting
Thomas Starai
Mark-Rene Uchida
John Vergis
J. Wiley
Yu Yuan
Oren Yuen
Janusz Zalewski
Daidi Zhong

Lorsque le Conseil des normes IEEE SA a approuvé la présente norme le 24 septembre 2020, il comprenait les membres suivants :

Gary Hoffman, *Président*
Jon Walter Rosdahl, *Vice-président*
John D. Kulick, *Ancien président*
Konstantinos Karachalios, *Secrétaire*

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

*Membre émérite

Introduction

Cette introduction ne fait pas partie de la norme IEEE 11073-40101-2020, Informatique de santé — Interopérabilité des dispositifs — Partie 40101 : Fondamentaux — Cybersécurité — Processus pour l'évaluation de la vulnérabilité.

Les utilisateurs de dispositifs de santé personnels (PHD) et de dispositifs sur les sites de soins (PoCD) ont des attentes implicites en matière de commodité, de connectivité, d'accessibilité et de sécurité des données. Par exemple, ils s'attendent à pouvoir connecter les PHD/PoCD à leurs appareils mobiles et à leurs tableaux de bord, à visualiser les données dans le Cloud et à partager facilement les informations avec les cliniciens ou les prestataires de soins de santé. Dans certains cas, les utilisateurs eux-mêmes prennent des mesures pour établir des connexions entre les PHD/PoCD, les appareils mobiles et le Cloud afin de créer le système souhaité. Alors que de nombreux fabricants s'efforcent de résoudre les problèmes de connectivité des PHD/PoCD avec des solutions propriétaires, il n'existe aucune approche normalisée visant à fournir une interopérabilité sécurisée de type « prêt à l'emploi ».

La famille de normes ISO/IEEE 11073 relative aux PHD/PoCD, les profils et les spécifications de services du Bluetooth Special Interest Group et les directives de conception Continua (PCHAlliance [B7]) ont été élaborés pour traiter spécifiquement l'interopérabilité « prêt à l'emploi » des PHD/PoCD (par exemple, moniteur d'activité physique, moniteur physiologique, oxymètre de pouls, équipement de thérapie respiratoire de l'apnée du sommeil, ventilateur, dispositif d'administration d'insuline, pompe à perfusion, glucomètre continu). Dans ce contexte, les termes suivants ont des significations spécifiques :

— L'*interopérabilité* est la capacité des composants clients à communiquer et à partager des données avec des composants de service de manière univoque et prévisible, ainsi qu'à comprendre et à utiliser les informations échangées (PCHAlliance [B7]).
— *Prêt à l'emploi* signifie que tout ce que l'utilisateur a à faire est d'établir la connexion — le système détecte, configure et communique automatiquement sans aucune autre interaction humaine (ISO/IEEE 11073-10201 [B5]).[1]

Dans le contexte de l'interopérabilité *sécurisée* de type prêt à l'emploi, la cybersécurité est le processus et la capacité d'empêcher l'accès ou la modification non autorisés, l'utilisation abusive, le déni d'utilisation ou l'utilisation non autorisée des informations qui sont stockées sur un PHD/PoCD, accessibles depuis celui-ci ou transférées vers et depuis celui-ci. La présente norme décrit la partie processus de la cybersécurité pour les applications indépendantes du moyen de transport et les profils d'information des PHD/PoCD. Ces profils définissent l'échange de données, la représentation des données et la terminologie employée pour la communication entre les agents (par exemple, oxymètres de pouls, équipement de thérapie respiratoire de l'apnée du sommeil) et les dispositifs connectés (par exemple, appareils de santé, terminaux numériques, téléphones portables, ordinateurs personnels, cockpits de surveillance, tableaux de bord de soins intensifs).

Pour les PHD/PoCD, la présente norme définit une approche itérative, systématique, évolutive et auditable de l'identification des vulnérabilités en matière de cybersécurité et l'estimation des risques. Cette norme présente une approche de l'évaluation itérative des vulnérabilités qui utilise le schéma de classification STRIDE (usurpation d'identité, falsification, répudiation, divulgation d'informations, déni de service, élévation du privilège) et le Système d'évaluation des vulnérabilités courantes intégré (eCVSS). L'évaluation comprend le contexte du système, la décomposition du système, la notation avant atténuation, l'atténuation et la notation après atténuation et se répète jusqu'à ce que les vulnérabilités restantes soient réduites à un niveau de risque acceptable.

[1] Les références numérotées entre crochets correspondent à celles indiquées dans la bibliographie de l'Annexe A.

Sommaire