EESTI STANDARD EVS-EN ISO/IEEE 11073-40102:2022

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

EESTI STANDARDI EESSÕNA

NATIONAL FOREWORD

See Eesti standard EVS-EN ISO/IEEE 11073-40102:2022 sisaldab Euroopa standardi EN ISO/IEEE 11073- 40102:2022 ingliskeelset teksti.	This Estonian standard EVS-EN ISO/IEEE 11073-40102:2022 consists of the English text of the European standard EN ISO/IEEE 11073-40102:2022.
Standard on jõustunud sellekohase teate avaldamisega EVS Teatajas.	This standard has been endorsed with a notification published in the official bulletin of the Estonian Centre for Standardisation and Accreditation.
Euroopa standardimisorganisatsioonid on teinud Euroopa standardi rahvuslikele liikmetele kättesaadavaks 30.03.2022.	Date of Availability of the European standard is 30.03.2022.
Standard on kättesaadav Eesti Standardimis- ja Akrediteerimiskeskusest.	The standard is available from the Estonian Centre for Standardisation and Accreditation.

Tagasisidet standardi sisu kohta on võimalik edastada, kasutades EVS-i veebilehel asuvat tagasiside vormi või saates e-kirja meiliaadressile standardiosakond@evs.ee.

ICS 75.200

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN ISO/IEEE 11073-40102

March 2022

ICS 35.240.80

English Version

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

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

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

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

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

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

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

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

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

Ref. No. EN ISO/IEEE 11073-40102:2022 E

European foreword

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

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

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

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

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

Endorsement notice

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

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.

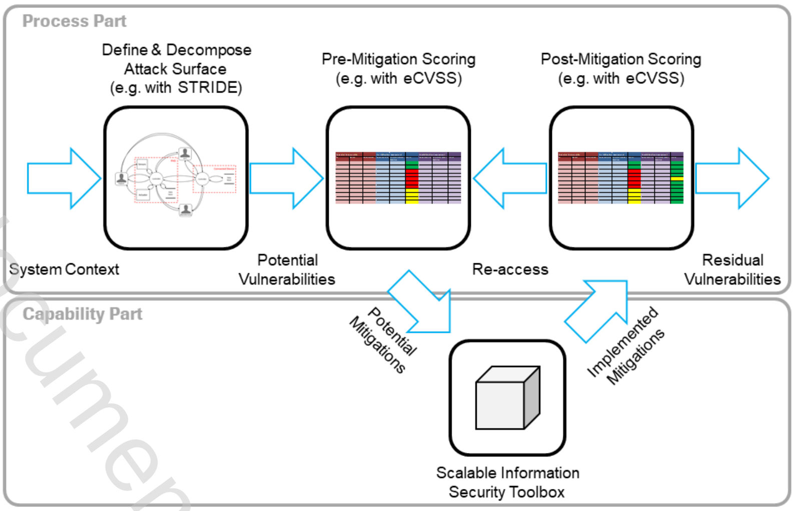
Process Part
Define & Decompose Attack Surface (e.g. with STRIDE)
Pre-Mitigation Scoring (e.g. with eCVSS)
Post-Mitigation Scoring (e.g. with eCVSS)
System Context
Potential Vulnerabilities
Re-access
Residual Vulnerabilities
Capability Part
Potential Mitigations
Implemented Mitigations
Scalable Information Security Toolbox

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.