Health informatics - Device interoperability - Part 40101: Foundational - Cybersecurity - Processes for vulnerability assessment (ISO/IEEE 11073- 40101:2022)

EESTI STANDARDI EESSÕNA

NATIONAL FOREWORD

See Eesti standard EVS-EN ISO/IEEE 11073-40101:2022 sisaldab Euroopa standardi EN ISO/IEEE 11073- 40101:2022 ingliskeelset teksti.	This Estonian standard EVS-EN ISO/IEEE 11073-40101:2022 consists of the English text of the European standard EN ISO/IEEE 11073-40101:2022.
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 11073-40101

March 2022

ICS 35.240.80

English Version

Health informatics - Device interoperability - Part 40101: Foundational - Cybersecurity - Processes for vulnerability assessment (ISO/IEEE 11073-40101:2022)

Informatique de santé - Interopérabilité des dispositifs - Partie 40101: Fondamentaux - Cybersécurité - Processus pour l'évaluation de la vulnérabilité (ISO/IEEE 11073-40101:2022)

Medizinische Informatik - Geräteinteroperabilität - Teil 40101: Grundlagen - Cybersicherheit - Prozess zur Schwachstellenanalyse (ISO/IEEE 11073-40101:2022)

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 11073-40101:2022 E

European foreword

This document (EN ISO/IEEE 11073-40101:2022) 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 11073-40101:2022 has been approved by CEN as EN ISO/IEEE 11073-40101:2022 without any modification.

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]).[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 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.

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

Contents

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.[2] 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.

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

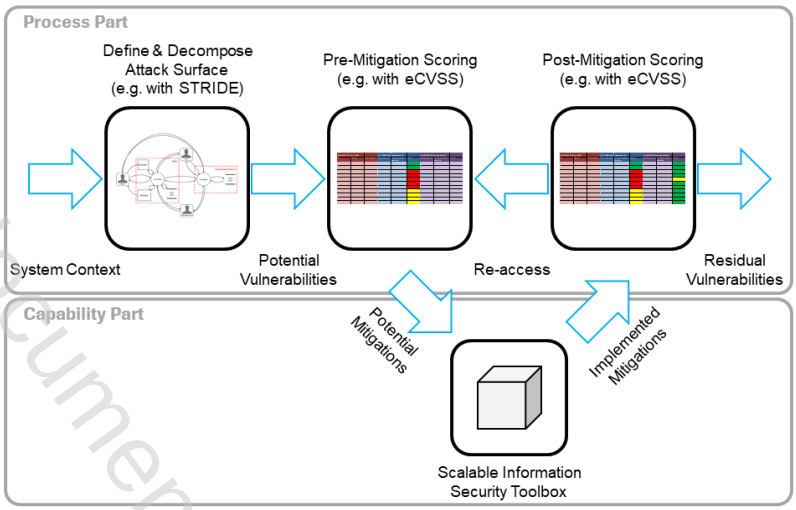

Figure 1—Vulnerability assessment workflow

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 process part of cybersecurity is risk analysis of use cases specific to a PHD/PoCD.

For PHDs/PoCDs, this standard defines an iterative, systematic, scalable, and auditable approach to identification of cybersecurity vulnerabilities and estimation of risk. This iterative vulnerability assessment 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.

1.3 Purpose

The purpose of this document is to define a common approach to cybersecurity assessment in PHDs/PoCDs and define an iterative, systematic, scalable, and auditable vulnerability assessment appropriate for use in the design of PHDs/PoCDs.

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]

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*).

[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 *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. Definitions, acronyms, and abbreviations

2.1 Definitions

For the purposes of this document, the terms and definitions provided in the PHD Cybersecurity Standards Roadmap (IEEE white paper [B4]) apply. The *IEEE Standards Dictionary Online* should be consulted for terms not defined there.[5]

2.2 Acronyms and abbreviations

CRUD	create, read, update, and delete
CVSS	Common Vulnerability Scoring System
DFD	data flow diagram
eCVSS	embedded Common Vulnerability Scoring System
HCP	Health Care Provider
PHD	Personal Health Device
PoCD	Point-of-Care Device
STRIDE	Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privileges
TMT	Threat Modeling Tool
UML	Unified Modeling Language

3. Risk management

Various regulations, standards, and guidelines address the subject of risk and risk management. In some cases, the application of specific standards may be mandated by regulations, contracts, or customer expectations. This standard does not define a specific risk management process as appropriate for all manufacturers because each manufacturer's risk management process needs to comply with the regulations, standards, contracts for the specific disease domain, and the jurisdiction in which the device is marketed.

Instead, this standard presents a repeatable, scalable, systematic, and auditable approach to vulnerability assessment that is adaptable to various mandates and can be used within a PHD/PoCD risk management process when evaluating PHD/PoCD communication. The assessment identifies and prioritizes vulnerabilities based on device use cases and, through iteration, helps to minimize reasonably foreseeable risks associated with PHD/PoCD communication to an acceptable level. It is the responsibility of the manufacturer's management to define the appropriate acceptable level. In the PHD/PoCD domain, there are fitness devices with low information security concerns and disease management devices with higher information security concerns. Therefore, the risk management process is based on the device's intended use cases within a specific domain, which represent a wide variance where high-risk PHDs/PoCDs represent the upper limit. As such, the risk evaluation of a PHD/PoCD with fewer information security concerns may identify only a subset of vulnerabilities.

[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.