SLOVENSKI STANDARD
SIST EN IEC 81001-5-1:2022

01-april-2022

Programska oprema ter varnost, učinkovitost in zaščita informacijskih sistemov v zdravstvu - 5-1. del: Varnost - Dejavnosti življenjskega cikla izdelka (IEC 81001-5-1:2021)

Health software and health IT systems safety, effectiveness and security - Part 5-1: Security - Activities in the product life cycle (IEC 81001-5-1:2021)

Gesundheitssoftware und Gesundheits-IT-Systeme Sicherheit, Effektivität und Security - Teil 5-1: Security - Aktivitäten im Produktlebenszyklus (IEC 81001-5-1:2021)

Logiciels de santé et sécurité, efficacité et sûreté des systèmes TI de santé - Partie 5-1 : Sûreté - Activités du cycle de vie du produit (IEC 81001-5-1:2021)

Ta slovenski standard je istoveten z: EN IEC 81001-5-1:2022

ICS:

11.040.01	Medicinska oprema na splošno	Medical equipment in general
35.030	Informacijska varnost	IT Security
35.240.80	Uporabniške rešitve IT v zdravstveni tehniki	IT applications in health care technology

SIST EN IEC 81001-5-1:2022 **en**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN IEC 81001-5-1

February 2022

ICS 11.040.01; 35.240.80

English Version

Health software and health IT systems safety, effectiveness and security - Part 5-1: Security - Activities in the product life cycle (IEC 81001-5-1:2021)

Logiciels de santé et sécurité, efficacité et sûreté des systèmes TI de santé - Partie 5-1 : Sûreté - Activités du cycle de vie du produit (IEC 81001-5-1:2021)

Gesundheitssoftware und Gesundheits-IT-Systeme Sicherheit, Effektivität und Security - Teil 5-1: Security - Aktivitäten im Produktlebenszyklus (IEC 81001-5-1:2021)

This European Standard was approved by CENELEC on 2022-01-20. CENELEC 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 CENELEC 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 CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

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

European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

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

Ref. No. EN IEC 81001-5-1:2022 E

European foreword

The text of document 62A/1458/FDIS, future edition 1 of IEC 81001-5-1, prepared by SC 62A "Common aspects of electrical equipment used in medical practice" of IEC/TC 62 "Electrical equipment in medical practice" was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN IEC 81001-5-1:2022.

The following dates are fixed:

- latest date by which the document has to be implemented at national level by publication of an identical national standard or by endorsement (dop) 2022-10-20
- latest date by which the national standards conflicting with the document have to be withdrawn (dow) 2025-01-20

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CENELEC 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 committee. A complete listing of these bodies can be found on the CENELEC website.

Endorsement notice

The text of the International Standard IEC 81001-5-1:2021 was approved by CENELEC as a European Standard without any modification.

In the official version, for Bibliography, the following notes have to be added for the standards indicated:

IEC 62304:2006	NOTE Harmonized as EN 62304:2006 (not modified)
IEC 62443-3-2	NOTE Harmonized as EN IEC 62443-3-2
IEC 62443-3-3	NOTE Harmonized as EN IEC 62443-3-3
IEC 62443-4-1:2018	NOTE Harmonized as EN IEC 62443-4-1:2018 (not modified)
IEC 62443-4-2:2019	NOTE Harmonized as EN IEC 62443-4-2:2019 (not modified)
IEC 62740:2015	NOTE Harmonized as EN 62740:2015 (not modified)
IEC 82304-1:2016	NOTE Harmonized as EN 82304-1:2017 (not modified)
ISO/TS 14441	NOTE Harmonized as CEN ISO/TS 14441
ISO 14971:2019	NOTE Harmonized as EN ISO 14971:2019 (not modified) +A11:2021
ISO/IEC 27000:2018	NOTE Harmonized as EN ISO/IEC 27000:2020 (not modified)
ISO 27789	NOTE Harmonized as EN ISO 27789
ISO 27799	NOTE Harmonized as EN ISO 27799
ISO/IEC 29147	NOTE Harmonized as EN ISO/IEC 29147
ISO/IEC 30111	NOTE Harmonized as EN ISO/IEC 30111

ISO 13485:2016	NOTE Harmonized as EN ISO 13485:2016 (not modified) +A11:2021
IEC 62366-1:2015	NOTE Harmonized as EN 62366-1:2015 (not modified)
IEC/TR 63069	NOTE Harmonized as CLC IEC/TR 63069
ISO 9000:2015	NOTE Harmonized as EN ISO 9000:2015 (not modified)

IEC 81001-5-1

Edition 1.0 2021-12

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Health software and health IT systems safety, effectiveness and security – Part 5-1: Security – Activities in the product life cycle

Logiciels de santé et sécurité, efficacité et sûreté des systèmes TI de santé – Partie 5-1: Sûreté – Activités du cycle de vie du produit

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

ICS 11.040.01; 35.240.80

ISBN 978-2-8322-1053-7

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

____

HEALTH SOFTWARE AND HEALTH IT SYSTEMS SAFETY, EFFECTIVENESS AND SECURITY –

Part 5-1: Security – Activities in the product life cycle

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 81001-5-1 has been prepared by a Joint Working Group of IEC subcommittee 62A: Common aspects of electrical equipment used in medical practice, of IEC technical committee 62: Electrical equipment in medical practice, and ISO technical committee 215: Health informatics.

It is published as a double logo standard.

The text of this document is based on the following documents:

Draft	Report on voting
62A/1458/FDIS	62A/1466/RVD

Full information on the voting for its approval can be found in the report on voting indicated in the above table.

The language used for the development of this International Standard is English.

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1 and ISO/IEC Directives, IEC Supplement, available at www.iec.ch/members_experts/refdocs. The main document types developed by IEC are described in greater detail at www.iec.ch/standardsdev/publications.

In this document, the following print types are used:

– requirements and definitions: roman type;

– informative material appearing outside of tables, such as notes, examples and references: in smaller type. Normative text of tables is also in a smaller type;

– TERMS DEFINED IN CLAUSE 3 OF THE GENERAL STANDARD, IN THIS PARTICULAR STANDARD OR AS NOTED: SMALL CAPITALS.

A list of all parts in the IEC 81001 series, published under the general title *Health software and health IT systems safety, effectiveness and security*, can be found on the IEC website.

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under webstore.iec.ch in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

IMPORTANT – The "colour inside" logo on the cover page of this document indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

0.1 Structure

PROCESS standards for HEALTH SOFTWARE provide a specification of ACTIVITIES that will be performed by the MANUFACTURER – including software incorporated in medical devices –as a part of a development LIFE CYCLE. The normative clauses of this document are intended to provide minimum best practices for a secure software LIFE CYCLE. Local legislation and regulation are considered.

PROCESS requirements (Clause 4 through Clause 9) have been derived from the IEC 62443-4-1[11][1] PRODUCT LIFE CYCLE management. Implementations of these specifications can extend existing PROCESSES at the MANUFACTURER's organization – notably existing PROCESSES conforming to IEC 62304[8]. This document can therefore support conformance to IEC 62443-4-1[11].

Normative clauses of this document specify ACTIVITIES that are the responsibility of the MANUFACTURER. The HEALTH SOFTWARE LIFE CYCLE can be part of an incorporating PRODUCT project. Some ACTIVITIES specified in this document depend on input and support from the PRODUCT LIFE CYCLE (for example to define specific criteria). Examples include:

- RISK MANAGEMENT;
- requirements;
- testing;
- post-release (after first placing HEALTH SOFTWARE on the market).

In cases where ACTIVITIES for HEALTH SOFTWARE need support from PROCESSES at the PRODUCT level, Clause 4 through Clause 9 of this document specify respective requirements beyond the HEALTH SOFTWARE LIFE CYCLE.

Similar to IEC 62304[8], this document does not prescribe a specific system of PROCESSES, but Clause 4 through Clause 9 of this document specify ACTIVITIES that are performed during the HEALTH SOFTWARE LIFE CYCLE.

Clause 4 specifies that MANUFACTURERS develop and maintain HEALTH SOFTWARE within a quality management system (see 4.1) and a RISK MANAGEMENT SYSTEM (4.2).

Clause 5 through Clause 8 specify ACTIVITIES and resulting output as part of the software LIFE CYCLE PROCESS implemented by the MANUFACTURER. These specifications are arranged in the ordering of IEC 62304[8].

Clause 9 specifies ACTIVITIES and resulting output as part of the problem resolution PROCESS implemented by the MANUFACTURER.

The scope of this document is limited to HEALTH SOFTWARE and its connectivity to its INTENDED ENVIRONMENT OF USE, based on IEC 62304[8], but with emphasis on CYBERSECURITY.

For expression of provisions in this document,

– "can" is used to describe a possibility or capability; and
– "must" is used to express an external constraint.

[1] Numbers in square brackets refer to the Bibliography.

NOTE HEALTH SOFTWARE can be placed on the market as software, as part of a medical device, as part of hardware specifically intended for health use, as a medical device (SaMD), or as a PRODUCT for other health use. (See Figure 2).

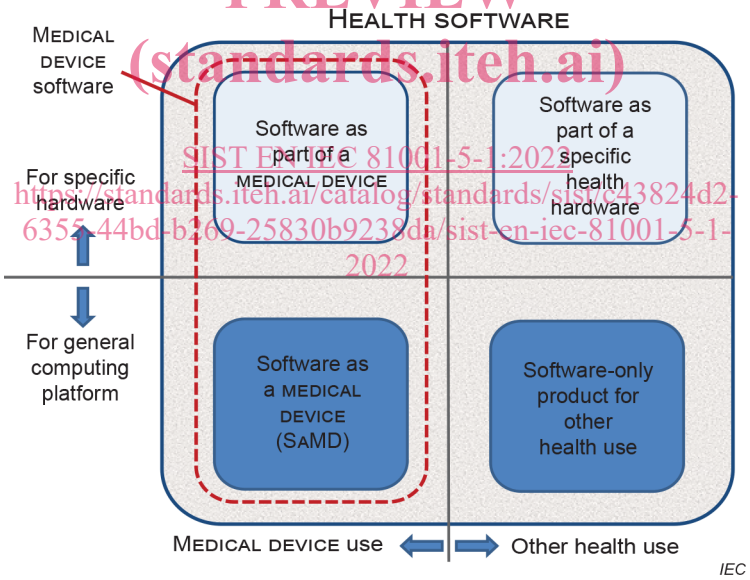
0.2 Field of application

This document applies to the development and maintenance of HEALTH SOFTWARE by a MANUFACTURER, but recognizes the critical importance of bi-lateral communication with organizations (e.g. HEALTHCARE DELIVERY ORGANIZATIONS, HDOs) who have SECURITY responsibilities for the HEALTH SOFTWARE and the systems it is incorporated into, once the software has been developed and released. The ISO/IEC 81001-5 series of standards (for which this is part -1), is therefore being designed to include future parts addressing SECURITY that apply to the implementation, operations and use phases of the LIFE CYCLE for organizations such as HDOs.

A medical device software is a subset of HEALTH SOFTWARE. A practical Venn diagram of HEALTH SOFTWARE types is shown in Figure 1. Therefore, this document applies to:

– software as part of a medical device;
– software as part of hardware specifically intended for health use;
– software as a medical device (SaMD); and
– software-only PRODUCT for other health use.

NOTE In this document, the scope of software considered part of the LIFE CYCLE ACTIVITIES for secure HEALTH SOFTWARE is larger and includes more software (drivers, platforms, operating systems) than for SAFETY, because for SECURITY the focus will be on any use including foreseeable unauthorized access rather than just the INTENDED USE.



[SOURCE: IEC 82304-1[18]]

Figure 1 – HEALTH SOFTWARE field of application

0.3 Conformance

Conformance with this document focuses on the implementation of requirements regarding PROCESSES, ACTIVITIES, and TASKS – and can be claimed in one of two alternative ways:

- for HEALTH SOFTWARE by implementing requirements in Clause 4 through Clause 9 of this document,
- for TRANSITIONAL HEALTH SOFTWARE by only implementing the PROCESSES, ACTIVITIES, and TASKS identified in Annex F.

This document is designed to assist in the implementation of the PROCESSES required by IEC 62443-4-1, however, conformance to this document is not necessarily a sufficient condition for conformance to IEC 62443-4-1[11]. More guidance on coverage can be found in Annex D.

MANUFACTURERS can implement the specifications for Annex E in order to achieve conformance of documentation to IEC 62443-4-1[11].

Clause 4 through Clause 9 of this document require establishing one or more PROCESSES that include identified ACTIVITIES. Per these normative parts of this document, the LIFE CYCLE PROCESSES implement these ACTIVITIES. None of the requirements in this document requires to implement these ACTIVITIES as one single PROCESS or as separate PROCESSES. The ACTIVITIES specified in this document will typically be part of an existing LIFE CYCLE PROCESS.