

© Copyright SEK Svensk Elstandard. Reproduction in any form without permission is prohibited.

Säkerhet, effektivitet och IT-säkerhet hos IT-system och programvara för hälsoapplikationer – Del 5-1: IT-säkerhet – Aktiviteter i produktens livscykel

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

Som svensk standard gäller europastandarden EN IEC 81001-5-1:2022. Den svenska standarden innehåller den officiella engelska språkversionen av EN IEC 81001-5-1:2022.

Nationellt förord

Europastandarden EN IEC 81001-5-1:2022

består av:

- **europastandardens ikraftsättningsdokument**, utarbetat inom CENELEC
- **IEC 81001-5-1, First edition, 2021 - Health software and health IT systems safety, effectiveness and security - Part 5-1: Security - Activities in the product life cycle**

utarbetad inom International Electrotechnical Commission, IEC.

ICS 11.040.01; 35.240.80

Denna standard är fastställd av SEK Svensk Elstandard, som också kan lämna upplysningar om **sakinnehållet** i standarden.
Postadress: Box 1284, 164 29 KISTA
Telefon: 08 - 444 14 00.
E-post: sek@elstandard.se. Internet: www.elstandard.se

Standarder underlättar utvecklingen och höjer elsäkerheten

Det finns många fördelar med att ha gemensamma tekniska regler för bl a mätning, säkerhet och provning och för utförande, skötsel och dokumentation av elprodukter och elanläggningar.

Genom att utforma sådana standarder blir säkerhetsfordringar tydliga och utvecklingskostnaderna rimliga samtidigt som marknadens acceptans för produkten eller tjänsten ökar.

Många standarder inom elområdet beskriver tekniska lösningar och metoder som åstadkommer den elsäkerhet som föreskrivs av svenska myndigheter och av EU.

SEK är Sveriges röst i standardiseringsarbetet inom elområdet

SEK Svensk Elstandard svarar för standardiseringen inom elområdet i Sverige och samordnar svensk medverkan i internationell och europeisk standardisering. SEK är en ideell organisation med frivilligt deltagande från svenska myndigheter, företag och organisationer som vill medverka till och påverka utformningen av tekniska regler inom elektrotekniken.

SEK samordnar svenska intressenters medverkan i SEKs tekniska kommittéer och stödjer svenska experters medverkan i internationella och europeiska projekt.

Stora delar av arbetet sker internationellt

Utformningen av standarder sker i allt väsentligt i internationellt och europeiskt samarbete. SEK är svensk nationalkommitté av International Electrotechnical Commission (IEC) och Comité Européen de Normalisation Electrotechnique (CENELEC).

Standardiseringsarbetet inom SEK är organiserat i referensgrupper bestående av ett antal tekniska kommittéer som speglar hur arbetet inom IEC och CENELEC är organiserat.

Arbetet i de tekniska kommittéerna är öppet för alla svenska organisationer, företag, institutioner, myndigheter och statliga verk. Den årliga avgiften för deltagandet och intäkter från försäljning finansierar SEKs standardiseringsverksamhet och medlemsavgift till IEC och CENELEC.

Var med och påverka!

Den som deltar i SEKs tekniska kommittéarbete har möjlighet att påverka framtida standarder och får tidig tillgång till information och dokumentation om utvecklingen inom sitt teknikområde. Arbetet och kontakterna med kollegor, kunder och konkurrenter kan gynnsamt påverka enskilda företags affärsutveckling och bidrar till deltagarnas egen kompetensutveckling.

Du som vill dra nytta av dessa möjligheter är välkommen att kontakta SEKs kansli för mer information.

SEK Svensk Elstandard

Box 1284
164 29 Kista
Tel 08-444 14 00
www.elstandard.se

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

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

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



**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

**Warning! Make sure that you obtained this publication from an authorized distributor.
Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.**

CONTENTS

FOREWORD.....	5
INTRODUCTION.....	7
0.1 Structure.....	7
0.2 Field of application.....	8
0.3 Conformance	8
1 Scope.....	10
2 Normative references	10
3 Terms and definitions	11
4 General requirements	18
4.1 Quality management.....	18
4.1.1 Quality management system.....	18
4.1.2 Identification of responsibilities.....	18
4.1.3 Identification of applicability.....	18
4.1.4 SECURITY expertise	18
4.1.5 SOFTWARE ITEMS from third-party suppliers.....	19
4.1.6 Continuous improvement	19
4.1.7 Disclosing SECURITY-related issues	19
4.1.8 Periodic review of SECURITY defect management	19
4.1.9 ACCOMPANYING DOCUMENTATION review	20
4.2 SECURITY RISK MANAGEMENT	20
4.3 SOFTWARE ITEM classification relating to risk transfer.....	20
5 Software development PROCESS.....	21
5.1 Software development planning	21
5.1.1 ACTIVITIES in the LIFE CYCLE PROCESS	21
5.1.2 Development environment SECURITY	21
5.1.3 Secure coding standards	21
5.2 HEALTH SOFTWARE requirements analysis	21
5.2.1 HEALTH SOFTWARE SECURITY requirements.....	21
5.2.2 SECURITY requirements review.....	22
5.2.3 SECURITY risks for REQUIRED SOFTWARE	22
5.3 Software architectural design.....	22
5.3.1 DEFENSE-IN-DEPTH ARCHITECTURE/design.....	22
5.3.2 Secure design best practices	22
5.3.3 SECURITY architectural design review.....	23
5.4 Software design	23
5.4.1 Software design best practices	23
5.4.2 Secure design	23
5.4.3 Secure HEALTH SOFTWARE interfaces	23
5.4.4 Detailed design VERIFICATION for SECURITY	24
5.5 Software unit implementation and VERIFICATION.....	24
5.5.1 Secure coding standards	24
5.5.2 SECURITY implementation review.....	24
5.6 Software integration testing	25
5.7 Software system testing	25
5.7.1 SECURITY requirements testing.....	25
5.7.2 THREAT mitigation testing.....	25

5.7.3	VULNERABILITY testing	25
5.7.4	Penetration testing	26
5.7.5	Managing conflicts of interest between testers and developers	26
5.8	Software release	26
5.8.1	Resolve findings prior to release	26
5.8.2	Release documentation	27
5.8.3	File INTEGRITY	27
5.8.4	Controls for private keys	27
5.8.5	Assessing and addressing SECURITY-related issues	27
5.8.6	ACTIVITY completion	27
5.8.7	SECURE decommissioning guidelines for HEALTH SOFTWARE	27
6	SOFTWARE MAINTENANCE PROCESS	28
6.1	Establish SOFTWARE MAINTENANCE plan	28
6.1.1	Timely delivery of SECURITY updates	28
6.2	Problem and modification analysis	28
6.2.1	Monitoring public incident reports	28
6.2.2	SECURITY update VERIFICATION	28
6.3	Modification implementation	29
6.3.1	SUPPORTED SOFTWARE SECURITY update documentation	29
6.3.2	MAINTAINED SOFTWARE SECURITY update delivery	29
6.3.3	MAINTAINED SOFTWARE SECURITY update INTEGRITY	29
7	SECURITY RISK MANAGEMENT PROCESS	29
7.1	RISK MANAGEMENT context	29
7.1.1	General	29
7.1.2	PRODUCT SECURITY CONTEXT	29
7.2	Identification of VULNERABILITIES, THREATS and associated adverse impacts	30
7.3	Estimation and evaluation of SECURITY risk	31
7.4	Controlling SECURITY risks	31
7.5	Monitoring the effectiveness of RISK CONTROLS	31
8	Software CONFIGURATION MANAGEMENT PROCESS	32
9	Software problem resolution PROCESS	32
9.1	Overview	32
9.2	Receiving notifications about VULNERABILITIES	32
9.3	Reviewing VULNERABILITIES	32
9.4	Analysing VULNERABILITIES	33
9.5	Addressing SECURITY-related issues	33
Annex A (informative)	Rationale	35
A.1	Relationship to IEC 62443	35
A.2	Relationship to IEC 62304	36
A.3	Risk transfer	37
A.3.1	Overview	37
A.3.2	MAINTAINED SOFTWARE	37
A.3.3	SUPPORTED SOFTWARE	37
A.3.4	REQUIRED SOFTWARE	37
A.4	Secure coding best practices	38
Annex B (informative)	Guidance on implementation of SECURITY LIFE CYCLE ACTIVITIES	39
B.1	Overview	39
B.2	Related work	39

B.3	THREAT / RISK ANALYSIS	39
B.4	THREAT and RISK MANAGEMENT.....	40
B.5	Software development planning	40
B.5.1	Development	40
B.5.2	HEALTH SOFTWARE requirements analysis	41
B.5.3	Software architectural design.....	41
B.5.4	Software unit implementation and VERIFICATION	41
B.5.5	Secure implementation	42
B.5.6	Not used.....	42
B.5.7	Software system testing.....	42
Annex C (informative)	THREAT MODELLING.....	44
C.1	General.....	44
C.2	ATTACK-defense trees	44
C.3	CAPEC / OWASP / SANS	44
C.4	CWSS.....	44
C.5	DREAD	45
C.6	List known potential VULNERABILITIES	45
C.7	OCTAVE	45
C.8	STRIDE	45
C.9	Trike	45
C.10	VAST	45
Annex D (informative)	Relation to practices in IEC 62443-4-1:2018	46
D.1	IEC 81001-5-1 to IEC 62443-4-1:2018	46
D.2	IEC 62443-4-1:2018 to IEC 81001-5-1	47
Annex E (informative)	Documents specified in IEC 62443-4-1	48
E.1	Overview.....	48
E.2	Release documentation.....	48
E.2.1	PRODUCT documentation	48
E.2.2	HEALTH SOFTWARE DEFENSE-IN-DEPTH documentation.....	49
E.2.3	DEFENSE-IN-DEPTH measures expected in the environment.....	49
E.2.4	SECURITY hardening guidelines	49
E.2.5	SECURITY update information	50
E.3	Documents for decommissioning HEALTH SOFTWARE	50
Annex F (normative)	TRANSITIONAL HEALTH SOFTWARE.....	51
F.1	Overview.....	51
F.2	Development assessment and gap closure activities	51
F.3	Rationale for use of TRANSITIONAL HEALTH SOFTWARE	52
F.4	Post-release ACTIVITIES	52
Annex G (normative)	Object identifiers.....	53
Bibliography	54
Figure 1	– HEALTH SOFTWARE field of application	8
Figure 2	– HEALTH SOFTWARE LIFE CYCLE PROCESSES.....	10
Table A.1	– Required level of independence of testers from developers.....	36
Table G.1	– Object identifiers for conformance concepts of this document.....	53

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).

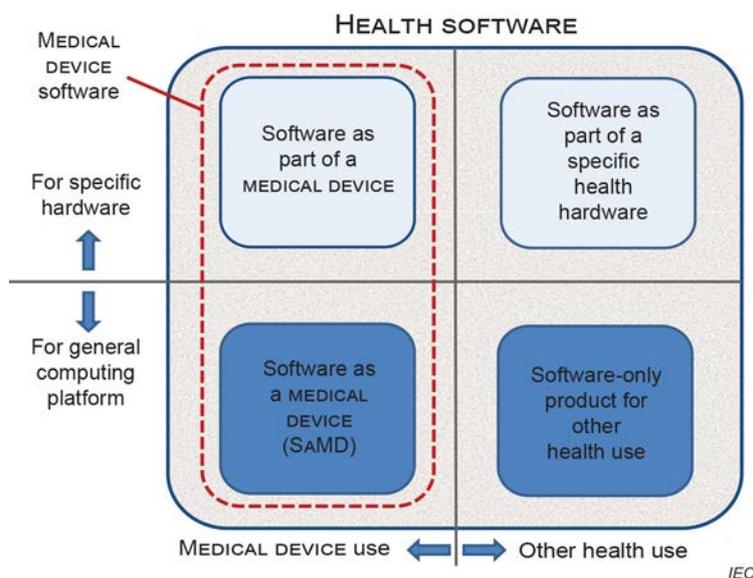
0.2 Field of application

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].

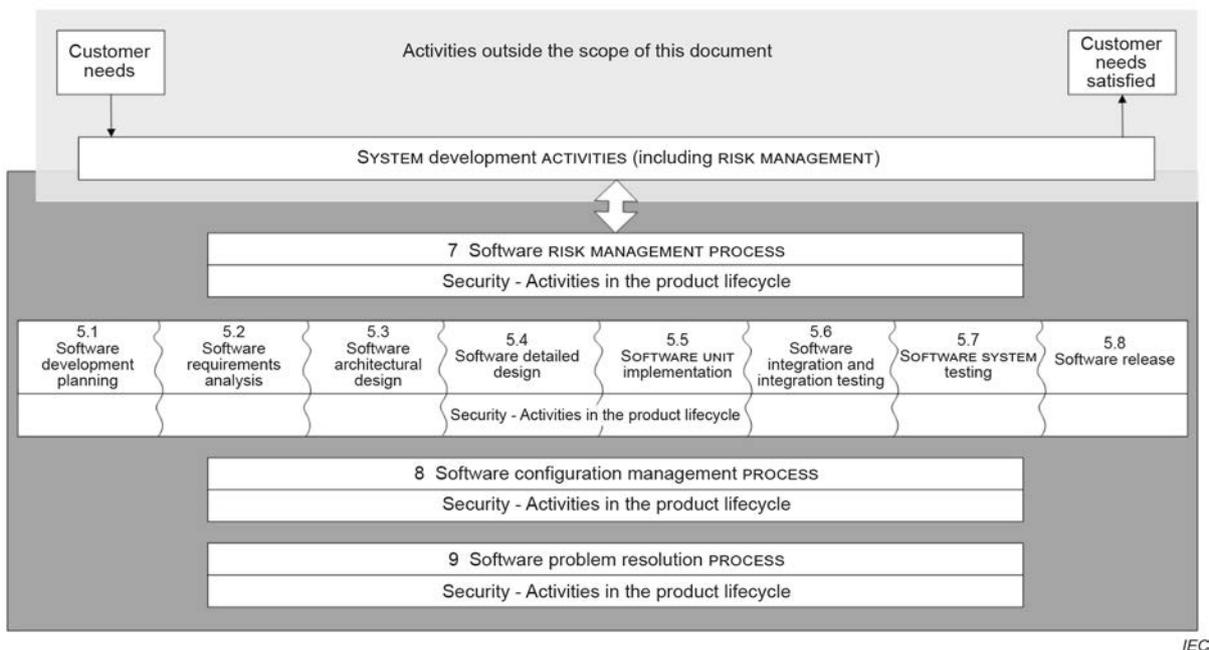
Clause 4 through Clause 9 of this document require establishing one or more PROCESSES that include identified ACTIVITIES. Per these normative parts of this document, the LIFE CYCLE PROCESSES implement these ACTIVITIES. None of the requirements in this document requires to implement these ACTIVITIES as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

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

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

1 Scope

This document defines the LIFE CYCLE requirements for development and maintenance of HEALTH SOFTWARE needed to support conformance to IEC 62443-4-1[11] – taking the specific needs for HEALTH SOFTWARE into account. The set of PROCESSES, ACTIVITIES, and TASKS described in this document establishes a common framework for secure HEALTH SOFTWARE LIFE CYCLE PROCESSES. An informal overview of activities for HEALTH SOFTWARE is shown in Figure 2.



IEC

[derived from IEC 62304:2006[8], Figure 2]

Figure 2 – HEALTH SOFTWARE LIFE CYCLE PROCESSES

The purpose is to increase the CYBERSECURITY of HEALTH SOFTWARE by establishing certain ACTIVITIES and TASKS in the HEALTH SOFTWARE LIFE CYCLE PROCESSES and also by increasing the SECURITY of SOFTWARE LIFE CYCLE PROCESSES themselves.

It is important to maintain an appropriate balance of the key properties SAFETY, effectiveness and SECURITY as discussed in ISO 81001-1[17].

This document excludes specification of ACCOMPANYING DOCUMENTATION contents.

2 Normative references

There are no normative references in this document.