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

IEC 81001-5-1:2021-12(en-fr)

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

About the IEC
The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications
The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigendum or an amendment might have been published.

IEC publications search - webstore.iec.ch/advsearchform
The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee, …). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

IEC Customer Service Centre - webstore.iec.ch/csc
If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: sales@iec.ch.

IEC online collection - oc.iec.ch
Discover our powerful search engine and read freely all the publications previews. With a subscription you will always have access to up to date content tailored to your needs.

Electropedia - www.electropedia.org
The world's leading online dictionary on electrotechnology, containing more than 22 000 terminological entries in English and French, with equivalent terms in 18 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

A propos de l'IEC
La Commission Electrotechnique Internationale (IEC) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications IEC
Le contenu technique des publications IEC est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

Recherche de publications IEC - webstore.iec.ch/advsearchform
La recherche avancée permet de trouver des publications IEC en utilisant différents critères (numéro de référence, texte, comité d'études, …). Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

IEC Just Published - webstore.iec.ch/justpublished
Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et une fois par mois par email.

Service Clients - webstore.iec.ch/csc
Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: sales@iec.ch.

IEC online collection - oc.iec.ch
Découvrez notre puissant moteur de recherche et consultez gratuitement tous les aperçus des publications. Avec un abonnement, vous aurez toujours accès à un contenu à jour adapté à vos besoins.

Electropedia - www.electropedia.org
Le premier dictionnaire d'électrotechnologie en ligne au monde, avec plus de 22 000 articles terminologiques en anglais et en français, ainsi que les termes équivalents dans 16 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

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).

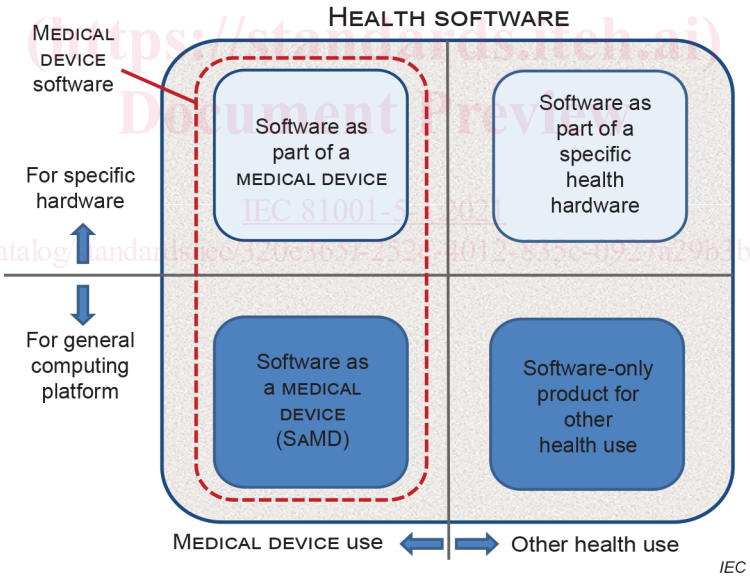
0.2 Field of application

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].

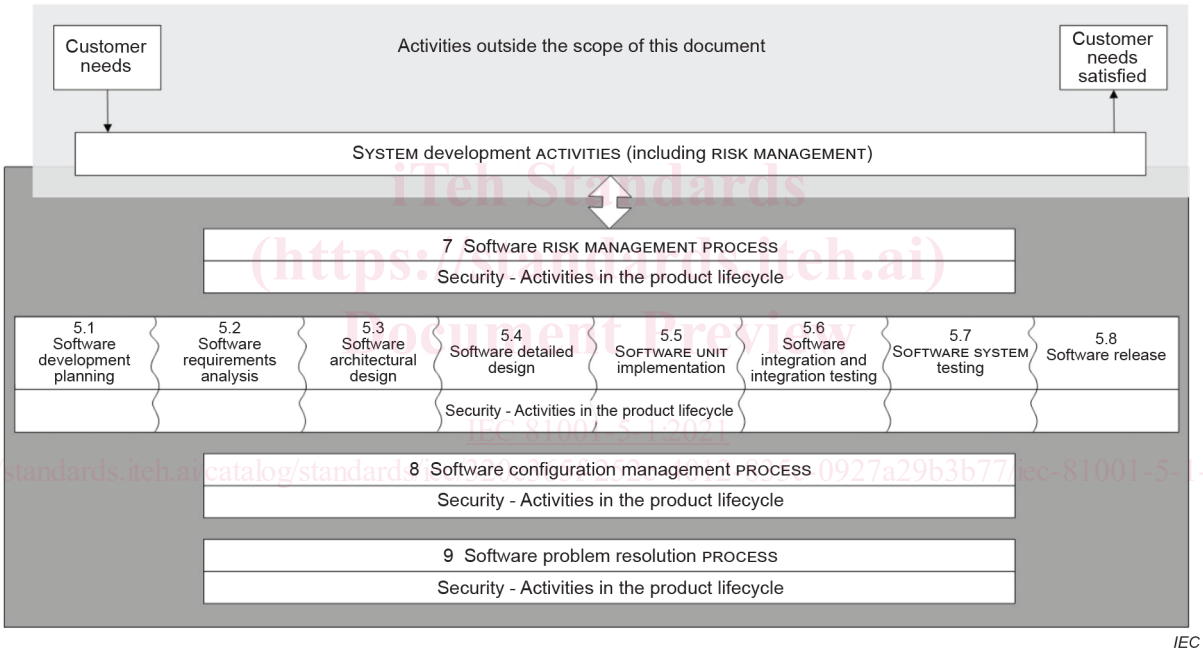
Clause 4 through Clause 9 of this document require establishing one or more PROCESSES that include identified ACTIVITIES. Per these normative parts of this document, the LIFE CYCLE PROCESSES implement these ACTIVITIES. None of the requirements in this document requires to implement these ACTIVITIES as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

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.



[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.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at www.electropedia.org/
- ISO Online browsing platform: available at www.iso.org/obp

3.1
ACCOMPANYING DOCUMENTATION
documentation intended to be used for a HEALTH SOFTWARE or a HEALTH IT SYSTEM or an accessory, containing information for the responsible organization or operator

3.2
ACTIVITY
set of one or more interrelated or interacting TASKS

[SOURCE: IEC 62304:2006[8], 3.1]

3.3
ARCHITECTURE
fundamental concepts or properties of a system in its environment, embodied in its elements, relationships, and in the principles of its design and evolution

[SOURCE: ISO/IEC/IEEE 24765:2017, 3.216, definition1]

3.4
ASSET
physical or digital entity that has value to an individual, an organization or a government

Note 1 to entry: As per the definition for ASSET this can include the following:

a) data and information;

b) HEALTH SOFTWARE and software needed for its operation;

c) hardware components such as computers, mobile devices, servers, databases, and networks;

d) services, including SECURITY, software development, IT operations and externally provided services such as data centres, internet and software-as-a-service and cloud solutions;

e) people, and their qualifications, skills and experience;

f) technical procedures and documentation to manage and support the HEALTH IT INFRASTRUCTURE;

g) HEALTH IT SYSTEMS that are configured and implemented to address organizational objectives by leveraging the ASSETS; and

h) intangibles, such as reputation and image.

[SOURCE: ISO 81001-1:2021[17] 3.3.2, modified – Addition of a new Note 1 to entry.]

3.5
ATTACK
attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an ASSET

[SOURCE: ISO/IEC 27000:2018, 3.2]

3.6
ATTACK SURFACE
physical and functional interfaces of a system that can be accessed and, therefore, potentially exploited by an attacker

[SOURCE: IEC 62443-4-1:2018[11], 3.1.7]

3.7
AVAILABILITY
property of being accessible and usable on demand by an authorized entity

[SOURCE: ISO/IEC 27000:2018, 3.7]

3.8
CONFIDENTIALITY
property that information is not made available or disclosed to unauthorized individuals, entities, or PROCESSES

[SOURCE: ISO/IEC 27000:2018, 3.10]

3.9
CONFIGURATION ITEM
entity that can be uniquely identified at a given reference point

[SOURCE: IEC 62304:2006[8], 3.5]

3.10
CONFIGURATION MANAGEMENT
PROCESS ensuring consistency of CONFIGURATION ITEMS by using mechanisms for identifying, controlling and tracking versions of CONFIGURATION ITEMS

3.11
DEFENSE-IN-DEPTH
approach to defend the system against any particular ATTACK using several independent methods

Note 1 to entry: DEFENSE-IN-DEPTH implies layers of SECURITY and detection, even on single systems, and provides the following features:

- is based on the idea that any one layer of protection, can and probably will be defeated;
- attackers are faced with breaking through or bypassing each layer without being detected;
- a flaw in one layer can be mitigated by capabilities in other layers;
- system SECURITY becomes a set of layers within the overall network SECURITY; and
- each layer is autonomous and not rely on the same functionality nor have the same failure modes as the other layers.

[SOURCE: IEC 62443-4-1:2018[11], 3.1.15]

3.12
EXPLOIT (noun)
defined way to breach the SECURITY of information systems through some VULNERABILITY

[SOURCE: ISO/IEC 27039:2015, 2.9]