IEC 81001-5-1

Edition 1.0 2021-12

Corrected version
2025-12

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 978-2-8322-5578-0

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.

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

IEC 81001-5-1
Edition 1.0 2021-12

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

INTERPRETATION SHEET 1

This interpretation sheet has been prepared by subcommittee 62A: Common aspects of medical equipment, software, and systems, of IEC technical committee 62: Medical equipment, software, and systems.

The text of this interpretation sheet is based on the following documents:

DISH	Report on voting
62A/1692/DISH	62A/1706/RVDISH

Full information on the voting for the approval of this interpretation sheet can be found in the report on voting indicated in the above table.

_____

This interpretation sheet is intended to clarify the following:

a) Requirements which are needed to provide essential ACCOMPANYING DOCUMENTATION to the operators of the HEALTH SOFTWARE product regarding the transfer of risk related to software items from the MANUFACTURER to the responsible organization or operator.

b) Requirements which are needed to maintain SECURITY of the HEALTH SOFTWARE product

Interpretation of IEC 81001-5-1:2021, Introduction, 0.2

The HEALTH SOFTWARE is part of a connected and complex healthcare ecosystem, which is integrated into a surrounding HEALTH IT SYSTEM and HEALTH IT INFRASTRUCTURE. ISO 81001-1 provides a definition of the sociotechnical ecosystem in which the HEALTH SOFTWARE operates in, and how to reference the security aspect of the HEALTH SOFTWARE within an IT-system inside a broader HEALTHCARE SYSTEM.

IEC 81001-5-1:2021-12/ISH1:2025-11(en)

ICS 11.040.01, 35.240.80

Interpretation of IEC 81001-5-1:2021, 4.1

4.1.7 Disclosing SECURITY-related issues

NOTE 1 This activity is related to 9.3 through 9.5 where additional supporting details are provided.

NOTE 2 On a) "CVSS" and "ranking" address the rating of the severity and characteristics of security vulnerabilities.

4.1.9 ACCOMPANYING DOCUMENTATION review

NOTE For clarification, the documents mentioned with "SECURITY guidelines" are detailed in 5.8.2 and 5.8.7.

Interpretation of IEC 81001-5-1:2021, 4.3

4.3 SOFTWARE ITEM classification relating to risk transfer

NOTE 1 (foundations, intentions):

Table 1 – SOFTWARE ITEM classification mapped to affected clauses

Activity Category	Clause	MAINTAINED	SUPPORTED (includes MAINTAINED)	REQUIRED (includes SUPPORTED)
Quality Management	4.3 Software Item classification related to risk transfer (Note: clarifying roles and responsibilities in support)	X	X	X
Software development	5.2.3 Security Risks for REQUIRED SOFTWARE	X*	X*	X
Software maintenance	6.3.1 SUPPORTED SOFTWARE update documentation	X*	X	
	6.3.2 MAINTAINED SOFTWARE security update delivery	X		
	6.3.3 MAINTAINED SOFTWARE security update INTEGRITY	X		

* Implied inclusion in clause since IEC 81001-5-1:2021, Clause 3 explicitly defines SUPPORTED SOFTWARE "includes MAINTAINED SOFTWARE" and REQUIRED SOFTWARE "includes SUPPORTED SOFTWARE".

SOFTWARE ITEM classification related to risk transfer from 4.3 is clarified as follows:

a) The SOFTWARE ITEM classification categories are nested, but only to ensure clauses that explicitly mention a category are also understood to include the nested categories. Table 1 above notes all clauses that detail requirements specific to a SOFTWARE ITEM classification and notes the implicit inclusion of nested categories. Further requirements of SOFTWARE ITEM classification that are not explicit in an associated clause are not part of this document.

b) The manufacturer shall apply risk transfer activities for all SOFTWARE ITEMS according to their associated category. An organization's policy and procedures may choose different terms for these classifications if clauses citing requirements for these SOFTWARE ITEM classifications are satisfied. Risks for all SOFTWARE ITEMS should be identified and managed (5.2.3), updates for SOFTWARE ITEMS controlled by the manufacturer or PRODUCT user should be communicated (6.3.1) and updates to manufacturer provided SOFTWARE ITEMS should be made available (6.3.2) and have verifiable integrity (6.3.3). For 4.3, any declaration of conformance, or internal policy/procedure, should state the alternative terminology leveraged and how it maps to the specific SOFTWARE ITEM categories when alternative approaches to MAINTAINED, SUPPORTED and REQUIRED SOFTWARE are utilized.

The following clarifying statements help illustrate how the implicit software category nesting affects the clauses that explicitly mention one of the SOFTWARE ITEM classifications:

1) 5.2.3 applies for all 3 categories of software. SECURITY Risks from REQUIRED, SUPPORTED and MAINTAINED software should be identified and managed.

2) 6.3.1 applies to MAINTAINED software in addition to SUPPORTED software. PRODUCT users also should be notified about updates to MAINTAINED software and SUPPORTED SOFTWARE.

3) 6.3.2 & 6.3.3 applies only to MAINTAINED software.

NOTE 2 (explain practical consequences)

It is generally understood that along with purchasing, installing, and using HEALTH SOFTWARE, the risk related to its use over time (often constrained by legal provisions) transitions to the operator. For the purposes of information security, MANUFACTURERS depend on information from suppliers of SOFTWARE ITEMS (being a logical part of the HEALTH SOFTWARE) for certain post-market activities, such as 9.3, to maintain a secure state.

Similarly, operators depend on information from MANUFACTURERS regarding which SOFTWARE ITEMS are intended to be used with HEALTH SOFTWARE product, which kind of support the MANUFACTURER declares for these SOFTWARE ITEMS and which are not supported. Therefore, aspects of risk transfer of the HEALTH SOFTWARE from the MANUFACTURER to the operator is addressed by the categories introduced in 4.3 and the associated clauses citing the SOFTWARE ITEM classifications.

For technical or organizational reasons, it is possible that operators wish to be in control of when or whether a new security update is being installed on related systems where the MANUFACTURER does not provide the security updates. As an example, updates to a database shared among several devices and services require good planning such that both selection and timing of updates cannot be left in the hands of a single MANUFACTURER. This is a reason for introducing the category of SUPPORTED SOFTWARE.

For technical or organizational reasons, MANUFACTURERS in some cases are not in a position to obtain security notifications or security updates for certain SOFTWARE ITEMS. This is a reason for introducing the category of REQUIRED SOFTWARE. When vulnerabilities for such (“end-of-support” or otherwise unsupported) software become known, MANUFACTURERS can still select other means of maintaining the overall security of the HEALTH SOFTWARE product.

Over the HEALTH SOFTWARE LIFE CYCLE, the MANUFACTURER can update the SOFTWARE ITEM categorization, which is typically done by downgrading SOFTWARE ITEMS from MAINTAINED to SUPPORTED, from MAINTAINED to REQUIRED or SUPPORTED to REQUIRED. When this happens, the requirements from associated clauses shall be evaluated to ensure appropriate risk transfer from MANUFACTURERS to operators.

NOTE 3 (distinguish from transitional software)

For clarification, *Transitional* (Annex F) is an attribute applied to the whole HEALTH SOFTWARE product – independent of the above categories for SOFTWARE ITEMS. The term “transitional“ does not specify a fourth category for SOFTWARE ITEMS – rather it is a circumstance in which the MANUFACTURER developed the HEALTH SOFTWARE product before IEC 81001-5-1 existed. Therefore, *Transitional HEALTH SOFTWARE* (Annex F) is an alternative approach for evaluating HEALTH SOFTWARE that was “developed without following all of the ACTIVITIES defined in of IEC 81001-5-1:2021, Clause 4 to Clause 9.

Interpretation of IEC 81001-5-1:2021, 6.1

6.2.1 Monitoring public incident reports

NOTE For clarification, this activity specifies “review of the information” rather than review of the source.

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.

The contents of the Interpretation sheet 1 (2025-12) have been included in this copy.

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).

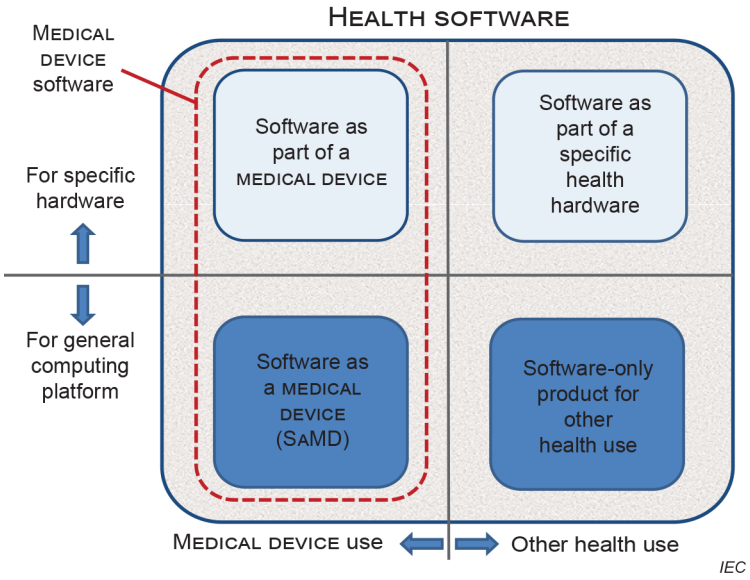
0.2 Field of application

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].

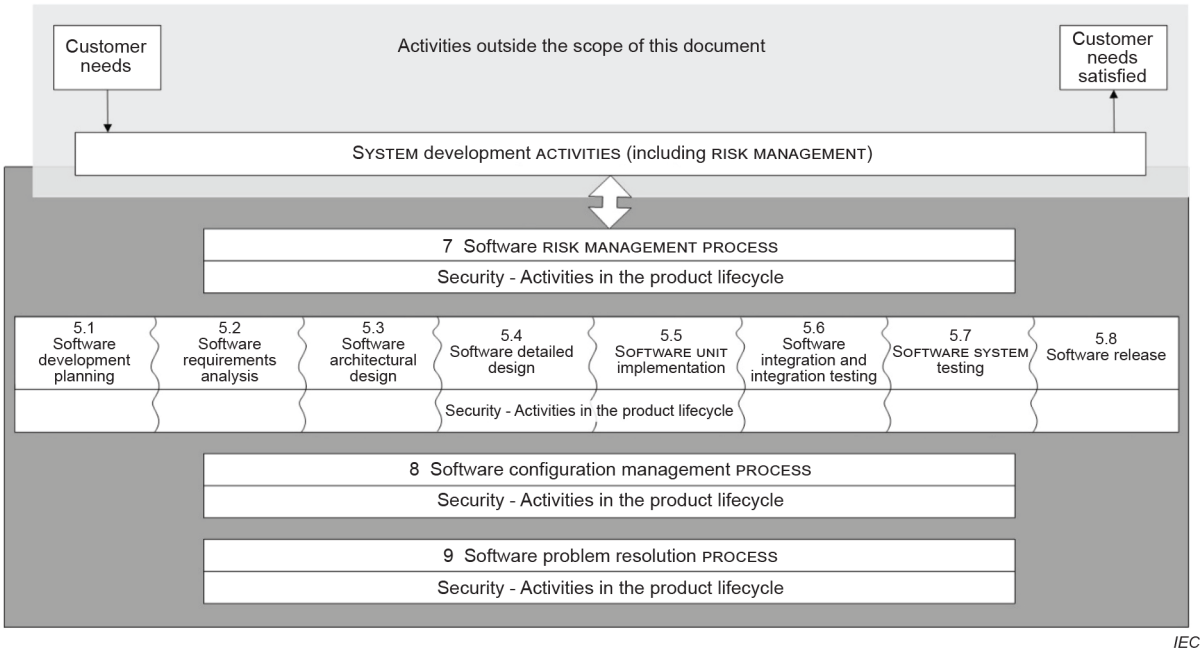
Clause 4 through Clause 9 of this document require establishing one or more PROCESSES that include identified ACTIVITIES. Per these normative parts of this document, the LIFE CYCLE PROCESSES implement these ACTIVITIES. None of the requirements in this document requires to implement these ACTIVITIES as 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.

Bibliography

[1] ISO/IEC Guide 63:2019, *Guide to the development and inclusion of aspects of safety in International Standards for medical devices*

[2] AAMI TIR 57:2016, *Principles for medical device security – Risk management*

[3] AAMI TIR 97:2019, *Principles for medical device security – Post-market risk management for device manufacturers*

[4] ANSI/NEMA HN1-2019, *Manufacturer Disclosure Statement for Medical Device Security MDS*, (available from nema.org)

[5] ETSI TS 102 165-1 TVRA CYBER, *Methods and protocols – Part 1: Method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA)*

[6] EU MDCG: MDCG 2019-16, *Guidance on Cybersecurity for medical devices*

[7] IEC TR 60601-4-5, *Medical electrical equipment – Part 4-5 Guidance and interpretation – Safety-related technical security specifications*

[8] IEC 62304:2006, *Medical device software – Software life cycle processes*
IEC 62304:2006/AMD1:2015

[9] IEC 62443-3-2, *Security for industrial automation and control systems – Part 3-2: Security risk assessment for system design*

[10] IEC 62443-3-3, *Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels*

[11] IEC 62443-4-1:2018, *Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements*

[12] IEC 62443-4-2:2019, *Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components*

[13] IEC 62740:2015, *Root cause analysis (RCA)*

[14] IEC TR 80001-2-2, *Application of risk management for IT-networks incorporating medical devices – Part 2-2: Guidance for the disclosure and communication of medical device security needs, risks and controls*

[15] IEC TR 80001-2-8, *Application of risk management for IT-networks incorporating medical devices – Part 2-8: Application guidance – Guidance on standards for establishing the security capabilities identified in IEC TR 80001-2-2*

[16] ISO/IEC Guide 51:2014, *Safety aspects – Guidelines for their inclusion in standards*

[17] ISO 81001-1:2021, *Health software and health IT systems safety, effectiveness and security – Part 1: Principles and concepts*

[18] IEC 82304-1:2016, *Health software – Part 1: General requirements for product safety*

[19] ISO TS 14441, *Health informatics – Security and privacy requirements of EHR systems for use in conformity assessment*

[20] ISO 14971:2019, *Medical devices – Application of risk management to medical devices*

[21] ISO/IEC TR 20004:2012, *Information technology – Security techniques – Refining software vulnerability analysis under ISO/IEC 15408 and ISO/IEC 18045*

[22] ISO TR 24971:2020, *Medical devices – Guidance on the application of ISO 14971*

[23] ISO/IEC 27000:2018, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*

[24] ISO/IEC TR 24772-1:2019, *Programming languages – Guidance to avoiding vulnerabilities in programming languages – Part 1: Language-independent guidance*

[25] ISO 27789, *Health informatics – Audit trails for electronic health records*

[26] ISO 27799, *Health informatics – Information security management in health using ISO/IEC 27002*

[27] ISO/IEC 29147, *Information technology – Security techniques – Vulnerability disclosure*

[28] ISO/IEC 30111, *Information technology – Security techniques – Vulnerability handling processes*

[29] MISRA-C, Motor Industry Software Reliability Association, HORIBA MIRA Ltd, MISRA-C3, 2012 (available at misra.org.uk)

[30] MITRE, Rubric for Applying CVSS to Medical Devices (see https://www.mitre.org/publications/technical-papers/rubric-for-applying-cvss-to-medical-devices)

[31] ISO 13485:2016, *Medical devices – Quality management systems – Requirements for regulatory purposes*

[32] ISO/IEC/IEEE 24765:2017, *Systems and software engineering – Vocabulary*

[33] ISO/IEC 24767-1:2008, *Information technology – Home network security – Part 1: Security requirements*

[34] ISO/IEC 27039:2015*, Information technology – Security techniques – Selection, deployment and operations of intrusion detection and prevention systems (IDPS)*

[35] ISO/IEC 14764:2006*, Software engineering – Software life cycle processes – Maintenance*

[36] IEC 62366-1:2015, *Medical devices – Part 1: Application of usability engineering to medical devices*

[37] IEC TR 63069, *Industrial-process measurement, control and automation – Framework for functional safety and security*

[38] ISO 9000:2015*, Quality management systems – Fundamentals and vocabulary*

[39] ISO/IEC 9834-1:2012, *Information technology – Procedures for the operation of object identifier registration authorities – Part 1: General procedures and top arcs of the international object identifier tree*

[40] NIST SP800-30 Rev 1. *Guide for Conducting Risk Assessments*, 2021

[41] SAMATE, *NIST Software Assurance Metrics and Tool Evaluation*, National Institute of Standards and Technology (NIST), Gaithersburg Md, January 16, 2020

[42] SEI CERT C, C Coding Standard, https://wiki.sei.cmu.edu/confluence/display/c, Carnegie Mellon University, 2018

_____

SOMMAIRE

AVANT-PROPOS 62
INTRODUCTION 64
0.1 Structure 64
0.2 Champ d'application 65
0.3 Conformité 66
1 Domaine d'application 67
2 Références normatives 68
3 Termes et définitions 68
4 Exigences générales 75
4.1 Management de la qualité 75
4.1.1 Système de management de la qualité 75
4.1.2 Identification des responsabilités 75
4.1.3 Identification de l'applicabilité 76
4.1.4 Expertise en matière de SÛRETÉ 76
4.1.5 ÉLEMENTS LOGICIELS provenant de fournisseurs tiers 76
4.1.6 Amélioration continue 76
4.1.7 Divulgation des problèmes liés à la SURETE 76
4.1.8 Revue périodique de la gestion des défauts de SURETE 77
4.1.9 Revue de la DOCUMENTATION D'ACCOMPAGNEMENT 77
4.2 GESTION DES RISQUES DE SÛRETÉ 77
4.3 Classification de l'ELEMENT LOGICIEL relatif au transfert de risque 78
5 PROCESSUS de développement logiciel 78
5.1 Planification du développement logiciel 78
5.1.1 ACTIVITES du PROCESSUS DU CYCLE DE VIE 78
5.1.2 SÛRETÉ de l'environnement de développement 78
5.1.3 Normes de codage sécurisé 79
5.2 Analyse des exigences relatives aux LOGICIELS DE SANTE 79
5.2.1 Exigences de SURETE relatives aux LOGICIELS DE SANTE 79
5.2.2 Revue des exigences de SÛRETÉ 79
5.2.3 Risques de SURETE pour les LOGICIELS EXIGES 80
5.3 Conception architecturale des logiciels 80
5.3.1 ARCHITECTURE/conception de la DEFENSE EN PROFONDEUR 80
5.3.2 Meilleures pratiques de conception sécurisée 80
5.3.3 Revue de conception architecturale de SURETE 80
5.4 Conception logicielle 81
5.4.1 Meilleures pratiques de conception logicielle 81
5.4.2 Conception sécurisée 81
5.4.3 Interfaces sécurisées des LOGICIELS DE SANTE 81
5.4.4 VERIFICATION de conception détaillée pour la SURETE 82
5.5 Mise en œuvre et VERIFICATION des unités logicielles 82
5.5.1 Normes de codage sécurisé 82
5.5.2 Revue de mise en œuvre de la SURETE 82
5.6 Essais d'intégration logicielle 82
5.7 Essais des systèmes logiciels 83
5.7.1 Vérification par essai des exigences de SURETE 83
5.7.2 Essais d'atténuation des MENACES 83

5.7.3 Essais de VULNÉRABILITÉS 83
5.7.4 Essais de pénétration 84
5.7.5 Gestion des conflits d'intérêts entre les contrôleurs et les développeurs 84
5.8 Diffusion des logiciels 84
5.8.1 Résolution des constatations préalablement à la diffusion 84
5.8.2 Documentation de diffusion 84
5.8.3 Intégrité des FICHIERS 85
5.8.4 Contrôles dédiés aux clés privées 85
5.8.5 Évaluation et traitement des problèmes liés à la SURETE 85
5.8.6 Réalisation des ACTIVITÉS 85
5.8.7 Lignes directrices applicables à la mise hors service sécurisée des LOGICIELS DE SANTE 85
6 PROCESSUS DE MAINTENANCE DU LOGICIEL 86
6.1 Établissement d'un plan de MAINTENANCE DU LOGICIEL 86
6.1.1 Mises à jour de SURETE ponctuelles 86
6.2 Analyse des problèmes et des modifications 86
6.2.1 Contrôle des rapports publics d'incidents 86
6.2.2 VERIFICATION des mises à jour de SURETE 86
6.3 Mise en œuvre des modifications 87
6.3.1 Documentation des mises à jour de SURETE des LOGICIELS PRIS EN CHARGE 87
6.3.2 Mise à disposition des mises à jour de SURETE des LOGICIELS MAINTENUS 87
6.3.3 INTEGRITE des mises à jour de SURETE des LOGICIELS MAINTENUS 87
7 PROCESSUS DE GESTION DES RISQUES DE SURETE 87
7.1 Contexte de GESTION DES RISQUES 87
7.1.1 Généralités 87
7.1.2 CONTEXTE DE SÛRETÉ DES PRODUITS 87
7.2 Identification des VULNERABILITES, MENACES et effets défavorables associés 88
7.3 Estimation et évaluation du risque de SURETE 89
7.4 MAÎTRISE DES RISQUES de SÛRETÉ 89
7.5 Contrôle de l'efficacité des mesures de MAITRISE DES RISQUES 89
8 PROCESSUS de GESTION DE LA CONFIGURATION logicielle 90
9 PROCESSUS de résolution des problèmes logiciels 90
9.1 Présentation 90
9.2 Réception des notifications concernant les VULNERABILITES 90
9.3 Revue des VULNÉRABILITÉS 90
9.4 Analyse des VULNÉRABILITÉS 91
9.5 Traitement des problèmes liés à la SURETE 91
Annexe A (informative) Justification 93
A.1 Relation avec l'IEC 62443 93
A.2 Relation avec l'IEC 62304 94
A.3 Transfert de risque 95
A.3.1 Présentation 95
A.3.2 LOGICIEL MAINTENU 95
A.3.3 LOGICIEL PRIS EN CHARGE 95
A.3.4 LOGICIEL EXIGÉ 95
A.4 Meilleures pratiques de codage sécurisé 96
Annexe B (informative) Recommandations concernant la mise en œuvre des ACTIVITÉS DU CYCLE DE VIE DE SÛRETÉ 97

B.1 Présentation 97
B.2 Tâches connexes 97
B.3 ANALYSE DES MENACES/RISQUES 97
B.4 GESTION DES MENACES et DES RISQUES 98
B.5 Planification du développement logiciel 99
B.5.1 Développement 99
B.5.1.1 PROCESSUS de développement logiciel 99
B.5.1.2 SÛRETÉ de l'environnement de développement 99
B.5.2 Analyse des exigences relatives aux LOGICIELS DE SANTÉ 99
B.5.2.1 Exigences de SÛRETÉ relatives aux LOGICIELS DE SANTÉ 99
B.5.2.2 Revue des exigences de SÛRETÉ 99
B.5.3 Conception architecturale des logiciels 99
B.5.3.1 ARCHITECTURE/conception de la DÉFENSE EN PROFONDEUR 99
B.5.3.2 Principes de conception sécurisée 99
B.5.3.3 Revue de conception architecturale de SÛRETÉ 100
B.5.4 Mise en œuvre et VÉRIFICATION des unités logicielles 100
B.5.5 Mise en œuvre sécurisée 100
B.5.6 Non utilisé 100
B.5.7 Essais des systèmes logiciels 100
B.5.7.1 Vérification par essai des exigences de SÛRETÉ 100
B.5.7.2 Essais d'atténuation des MENACES 101
B.5.7.3 Analyse des VULNÉRABILITÉS 101
B.5.7.4 Essais de pénétration 101
B.5.7.5 Indépendance du contrôleur 101
Annexe C (informative) MODÉLISATION D'UNE MENACE 102
C.1 Généralités 102
C.2 Arbres d'ATTAQUE-défense 102
C.3 CAPEC/OWASP/SANS 102
C.4 CWSS 102
C.5 DREAD 103
C.6 Liste des VULNÉRABILITÉS potentielles connues 103
C.7 OCTAVE 103
C.8 STRIDE 103
C.9 Trike 103
C.10 VAST 103
Annexe D (informative) Relation avec les pratiques spécifiées dans l'IEC 62443-4-1:2018 104
D.1 IEC 81001-5-1 avec IEC 62443-4-1:2018 104
D.2 IEC 62443-4-1:2018 avec IEC 81001-5-1 105
Annexe E (informative) Documents spécifiés dans l'IEC 62443-4-1 106
E.1 Présentation 106
E.2 Documentation de diffusion 106
E.2.1 Documentation liée au PRODUIT 106
E.2.2 Documentation relative à la DÉFENSE EN PROFONDEUR des LOGICIELS DE SANTÉ 107
E.2.3 Mesures de DÉFENSE EN PROFONDEUR et environnement 107
E.2.4 Lignes directrices pour un renforcement de la SÛRETÉ 107
E.2.5 Informations relatives aux mises à jour de SÛRETÉ 108

E.3 Documents relatifs à la mise hors service des LOGICIELS DE SANTÉ 108
Annexe F (normative) LOGICIEL DE SANTÉ TRANSITOIRE 109
F.1 Présentation 109
F.2 Activités d'évaluation du développement et de comblement des lacunes 109
F.3 Justification de l'utilisation des LOGICIELS DE SANTÉ TRANSITOIRES 110
F.4 ACTIVITÉS post-diffusion 110
Annexe G (normative) Identificateurs d'objet 111
Bibliographie 112

Figure 1 – Champ d'application des LOGICIELS DE SANTE 65
Figure 2 – PROCESSUS DU CYCLE DE VIE DES LOGICIELS DE SANTE 67

Tableau A.1 – Niveau d'indépendance exigé des contrôleurs par rapport aux développeurs 94
Tableau G.1 – Identificateurs d'objet pour les concepts de conformité du présent document 111

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

LOGICIELS DE SANTÉ ET SÉCURITÉ, EFFICACITÉ ET SÛRETÉ DES SYSTÈMES TI DE SANTÉ –

Partie 5-1: Sûreté – Activités du cycle de vie du produit

AVANT-PROPOS

1) La Commission Électrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. À cet effet, l'IEC – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de l'IEC"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'IEC, participent également aux travaux. L'IEC collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à l'IEC, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de l'IEC, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de l'IEC ou de toute autre Publication de l'IEC, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de l'IEC peuvent faire l'objet de droits de brevet. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets.

La Norme internationale IEC 81001-5-1 a été établie par un Groupe de travail commun du sous-comité 62A de l'IEC: Aspects généraux des équipements électriques utilisés en pratique médicale, du comité d'études 62 de l'IEC: Équipements électriques dans la pratique médicale, et du comité technique 215 de l'ISO: Informatique de santé.

Elle est publiée en tant que norme double logo.

Le texte de ce document est issu des documents suivants:

Projet	Rapport de vote
62A/1458/FDIS	62A/1466/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à son approbation.

La langue employée pour l'élaboration de cette Norme internationale est l'anglais.

Le présent document a été rédigé selon les Directives ISO/IEC, Partie 2, il a été développé selon les Directives ISO/IEC, Partie 1 et les Directives ISO/IEC, Supplément IEC, disponibles sous www.iec.ch/members_experts/refdocs. Les principaux types de documents développés par l'IEC sont décrits plus en détail sous www.iec.ch/standardsdev/publications.

Dans le présent document, les caractères d'imprimerie suivants sont utilisés:

– exigences et définitions: caractères romains;

– Indications de nature informative apparaissant hors des tableaux, comme les notes, les exemples et les références: petits caractères. Le texte normatif à l'intérieur des tableaux est également en petits caractères;

– TERMES DEFINIS A L'ARTICLE 3 DE LA NORME GENERALE, DANS LA PRESENTE NORME PARTICULIERE OU COMME NOTES: PETITES MAJUSCULES.

Une liste de toutes les parties de la série IEC 81001, publiées sous le titre général *Logiciels de santé et sécurité, efficacité et sûreté des systèmes TI de santé*, peut être consultée sur le site web de l'IEC.

Le comité a décidé que le contenu de ce document ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous webstore.iec.ch dans les données relatives au document recherché. À cette date, le document sera

- reconduit,
- supprimé,
- remplacé par une édition révisée, ou
- amendé.

IMPORTANT – Le logo "colour inside" qui se trouve sur la page de couverture de ce document indique qu'il contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer ce document en utilisant une imprimante couleur.

Le contenu de la feuille d'interprétation 1 (2025-12) s'applique à la version anglaise uniquement.

INTRODUCTION

0.1 Structure

Les normes de PROCESSUS relatives aux LOGICIELS DE SANTE fournissent une spécification des ACTIVITES réalisées par le FABRICANT – y compris les logiciels incorporés dans les dispositifs médicaux – comme partie intégrante d'un CYCLE DE VIE de développement. Les articles normatifs du présent document sont destinés à fournir les meilleures pratiques minimales pour un CYCLE DE VIE du logiciel sécurisé. La législation et la réglementation locales sont prises en considération.

Les exigences relatives aux PROCESSUS (de l'Article 4 à l'Article 9) sont issues de la gestion du CYCLE DE VIE DU PRODUIT (IEC 62443-4-1)[1][11]. Les mises en œuvre de ces spécifications peuvent étendre les PROCESSUS existants au sein de l'organisation du FABRICANT – notamment les PROCESSUS existants conformes à l'IEC 62304[8]. Le présent document peut par conséquent venir à l'appui de la conformité à l'IEC 62443-4-1[11].

Les articles normatifs du présent document définissent les ACTIVITES incombant au FABRICANT. Le CYCLE DE VIE DES LOGICIELS DE SANTE peut faire partie intégrante d'un projet de PRODUIT d'intégration. Certaines ACTIVITES définies dans le présent document dépendent de l'élément d'entrée et de la prise en charge par le CYCLE DE VIE DU PRODUIT (par exemple pour définir des critères spécifiques). Exemples:

- GESTION DES RISQUES;
- exigences;
- essais;
- activités post-diffusion (après la mise sur le marché des LOGICIELS DE SANTE).

Dans les cas où les ACTIVITES relatives aux LOGICIELS DE SANTE nécessitent une prise en charge par les PROCESSUS au niveau du PRODUIT, les Articles 4 à 9 du présent document définissent des exigences respectives au-delà du CYCLE DE VIE DES LOGICIELS DE SANTE.

Tout comme l'IEC 62304[8], le présent document ne définit pas un système spécifique de PROCESSUS, mais les Articles 4 à 9 du présent document spécifient les ACTIVITES qui sont réalisées pendant le CYCLE DE VIE DES LOGICIELS DE SANTE.

L'Article 4 précise que les FABRICANTS développent et assurent la maintenance du LOGICIEL DE SANTE au sein d'un système de management de la qualité (voir 4.1) et d'un SYSTEME DE GESTION DES RISQUES (4.2).

Les Articles 5 à 8 définissent les ACTIVITES et l'élément de sortie obtenu comme partie intégrante du PROCESSUS DU CYCLE DE VIE du logiciel mis en œuvre par le FABRICANT. Ces spécifications sont présentées dans l'ordre défini dans l'IEC 62304[8].

L'Article 9 définit les ACTIVITES et l'élément de sortie obtenu comme partie intégrante du PROCESSUS de résolution des problèmes, mis en œuvre par le FABRICANT.

Le domaine d'application du présent document est limité au LOGICIEL DE SANTE et à sa connectivité avec son ENVIRONNEMENT D'UTILISATION PREVU, sur la base de l'IEC 62304[8], en insistant toutefois sur la CYBERSECURITE.

---

1 Les chiffres entre crochets se réfèrent à la Bibliographie.

Pour l'expression des dispositions spécifiées dans le présent document,

– "peut" sert à décrire une possibilité ou une capacité; et
– "doit" sert à exprimer une contrainte externe.

NOTE Le LOGICIEL DE SANTE peut être commercialisé en tant que logiciel, comme partie intégrante d'un dispositif médical, comme partie intégrante d'un matériel spécifiquement destiné à un usage sanitaire, comme logiciel faisant partie intégrante d'un dispositif médical (SaMD - *software as a medical device*) ou en tant que PRODUIT pour autre usage sanitaire. (Voir la Figure 2).

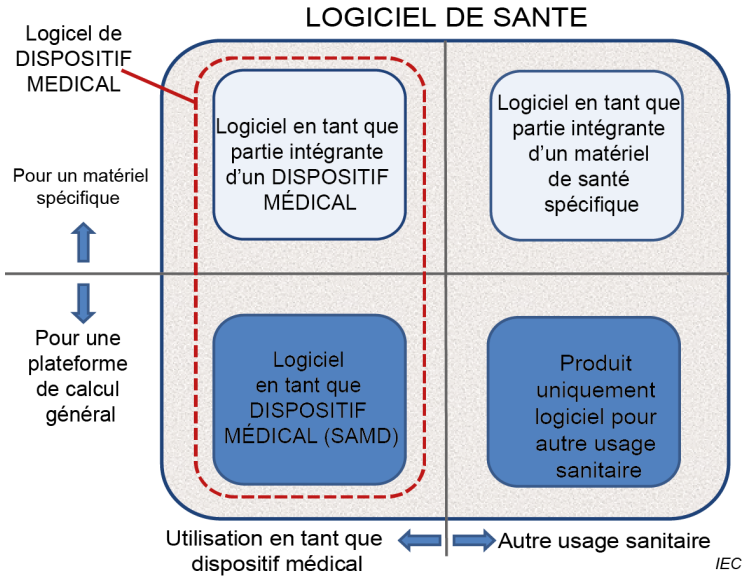
0.2 Champ d'application

Le présent document s'applique au développement et à la maintenance d'un LOGICIEL DE SANTE par un FABRICANT, mais reconnaît l'importance critique d'une communication bilatérale avec les organismes (par exemple, ORGANISMES DE PRESTATION DE SOINS DE SANTE (HDO)) responsables de la SURETE du LOGICIEL DE SANTE et des systèmes TI dans lesquels il est incorporé, après développement et diffusion du logiciel. La série de normes ISO/IEC 81001-5 (pour laquelle la présente partie -1 est conçue de manière à inclure de futures parties qui traitent de la SURETE et s'appliquent à la mise en œuvre, aux opérations et aux phases d'utilisation du CYCLE DE VIE pour des organismes tels que les HDO).

Un logiciel de dispositif médical constitue un sous-ensemble de LOGICIEL DE SANTE. Un diagramme pratique de Venn des types de LOGICIELS DE SANTE est présenté à la Figure 1. Par conséquent, le présent document s'applique aux:

– logiciels comme partie intégrante d'un dispositif médical;
– logiciels comme partie intégrante de matériels spécifiquement destinés à un usage sanitaire;
– logiciels en tant que dispositif médical (SaMD); et
– PRODUITS uniquement logiciels pour autre usage sanitaire.

NOTE Dans le présent document, le domaine d'application du logiciel considéré comme partie intégrante des ACTIVITES DU CYCLE DE VIE pour les LOGICIELS DE SANTE sécurisés est plus étendu et inclut un nombre d'éléments logiciels (pilotes, plateformes, systèmes d'exploitation) plus important que dans le cas de la SECURITE. En revanche, l'objectif de la SURETE concerne toute utilisation, y compris un accès non autorisé prévisible plutôt que le seul EMPLOI PREVU.



[SOURCE: IEC 82304-1[18]]

Figure 1 – Champ d'application des LOGICIELS DE SANTE

0.3 Conformité

La conformité au présent document repose sur la mise en œuvre des exigences relatives aux PROCESSUS, ACTIVITES et TACHES – et peut être revendiquée de l'une des deux manières suivantes:

- pour les LOGICIELS DE SANTE, par la mise en œuvre des exigences spécifiées de l'Article 4 à l'Article 9 du présent document,
- pour les LOGICIELS DE SANTE TRANSITOIRES, seulement par la mise en œuvre des PROCESSUS, ACTIVITES et TACHES identifiés à l'Annexe F.

Le présent document est conçu pour aider à la mise en œuvre des PROCESSUS exigés par l'IEC 62443-4-1. Cependant, la conformité au présent document n'est pas nécessairement une condition suffisante pour la conformité à l'IEC 62443-4-1[11]. D'autres recommandations relatives au champ d'application sont disponibles à l'Annexe D.

Les FABRICANTS peuvent mettre en œuvre les spécifications relatives à l'Annexe E afin d'obtenir une conformité de la documentation à l'IEC 62443-4-1[11].

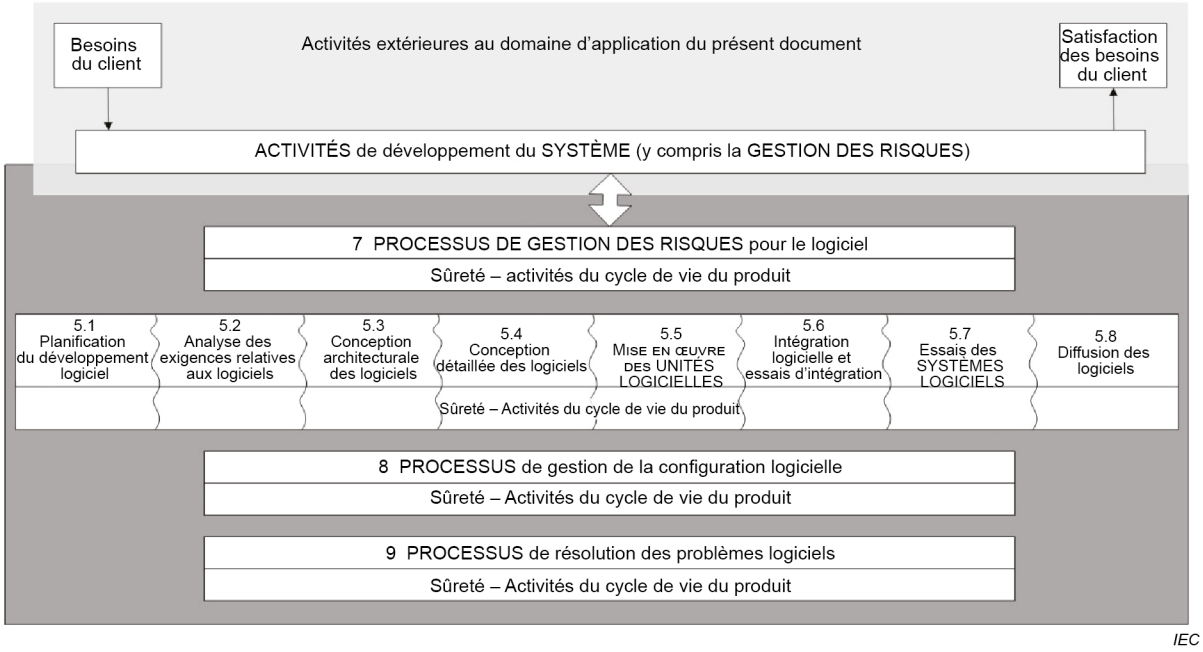
Les Articles 4 à 9 du présent document exigent l'établissement d'un ou plusieurs PROCESSUS comprenant des ACTIVITES identifiées. Selon les parties normatives du présent document, les PROCESSUS DU CYCLE DE VIE mettent en œuvre ces ACTIVITES. Aucune exigence définie dans le présent document n'impose la mise en œuvre de ces ACTIVITES sous forme de PROCESSUS unique ou de PROCESSUS distincts. Les ACTIVITES définies dans le présent document font typiquement partie intégrante d'un PROCESSUS DU CYCLE DE VIE existant.

LOGICIELS DE SANTÉ ET SÉCURITÉ, EFFICACITÉ ET SÛRETÉ DES SYSTÈMES TI DE SANTÉ –

Partie 5-1: Sûreté – Activités du cycle de vie du produit

1 Domaine d'application

Le présent document définit les exigences de CYCLE DE VIE relatives au développement et à la maintenance des LOGICIELS DE SANTE, nécessaires pour venir à l'appui de la conformité à l'IEC 62443-4-1[11] – compte tenu des besoins spécifiques pour les LOGICIELS DE SANTE. L'ensemble des PROCESSUS, ACTIVITES et TACHES décrits dans le présent document établit un cadre commun pour des PROCESSUS sécurisés du CYCLE DE VIE DES LOGICIELS DE SANTE. Une présentation informelle des activités relatives au LOGICIEL DE SANTE est donnée à la Figure 2.



[Source: IEC 62304:2006[8], Figure 2]

Figure 2 – PROCESSUS DU CYCLE DE VIE DES LOGICIELS DE SANTE

Ces processus ont pour objet de renforcer la CYBERSECURITE des LOGICIELS DE SANTE par l'établissement de certaines ACTIVITES et TACHES dans les PROCESSUS DU CYCLE DE VIE desdits LOGICIELS, ainsi que par le renforcement de la SURETE des PROCESSUS DU CYCLE DE VIE DES LOGICIELS proprement dit.

Il est important de maintenir un équilibre approprié des propriétés clés (SECURITE, efficacité et SURETE) traitées dans l'ISO 81001-1[17].

Le présent document exclut la spécification du contenu de la DOCUMENTATION D'ACCOMPAGNEMENT.

2 Références normatives

Le présent document ne contient aucune référence normative.

Bibliographie

[1] Guide ISO/IEC 63:2019, *Guide to the development and inclusion of aspects of safety in International Standards for medical devices* (disponible en anglais seulement)

[2] AAMI TIR 57:2016, *Principles for medical device security – Risk management*

[3] AAMI TIR 97:2019, *Principles for medical device security – Post-market risk management for device manufacturers*

[4] ANSI/NEMA HN1-2019, *Manufacturer Disclosure Statement for Medical Device Security MDS*, (available from nema.org)

[5] ETSI TS 102 165-1 TVRA CYBER, *Methods and protocols – Part 1: Method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA)*

[6] EU MDCG: MDCG 2019-16, *Guidance on Cybersecurity for medical devices*

[7] IEC TR 60601-4-5, *Medical electrical equipment – Part 4-5 Guidance and interpretation – Safety-related technical security specifications* (disponible en anglais seulement)

[8] IEC 62304:2006, *Logiciels de dispositifs médicaux – Processus du cycle de vie du logiciel*
IEC 62304:2006/AMD1:2015

[9] IEC 62443-3-2, *Sécurité des systèmes d'automatisation et de commande industriels – Partie 3-2: Évaluation des risques de sécurité pour la conception des systèmes*

[10] IEC 62443-3-3, *Réseaux industriels de communication – Sécurité dans les réseaux et les systèmes – Partie 3-3: Exigences de sécurité des systèmes et niveaux de sécurité*

[11] IEC 62443-4-1:2018, *Sécurité des automatismes industriels et des systèmes de commande – Partie 4-1: Exigences relatives au cycle de développement de produit sécurisé*

[12] IEC 62443-4-2:2019, *Sécurité des systèmes d'automatisation et de commande industrielles – Partie 4-2: Exigences de sécurité technique des composants IACS*

[13] IEC 62740:2015, *Analyse de cause initiale (RCA)*

[14] IEC TR 80001-2-2, *Application of risk management for IT-networks incorporating medical devices – Part 2-2: Guidance for the disclosure and communication of medical device security needs, risks and controls* (disponible en anglais seulement)

[15] IEC TR 80001-2-8, *Application of risk management for IT-networks incorporating medical devices – Part 2-8: Application guidance – Guidance on standards for establishing the security capabilities identified in IEC TR 80001-2-2* (disponible en anglais seulement)

[16] Guide ISO/IEC 51:2014, *Aspects liés à la sécurité – Principes directeurs pour les inclure dans les normes*

[17] ISO 81001-1:2021, *Application de la gestion des risques aux réseaux des technologies de l'information contenant des dispositifs médicaux – Partie 1: Sûreté, efficacité et sécurité dans la mise en œuvre et l'utilisation des dispositifs médicaux connectés ou des logiciels de santé connectés*

[18] IEC 82304-1:2016, *Logiciels de santé - Partie 1*: *Exigences générales pour la sécurité des produits*

[19] ISO TS 14441, *Informatique de santé — Sécurité et exigences d'intimité des systèmes de EHR pour l'évaluation de la conformité*)

[20] ISO 14971:2019, *Dispositifs médicaux – Application de la gestion des risques aux dispositifs médicaux*

[21] ISO/IEC TR 20004:2012, *Information technology – Security techniques – Refining software vulnerability analysis under ISO/IEC 15408 and ISO/IEC 18045* (disponible en anglais seulement)

[22] ISO TR 24971:2020, *Dispositifs médicaux - Recommandations relatives à l'application de l'ISO 14971*

[23] ISO/IEC 27000:2018, *Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Vue d'ensemble et vocabulaire*

[24] ISO/IEC TR 24772-1:2019, *Programming languages – Guidance to avoiding vulnerabilities in programming languages – Part 1: Language-independent guidance* (disponible en anglais seulement)

[25] ISO 27789, *Informatique de santé – Historique d'expertise des dossiers de santé informatisés*

[26] ISO 27799, *Informatique de santé – Management de la sécurité de l'information relative à la santé en utilisant l'ISO/IEC 27002*

[27] ISO/IEC 29147, *Technologies de l'information – Techniques de sécurité – Divulgation de vulnérabilité*

[28] ISO/IEC 30111, *Technologies de l'information – Techniques de sécurité – Processus de traitement de la vulnérabilité*

[29] MISRA-C, Motor Industry Software Reliability Association, HORIBA MIRA Ltd, MISRA-C3, 2012 (available at misra.org.uk)

[30] MITRE, Rubric for Applying CVSS to Medical Devices (see https://www.mitre.org/publications/technical-papers/rubric-for-applying-cvss-to-medical-devices)

[31] ISO 13485:2016, *Dispositifs médicaux – Systèmes de management de la qualité – Exigences à des fins réglementaires*

[32] ISO/IEC/IEEE 24765:2017, *Systems and software engineering – Vocabulary* (disponible en anglais seulement)

[33] ISO/IEC 24767-1:2008, *Information technology – Home network security – Part 1: Security requirements* (disponible en anglais seulement)

[34] ISO/IEC 27039:2015*, Information technology – Security techniques – Selection, deployment and operations of intrusion detection and prevention systems (IDPS)* (disponible en anglais seulement)

[35] ISO/IEC 14764:2006, *Ingénierie du logiciel – Processus du cycle de vie du logiciel – Maintenance*

[36] IEC 62366-1:2015, *Dispositifs médicaux – Partie 1: Application de l'ingénierie de l'aptitude à l'utilisation aux dispositifs médicaux*

[37] IEC TR 63069, *Industrial-process measurement, control and automation – Framework for functional safety and security* (disponible en anglais seulement)

[38] ISO 9000:2015*, Systèmes de management de la qualité – Principes essentiels et vocabulaire*

[39] ISO/IEC 9834-1:2012, *Technologies de l'information – Procédures opérationnelles pour les organismes d'enregistrement d'identificateur d'objet – Partie 1: Procédures générales et arcs sommitaux de l'arborescence des identificateurs d'objet internationale*

[40] NIST SP800-30 Rev 1. *Guide for Conducting Risk Assessments*, 2021

[41] SAMATE, *NIST Software Assurance Metrics and Tool Evaluation*, National Institute of Standards and Technology (NIST),Gaithersburg Md, January 16, 2020

[42] SEI CERT C, C Coding Standard, https://wiki.sei.cmu.edu/confluence/display/c, Carnegie Mellon University, 2018

_____