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 It also gives information on projects, replaced and withdrawn publications.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).

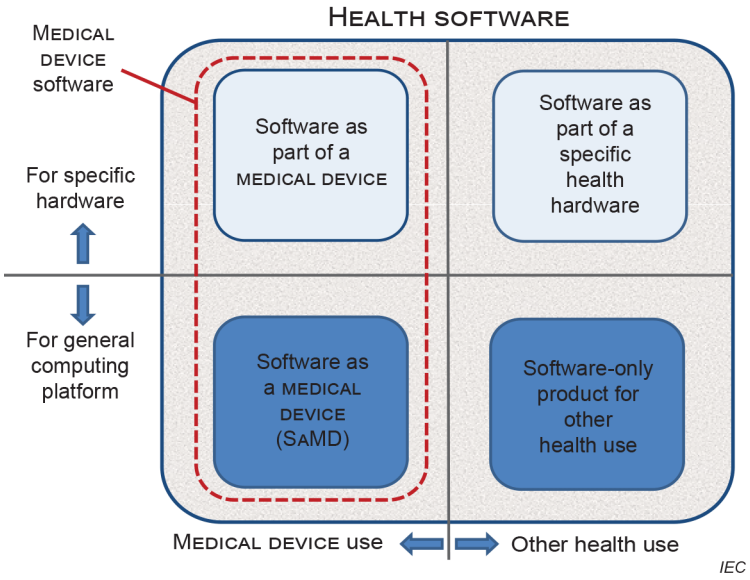
0.2 Field of application

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].

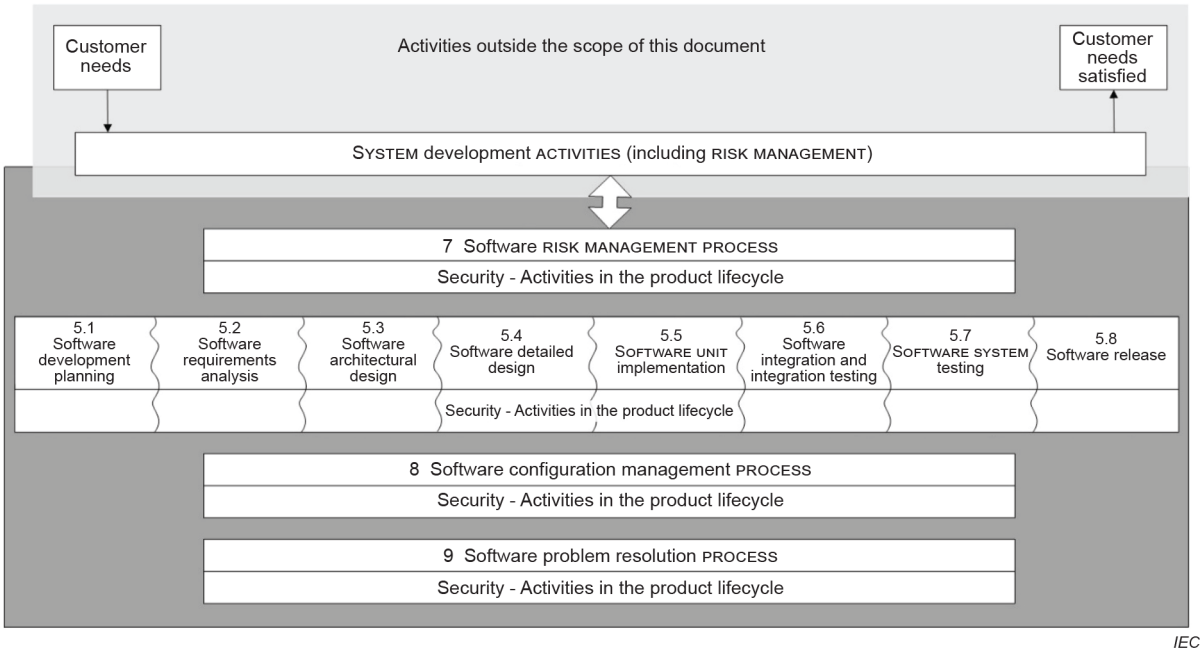
Clause 4 through Clause 9 of this document require establishing one or more PROCESSES that include identified ACTIVITIES. Per these normative parts of this document, the LIFE CYCLE PROCESSES implement these ACTIVITIES. None of the requirements in this document requires to implement these ACTIVITIES as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

3.13
HEALTH IT INFRASTRUCTURE
combined set of IT ASSETS available to the individual or organization for developing, configuring, integrating, maintaining, and using IT services and supporting health, patient care and other organizational objectives

[SOURCE: ISO 81001-1:2021[17], 3.3.7, modified – Deletion of the Note 1 to entry.]

3.14
HEALTH IT SYSTEM
a combination of interacting health information elements (including HEALTH SOFTWARE, medical devices, IT hardware, interfaces, data, procedures and documentation) that is configured and implemented to support and enable an individual or organization's specific health objectives

[SOURCE: ISO 81001-1:2021[17], 3.3.8, modified – Addition of "(including HEALTH SOFTWARE, medical devices, IT hardware, interfaces, data, procedures and documentation)".]

3.15
HEALTH SOFTWARE
software intended to be used specifically for managing, maintaining, or improving health of individual persons, or the delivery of care, or which has been developed for the purpose of being incorporated into a medical device

Note 1 to entry: HEALTH SOFTWARE fully includes what is considered software as a medical device.

[SOURCE: ISO 81001-1:2021[17], 3.3.9]

3.16
HEALTHCARE DELIVERY ORGANIZATION
HDO
facility or enterprise such as a clinic or hospital that provides healthcare services

[SOURCE: ISO 81001-1:2021[17], 3.1.4]

3.17
INTEGRITY
property of accuracy and completeness

[SOURCE: ISO/IEC 27000:2018, 3.36]

3.18
INTENDED ENVIRONMENT OF USE
conditions and setting in which users interact with the HEALTH SOFTWARE – as specified by the MANUFACTURER

3.19
INTENDED USE
INTENDED PURPOSE
use for which a PRODUCT, PROCESS or service is intended according to the specifications, instructions and information provided by the MANUFACTURER

Note 1 to entry: The intended medical indication, patient population, part of the body or type of tissue interacted with, user profile, INTENDED ENVIRONMENT OF USE, and operating principle are typical elements of the INTENDED USE.

[SOURCE: ISO 81001-1:2021[17], 3.2.7, modified – In Note 1 to entry, replacement of "USE ENVIRONMENT" with "INTENDED ENVIRONMENT OF USE".]

3.20
LIFE CYCLE
series of all phases in the life of a PRODUCT or system, from the initial conception to final decommissioning and disposal

[SOURCE: ISO 81001-1:2021[17], 3.3.12]

3.21
MAINTAINED SOFTWARE
SOFTWARE ITEM for which the MANUFACTURER will assume the risk related to SECURITY

Note 1 to entry: See also A.3.

3.22
MANUFACTURER
organization with responsibility for design or manufacture of a PRODUCT

Note 1 to entry: Responsibility extends to supporting ACTIVITIES during operations.

Note 2 to entry: There is only one MANUFACTURER, but technical responsibility can be with multiple entities along the supply chain, with service providers, or with entities at different stages in the LIFE CYCLE.

Note 3 to entry: Independent of the MANUFACTURER's responsibility, any specific legal accountability is defined by contracts and legislation.

[SOURCE: ISO 81001-1:2021[17], 3.1.7– Addition of the notes to entry.]

3.23
PROCESS
set of interrelated or interacting ACTIVITIES that use inputs to deliver an intended result (outcome)

[SOURCE: ISO 81001-1:2021[17], 3.2.10, modified – Added "(outcome)" after "result".]

3.24
PRODUCT
output of an organization that can be produced without any transaction taking place between the organization and the customer

Note 1 to entry: Production of a PRODUCT is achieved without any transaction necessarily taking place between provider and customer, but can often involve this service element upon its delivery to the customer.

Note 2 to entry: The dominant element of a PRODUCT is that it is generally tangible.

[SOURCE: ISO 81001-1:2021[17], 3.3.15]

3.25
REQUIRED SOFTWARE
SOFTWARE ITEM for which the MANUFACTURER will consider SECURITY-related risks known before release of the HEALTH SOFTWARE

Note 1 to entry: This includes SUPPORTED SOFTWARE. See A.3.

3.26
RESIDUAL RISK
risk remaining after RISK CONTROL measures have been implemented

[SOURCE: ISO 81001-1:2021[17], 3.4.9]

3.27
RISK CONTROL
PROCESS in which decisions are made and measures implemented by which risks are reduced to, or maintained within, specified levels

[SOURCE: ISO 81001-1:2021[17], 3.4.13, modified – Replacement of "limits" with "levels".]

3.28
RISK MANAGEMENT
systematic application of management policies, procedures and practices to the TASKS of analysing, evaluating, controlling and monitoring risk

[SOURCE: ISO 81001-1:2021[17], 3.4.16]

3.29
SAFETY
freedom from unacceptable risk

Note 1 to entry: In the context of SAFETY, risk is the combination of probability of occurrence of harm and severity of harm (see ISO/IEC Guide 51:2014).

Note 2 to entry: SECURITY incidents can lead to harm and can therefore have an impact on SAFETY.

[SOURCE: ISO 81001-1:2021[17], 3.2.12, modified – Addition of the notes to entry.]

3.30
SECURITY
CYBERSECURITY
state where information and systems are protected from unauthorized ACTIVITIES, such as access, use, disclosure, disruption, modification, or destruction to a degree that the related risks to violation of CONFIDENTIALITY, INTEGRITY, and AVAILABILITY are maintained at an acceptable level throughout the LIFE CYCLE

[SOURCE: ISO 81001-1:2021[17], 3.2.13]

3.31
SECURITY CAPABILITY
broad category of technical, administrative or organizational controls to manage risks to CONFIDENTIALITY, INTEGRITY, AVAILABILITY and accountability of data and systems

[SOURCE: ISO 81001-1:2021[17], 3.2.14]

3.32
SECURITY CONTEXT
minimum requirements and assumptions about the environment of HEALTH SOFTWARE – derived from the INTENDED ENVIRONMENT OF USE at PRODUCT-level, considering also the configuration and integration of HEALTH SOFTWARE and taking into account foreseeable unauthorized or unintended access

3.33
SOFTWARE COMPOSITION ANALYSIS
(electronic) analysis of binaries

Note 1 to entry: SOFTWARE COMPOSITION ANALYSIS can be supported by tools or online services.

3.34
SOFTWARE ITEM
identifiable part of a computer program, i.e. source code, object code, control code, control data, or a collection of these items

[SOURCE: IEC 62304:2006 and IEC 62304:2006/AMD1:2015, 3.25, modified – Deletion of the note.]

3.35
SOFTWARE MAINTENANCE
modification of HEALTH SOFTWARE after release

Note 1 to entry: Maintenance keeps the INTENDED USE and is done for one or more of the following reasons:

a) corrective, as fixing faults;

b) adaptive, as adapting to new hardware or software platform;

c) perfective, as implementing new requirements;

d) preventive, as making the PRODUCT more maintainable.

Note 2 to entry: See also ISO/IEC 14764:2006, 3.10.

[SOURCE: IEC 82304-1:2016, 3.21, modified – In the definition, the words "HEALTH SOFTWARE PRODUCT" have been replaced by "HEALTH SOFTWARE"; purposes of maintenance have been placed into a note that also highlights keeping the INTENDED USE, reference 3.10 has been added to the second note to entry; and “hard-“ has been replaced by “hardware”.]

3.36
SUPPORTED SOFTWARE
SOFTWARE ITEM for which the MANUFACTURER will notify the customer regarding known risks related to SECURITY

Note 1 to entry: This includes MAINTAINED SOFTWARE. See A.3.

3.37
TASK
single piece of work that needs to be done to achieve a specific goal

[SOURCE: IEC 62304:2006[8], 3.31, modified – Addition of "to achieve a specific goal".]

3.38
THREAT
potential for violation of SECURITY, which exists when there is a circumstance, capability, action, or event that could breach SECURITY and cause damage to CONFIDENTIALITY, INTEGRITY, AVAILABILITY of information ASSETS

[SOURCE: ISO 81001-1:2021[17], 3.4.1.21, modified – "Harm" replaced with "damage to CONFIDENTIALITY, INTEGRITY, AVAILABILITY of information ASSETS".]

3.39
THREAT MODEL
documented result of the THREAT MODELLING ACTIVITY

3.40
THREAT MODELLING
systematic exploration technique to expose any circumstance or event having the potential to cause damage to a system in the form of destruction, disclosure, modification of data, or denial of service

[SOURCE. ISO/IEC/IEEE 24765:2017, 3.4290, modified – Replacement of “harm” with “damage”.]

3.41
TRACEABILITY
link between the origin of requirements throughout the project LIFE CYCLE to design elements, and test cases

3.42
TRANSITIONAL HEALTH SOFTWARE
HEALTH SOFTWARE, which was released prior to publication of this document and which does not meet all requirements specified in Clause 4 through Clause 9 of this document

Note 1 to entry: For TRANSITIONAL HEALTH SOFTWARE its MANUFACTURER can claim conformance to the Annex F.

3.43
TRUST BOUNDARY
element of a THREAT MODEL that depicts a boundary where authentication is required or a change in trust level occurs (higher to lower or vice versa)

Note 1 to entry: TRUST BOUNDARY enforcement mechanisms for PRODUCT users typically include authentication (for example, challenge/response, passwords, biometrics or digital signatures) and associated authorization (for example, access control rules).

Note 2 to entry: TRUST BOUNDARY enforcement mechanisms for data typically include source authentication (for example, message authentication codes and digital signatures) and/or content VALIDATION.

3.44
USE ENVIRONMENT
actual conditions and setting in which users interact with the HEALTH SOFTWARE

Note 1 to entry: For the purpose of this document, that includes data interfaces.

[SOURCE: IEC 62366-1:2015 and IEC 62366-1:2015/AMD1:2020; 3.20, modified – "Medical device" replaced with "HEALTH SOFTWARE" in the definition, and replacement of Note 1 to entry.]

3.45
VALIDATION
confirmation, through the provision of objective evidence, that the requirements for a specific INTENDED USE or application have been fulfilled

Note 1 to entry: The objective evidence needed for a VALIDATION is the result of a test or other form of determination such as performing alternative calculations or reviewing documents.

Note 2 to entry: The word “validated” is used to designate the corresponding status.

Note 3 to entry: The use conditions for VALIDATION can be real or simulated.

[SOURCE: ISO 9000:2015, 3.8.13]

3.46
VERIFICATION
confirmation, through provision of objective evidence, that specified requirements have been fulfilled

Note 1 to entry: The objective evidence needed for a VERIFICATION can be the result of an inspection or of other forms of determination such as performing alternative calculations or reviewing documents.

Note 2 to entry: The ACTIVITIES carried out for VERIFICATION are sometimes called a qualification PROCESS.

Note 3 to entry: The word "verified" is used to designate the corresponding status.

[SOURCE: ISO 81001-1:2021[17], 3.2.16]

3.47
VULNERABILITY
flaw or WEAKNESS in a system's design, implementation, or operation and management that could be exploited to violate the system's SECURITY policy

[SOURCE: ISO 81001-1:2021[17], 3.4.22]

3.48
WEAKNESS
kind of deficiency

Note 1 to entry: A WEAKNESS can result in a SECURITY risk.

[SOURCE: ISO 81001-1:2021[17], 3.4.23, modified – Deletion of "and/or privacy risks" in Note 1 to entry.]

4 General requirements

4.1 Quality management

4.1.1 Quality management system

The MANUFACTURER shall perform SECURITY ACTIVITIES in the PRODUCT LIFE CYCLE on the basis of an established and documented quality management system.

The quality management system can be implemented according to ISO 13485 or other equivalent quality management system standards.

Throughout this document "establish an ACTIVITY (or ACTIVITIES)" means that the MANUFACTURER shall document this ACTIVITY (or ACTIVITIES) and shall ensure that this ACTIVITY (or ACTIVITIES) is done effectively and completely.

4.1.2 Identification of responsibilities

The MANUFACTURER shall designate and document the organizational roles and personnel responsible for each of the ACTIVITIES and PROCESSES required by this document.

NOTE Personnel can be identified through functional roles instead of names.

4.1.3 Identification of applicability

The MANUFACTURER shall identify the PRODUCTS or parts of PRODUCTS to which the secure LIFE CYCLE applies.

NOTE 1 For HEALTH SOFTWARE some IT exposure, networking, or data interfacing capabilities are assumed and therefore a secure software LIFE CYCLE is followed.

NOTE 2 This requirement is not about PRODUCT instances (and their identification) but about types of PRODUCTS or their parts – for example SOFTWARE ITEMS. Having this ACTIVITY (or ACTIVITIES) means that the MANUFACTURER has criteria for identifying which parts of its PRODUCTS are developed, maintained and supported using the ACTIVITIES described by this document.

4.1.4 SECURITY expertise

The MANUFACTURER shall establish an ACTIVITY (or ACTIVITIES) for identifying and providing SECURITY training and assessment programs to ensure that personnel assigned to the organizational roles and duties specified in 4.1.2 have demonstrated SECURITY expertise appropriate for those PROCESSES. Results of this ACTIVITY (or ACTIVITIES) include role descriptions, training profiles and training records.

NOTE This ACTIVITY (or ACTIVITIES) can be implemented for example as a part of 6.2 of ISO 13485:2016.

4.1.5 SOFTWARE ITEMS from third-party suppliers

The MANUFACTURER shall ensure that third-party suppliers perform applicable SECURITY LIFE CYCLE ACTIVITIES for each SOFTWARE ITEM if it meets both of the following criteria:

a) the SOFTWARE ITEM is mainly developed specifically for the MANUFACTURER and for a specific purpose; and

b) the SOFTWARE ITEM can have an impact on SECURITY.

The MANUFACTURER shall communicate requirements related to SECURITY for each SOFTWARE ITEM specifically developed by a third-party for the MANUFACTURER and for a specific purpose.

NOTE This requirement applies when the MANUFACTURER subcontracts a third-party to specifically develop a SOFTWARE ITEM which can have SECURITY implications. THREAT MODELLING is usually used to determine which SOFTWARE ITEM will have SECURITY implications.

4.1.6 Continuous improvement

The MANUFACTURER shall establish an ACTIVITY (or ACTIVITIES) for continuously improving the SECURITY development LIFE CYCLE. This ACTIVITY (or ACTIVITIES) shall include the analysis of SECURITY defects in SOFTWARE ITEMS / HEALTH SOFTWARE / PRODUCTS that have been deployed to the field – due to insufficient or lacking ACTIVITIES.

NOTE 1 This ACTIVITY (or ACTIVITIES) can be implemented for example as a part of 8.5 of ISO 13485:2016.

NOTE 2 This ACTIVITY (or ACTIVITIES) ensures that the MANUFACTURER improves the rigor of their SECURITY ACTIVITIES over time. In case of PROCESS-dependent SECURITY defects, it is important for the MANUFACTURER to help compensate for this by continuously improving their SECURITY ACTIVITIES.

4.1.7 Disclosing SECURITY-related issues

The MANUFACTURER shall establish an ACTIVITY (or ACTIVITIES) for informing regulatory authorities and PRODUCT users about VULNERABILITIES (that have been identified through ACTIVITIES as specified in 9.5) in supported PRODUCTS in a timely manner with content that includes but is not limited to the following information:

a) VULNERABILITY description, VULNERABILITY score as per CVSS or a similar system for ranking VULNERABILITIES, and affected PRODUCT version(s); and

b) description of the resolution.

NOTE 1 The description of the resolution can include references to installation of SECURITY updates – see Clause 12 of IEC 62443-4-1:2018[11].

NOTE 2 Timeliness is driven by authorities, applicable legislation, regulatory policy, PRODUCT SAFETY, and market forces. The strategy for handling third-party component VULNERABILITIES discovered by the PRODUCT developer takes into account the possibility of public disclosure by the third-party component supplier.

NOTE 3 This ACTIVITY (or ACTIVITIES) can be implemented for example as a part of 7.2.3 of ISO 13485:2016.

NOTE 4 See 4.1.9, 4.2 and 6.2.

4.1.8 Periodic review of SECURITY defect management

The MANUFACTURER shall establish an ACTIVITY (or ACTIVITIES) for conducting periodic reviews of the software problem resolution PROCESS.

Periodic reviews of the ACTIVITIES shall, at a minimum, examine SECURITY-related issues managed through the PROCESS since the last periodic review to determine if the management PROCESS was complete, efficient, and led to the resolution of SECURITY-related issues.

Periodic reviews of the SECURITY-related issue management PROCESS shall be conducted at least annually or as part of monitoring, measurement and analysis of PROCESSES of 4.1.3 of ISO 13485:2016.

NOTE This ACTIVITY (or ACTIVITIES) can be implemented for example as a part of 5.6 of ISO 13485:2016.

4.1.9 ACCOMPANYING DOCUMENTATION review

The MANUFACTURER shall establish an ACTIVITY (or ACTIVITIES) for identifying, characterizing and tracking to closure SECURITY-related errors and omissions in ACCOMPANYING DOCUMENTATION including the SECURITY guidelines.

NOTE This ACTIVITY (or ACTIVITIES) can be implemented for example as a part of 7.3 of ISO 13485:2016.

4.2 SECURITY RISK MANAGEMENT

The MANUFACTURER shall establish a PROCESS for managing RISKS associated with SECURITY. This PROCESS shall use THREAT MODELLING for identifying VULNERABILITIES, estimating and evaluating the associated THREATS, controlling these THREATS, and monitoring the effectiveness of the RISK CONTROL (SECURITY) measures, taking into account the INTENDED USE and the USE ENVIRONMENT of the HEALTH SOFTWARE.

NOTE 1 A medical device designed in a layered DEFENSE-IN-DEPTH approach does not rely on SECURITY controls in the operating environment. Nevertheless, as part of this layered DEFENSE-IN-DEPTH approach, there are expectations on the intended operating environment. Expectations on the operating environment can include protection and performance characteristics and can be inputs to THREAT MODELLING.

The MANUFACTURER shall establish the criteria for risk acceptability that shall be applied when determining the appropriate way to address each VULNERABILITY.

The SECURITY RISK MANAGEMENT should incorporate outcomes of the THREAT MODELLING ACTIVITY (or ACTIVITIES) and follow guidelines and industry best practice.

Detailed PROCESS steps are described in Clause 7.

NOTE 2 This PROCESS can be part of an existing general RISK MANAGEMENT PROCESS. SECURITY RISK MANAGEMENT can be conducted under the framework of ISO 14971 with an appropriate mapping of VULNERABILITY, THREAT and other SECURITY-related terms and addition of SECURITY-relevant ACTIVITIES. (See ISO TR 24971:2020 for possible mapping.)

The MANUFACTURER shall document any RESIDUAL RISK associated with a VULNERABILITY that remains in the system and shall also document respective compensating controls applied.

See Annex C on THREAT MODELLING.

4.3 SOFTWARE ITEM classification relating to risk transfer

The MANUFACTURER shall document which SOFTWARE ITEM is either

a) MAINTAINED SOFTWARE;

b) SUPPORTED SOFTWARE; or

c) REQUIRED SOFTWARE.

NOTE This ACTIVITY (or ACTIVITIES) can be implemented for example as a part of 7.4 of ISO 13485:2016.

5 Software development PROCESS

5.1 Software development planning

5.1.1 ACTIVITIES in the LIFE CYCLE PROCESS

The MANUFACTURER shall establish general LIFE CYCLE ACTIVITIES – from conception to decommissioning – that are consistent and integrated with a commonly accepted PRODUCT development PROCESS including but not limited to:

a) CONFIGURATION MANAGEMENT with change controls and change history;

b) PRODUCT description and requirements definition with requirements TRACEABILITY;

c) software or hardware design and implementation practices, such as modular design;

d) repeatable testing VERIFICATION and VALIDATION PROCESS;

e) review and approval of all development PROCESS records;

f) PRODUCT support; and

g) SECURITY updates and patching for HEALTH SOFTWARE.

NOTE PRODUCT support means providing of information, assistance and training to install and make HEALTH SOFTWARE operational in its intended environment and to distribute improved capabilities to users. See ISO/IEC/IEEE 24765:2017.

The MANUFACTURER shall document the justification for not implementing requirements of this document within a given HEALTH SOFTWARE project based on review and approval by personnel with the appropriate SECURITY expertise.

5.1.2 Development environment SECURITY

The MANUFACTURER shall establish risk-based procedural and technical controls for protecting the IT infrastructure used for development, production delivery and maintenance from unauthorized access, corruption and deletion. This includes protecting the HEALTH SOFTWARE during design, implementation, updates, testing and release.

5.1.3 Secure coding standards

The MANUFACTURER shall establish and maintain secure coding standards consistent with current best practices related to the design and implementation of secure software systems.

See Annex A.

5.2 HEALTH SOFTWARE requirements analysis

5.2.1 HEALTH SOFTWARE SECURITY requirements

The MANUFACTURER shall establish an ACTIVITY (or ACTIVITIES) for ensuring that SECURITY requirements are documented for the HEALTH SOFTWARE including requirements for SECURITY CAPABILITIES related to installation, operation, maintenance and decommissioning.

NOTE 1 IEC TR 60601-4-5 gives guidance on the specification of SECURITY CAPABILITIES and their documentation in the ACCOMPANYING DOCUMENTATION and provides a method of determining requirements from the SECURITY CAPABILITY level.

NOTE 2 IEC TR 80001-2-2 specifies SECURITY-related needs, risks and controls as a guidance for disclosure and communication between the MANUFACTURER and the HEALTHCARE DELIVERY ORGANIZATION.

NOTE 3 The PRODUCT requirements PROCESS interfaces with HEALTH SOFTWARE requirements. Some technical controls can be implemented at PRODUCT level (for example by hardware). See E.2.1.

5.2.2 SECURITY requirements review

The MANUFACTURER shall establish an ACTIVITY (or ACTIVITIES) for ensuring that SECURITY requirements

a) implement PRODUCT requirements including those relating to RISK CONTROL;
b) do not contradict one another;
c) are expressed in terms that avoid ambiguity; and
d) are stated in terms that permit establishment of test criteria and performance of tests.

The MANUFACTURER shall document the level of independence of the reviewers. Each of the following representative disciplines shall participate in this ACTIVITY (or ACTIVITIES):

a) architects/developers (those who will implement the requirements);
b) testers (those who will validate that the requirements have been met);
c) cross-functional experts (can include those with clinical expertise); and
d) SECURITY advisor(s).

NOTE 1 A single person can be responsible for multiple disciplines. It is not advisable to have a single person representing all disciplines.

NOTE 2 The list of disciplines is documented at least once per project.

NOTE 3 A quality management system like that of ISO 13485 implies consideration of independence of reviewers.

5.2.3 SECURITY risks for REQUIRED SOFTWARE

The MANUFACTURER shall establish an ACTIVITY (or ACTIVITIES) that identifies and manages the SECURITY risks of all REQUIRED SOFTWARE.

NOTE 1 This ACTIVITY (or ACTIVITIES) ensures that HEALTH SOFTWARE requirements are aware of the SECURITY needs of REQUIRED SOFTWARE.

NOTE 2 This ACTIVITY(or ACTIVITIES) can be part of supply chain SECURITY ACTIVITIES.

5.3 Software architectural design

5.3.1 DEFENSE-IN-DEPTH ARCHITECTURE/design

The MANUFACTURER shall establish an ACTIVITY(or ACTIVITIES) to specify a secure ARCHITECTURE.

At each stage of development, the MANUFACTURER should consider DEFENSE-IN-DEPTH and assign technical requirements to each layer of defense.

When identifying technical SECURITY RISK CONTROLS, the MANUFACTURER shall take into account requirements regarding SAFETY or performance of HEALTH SOFTWARE.

NOTE DEFENSE-IN-DEPTH can include SECURITY requirements in the ACCOMPANYING DOCUMENTATION to be implemented by the HDO.

5.3.2 Secure design best practices

The MANUFACTURER shall establish an ACTIVITY (or ACTIVITIES) to identify, enforce and maintain secure design practices. The MANUFACTURER shall document secure design best practices, which should include but are not limited to:

a) documenting all TRUST BOUNDARIES as part of the design;
b) least privilege (granting only the privileges to users/software necessary to perform intended operations);
c) using proven secure SOFTWARE ITEMS/designs where possible;

d) economy of mechanism (striving for simple designs);

e) using secure design patterns;

f) ATTACK SURFACE reduction;

g) removing backdoors, debug access and debug information used during development or documenting their presence and the need to protect them from unauthorized access; and

h) protecting any remaining debug information from unauthorized access.

The MANUFACTURER shall define a SECURITY ARCHITECTURE as part of DEFENSE-IN-DEPTH, including the practices listed above as appropriate.

NOTE See Annex B.

5.3.3 SECURITY architectural design review

The MANUFACTURER shall implement an architectural review of the HEALTH SOFTWARE with respect to behavior under adverse conditions:

a) effective segregation of SOFTWARE ITEMS;

b) the secure design best practices (see 5.3.2); and

c) potential SECURITY flaws introduced by the ARCHITECTURE.

The MANUFACTURER shall document and implement the architectural design review.

NOTE Segregation uses technical controls in design and implementation in order to ensure that SOFTWARE ITEMS cannot be influenced by other SOFTWARE ITEMS of the HEALTH SOFTWARE in an unintended way.

5.4 Software design

5.4.1 Software design best practices

The MANUFACTURER shall establish an ACTIVITY (or ACTIVITIES) to develop and document a secure HEALTH SOFTWARE design and maintain the use of best practices for the secure design, taking into account:

a) software technology at application level (for examples algorithms, methods);

b) the programming technology used, (for example programming language);

c) the secure design best practices in 5.3.2.

5.4.2 Secure design

The HEALTH SOFTWARE design shall include measures to address the THREATS identified in the THREAT MODEL.

NOTE The SECURITY CONTEXT for HEALTH SOFTWARE is derived from the INTENDED ENVIRONMENT OF USE at PRODUCT-level, considering also the configuration and integration of HEALTH SOFTWARE.

5.4.3 Secure HEALTH SOFTWARE interfaces

The HEALTH SOFTWARE design shall identify and characterize each interface of the HEALTH SOFTWARE including physical and logical interfaces. As appropriate, the MANUFACTURER identifies as part of the design:

a) whether the interface is externally accessible (by other PRODUCTS) or internally accessible – between SOFTWARE ITEMS of the HEALTH SOFTWARE- or both;

b) SECURITY implications of the HEALTH SOFTWARE SECURITY CONTEXT on the external interface;

c) potential users of the interface and the ASSETS that can be accessed through the interfaces (directly or indirectly);

d) whether the static design includes access to interfaces across TRUST BOUNDARIES;

e) SECURITY considerations, assumptions and/or constraints associated with the use of the interface within the HEALTH SOFTWARE SECURITY CONTEXT; including applicable THREATS;

f) the SECURITY roles, privileges/rights and access control permissions needed to use the interface and to access the ASSETS defined in c);

g) the SECURITY CAPABILITIES and/or compensating mechanisms used to safeguard the interface and the ASSETS identified in c) including run-time VALIDATION of inputs as well as handling outputs and errors;

h) the use of third-party SOFTWARE ITEMS to implement the interface and their SECURITY CAPABILITIES;

i) documentation that describes how to use the interface if it is externally accessible; and

j) description of how the design mitigates the THREATS identified in the THREAT MODEL.

NOTE The SECURITY CONTEXT for HEALTH SOFTWARE is derived from the INTENDED ENVIRONMENT OF USE at PRODUCT-level, considering also the configuration and integration of HEALTH SOFTWARE.

5.4.4 Detailed design VERIFICATION for SECURITY

The MANUFACTURER shall establish an ACTIVITY (or ACTIVITIES) for conducting design reviews to identify, characterize and track to closure WEAKNESSES associated with each significant revision of the secure design including but not limited to:

a) SECURITY requirements that were not adequately addressed by the design;

b) THREATS and their ability to exploit VULNERABILITIES in PRODUCT interfaces, TRUST BOUNDARIES and ASSETS;

c) identification, documentation and characterization of detailed design best-practices that were not followed (5.3.2 and 5.4.1).

NOTE The design reviews also take into account each software service that is used by HEALTH SOFTWARE to achieve its intended functionality, for example: cloud, software-/ infrastructure-/ platform-as-a-service.

5.5 Software unit implementation and VERIFICATION

5.5.1 Secure coding standards

The MANUFACTURER shall establish an implementation ACTIVITY (or ACTIVITIES) following secure coding standards.

See clause A.4.

5.5.2 SECURITY implementation review

The MANUFACTURER shall establish an ACTIVITY (or ACTIVITIES) to ensure that implementation reviews are performed for identifying, characterizing and feeding into the problem resolution PROCESS all SECURITY-related issues associated with the implementation of the secure design including:

a) identification of SECURITY requirements (see 5.2) that were not adequately addressed by the implementation;

NOTE Requirements allocation, including SECURITY requirements, is part of typical design PROCESSES.

b) identify secure coding standards used and document any parts of the secure coding standards that were not followed (for example, use of banned functions or failure to apply the principle of least privilege);

c) Static Code Analysis (SCA) for source code to determine secure coding errors using the secure coding standard for the supported programming language, as established in 5.1.3. SCA is often supported by tools, but it can be done through code inspections and code-walkthroughs.

d) review of the implementation and its TRACEABILITY to the SECURITY CAPABILITIES defined to support the SECURITY design (see 5.3 and 5.4); and

e) examination of THREATS and their ability to exploit implementation interfaces, TRUST BOUNDARIES and ASSETS (see 5.3 and 5.4).

5.6 Software integration testing

The MANUFACTURER can perform some of the software system testing as a part of software integration testing (see 5.7).

As a part of HEALTH SOFTWARE integration testing, the MANUFACTURER should consider SECURITY policy differences across TRUST BOUNDARIES.

5.7 Software system testing

5.7.1 SECURITY requirements testing

The MANUFACTURER shall establish an ACTIVITY (or ACTIVITIES) for verifying that the HEALTH SOFTWARE SECURITY functions meet the SECURITY requirements and that the HEALTH SOFTWARE handles error scenarios and invalid input. Based on the INTENDED ENVIRONMENT OF USE, types of testing shall include:

a) functional testing of SECURITY requirements;

b) performance and scalability testing;

c) boundary/edge condition, stress and malformed or unexpected input tests with potential SECURITY consequences; and

d) testing each software service that is used by HEALTH SOFTWARE to achieve its intended functionality, in the context of responsibility agreements among service providers, MANUFACTURERS and operators, for example: cloud services, software-as-a-service, infrastructure-as-a-service, platform-as-a-service.

NOTE See B.5.7.1.

5.7.2 THREAT mitigation testing

The MANUFACTURER shall establish an ACTIVITY (or ACTIVITIES) for testing the effectiveness of the mitigation for the THREATS identified and assessed in the THREAT MODEL. ACTIVITIES shall include:

a) creating and executing adequate testing for each mitigation implemented to address a specific THREAT, in order to ensure that the mitigation works as designed;

b) creating and executing plans for attempting to thwart each mitigation; and

c) ensuring that the mitigation does not introduce other VULNERABILITIES to the design.

5.7.3 VULNERABILITY testing

The MANUFACTURER shall establish an ACTIVITY (or ACTIVITIES) for performing tests that focus on identifying and characterizing potential SECURITY VULNERABILITIES in the HEALTH SOFTWARE. Known VULNERABILITY testing shall be based upon, at a minimum, recent contents of an established, industry-recognized, public source for known VULNERABILITIES. As appropriate, testing shall include:

a) abuse case for malformed or unexpected input testing focused on uncovering SECURITY issues. This shall include manual or automated abuse case testing and specialized types of abuse case testing on all external interfaces and protocols. Examples include fuzz testing and network traffic load testing and capacity testing;

b) ATTACK SURFACE testing to determine all avenues of ingress and egress to and from the system, common VULNERABILITIES including but not limited to weak access-control-lists (ACLs), exposed ports and services running with elevated privileges;

c) “closed box” known VULNERABILITY scanning focused on detecting known VULNERABILITIES in (if applicable) hardware, host, interfaces or SOFTWARE ITEMS;

NOTE 1 For example, this could be a network based known VULNERABILITY scan.

d) SOFTWARE COMPOSITION ANALYSIS on all binary executable files including embedded firmware, to be used with HEALTH SOFTWARE and delivered by a third-party supplier. This analysis can be used to detect:

1) known VULNERABILITIES in the SOFTWARE ITEMS;
2) linking to vulnerable libraries;
3) SECURITY rule violations;
4) compiler settings that can lead to VULNERABILITIES; and
5) comparison of the software encountered to the software bill of materials.

NOTE 2 Tools can support SOFTWARE COMPOSITION ANALYSIS by generating a list of software packages included.

e) dynamic SECURITY testing – like e.g. fuzz testing, that detects flaws not visible under static code analysis, including but not limited to denial of service conditions due to failing to release runtime handles, memory leaks and accesses made to shared memory without authentication. This testing shall be applied if such tools are available.

NOTE 3 Exhaustive runtime testing cannot be done effectively without tools.

5.7.4 Penetration testing

The MANUFACTURER shall establish an ACTIVITY (or ACTIVITIES) to identify and characterize WEAKNESSES via tests that focus on discovering and exploiting SECURITY VULNERABILITIES in the HEALTH SOFTWARE.

See B.5.7.4.

5.7.5 Managing conflicts of interest between testers and developers

The MANUFACTURER shall document means of ensuring objectivity of the test effort for these tests:

a) ATTACK SURFACE analysis,
b) SECURITY requirements testing,
c) THREAT mitigation testing,
d) VULNERABILITY testing,
e) known VULNERABILITY scanning and
f) penetration testing.

NOTE Objectivity intends to support reproducibility of outcomes based on facts.

See A.1 and B.5.7.5.

5.8 Software release

5.8.1 Resolve findings prior to release

The MANUFACTURER shall establish an ACTIVITY (or ACTIVITIES) to ensure that all findings from system testing have been handled by the problem resolution PROCESS (Clause 9).

5.8.2 Release documentation

As a part of the software release ACTIVITY (or ACTIVITIES), the MANUFACTURER shall establish requirements for ACCOMPANYING DOCUMENTATION:

a) secure operation guidelines;

b) PROCESS rigor and conformance documentation including the scoping (Clause 4), tailoring (Clause 5) and information on coverage of documentation (Annex E);

NOTE These documents help meet any regulatory or contractual obligations.

c) account management guidelines (if applicable); and

d) appropriate information about relevant RESIDUAL RISKS to SECURITY remaining in the HEALTH SOFTWARE.

See Annex E for an informative specification of documentation contents.

5.8.3 File INTEGRITY

The MANUFACTURER shall establish an ACTIVITY (or ACTIVITIES) to provide an INTEGRITY VERIFICATION mechanism for all scripts, executables and other SECURITY-relevant files used with a HEALTH SOFTWARE.

This ACTIVITY (or ACTIVITIES) is required to ensure that PRODUCT users can verify that executables, scripts, and other important files received from the MANUFACTURER have not been altered. Common methods of meeting this requirement include cryptographic hashes and digital signatures (which also provide proof of origin).

5.8.4 Controls for private keys

The MANUFACTURER shall have procedural and technical controls in place to protect private keys used for code signing from unauthorized access or modification.

NOTE This refers to the software supply chain and the focus is on code signing to support secure distribution and delivery of HEALTH SOFTWARE.

5.8.5 Assessing and addressing SECURITY-related issues

The MANUFACTURER shall establish an ACTIVITY (or ACTIVITIES) for verifying that a HEALTH SOFTWARE or an update is not released until its SECURITY-related issues have been addressed and tracked to closure (see 9.5). This includes issues associated with:

a) requirements (see 5.2);

b) SECURITY by design (see 5.3 and 5.4);

c) implementation (see 5.5);

d) VERIFICATION / VALIDATION (see 5.5, 5.6 and 5.7); and

e) SECURITY defect management (see 9.4).

5.8.6 ACTIVITY completion

The MANUFACTURER shall establish an ACTIVITY (or ACTIVITIES) for verifying that, prior to HEALTH SOFTWARE release, all applicable SECURITY-related PROCESSES required by this document have been completed with records documenting the completion of each ACTIVITY (or ACTIVITIES) or PROCESS.

5.8.7 SECURE decommissioning guidelines for HEALTH SOFTWARE

The MANUFACTURER shall establish an ACTIVITY (or ACTIVITIES) to create PRODUCT user documentation that includes guidelines for removing the HEALTH SOFTWARE from use.

6 SOFTWARE MAINTENANCE PROCESS

6.1 Establish SOFTWARE MAINTENANCE plan

6.1.1 Timely delivery of SECURITY updates

The MANUFACTURER shall establish – as a part of the update ACTIVITIES – a policy that specifies the timeframes for delivering and qualifying SECURITY updates to PRODUCT users. At a minimum, this policy shall consider the following factors:

a) the potential impact (technical, for SAFETY, effectiveness, SECURITY) of the VULNERABILITY;

b) public knowledge of the VULNERABILITY;

c) whether published EXPLOITS exist for the VULNERABILITY;

d) the volume of deployed PRODUCTS that are affected; and

e) the AVAILABILITY of an effective external control when no HEALTH SOFTWARE update is being provided.

NOTE 1 Some regulatory authorities can have specific timeframe requirements.

NOTE 2 The MANUFACTURER can categorize SECURITY updates (for example by potential impact) and specify appropriate timeframes. See IEC TR 60601-4-5.

NOTE 3 During an acceptable time-interval in which the MANUFACTURER develops a technical control, any documented mitigations and constraints on the INTENDED USE can be based on RISK MANAGEMENT. It is advisable to develop and deploy a technical mitigation in HEALTH SOFTWARE.

NOTE 4 IEC TR 60601-4-5 specifies a minimum performance ("Essential Function" term as used in IEC 62443 series) to be available with medical devices in case of relevant CYBERSECURITY ATTACKS on the HEALTHCARE DELIVERY ORGANIZATION'S (HDO) IT network. Such minimum performance ensures basic functionality until a verified SECURITY update is available in situations in which all medical devices of the same type in the HDO can be affected by a given CYBERSECURITY ATTACK simultaneously. Therefore, for medical devices, the software LIFE CYCLE ACTIVITIES ensure that:

a) "essential functions" remain secure for the interval until a SECURITY update is installed, and

b) SECURITY updates always re-establish the SECURITY CAPABILITY as specified in the ACCOMPANYING DOCUMENTATION.

Additional guidance is provided by IEC TR 60601-4-5.

6.2 Problem and modification analysis

6.2.1 Monitoring public incident reports

The MANUFACTURER shall establish an ACTIVITY (or ACTIVITIES) to actively collect and review relevant sources of information about VULNERABILITIES regarding SUPPORTED SOFTWARE.

NOTE This includes HEALTH SOFTWARE.

6.2.2 SECURITY update VERIFICATION

The MANUFACTURER shall establish an ACTIVITY (or ACTIVITIES) for verifying that SECURITY updates created by the MANUFACTURER address the intended SECURITY VULNERABILITIES.

The MANUFACTURER shall establish an ACTIVITY (or ACTIVITIES) for verifying that SECURITY updates do not introduce unintended effects to functional or quality attributes of HEALTH SOFTWARE. Such SECURITY updates include but are not limited to updates created by:

a) the HEALTH SOFTWARE MANUFACTURER,

b) suppliers of SOFTWARE ITEMS used in the HEALTH SOFTWARE, and

c) suppliers of SOFTWARE ITEMS or platforms on which the HEALTH SOFTWARE depends.

The MANUFACTURER can define that for certain SOFTWARE ITEMS or platforms, there is a shared responsibility for such VERIFICATION.

NOTE Also see Clause 9.

6.3 Modification implementation

6.3.1 SUPPORTED SOFTWARE SECURITY update documentation

The MANUFACTURER shall establish a policy to inform PRODUCT users about updates for SUPPORTED SOFTWARE. This information shall include:

a) stating whether the HEALTH SOFTWARE is compatible with the SUPPORTED SOFTWARE SECURITY update; and

b) for SECURITY updates that are unapproved by the HEALTH SOFTWARE MANUFACTURER, the mitigations that can be used instead of applying the update.

6.3.2 MAINTAINED SOFTWARE SECURITY update delivery

The MANUFACTURER shall establish an ACTIVITY (or ACTIVITIES) to ensure that SECURITY updates are made available for MAINTAINED SOFTWARE to PRODUCT users.

See E.2.5.

6.3.3 MAINTAINED SOFTWARE SECURITY update INTEGRITY

The MANUFACTURER shall establish an ACTIVITY (or ACTIVITIES) to ensure that each applicable update for MAINTAINED SOFTWARE is made available to PRODUCT users in a manner that facilitates INTEGRITY VERIFICATION of the SECURITY update.

This ACTIVITY (or ACTIVITIES) is required to ensure that HEALTH SOFTWARE users can obtain applicable SECURITY patches for the MAINTAINED SOFTWARE to reduce the possibility that the SECURITY patches are fraudulent. Having this ACTIVITY (or ACTIVITIES) means that the MANUFACTURER provides a mechanism or technique that allows HEALTH SOFTWARE users to verify the authenticity of patches. Concurrent release of patches for all MAINTAINED SOFTWARE can reduce the time window between awareness of the VULNERABILITY and the AVAILABILITY of patches.

7 SECURITY RISK MANAGEMENT PROCESS

7.1 RISK MANAGEMENT context

7.1.1 General

The MANUFACTURER shall establish and maintain a PROCESS for managing SECURITY risks related to HEALTH SOFTWARE as a part of its PRODUCT RISK MANAGEMENT approach. This PROCESS should consist of the following PROCESS steps described in 7.1.2, 7.2, 7.3, 7.4 and 7.5.

See Annex C.

7.1.2 PRODUCT SECURITY CONTEXT

The MANUFACTURER shall establish an ACTIVITY (or ACTIVITIES) to ensure that the intended PRODUCT SECURITY CONTEXT is documented. This ACTIVITY (or ACTIVITIES) is required to ensure that the minimum requirements of the environment and the assumptions about that environment are documented in order to achieve the SECURITY level for which the PRODUCT was designed.

The purpose of defining this information is so that both the developers of the HEALTH SOFTWARE and the PRODUCT users have the same understanding about how the PRODUCT is intended to be used. This will help the developers make appropriate design decisions and the users to use the PRODUCT as it was intended.

The SECURITY CONTEXT could include:

a) location in the network;

b) physical SECURITY or CYBERSECURITY provided by the environment where the PRODUCT will be deployed;

c) isolation (from a network perspective);

d) if known, potential impact to SAFETY caused by degradation of SECURITY;

e) SECURITY controls implemented in dedicated hardware with which the HEALTH SOFTWARE is intended to be used.

For example, it is important to document whether physical SECURITY is required. If no physical SECURITY is expected to be present, then that can add a number of related requirements such as not allowing push-button configuration on the PRODUCT. Another example is if the PRODUCT cannot feasibly (i.e. without reducing SAFETY or performance) implement a firewall of its own, it can be expected to be protected by a user-supplied firewall that connects it to the health-IT-network.

Documenting these external SECURITY features for the PRODUCT (its SECURITY CONTEXT) allows developers to design a DEFENSE-IN-DEPTH strategy that complements this SECURITY CONTEXT and testers to validate and verify the SECURITY of a PRODUCT in an environment similar to how it is intended to be deployed.

Having this PROCESS means that the deployment environment in which the PRODUCT is intended to be used is correctly represented in all PROCESSES involved in the development and testing of this PRODUCT and are documented.

7.2 Identification of VULNERABILITIES, THREATS and associated adverse impacts

The MANUFACTURER shall establish an ACTIVITY (or ACTIVITIES) which identifies and documents any vulnerabilities, THREATS and associated adverse impacts affecting CONFIDENTIALITY, INTEGRITY, AVAILABILITY of ASSETS in HEALTH SOFTWARE. This ACTIVITY (or ACTIVITIES) shall consider the INTENDED USE and the INTENDED ENVIRONMENT OF USE with respect to the SECURITY CONTEXT.

This ACTIVITY (or ACTIVITIES) shall be employed to ensure that all PRODUCTS shall have a THREAT MODEL specific to the current development scope of the PRODUCT with the following characteristics (where applicable):

a) correct flow of categorized information throughout the system;

b) TRUST BOUNDARIES;

c) PROCESSES;

d) data stores;

e) interacting external entities;

f) internal and external communication protocols implemented in the PRODUCT;

g) externally accessible physical ports including debug ports;

h) circuit board connections such as Joint Test Action Group (JTAG) connections or debug headers which might be used to ATTACK the hardware;

i) potential ATTACK vectors including ATTACK on the (intended) hardware;

j) potential THREATS;

k) SECURITY-related issues identified; and

l) external dependencies in the form of drivers or third-party applications (code that is not developed by the supplier) that are linked into the application.

The THREAT MODEL shall be reviewed and verified by the development team to ensure that it is correct and understood.

The THREAT MODEL shall be reviewed periodically (at least once a year) for released PRODUCTS and updated if required in response to the emergence of new THREATS to the PRODUCT even if the design does not change.

Any issues identified in the THREAT MODEL shall be addressed as defined in 9.4 and 9.5.

7.3 Estimation and evaluation of SECURITY risk

The MANUFACTURER shall establish an ACTIVITY (or ACTIVITIES) to:

a) estimate the risk of the VULNERABILITIES identified above. Risk estimation is done considering the adverse impact of that VULNERABILITY to CYBERSECURITY. This estimation can be supported by using VULNERABILITY scoring, such as the Common VULNERABILITY Scoring System (CVSS) or MITRE[30] scoring rubric for medical devices. The scoring system can also be based on a likelihood/severity scheme used by the MANUFACTURER for other risks (see e.g. ISO/IEC Guide 51 or ISO 14971);

b) evaluate the estimated risks and – based on scoring – determine if the risk is acceptable or not; and

c) inform the PRODUCT RISK MANAGEMENT PROCESS about any updates to the THREAT MODEL.

7.4 Controlling SECURITY risks

The MANUFACTURER shall determine whether SECURITY RISK CONTROL measures are appropriate for reducing the SECURITY risks to an acceptable level based on SECURITY risk acceptance policies. If RISK CONTROLS are deemed appropriate, the MANUFACTURER shall:

- select appropriate mitigations;
- determine whether these mitigations result in new risks or increase other risks;
- implement selected mitigations; and
- verify the effectiveness of the implemented measures.

The MANUFACTURER shall document the results of these ACTIVITIES.

Handling of RESIDUAL RISKS to SECURITY shall be done in cooperation with the PRODUCT RISK MANAGEMENT.

NOTE The assessment of SECURITY RISKS is influenced by the SECURITY CONTEXT. The SECURITY RISK acceptability is based on the respective score and the acceptability threshold for SECURITY RISKS. Also see 4.2.

7.5 Monitoring the effectiveness of RISK CONTROLS

The MANUFACTURER shall monitor the effectiveness of RISK CONTROLS by information collection and review during the post-release phase.

This ACTIVITY (or ACTIVITIES) shall also inform other ACTIVITIES and PROCESSES of the issue or related issue(s), including PROCESSES for other PRODUCTS / revisions; and inform third parties (e.g. suppliers) if problems have been found in third-party source code to be used with the HEALTH SOFTWARE.

Any issues identified in the THREAT MODEL of released HEALTH SOFTWARE will be addressed as defined in 9.4 and 9.5.

8 Software CONFIGURATION MANAGEMENT PROCESS

The MANUFACTURER shall establish a general PRODUCT development/maintenance/support PROCESS that includes CONFIGURATION MANAGEMENT with change controls and change history.

For SECURITY obligations with HEALTH SOFTWARE already released or in the market, CONFIGURATION MANAGEMENT shall provide the capability to reproduce a list of included external components that are or could become susceptible to VULNERABILITIES.

9 Software problem resolution PROCESS

9.1 Overview

The ACTIVITIES specified by this clause are used for handling SECURITY-related issues of HEALTH SOFTWARE.

9.2 Receiving notifications about VULNERABILITIES

The MANUFACTURER shall establish an ACTIVITY (or ACTIVITIES) that enables the reporting of information regarding VULNERABILITIES to the MANUFACTURER – independent of whether they come from an internal entity, an external entity or via a complaint-handling system.

This reception ACTIVITY (or ACTIVITIES) shall receive and track to closure reports on SECURITY-related issues in the HEALTH SOFTWARE from the following sources including at a minimum:

a) SECURITY VERIFICATION and VALIDATION testers;

b) suppliers of third-party components used in the PRODUCT;

c) PRODUCT developers and testers;

d) PRODUCT users including integrators, operators, administrators, and maintenance personnel;

e) data obtained from audit event log information;

f) SECURITY researchers (SECURITY VULNERABILITY reporters), also see ISO/IEC 29147; and

g) data or notifications about widespread VULNERABILITIES that can affect the HEALTH SOFTWARE – See 6.2.

NOTE Typically, such information comes from publications, reports, independent SECURITY research, internal investigations, CERTs and Information Sharing and Analysis Organizations (ISAOs).

9.3 Reviewing VULNERABILITIES

The MANUFACTURER shall establish an ACTIVITY (or ACTIVITIES) that enables the investigation of VULNERABILITIES in a timely manner to determine their:

a) applicability to the PRODUCT;

b) verifiability; and

c) related THREATS.

NOTE 1 Timeliness is driven by authorities, applicable legislation, regulatory policy and market forces.

NOTE 2 This PROCESS can be implemented for example as a part of the PROCESSES per 8.2.1, 8.2.2 and 8.2.3 of ISO 13485:2016.

9.4 Analysing VULNERABILITIES

The MANUFACTURER shall establish an ACTIVITY (or ACTIVITIES) for analysing VULNERABILITIES in the PRODUCT to include:

a) assessing their impact with respect to:
   1) the technical SECURITY CONTEXT in which they were discovered; (see Clause 6 of IEC 62443-4-1:2018[11]);
   2) the PRODUCT'S INTENDED ENVIRONMENT OF USE, and
   3) the PRODUCT'S DEFENSE-IN-DEPTH strategy;
b) impact as defined by a VULNERABILITY scoring system (for example CVSS);
c) identifying all other PRODUCTS / PRODUCT versions containing the SECURITY-related issue (if any);
d) identifying the root cause of the issue;
e) identifying related SECURITY issues (that is, in the same PRODUCT); and
f) impact on PRODUCT SAFETY and effectiveness.

NOTE 1 For root cause analysis, a methodical approach such as described in IEC 62740 can be employed.

NOTE 2 A root cause is the first event in a sequence of causal factors which is deviating from the intended sequence.

NOTE 3 Not all root causes can be fixed by technical measures in HEALTH SOFTWARE.

NOTE 4 This PROCESS can be implemented for example as a part of 8.5.2 of ISO 13485:2016 and 8.5.3 of ISO 13485:2016.

9.5 Addressing SECURITY-related issues

The MANUFACTURER shall establish an ACTIVITY (or ACTIVITIES) to address SECURITY-related issues and determine whether to disclose them (under 4.1.7) based on the results of the impact assessment and the acceptable level of RESIDUAL RISK.

The MANUFACTURER shall establish an ACTIVITY (or ACTIVITIES) to determine whether and how identified SECURITY risks will be handled – via the problem resolution PROCESS or through updated specifications regarding the INTENDED ENVIRONMENT OF USE.

The MANUFACTURER shall establish an ACTIVITY (or ACTIVITIES) to review any changes to the design or implementation for impact on SAFETY, SECURITY and effectiveness.

The MANUFACTURER shall inform other PROCESSES of the issue or related issue(s), including PROCESSES for other PRODUCTS / PRODUCT revisions. This can be done by submitting problem reports or similar into other PROCESSES.

The MANUFACTURER shall inform third parties if problems have been found in third-party source code to be used with SUPPORTED HEALTH SOFTWARE. In case of open-source software, the publishing platform can be used to inform about or fix the issue found.

This ACTIVITY shall include a periodic review of open SECURITY-related issues to ensure that issues are being addressed appropriately. This periodic review shall at a minimum occur during each PRODUCT release; see 4.1.6 and 4.1.8.

NOTE 1 This periodic review can be implemented for example as a part of 8.2.6 of ISO 13485:2016.

NOTE 2 As an example, an intended function including the transmission of personally identifiable information through an external network can raise the need for data encryption.

NOTE 3

- For some THREATS it can be feasible to not mitigate them through technical measures in HEALTH SOFTWARE, because they can be linked to the INTENDED USE or essential functions.
  - Example: Console access to emergency / acute care devices would be hindered by overly complex authentication procedures and might delay the delivery of urgent care.
  - Example: Strong cryptography algorithms for encrypting data used for near-field transmission in principle use considerable computing power and can drain the battery when implemented in smaller, mobile devices.
- Some THREATS can be better addressed by mitigations in the INTENDED ENVIRONMENT OF USE which are expressed via ACCOMPANYING DOCUMENTATION (see Annex E).
- There are VULNERABILITIES that cannot be exploited because of measures in the design of the HEALTH SOFTWARE.

NOTE 4 Because of the complexity in determining the probability related to THREATS, the concept of likelihood is more appropriate and commonly used for IT- SECURITY. Likelihood of identified THREATS is typically expressed through structured scoring systems like Common VULNERABILITY Scoring Systems (CVSS), which can also take into account the attacker's gain in relation to the applicable effort.

NOTE 5 RISK MANAGEMENT for medical device SAFETY – as in ISO 14971 – can be supported by a THREAT MODELLING method to cover SECURITY THREATS.

NOTE 6 IEC TR 63069 explains the relationship between the SAFETY / SECURITY PROCESSES.

Annex A
(informative)

Rationale

A.1 Relationship to IEC 62443

IEC 62443 is a series of Industrial Automation and Controls Systems SECURITY specifications. This series is the successor of ISA-99 and a well-recognized set of SECURITY standards for operational technology. Parts of the IEC 62443 series are recognized by the FDA, furthermore the EU “MDCG 2019-16 Guidance on Cybersecurity for medical devices” and the German BSI Guidance CS 132 refer to the IEC 62443 specifications.

Industrial Automation and Control Systems (IACS) recognize SECURITY as well as SAFETY and effectiveness. These are key properties that can also be applied in the field of HEALTH SOFTWARE.

Risk is a term used to describe the potential of damage towards certain protection goals. As an example, for medical devices these goals are the safe and performant operation of devices. In standards related to medical devices, risk is defined following 3.9 of ISO/IEC Guide 51:2014 or 3.10 of ISO/IEC Guide 63 as “combination of the probability of occurrence of harm and the severity of that harm” (with harm being defined as damage to *external* ASSETS like health, environment or property), while standards in the IEC 62443 series use the term risk to describe the potential of reduction of CONFIDENTIALITY, INTEGRITY, AVAILABILITY of rather system-*internal* ASSETS. However, the perspective of IEC 62443 includes risks that have the potential to cause *external* harm in the sense of ISO/IEC Guide 51 or ISO/IEC Guide 63. As this document dominantly uses this wider concept of (SECURITY) risk, we will not give a definition of the term as to avoid confusion with the more specific use of that term.

Due to the wide spectrum of technologies and applications for HEALTH SOFTWARE, it is difficult to prescribe a specific set of SECURITY CONTROLS. Practice in industry has shown that SECURITY measures in the LIFE CYCLE PROCESSES lead to secure PRODUCTS. This document therefore addresses LIFE CYCLE PROCESSES in responsibility of the MANUFACTURER and takes the requirements of IEC 62443-4-1[11], in consideration that the requirements:

- are relevant for HEALTH SOFTWARE;
- specify PROCESS-related requirements;
- address the MANUFACTURER;
- do not specify PRODUCT capabilities;
- do not specify documentation content for ACCOMPANYING DOCUMENTATION – which will be specified by IEC TR 60601-4-5.

Satisfying the requirements of this document will support conformance towards IEC 62443-4-1[11]. However, this document contains some adaptions and clarifications to the healthcare sector.

MANUFACTURERS striving at full conformance to IEC 62443-4-1[11] consider the following additional provisions regarding the independence from the developers “who designed and implemented the PRODUCT according to Table A.1.

Table A.1 – Required level of independence of testers from developers

Test type	Reference	Level of independence
SECURITY requirements testing	SVV-1 SECURITY requirements testing	Independent department
THREAT mitigation testing	SVV-2 THREAT mitigation testing	Independent department
VULNERABILITY testing	SVV-3 VULNERABILITY testing	Independent person
Static code analysis	SI-1 SECURITY implementation review	None
ATTACK SURFACE analysis	SVV-3 VULNERABILITY testing	Independent person
Known VULNERABILITY scanning	SVV-3 VULNERABILITY testing	Independent person
SOFTWARE COMPOSITION ANALYSIS	SVV-3 VULNERABILITY testing	None
Penetration testing	SVV-4 Penetration testing	Independent department or organization
SOURCE: IEC 62443-4-1:2018[11], SVV-5, 9.6.1.		

The MANUFACTURER can implement a (semi-)independent internal testing team and/or the use of a third-party SECURITY test organization. Individuals who are independent from the developers who designed and implemented the SECURITY features should do the SECURITY testing. The levels of independence can be “as follows:

- None – no independence required. Developer can perform the testing.
- Independent person – the person who performs the testing cannot be one of the developers of the PRODUCT.
- Independent department – the person who performs the testing cannot report to the same first line manager as any developers of the PRODUCT. Alternatively, they could be a member of a quality assurance (QA) department.
- Independent organization – the person who performs the testing cannot be part of the same organization as any developers of the PRODUCT. An organization can be a separate legal entity, a division of a company or a department of a company that reports to a different executive such as a vice president or similar level.”

For the use of this document, "Abuse case" in IEC 62443-4-1:2018[11], SVV-5, 9.6.1 was modified to "VULNERABILITY".

A.2 Relationship to IEC 62304

In order to extend existing LIFE CYCLE PROCESSES for HEALTH SOFTWARE, these requirements have been arranged in a structure reflecting that of IEC 62304[8].

Implementation of IEC 62304[8] is not required for implementing the PROCESSES specified in this document. However, if a MANUFACTURER identifies in their PROCESSES those ACTIVITIES specified in IEC 62304[8], it is easier to determine the related ACTIVITY (or ACTIVITIES) for CYBERSECURITY specified in this document.

IEC 62304[8] specifies ACTIVITIES, based on the software SAFETY classification. The required ACTIVITIES are indicated in the normative text of IEC 62304[8] as "[Class A, B, C]", "[Class B, C]" or "[Class C]", indicating that they are required selectively depending on the classification of the software to which they apply. The requirements in Clause 4 through Clause 9 of this document have a special focus on CYBERSECURITY and therefore do not follow the concept of SAFETY classes. For conformance to this document the selection of ACTIVITIES is independent of SAFETY classes.

A.3 Risk transfer

A.3.1 Overview

There are shared responsibilities for using HEALTH SOFTWARE in a secure way. As a part of deploying HEALTH SOFTWARE to the customer, some of the risk of secure operation is transferred, while some of the risk remains with the MANUFACTURER.

IEC 62443-4-1 does not clearly define terms or concepts for risk transfer, as it just notes that for "external provided components", "dependent components", and "custom development components" different requirements apply. Therefore, this document introduces categories for SOFTWARE ITEMS that declare different levels of transfer of responsibility and risk from the MANUFACTURER to the customer.

The MANUFACTURER will identify the following categories of risk transfer for each software that is required by HEALTH SOFTWARE to achieve its INTENDED PURPOSE.

A.3.2 MAINTAINED SOFTWARE

The MANUFACTURER will assume the risk related to the SECURITY of MAINTAINED SOFTWARE (6.3.2, 6.3.3). As a result, the MANUFACTURER will provide SECURITY updates for all software in this category.

Examples for MAINTAINED SOFTWARE include

- software from third party, specifically developed for use with HEALTH SOFTWARE;
- embedded off-the-shelf software; and
- HEALTH SOFTWARE including those developed prior to publication of this document.

A.3.3 SUPPORTED SOFTWARE

The MANUFACTURER will notify the customer about known risks related to the SECURITY of that software (6.3.1).

Examples for SUPPORTED SOFTWARE include

- generally available off-the-shelf software;
- software from third party, also intended for other uses than with HEALTH SOFTWARE; and
- MAINTAINED SOFTWARE.

A.3.4 REQUIRED SOFTWARE

The MANUFACTURER will assume known risks related to the SECURITY (5.2.1, 5.2.3) known before release of the software.

That means that all SECURITY requirements for each SOFTWARE ITEMS required by HEALTH SOFTWARE to achieve its INTENDED PURPOSE will be considered as part of the requirements specification of that HEALTH SOFTWARE.

Examples for REQUIRED SOFTWARE include

- software for which no updates can be provided;
- obsolete third-party software; and
- SUPPORTED SOFTWARE.

A.4 Secure coding best practices

The secure coding best practices for HEALTH SOFTWARE should include at a minimum:

a) avoidance of potentially exploitable implementation constructs – implementation design patterns that are known to have SECURITY WEAKNESSES,

b) avoidance of banned functions and coding constructs/design patterns – software functions and design patterns that should not be used because they have known SECURITY WEAKNESSES,

NOTE 1 Best coding practices avoid coding based on unspecified or undefined behaviour of the programming environment.

NOTE 2 For common libraries and programming languages there are public lists of banned functions. Per secure coding best practices, the MANUFACTURER can decide to avoid using these or more functions.

NOTE 3 Information on bad practices are available from coding standards, library providers, tools and other sources.

c) automated tool use and settings (for example, for static analysis tools),

d) general secure coding best practices,

NOTE 4 The secure coding best practices can be based on published specifications, for example ISO/IEC TR 24772, MISRA-C or SEI CERT C and SEI CERT C++ coding standards.

e) validity checking of all inputs that cross a TRUST BOUNDARY,

f) error handling.

The MANUFACTURER should evaluate each type of alert from static analysis whether it justifies a code change.

The application of secure coding standards can be based on SECURITY ARCHITECTURE, programming technology and context.

Annex B
(informative)

Guidance on implementation of SECURITY LIFE CYCLE ACTIVITIES

B.1 Overview

CYBERSECURITY of a PRODUCT containing software can be supported by SECURITY CAPABILITIES of that software – typically implementing protection from, detection of, response to and recovery from incidents that can compromise the CONFIDENTIALITY, INTEGRITY or AVAILABILITY of the PRODUCT'S ASSETS.

B.2 Related work

Although this document focuses on software there are additional SECURITY considerations for the physical device that the software is running on that should be included in all PROCESS ACTIVITIES. Examples are to reduce physical interface ports, like JTAG or unused USB ports, similar to limiting open network ports at the software level. Similarly, there are mitigations provided by the device, such as physical locks to provide access control to internal media.

The technical reports IEC TR 60601-4-5 and IEC TR 80001-2-2 give guidance for the identification and communication of such SECURITY CAPABILITIES. While these technical reports address medical devices, their concepts and measures can easily be transferred to HEALTH SOFTWARE.

Another aspect is related to the LIFE CYCLE: MANUFACTURERS of HEALTH SOFTWARE can establish PROCESSES that avoid or mitigate VULNERABILITIES or reduce their impact to the PRODUCTS' INTENDED PURPOSE. Some PROCESSES – for instance requirements engineering and THREAT / RISK ANALYSIS (TRA) link the perspective of PRODUCT aspects with the view on PROCESSES. It is important to understand that only the combination of both PRODUCT capabilities as well as measures in the LIFE CYCLE PROCESSES can provide effective CYBERSECURITY.

B.3 THREAT / RISK ANALYSIS

SECURITY incidents can affect the PRODUCT'S SAFETY or effectiveness. The specific relationship between VULNERABILITIES and risks regarding SAFETY or effectiveness depends on the design, implementation and purpose of the respective PRODUCT. A PRODUCT risk analysis for SAFETY therefore shall consider the effects of VULNERABILITIES to the key functions of the PRODUCT. As a part of that ACTIVITY (or ACTIVITIES), TRA is performed for the PRODUCT.

SAFETY is defined as freedom from unacceptable risk, where risk is the combination of severity and probability of potential harm. The harm is expressed as injury, damage to health, property or environment (see ISO/IEC Guide 51). Where the INTENDED USE is known, the impact of SECURITY incidents finally can be expressed in terms of severity of the respective harm. In this case, SECURITY RISK MANAGEMENT can be integrated in a general RISK MANAGEMENT as applied by the MANUFACTURER based on ISO/IEC Guide 51 or ISO 14971 for medical devices. When following such an integrated approach, it shall be considered that management of risks arising from unauthorized activities (i.e. SECURITY-related risks) requires the application of specific methods and techniques differing from those for risks arising e.g. from non-reliable software, electrical failures, radiation, biological contamination or use errors. These SECURITY-specific methods and techniques include TRA and others as described in this document. TRA aims at identifying and evaluating scenarios of intrusion and the resulting WEAKNESSES. The scenarios considered during TRA are based on the actual context of use, which is not limited to the PRODUCT'S INTENDED USE, however TRA takes the USE ENVIRONMENT into account. Those scenarios with an attacker exploiting a known VULNERABILITY can be considered as "foreseeable" with respect to PRODUCT RISK MANAGEMENT and are also part of the actual context of use.

NOTE 1 The INTENDED USE can typically be determined at PRODUCT level.

NOTE 2 ISO 14971 specifies the consideration of reasonably foreseeable misuse.

In case the USE ENVIRONMENT or other mitigation controls might fail to prevent a certain type of ATTACK, that scenario becomes "foreseeable" from the MANUFACTURER'S perspective. TRA identifies and evaluates such THREAT scenarios – taking into account:

a) the dedicated hardware with which the HEALTH SOFTWARE is intended to be use,

b) the intended operational context, and

c) the potential data/control flows from external actors into the HEALTH SOFTWARE.

B.4 THREAT and RISK MANAGEMENT

One outcome of applying THREAT and RISK MANAGEMENT is an evaluation of known VULNERABILITIES that can affect the HEALTH SOFTWARE'S ASSETS (data, software functions, software services) with respect to CONFIDENTIALITY, INTEGRITY or AVAILABILITY – and how that is related to the overall SAFETY, SECURITY and effectiveness of the PRODUCT as a whole.

Options for controlling SECURITY risk with remaining VULNERABILITIES include one or more of the following:

a) fixing the issue through one or more of the following:
   1) DEFENSE-IN-DEPTH strategy or design change;
   2) addition of one or more SECURITY requirements and/or capabilities;
   3) use of compensating mechanisms; and/or
   4) disabling or removing features; with respect to the safe and effective use of HEALTH SOFTWARE;

b) creating a remediation plan to fix the problem;

c) deferring the problem for future resolution (reapply this requirement at some time in the future) and specifying the reason(s) and associated risk(s); and

d) not fixing the problem, if the RESIDUAL RISK meets the acceptance criteria.

When the resolution decision is to fix the SECURITY-related issue in the PRODUCT implementation, the timing of the release of the fix can result in a SECURITY update to be deferred until the next release.

B.5 Software development planning

B.5.1 Development

B.5.1.1 Software development PROCESS

An appropriate development PROCESS for HEALTH SOFTWARE should implement a development/ maintenance/ support PROCESS as required in IEC 62304[8] and should additionally implement items of the list specified in 5.1.1.

B.5.1.2 Development environment SECURITY

HEALTH SOFTWARE shall be protected from any compromises via the development environment. For instance, the introduction of malicious software or the theft of credentials such as software signing certificates.

B.5.2 HEALTH SOFTWARE requirements analysis

B.5.2.1 HEALTH SOFTWARE SECURITY requirements

In some circumstances a system at a higher level has already defined a SECURITY level for this (sub)system. This is described per IEC 62443-3-2 in general and via IEC TR 60601-4-5 for Programmable Electrical Medical Systems (PEMS).

B.5.2.2 SECURITY requirements review

The implementation of SECURITY CAPABILITIES can have an impact on the PRODUCT'S SAFETY or effectiveness. This review can determine an appropriate requirement for implementing SECURITY CAPABILITIES in a balanced way.

B.5.3 Software architectural design

B.5.3.1 DEFENSE-IN-DEPTH ARCHITECTURE /design

DEFENSE-IN-DEPTH is an approach to CYBERSECURITY in which a series of defensive mechanisms are layered in order to protect information ASSETS. If one mechanism fails, another layer will thwart an ATTACK. This multi-layered approach with intentional redundancies increases the SECURITY of a system as a whole and addresses many different ATTACK vectors. DEFENSE-IN-DEPTH is commonly referred to as the "castle approach" because it mirrors the layered defenses of a medieval castle.

DEFENSE-IN-DEPTH reduces the likelihood of ATTACKS to succeed, it reduces the impact of ATTACKS and allows the target system to take compensating actions.

B.5.3.2 Secure design principles

The principles described in this requirement are relevant to the design of any system, whether for apps, client or server, cloud-based services, or Internet-of-Things devices. The specifics of their application will vary – a cloud service can require multiple administrative roles, each with its own least privilege, while an IoT device will require special considerations of the need for SECURITY updates and of the need to fail securely and safely.

However, the principles are general and provide valuable SECURITY guidance for the designers and architects of all classes of systems. Elements of such a PROCESS need additional specifications that depend on the programming environment and the information technology used. There are specifications from Standard-Developing Organisations (SDOs) or associations with more detailed specifications (potentially depending on technology or context).

B.5.3.3 SECURITY architectural design review

The ability of an ARCHITECTURE to ensure stable and predictable behavior is important, because adverse conditions can come intentionally or unintentionally; they can show up via adverse calls / data when HEALTH SOFTWARE is being used in its USE ENVIRONMENT.

B.5.4 Software unit implementation and VERIFICATION

Secure coding standards should incorporate the following principles:

- establish coding standards and conventions;
- use safe functions only (i.e. reliable functions);
- use current compiler and toolchain versions and secure compiler options;
- handle input and other data safely (i.e. in a restrictive, cautious way…);
- use static code analysis tools to find SECURITY issues early;
- handle errors.

NOTE 1 Best coding practices avoid coding based on unspecified or undefined behaviour of the programming environment.

NOTE 2 Static Code Analysis (SCA) detects the potential for errors such as buffer overflows, null pointer dereferencing, and similar.

NOTE 3 SCA can be done using a tool if one is available for the language used. In addition, static code analysis can be done on all source code changes including new source code.

B.5.5 Secure implementation

The MANUFACTURER can implement an ARCHITECTURE and design that allow for updating or substituting hardware components and SOFTWARE ITEMS – for example cryptographic modules. The goal here is to implement with technology agility in mind: e.g. encryption algorithms might potentially be broken at any time, even if they are considered current best practices, and encryption libraries can have VULNERABILITIES that undermine otherwise sound algorithms. In the example, a secure implementation should ensure that some encryption strategy specifies how applications and services should implement their encryption to enable transition to new cryptographic mechanisms, libraries and keys when the need arises. The above is just an example; substitution in the ARCHITECTURE also serves as a means to be able to support necessary SECURITY updates and upgrades.

B.5.6 Not used

B.5.7 Software system testing

B.5.7.1 SECURITY requirements testing

Subclause 5.7 on software system testing provides the requirements and more detail related to SECURITY testing.

An overview of some automated and manual testing techniques includes the techniques described from B.5.7.2 to B.5.7.5.

B.5.7.2 THREAT mitigation testing

As an example for THREAT mitigation testing, input VALIDATION testing plays an important role.

Input VALIDATION testing tries to detect undesired system behavior when incorrect data or excessive load of data are sent to a system interface. Often automated tools are used and the more specialized the tool is for a certain interface protocol, the more accurate the test results will be. Examples are fuzz testing, buffer overflow and format error testing. Specialized injection testing techniques exist for protocols such as SQL, LDAP, XML and cross-site scripting.

B.5.7.3 VULNERABILITY scanning

VULNERABILITY scanning is the automated detection of known VULNERABILITIES. Scanners will detect installed software, open network ports, operating system configuration and other SECURITY relevant information. Many VULNERABILITY scanners allow for both authenticated and unauthenticated scans. An authenticated scan means that the tool has administrative system credentials to bypass certain protections and will be able to assess the systems configuration with much more detail and accuracy. OWASP (“the Open Web Application SECURITY Project” foundation) maintains a list of VULNERABILITY scanning tools.

B.5.7.4 Penetration testing

Penetration testing, also called pen-testing, focuses specifically on compromising CONFIDENTIALITY, INTEGRITY or AVAILABILITY. It can involve defeating multiple aspects of the DEFENSE-IN-DEPTH design. For example, bypassing authentication to access the PRODUCT, using elevation of privilege to gain administrative access and then compromising CONFIDENTIALITY by breaking encryption. As this example shows, penetration testing involves approaching testing like an attacker and often involves exploiting chained VULNERABILITIES in a PRODUCT using both tools and manual skills. Results of the VULNERABILITY scanning and other tests could provide valuable input to develop manual ATTACK scenarios.

Penetration testing should include an individual who was not involved in the development of the HEALTH SOFTWARE.

B.5.7.5 Managing conflicts of interest between testers and developers

Objectivity aims at making decisions by applying established methods to facts, such that any other tester can reproduce the decision at a later time. Independence can support objectivity. The MANUFACTURER can implement a (semi-)independent internal testing team and/or the use of a SECURITY test organization.

Static code analysis and SOFTWARE COMPOSITION ANALYSIS (binary analysis) typically depend on the use of automated tools. These tests are mentioned in IEC 62443-4-1 but that document does not specify independence requirements. The way how automated tools are being used and how their outcomes are being interpreted needs objectivity as well, however the calibration required for different tools (and different programming environments) does not ensure that outcomes are always consistent across tools. Therefore, implementing reproducibility within a given tool chain is recommended[41].

Annex C
(informative)

THREAT MODELLING

C.1 General

THREAT MODELLING is a systematic approach for analyzing the SECURITY of an item in a structural way such that VULNERABILITIES can be identified, enumerated, and prioritized, all from a hypothetical attacker's point of view. THREAT MODELLING can be applied to a wide range of things, including software, devices, systems, networks, distributed systems and business PROCESSES. THREAT MODELLING typically employs a systematic approach to identify ATTACK vectors and ASSETS most desired by different THREAT actors. This leads to a decomposition of the item (software, device, system, and so on) to look at each possible ATTACK vector and ASSET individually and determine to which kind of ATTACKS they are vulnerable. From this, a list of VULNERABILITIES can be created and ordered in terms of risk, potential to impact SAFETY, effectiveness, or any other criteria deemed appropriate (like privacy).

There are various approaches to creating a THREAT MODEL that range from making a list of known VULNERABILITIES to adopting a framework; some examples are described from C.2 to C.10.

A THREAT actor or malicious actor is a person, group, or organization attacking an organization with the potential to impact, the SAFETY or SECURITY of systems. THREAT actors will have different motivations to ATTACK certain organizations or systems such as financial gain, data theft, intellectual property theft or just to disrupt the trust in the targeted organization. A THREAT actor can have limited skills and resources (script kiddy) or significant skills and resources (cyberterrorists and state actors). THREAT actors are often further categorized as intentional or unintentional (use errors) and can be external or internal to the organization. Typical THREAT actors that could be taken into consideration during THREAT MODELLING are insiders (clinical users, system administrators), script kiddies, cyber criminals, hacktivists, and nation state actors.

C.2 ATTACK-defense trees

An ATTACK-Defense Tree (ADTree) is a node-labeled rooted tree describing the measures an attacker might take to ATTACK a system and the defenses that a defender can employ to protect the system.

C.3 CAPEC / OWASP / SANS

A basic approach is to use lists of known top THREATS such as the OWASP Top 10 or the CWE/SANS Top 25. The "Common Attack Pattern Enumeration and Classification" (CAPEC) has a more comprehensive dictionary of known patterns of ATTACK employed by adversaries to exploit known WEAKNESSES.

C.4 CWSS

The Common WEAKNESS Scoring System (CWSS) both identifies VULNERABILITIES and provides a scoring system to prioritize them. It is a collaborative, community-based effort that focuses on analyzing software and reported bugs to determine the relative importance of the detected WEAKNESSES.

C.5 DREAD

DREAD is a classification scheme for quantifying, comparing and prioritizing the amount of risk presented by each evaluated THREAT. DREAD modelling focuses on risk rating. The DREAD algorithm is used to compute a risk value, which is an average of all five categories: **D**amage, **R**eproducibility, **E**xploitability, **A**ffected users, and **D**iscoverability.

C.6 List known potential VULNERABILITIES

One can attempt listing all the VULNERABILITIES that could affect your system. While it is impossible to list all potential VULNERABILITIES, one should concentrate on those VULNERABILITIES that could be exercised by known THREATS.

C.7 OCTAVE

OCTAVE is a heavyweight risk methodology approach originating from Carnegie Mellon University's Software Engineering Institute (SEI) in collaboration with CERT. OCTAVE focuses on organizational risk, not technical risk.

C.8 STRIDE

STRIDE is a model for system decomposition, by characterizing known THREATS according to the kinds of EXPLOITS used. The STRIDE acronym stands for each of the categories: **S**poofing, **T**ampering, **R**epudiation, **I**nformation disclosure, **D**enial of service, and **E**levation of Privilege. STRIDE does not include a scoring system.

C.9 Trike

Trike is a THREAT MODELLING framework with similarities to the STRIDE and DREAD THREAT MODELLING PROCESSES. Trike differs in that it uses a risk-based approach with distinct implementation, THREAT, and risk models, instead of using the STRIDE/DREAD aggregated THREAT MODEL (ATTACKs, THREATS, and WEAKNESSES).

C.10 VAST

VAST is an acronym for Visual, Agile, and Simple THREAT MODELLING. The principle of this approach is the necessity of scaling the THREAT MODELLING PROCESS across the infrastructure and entire software development LIFE CYCLE. The approach integrates into an agile software development methodology. The methodology provides an application and infrastructure visualization scheme such that the creation and use of THREAT MODELs do not require specific SECURITY subject matter expertise.

Annex D
(informative)

Relation to practices in IEC 62443-4-1:2018

D.1 IEC 81001-5-1 to IEC 62443-4-1:2018

IEC 81001-5-1	IEC 62443-4-1:2018		IEC 81001-5-1	IEC 62443-4-1:2018
4.1.1	Not in IEC 62443-4-1		5.7.4	SVV-4
4.1.2	SM-2		5.7.5	SVV-5
4.1.3	SM-3		5.8.1	SM-11
4.1.4	SM-4		5.8.2	SG-5, SG-6
4.1.5	SM-10		5.8.3	SM-6
4.1.6	SM-13		5.8.4	SM-8
4.1.7	DM-5		5.8.5	SM-11
4.1.8	DM-6		5.8.6	SM-12
4.1.9	SG-7		5.8.7	SG-4
4.2	Not in IEC 62443-4-1		6.1.1	SUM-5
5.1.1	SM-1, SM-5		6.2.1	DM-1
5.1.2	SM-7		6.2.2	SUM-1
5.1.3	SI-2		6.3.1	SUM-3
5.2.1	SR-3, SR-4		6.3.2	SUM-2, SUM-4
5.2.2	SR-5		6.3.3	SM-6
5.2.3	SM-9		7.1	SR-1
5.3.1	SD-2		7.2	SR-2
5.3.2	SD-4		7.3	Not in IEC 62443-4-1
5.3.3	SD-3		7.4	Not in IEC 62443-4-1
5.4.1	SD-4		7.5	Not in IEC 62443-4-1
5.4.2	SD-2		8	SM-1
5.4.3	SD-1		9.1	Not in IEC 62443-4-1
5.4.4	SD-3		9.2	DM-1
5.5.1	SI-2		9.3	DM-2
5.5.2	SI-1		9.4	DM-3
5.6	Not in IEC 62443-4-1		9.5	DM-4
5.7.1	SVV-1		A.4	SI-2
5.7.2	SVV-2		E.2	SG-1, SG-2, SG-3
5.7.3	SVV-3		E.3	SG-4

D.2 IEC 62443-4-1:2018 to IEC 81001-5-1

Note that requirements SG-1,2,3 are not required normatively as explained in Annex A (rationale), which is why the normative parts of this document exclude requirements of ACCOMPANYING DOCUMENTATION contents.

IEC 62443-4-1:2018	IEC 81001-5-1		IEC 62443-4-1:2018	IEC 81001-5-1
SM-1	5.1.1, 8		SVV-1	5.7.1
SM-2	4.1.2		SVV-2	5.7.2
SM-3	4.1.3		SVV-3	5.7.3
SM-4	4.1.4		SVV-4	5.7.4
SM-5	5.1.1		SVV-5	5.7.5
SM-6	5.8.3, 6.3.3		DM-1	6.2.1, 9.2
SM-7	5.1.2		DM-2	9.3
SM-8	5.8.4		DM-3	9.4
SM-9	5.2.3		DM-4	9.5
SM-10	4.1.5		DM-5	4.1.7
SM-11	5.8.1, 5.8.5		DM-6	4.1.8
SM-12	5.8.6		SUM-1	6.2.2
SM-13	4.1.6		SUM-2	6.3.2
SR-1	7.1		SUM-3	6.3.1
SR-2	7.2		SUM-4	6.3.2
SR-3	5.2.1		SUM-5	6.1.1
SR-4	5.2.1		SG-1	E.2
SR-5	5.2.2		SG-2	E.2
SD-1	5.4.3		SG-3	E.2
SD-2	5.3.1, 5.4.2		SG-4	5.8.7, E.3
SD-3	5.3.3, 5.4.4		SG-5	5.8.2
SD-4	5.3.2, 5.4.1		SG-6	5.8.2
SI-1	5.5.2		SG-7	4.1.9
SI-2	5.1.3, 5.5.1, A.4			

Annex E
(informative)

Documents specified in IEC 62443-4-1

E.1 Overview

This annex specifies PRODUCT-related documents which support the secure use of HEALTH SOFTWARE.

For full conformance to IEC 62443-4-1[11], the MANUFACTURER will need to demonstrate conformance to this document including this annex on PRODUCT-related documentation.

The PROCESSES specified by this annex are used to provide documentation that describes how to integrate, configure and maintain the DEFENSE-IN-DEPTH strategy of the HEALTH SOFTWARE in accordance with its SECURITY CONTEXT. Applying and maintaining the DEFENSE-IN-DEPTH strategy for a specific HEALTH SOFTWARE installation will typically address the following:

1) policies and procedures associated with the HEALTH SOFTWARE SECURITY CONTEXT;
2) architectural considerations, such as firewall placement and the use of compensating mechanisms including SECURITY measures;
3) configuring SECURITY settings/options such as configuring firewall rules and managing user accounts; and
4) use of tools to assist in hardening HEALTH SOFTWARE.

E.2 Release documentation

E.2.1 PRODUCT documentation

The MANUFACTURER should include in the PRODUCT requirements, the following:

a) SECURITY privileges required to install, operate, and maintain the PRODUCT;
b) SECURITY options, including removal of default passwords, used to install, configure, operate and maintain the PRODUCT; and
c) SECURITY considerations/actions associated with removing the PRODUCT from use (for example removing sensitive data).

NOTE 1 Specifications in 5.2.1 cover SECURITY requirements documentation at the level of HEALTH SOFTWARE. PRODUCT release documentation addresses SECURITY specifications.

The MANUFACTURER should include in the SECURITY requirements the following information:

a) the scope and boundaries of the SOFTWARE ITEMS of the PRODUCT, in both a physical and logical way;
b) identification of REQUIRED SOFTWARE including its version;
c) information on interfaces: the integration capabilities of the PRODUCT'S identity and access management with that of the deployment infrastructure; and the integration capabilities of the PRODUCT within the deployment environment;
d) controls implemented in the PRODUCT; and
e) design for SECURITY update of the PRODUCT including the update of incorporated software from external sources. See ISO/IEC 30111.

NOTE 2 This is intended to cover the concept of SECURITY CAPABILITY levels.

E.2.2 HEALTH SOFTWARE DEFENSE-IN-DEPTH documentation

The MANUFACTURER should establish an ACTIVITY to create HEALTH SOFTWARE documentation that describes the compensating controls for the HEALTH SOFTWARE to support installation, operation and maintenance that includes:

a) SECURITY CAPABILITIES implemented by the HEALTH SOFTWARE and their role in the DEFENSE-IN-DEPTH strategy;

b) THREATS addressed by the DEFENSE-IN-DEPTH strategy;

c) HEALTH SOFTWARE user mitigation strategies for known SECURITY risks associated with the HEALTH SOFTWARE, including risks associated with REQUIRED SOFTWARE; and

d) appropriate information about relevant RESIDUAL RISKS to SECURITY remaining in the HEALTH SOFTWARE PRODUCT.

NOTE 1 IEC TR 60601-4-5 gives guidance on the specification of SECURITY CAPABILITIES and their documentation in the ACCOMPANYING DOCUMENTATION and provides a method of determining requirements from the SECURITY CAPABILITY level.

NOTE 2 IEC TR 80001-2-2 specifies SECURITY-related needs, risks and controls as a guidance for disclosure and communication between the MANUFACTURER and the HEALTHCARE DELIVERY ORGANIZATION.

NOTE 3 HEALTH SOFTWARE DEFENSE-IN-DEPTH documentation can be used to explain the relationship between component VULNERABILITIES and SAFETY.

E.2.3 DEFENSE-IN-DEPTH measures expected in the environment

In HEALTH SOFTWARE there can be VULNERABILITIES for which technical controls could adversely affect the SAFETY and effectiveness of the PRODUCT when used as intended.

The PRODUCT should anticipate its INTENDED ENVIRONMENT OF USE to a certain extent. A declaration of external controls expected to be provided can be used to define shared responsibilities – for example as specified in IEC TR 60601-4-5 and in IEC TR 80001-2-2 for which a well-established guidance is published as HIMSS/NEMA “MDS2”.

The MANUFACTURER should establish an ACTIVITY to create PRODUCT documentation that declares external SECURITY controls expected to be provided or implemented by the external environment.

E.2.4 SECURITY hardening guidelines

The MANUFACTURER should establish an ACTIVITY to create HEALTH SOFTWARE documentation that includes guidelines for hardening the HEALTH SOFTWARE when deploying, installing and maintaining the HEALTH SOFTWARE. If applicable, the guidelines should include but are not limited to, instructions, rationale and recommendations for the following:

a) integration of the HEALTH SOFTWARE, including third-party SOFTWARE ITEMS, into its HEALTH SOFTWARE SECURITY CONTEXT;

b) integration of the HEALTH SOFTWARE’S application programming interfaces/protocols with user applications;

c) applying and maintaining the HEALTH SOFTWARE’S DEFENSE-IN-DEPTH strategy;

d) configuration and use of SECURITY options and SECURITY CAPABILITIES in support of local SECURITY policies, and for each SECURITY option/ SECURITY CAPABILITY:

   1) its contribution to the HEALTH SOFTWARE’S DEFENSE-IN-DEPTH strategy;

   2) descriptions of configurable and default values that includes how each affects SECURITY along with any potential impact each has on work practices; and

   3) setting/changing/deleting its value;

e) instructions and recommendations for the use of all SECURITY-related tools and utilities that support administration, monitoring, incident handling and evaluation of the SECURITY of the HEALTH SOFTWARE;

f) instructions and recommendations for periodic SECURITY maintenance ACTIVITIES;

g) instructions for reporting SECURITY incidents involving the HEALTH SOFTWARE to the MANUFACTURER; and

h) description of the SECURITY best practices for maintenance and administration of the HEALTH SOFTWARE.

NOTE The software bill of material (SBOM) is a documentation that tracks all incorporated software. The SBOM is a customer-facing documentation which is not required by IEC 62443-4-1[11], but by IEC TR 60601-4-5. SBOMs enable the customers to monitor the SECURITY risk environment, to communicate that risk with the MANUFACTURER, as an example regarding related SECURITY patches for the software listed.

E.2.5 SECURITY update information

The MANUFACTURER shall establish an ACTIVITY (or ACTIVITIES) to ensure that DOCUMENTATION about PRODUCT SECURITY updates is made available to PRODUCT users that includes but is not limited to:

a) the PRODUCT version number(s) to which the SECURITY patch applies;

b) instructions on how to apply approved patches manually and via an automated PROCESS;

c) description of any impacts that applying the patch to the PRODUCT can have, including reboot;

d) instructions on how to verify that an approved patch has been applied;

e) risks (potential impact to SAFETY, effectiveness, SECURITY) of not applying the update and mitigations that can be used for updates that are not approved or deployed by the ASSET owner;

f) the potential for damage to CONFIDENTIALITY, INTEGRITY, AVAILABILITY if the update is not installed; and

g) guidance reducing potential for damage to CONFIDENTIALITY, INTEGRITY, AVAILABILITY.

E.3 Documents for decommissioning HEALTH SOFTWARE

The guidelines for HEALTH SOFTWARE decommissioning should include, but are not limited to instructions and recommendations for the following:

a) removing the HEALTH SOFTWARE from its INTENDED ENVIRONMENT OF USE (see Clause 6 of IEC 62443-4-1:2018[11]);

b) removing patient and configuration data stored within the environment;

c) secure transfer, migration, archiving and deletion of data stored in the HEALTH SOFTWARE; and

d) secure disposal of the HEALTH SOFTWARE to prevent potential disclosure of data contained in the HEALTH SOFTWARE that could not be removed as described in c) above.

Annex F
(normative)

TRANSITIONAL HEALTH SOFTWARE

F.1 Overview

This annex specifies a number of ACTIVITIES to improve the SECURITY of TRANSITIONAL HEALTH SOFTWARE which was developed without following all of the ACTIVITIES defined in Clause 4 through Clause 9 of this document. The results are documented as a “Conformance claim to the TRANSITIONAL HEALTH SOFTWARE activities of Annex F”.

For HEALTH SOFTWARE for which the MANUFACTURER’S PROCESS does not meet all requirements specified in the normative part of Clause 4 through Clause 9 of this document there are two alternatives:

1) re-develop the HEALTH SOFTWARE according to the normative parts of this document;
2) improve the SECURITY of the existing HEALTH SOFTWARE by ACTIVITIES such as updating the SECURITY operating guidelines, mandating compensating controls or partially re-writing the HEALTH SOFTWARE. These are the ACTIVITIES described in F.2 to F.4.

The results of the activities described in F.2 to F.4 are documented as a “Conformance claim to the TRANSITIONAL HEALTH SOFTWARE activities of IEC 81001-5-1:2021, Annex F”.

As an outcome of applying Annex F, the MANUFACTURER can keep the unmodified TRANSITIONAL HEALTH SOFTWARE or can decide to redo ACTIVITIES as specified in Clause 5 for selected SOFTWARE ITEMS.

NOTE 1 The concept of “legacy software”, as defined in IEC 62304[8], cannot be directly applied to the SECURITY domain. The main reasons are that:

– Assessment of “any feedback, including post-production information, on “legacy software” regarding incidents and / or near incidents” (IEC 62304:2006/AMD1:2015, 4.4.2 a)) cannot be relied upon to keep up with the state of the art in CYBERSECURITY .
– “continuing validity of RISK CONTROL measures” (IEC 62304:2006/AMD1:2015, 4.4.2 b)) cannot be relied on to give protection in the fast-changing CYBERSECURITY environment.

NOTE 2 TRANSITIONAL HEALTH SOFTWARE can be partially conforming to Clause 4 through Clause 9 of this document. The PROCESSES for TRANSITIONAL HEALTH SOFTWARE can implement a subset of the normative requirements of this document.

NOTE 3 TRANSITIONAL HEALTH SOFTWARE will be part of the set of REQUIRED SOFTWARE.

F.2 Development assessment and gap closure activities

The MANUFACTURER of TRANSITIONAL HEALTH SOFTWARE shall implement ACTIVITIES specified in Clause 4.

The MANUFACTURER shall perform a gap analysis of available deliverables against those required according to 5.2, 5.7, 7.1.1, 7.2 and 7.3 as described below.

The MANUFACTURER shall perform the following gap closure activities:

a) documenting system-level SECURITY requirements, as described in 5.2.1;
b) performing and documenting system-level tests (to the full extent) as described in 5.7 software system testing;
c) assessing and evaluating the SECURITY risk. This shall be done by documenting the SECURITY CONTEXT and THREAT MODEL as described in 7.1.1, 7.2 and 7.3;

d) controlling SECURITY risk as described in 7.4. In some instances, the residual SECURITY risk will mandate compensating controls – external to HEALTH SOFTWARE – which are documented in the secure operation guidelines;

e) creating, or updating existing, secure operation guidelines and account management guidelines as described in 5.8.2; and

NOTE 1 See E.2.1 HEALTH SOFTWARE DEFENSE-IN-DEPTH documentation for recommendations for disclosure.

f) evaluating the overall residual SECURITY risk and based on this evaluation, decide if the TRANSITIONAL HEALTH SOFTWARE is fit for continued use.

NOTE 2 The MANUFACTURER can also choose to re-implement some parts of the HEALTH SOFTWARE according to this document, for example network-interfacing components.

F.3 Rationale for use of TRANSITIONAL HEALTH SOFTWARE

The MANUFACTURER shall document the version of the TRANSITIONAL HEALTH SOFTWARE together with a rationale for the continued use of the TRANSITIONAL HEALTH SOFTWARE based on the outputs of the gap closure activities.

The MANUFACTURER shall establish and make available a plan to migrate TRANSITIONAL HEALTH SOFTWARE to be conformant to Clause 6 to Clause 9.

In some cases where it is not appropriate to upgrade certain components, the plan shall document the respective version and the rationale for the continued use of those components. Per F.2, those components not being updated are considered in RISK MANAGEMENT and the resulting RESIDUAL RISK and appropriate compensating controls shall clearly be communicated as part of the release documentation as described in 5.8.2 or Annex E.

NOTE 1 The term “certain components” can comprise the whole HEALTH SOFTWARE.

NOTE 2 When these activities have been completed, the MANUFACTURER has documented a baseline of the level of CYBERSECURITY implemented in the TRANSITIONAL HEALTH SOFTWARE.

F.4 Post-release ACTIVITIES

The post-release ACTIVITIES described in Clause 6 to Clause 9 shall be fulfilled for TRANSITIONAL HEALTH SOFTWARE to claim conformance with Annex F.

Annex G
(normative)

Object identifiers

Following ISO 9834-1:2012, 6.1.3, the “Registration (of elements and their associated OIDs) can be effected by an ITU-T Recommendation and/or International Standard, by publishing in the ITU-T Recommendation and/or International Standard the names and the corresponding definitions of the object“.

Therefore, this annex defines OIDs for conformance concepts defined in this document.

Table G.1 specifies the object identifiers and symbolic names for the ITU-T / ISO / IEC registration authority (currently under oid-info.com) towards stable, versioned references to these conformance concepts.

Table G.1 – Object identifiers for conformance concepts of this document

OID	Concept definition	Symbolic name
1.0.81001	ISO/IEC 81001 series, *Health software and health IT systems safety, effectiveness and security*	health-software
1.0.81001.5	ISO/IEC 81001-5, *Health software and health IT systems safety, effectiveness and security – Part 5: Security*	security
1.0.81001.5.1	IEC 81001-5-1, *Health software and health IT systems safety, effectiveness and security – Part 5-1: Security – Activities in the product life cycle*	lifecycle
1.0.81001.5.1.2021	IEC 81001-5-1:2021	edition1
1.0.81001.5.1.2021.1	Conformance to Clause 4 through Clause 9	full
1.0.81001.5.1.2021.2	Conformance of documentation	documentation
1.0.81001.5.1.2021.3	Conformance of TRANSITIONAL HEALTH SOFTWARE	transitional-sw

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

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.

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).

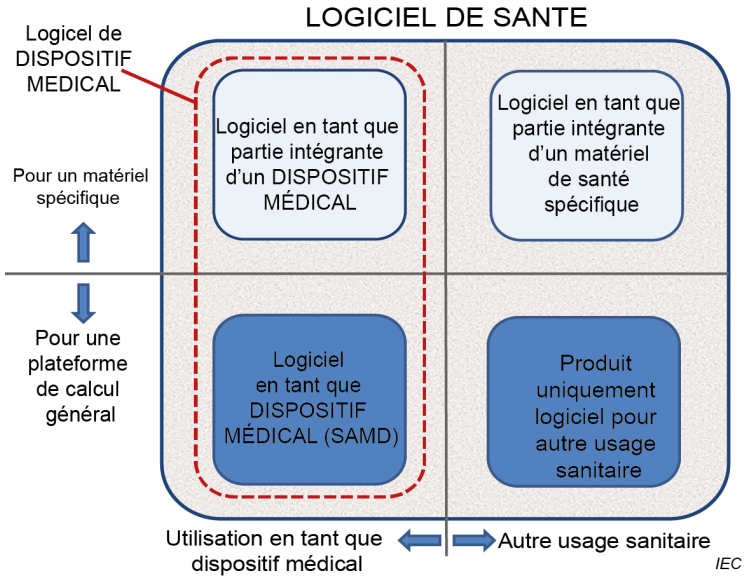
0.2 Champ d'application

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].

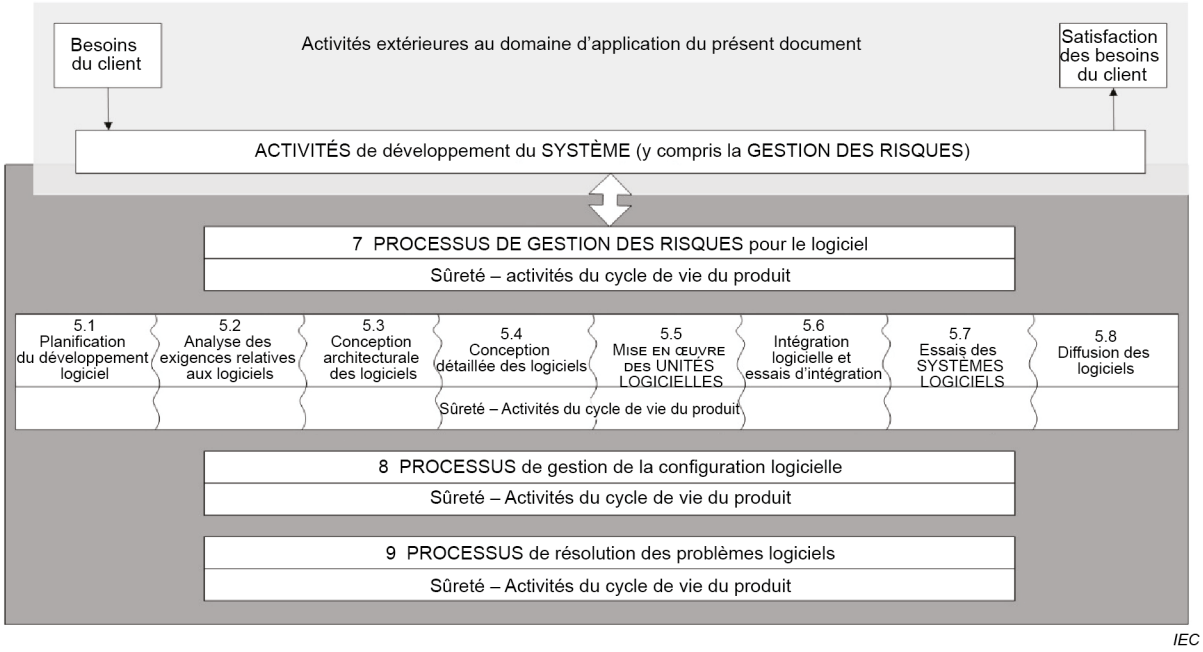
Les Articles 4 à 9 du présent document exigent l'établissement d'un ou plusieurs PROCESSUS comprenant des ACTIVITES identifiées. Selon les parties normatives du présent document, les PROCESSUS DU CYCLE DE VIE mettent en œuvre ces ACTIVITES. Aucune exigence définie dans le présent document n'impose la 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.

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions suivants s'appliquent.

L'ISO et l'IEC tiennent à jour des bases de données terminologiques destinées à être utilisées en normalisation, consultables aux adresses suivantes:

- IEC Electropedia: disponible à l'adresse www.electropedia.org/
- ISO Online browsing platform: disponible à l'adresse www.iso.org/obp

3.1
DOCUMENTATION D'ACCOMPAGNEMENT
documentation destinée à être utilisée pour un LOGICIEL DE SANTE ou un SYSTEME TI DE SANTE ou un accessoire, et qui contient des informations pour l'organisme responsable ou l'opérateur

3.2
ACTIVITE
ensemble d'une ou de plusieurs TACHES corrélées ou interactives

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

3.3
ARCHITECTURE
concepts fondamentaux ou propriétés fondamentales d'un système dans son environnement, incorporés dans ses éléments et dans ses relations, ainsi que dans les principes de sa conception et de son évolution

[SOURCE: ISO/IEC/IEEE 24765:2017, 3.216, définition 1]

3.4
ACTIF
entité physique ou numérique qui présente une valeur pour un individu, un organisme ou un gouvernement

Note 1 à l'article: Selon la définition du terme "ACTIF", ce concept peut inclure les éléments suivants:

a) des données et des informations;

b) le LOGICIEL DE SANTE et le ou les logiciels nécessaires pour son fonctionnement;

c) les composants matériels tels que les ordinateurs, dispositifs mobiles, serveurs, bases de données et réseaux;

d) les services, y compris, la SURETE, le développement logiciel, les opérations TI et les services externalisés tels que les centres de données, l'Internet et les solutions logicielles en tant que service et les solutions en nuage;

e) le personnel, et ses qualifications, compétences et expérience;

f) les procédures et la documentation techniques de gestion et de prise en charge de l'INFRASTRUCTURE TI DE SANTE;

g) les SYSTEMES TI DE SANTE configurés et mis en œuvre afin de répondre aux objectifs organisationnels par un recours aux ACTIFS; et

h) les facteurs incorporels, tels que la réputation et l'image.

[SOURCE: ISO 81001-1:2021[17] 3.3.2, modifié – Ajout d'une nouvelle Note 1 à l'article.]

3.5
ATTAQUE
tentative de détruire, de rendre public, de modifier, d'invalider, de voler ou d'utiliser sans autorisation un ACTIF, ou de faire un usage non autorisé de celui-ci

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

3.6
SURFACE D'ATTAQUE
interfaces physiques et fonctionnelles d'un système qui peuvent être accessibles et, de ce fait, potentiellement exploitées par un pirate

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

3.7
DISPONIBILITÉ
propriété d'être accessible et utilisable à la demande par une entité autorisée

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

3.8
CONFIDENTIALITÉ
propriété selon laquelle l'information n'est pas diffusée ni divulguée à des personnes, des entités ou des PROCESSUS non autorisés

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

3.9
ÉLÉMENT DE CONFIGURATION
entité qui peut être identifiée de manière univoque en un point de référence donné

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

3.10
GESTION DE LA CONFIGURATION
PROCESSUS assurant la cohérence des ELEMENTS DE CONFIGURATION par l'utilisation de mécanismes pour identifier, contrôler et assurer la traçabilité des versions des ELEMENTS DE CONFIGURATION

3.11
DEFENSE EN PROFONDEUR
démarche visant à défendre le système contre toute ATTAQUE particulière à l'aide de plusieurs méthodes indépendantes

Note 1 à l'article: La DEFENSE EN PROFONDEUR implique des couches de SECURITE et de détection, même sur des systèmes simples, et repose sur les caractéristiques suivantes:

- elle repose sur l'idée selon laquelle l'une des couches de protection peut éventuellement être mise en échec;
- il s'agit pour les pirates de transpercer ou contourner chaque couche sans être détectés;
- une faille dans une couche peut être atténuée par les capacités des autres couches;
- la SECURITE du système devient un ensemble de couches dans l'ensemble de la SECURITE du réseau; et
- il convient que chaque couche soit autonome et ne fasse pas appel aux mêmes fonctionnalités ni ne fasse l'objet des mêmes modes de défaillance que les autres couches.

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

3.12
EXPLOIT (substantif)
méthode définie de violation de la SURETE des systèmes d'information par une certaine VULNERABILITE

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

3.13
INFRASTRUCTURE TI DE SANTÉ
ensemble combiné d'ACTIFS TI à disposition de l'individu ou de l'organisme pour le développement, la configuration, l'intégration, la maintenance et l'utilisation des services TI, ainsi que pour la prise en charge de la santé, des soins au patient et d'autres objectifs organisationnels

[SOURCE: ISO 81001-1:2021[17], 3.3.7, modifié – Suppression de la Note 1 à l'article.]

3.14
SYSTEME TI DE SANTE
combinaison des éléments interactifs des informations de santé (y compris les LOGICIELS DE SANTE, les dispositifs médicaux, le matériel TI, les interfaces, les données, les procédures et la documentation) qui est configurée et mise en œuvre afin de prendre en charge et rendre possibles les objectifs de santé spécifiques à un individu ou un organisme

[SOURCE: ISO 81001-1:2021[17], 3.3.8, modifié – Ajout de "(y compris les LOGICIELS DE SANTE, les dispositifs médicaux, le matériel TI, les interfaces, les données, les procédures et la documentation)".]

3.15
LOGICIEL DE SANTE
logiciel destiné à être utilisé spécifiquement pour la gestion, le maintien ou l'amélioration de la santé des individus, ou la prestation de soins, ou dont le développement a pour objet son incorporation dans un dispositif médical

Note 1 à l'article: Le LOGICIEL DE SANTE inclut entièrement le logiciel considéré comme un dispositif médical.

[SOURCE: ISO 81001-1:2021[17], 3.3.9]

3.16
ORGANISME DE PRESTATION DE SOINS DE SANTE
HDO
établissement ou entreprise (par exemple, une clinique ou un hôpital) qui fournit des services de soin de santé

Note 1 à l'article: L'abréviation "HDO" est dérivée du terme anglais développé correspondant "healthcare delivery organization".

[SOURCE: ISO 81001-1:2021[17], 3.1.4]

3.17
INTÉGRITÉ
propriété d'exactitude et de complétude

[SOURCE: ISO/IEC 27000:2018, 3.36]

3.18
ENVIRONNEMENT D'UTILISATION PRÉVU
conditions et cadre dans lesquels les utilisateurs interagissent avec le LOGICIEL DE SANTE – selon les spécifications du FABRICANT

3.19
EMPLOI PREVU
DESTINATION PREVUE
utilisation à laquelle un PRODUIT, un PROCESSUS ou un service est destiné conformément aux spécifications, aux instructions et aux informations fournies par le FABRICANT

Note 1 à l'article: L'indication médicale prévue, la population de patients, la partie du corps ou le type de tissu soumis à une interaction, le profil de l'utilisateur, l'ENVIRONNEMENT D'UTILISATION PREVU et le principe de fonctionnement constituent des éléments typiques de l'EMPLOI PREVU.

[SOURCE: ISO 81001-1:2021[17], 3.2.7, modifié – Remplacement dans la Note 1 à l'article de "ENVIRONNEMENT D'UTILISATION" par "ENVIRONNEMENT D'UTILISATION PREVU".]

3.20
CYCLE DE VIE
série de toutes les phases de la vie d'un PRODUIT ou d'un système, de la conception initiale à la mise hors service et la mise au rebut finales

[SOURCE: ISO 81001-1:2021[17], 3.3.12]

3.21
LOGICIEL MAINTENU
ELEMENT LOGICIEL dont le FABRICANT tient compte par hypothèse du risque lié à la SURETE

Note 1 à l'article: Voir aussi l'Article A.3.

3.22
FABRICANT
organisme ayant pour responsabilité la conception ou la fabrication d'un PRODUIT

Note 1 à l'article: La responsabilité englobe la prise en charge des ACTIVITES au cours d'opérations.

Note 2 à l'article: Il n'y a qu'un seul FABRICANT, mais la responsabilité technique peut être celle de plusieurs entités tout au long de la chaîne d'approvisionnement, celle de fournisseurs de services ou celle de différentes entités à des stades différents du CYCLE DE VIE.

Note 3 à l'article: Indépendamment de la responsabilité du FABRICANT, toute responsabilité juridique spécifique est définie de manière contractuelle et par la législation.

[SOURCE: ISO 81001-1:2021[17], 3.1.7 – Ajout des notes à l'article.]

3.23
PROCESSUS
ensemble d'ACTIVITES corrélées ou interactives qui utilisent des éléments d'entrée pour produire un résultat prévu (effet)

[SOURCE: ISO 81001-1:2021[17], 3.2.10, modifié – Ajout de "(effet)" après "résultat prévu".]

3.24
PRODUIT
élément de sortie d'un organisme qui peut être produit sans aucune transaction entre celui-ci et le client

Note 1 à l'article: Un PRODUIT est obtenu sans la nécessité absolue d'une transaction entre le fournisseur et le client, mais ce processus peut souvent impliquer cet élément de service à la livraison du produit au client.

Note 2 à l'article: L'élément dominant d'un PRODUIT est l'élément généralement tangible.

[SOURCE: ISO 81001-1:2021[17], 3.3.15]

3.25
LOGICIEL EXIGÉ
ELEMENT LOGICIEL pour lequel le FABRICANT considère que les risques liés à la SURETE sont identifiés préalablement à la diffusion du LOGICIEL DE SANTE

Note 1 à l'article: Le LOGICIEL EXIGE inclut le LOGICIEL PRIS EN CHARGE. Voir l'Article A.3.

3.26
RISQUE RÉSIDUEL
risque subsistant après que des mesures de MAITRISE DES RISQUES ont été prises

[SOURCE: ISO 81001-1:2021[17], 3.4.9]

3.27
MAÎTRISE DES RISQUES
PROCESSUS au cours duquel les décisions sont prises et les mesures qui visent à réduire les risques ou à les maintenir dans les limites spécifiées sont mises en place

[SOURCE: ISO 81001-1:2021[17], 3.4.13, modifié – Cette modification ne s'applique qu'à la version anglaise.]

3.28
GESTION DES RISQUES
application systématique des politiques de gestion, des procédures et des pratiques à des TACHES d'analyse, d'évaluation, de contrôle et de maîtrise des risques

[SOURCE: ISO 81001-1:2021[17], 3.4.16]

3.29
SÉCURITÉ
absence de risque inacceptable

Note 1 à l'article: Dans le contexte de la SECURITE, le risque est la combinaison de la probabilité d'occurrence d'un dommage et de la gravité de ce dommage (voir le Guide ISO/IEC 51:2014).

Note 2 à l'article: Les incidents de SURETE peuvent entraîner un dommage et peuvent par conséquent influer sur la SECURITE.

[SOURCE: ISO 81001-1:2021[17], 3.2.12, modifié – Ajout des notes à l'article.]

3.30
SURETE
CYBERSECURITE
état de protection des informations et des systèmes contre les ACTIVITES non autorisées telles que l'accès, l'utilisation, la divulgation, l'interruption, la modification ou la destruction à un degré auquel les risques liés à la violation de la CONFIDENTIALITE, de l'INTEGRITE et de la DISPONIBILITE sont maintenus à un niveau acceptable tout au long du CYCLE DE VIE

[SOURCE: ISO 81001-1:2021[17], 3.2.13]

3.31
CAPACITÉ DE SÛRETÉ
large catégorie de contrôles techniques, administratifs ou organisationnels destinés à gérer les risques pour la CONFIDENTIALITE, l'intégrité, la disponibilité et la responsabilité des données et des systèmes

[SOURCE: ISO 81001-1:2021[17], 3.2.14]

3.32
CONTEXTE DE SÛRETÉ
exigences et hypothèses minimales concernant l'environnement des LOGICIELS DE SANTE - issu de l'ENVIRONNEMENT D'UTILISATION PREVU au niveau du PRODUIT, avec prise en considération également de la configuration et de l'intégration des LOGICIELS DE SANTE, ainsi que de l'accès non autorisé ou fortuit prévisible

3.33
ANALYSE DE COMPOSITION LOGICIELLE
analyse (électronique) des éléments binaires

Note 1 à l'article: L'ANALYSE DE COMPOSITION LOGICIELLE peut être prise en charge par des outils ou des services en ligne.

3.34
ELEMENT LOGICIEL
partie identifiable d'un programme informatique, c'est-à-dire: code source, code objet, code de contrôle, données de contrôle, ou un ensemble de ces éléments

[SOURCE: IEC 62304:2006 et IEC 62304:2006/AMD1:2015, 3.25, modifié – Suppression de la note.]

3.35
MAINTENANCE DU LOGICIEL
modification d'un LOGICIEL DE SANTE après son lancement

Note 1 à l'article: La maintenance préserve l'EMPLOI PREVU et est faite pour une ou plusieurs des raisons suivantes:

a) corrective, au sens de la correction des anomalies;

b) adaptative, au sens de l'adaptation à une nouvelle plate-forme matérielle ou logicielle;

c) améliorante, au sens de la mise en œuvre de nouvelles exigences;

d) préventive, au sens d'une meilleure maintenance du PRODUIT.

Note 2 à l'article: Voir également ISO/IEC 14764:2006, 3.10.

[SOURCE: IEC 82304-1:2016, 3.21, modifié – Dans la définition, l'expression "PRODUIT LOGICIEL DE SANTE" a été remplacée par "LOGICIEL DE SANTE", les raisons de la maintenance sont placées dans une note qui souligne également l'UTILISATION PREVUE et la référence 3.10 a été ajoutée à la deuxième note à l'article.]

3.36
LOGICIEL PRIS EN CHARGE
ELEMENT LOGICIEL dont le FABRICANT informe le client des risques liés à la SURETE identifiés

Note 1 à l'article: Le logiciel exigé inclut le LOGICIEL MAINTENU. Voir l'Article A.3.

3.37
TÂCHE
partie unique d'un travail qui doit être effectué pour atteindre un objectif spécifique

[SOURCE: IEC 62304:2006[8], 3.31, modifié – Ajout de l'expression "pour atteindre un objectif spécifique".]

3.38
MENACE
possibilité de violation de la SURETE, qui survient en cas de circonstance, de capacité, d'action ou d'événement qui peut porter atteinte à la SURETE, ainsi qu'à la CONFIDENTIALITE, l'INTEGRITE et la DISPONIBILITE des ACTIFS informationnels

[SOURCE: ISO 81001-1:2021[17], 3.4.1.21, modifié – Cette modification ne s'applique qu'à la version anglaise.]

3.39
MODELE DE MENACE
résultat documenté de l'ACTIVITE DE MODELISATION D'UNE MENACE

3.40
MODELISATION D'UNE MENACE
technique d'exploration systématique qui vise à exposer toute circonstance ou tout événement susceptible d'endommager un système sous la forme d'une destruction, d'une divulgation, d'une modification de données ou d'un refus de service

[SOURCE: ISO/IEC/IEEE 24765:2017, 3.4290, modifié – Cette modification ne s'applique qu'à la version anglaise.]

3.41
TRAÇABILITE
lien entre l'origine des exigences tout au long du CYCLE DE VIE d'un projet de conception des éléments et les cas d'essai

3.42
LOGICIEL DE SANTE TRANSITOIRE
LOGICIEL DE SANTE, diffusé préalablement à la publication du présent document et qui ne satisfait pas à toutes les exigences spécifiées de l'Article 4 à l'Article 9 du présent document

Note 1 à l'article: Le FABRICANT d'un LOGICIEL DE SANTE TRANSITOIRE peut revendiquer la conformité à l'Annexe F.

3.43
LIMITE DE CONFIANCE
élément d'un MODELE de MENACE qui représente une limite qui exige une authentification ou qui est soumise à une modification du niveau de confiance (de plus élevé à moins élevé ou inversement)

Note 1 à l'article: Les mécanismes de mise en œuvre de la LIMITE DE CONFIANCE pour les utilisateurs de PRODUITS incluent généralement l'authentification (par exemple, question/réponse, mots de passe, biométrie ou signatures numériques) et l'autorisation associée (par exemple, règles de contrôle d'accès).

Note 2 à l'article: Les mécanismes de mise en œuvre de la LIMITE DE CONFIANCE pour les données incluent généralement l'authentification de la source (par exemple, codes d'authentification du ou des messages et signatures numériques) et/ou la VALIDATION du contenu.

3.44
ENVIRONNEMENT D'UTILISATION
conditions et cadre réels dans lesquels les utilisateurs interagissent avec le LOGICIEL DE SANTE

Note 1 à l'article: Pour les besoins du présent document, l'ENVIRONNEMENT D'UTILISATION inclut les interfaces de données.

[SOURCE: IEC 62366-1:2015 et IEC 62366-1:2015/AMD1:2020; 3.20, modifié – "Dispositif médical" remplacé par "LOGICIEL DE SANTE" dans la définition, et remplacement du contenu de la Note 1 à l'article.]

3.45
VALIDATION
confirmation par des preuves objectives que les exigences pour une UTILISATION spécifique ou une application prévue ont été satisfaites

Note 1 à l'article: Les preuves objectives requises pour la VALIDATION peuvent être le résultat d'un essai ou d'une autre forme de détermination, telle que la réalisation de calculs ou la revue de documents.

Note 2 à l'article: Le terme "validé" est utilisé pour désigner l'état correspondant.

Note 3 à l'article: Pour la VALIDATION, les conditions d'utilisation peuvent être réelles ou simulées.

[SOURCE: ISO 9000:2015, 3.8.13]

3.46
VÉRIFICATION
confirmation par des preuves tangibles que les exigences spécifiées ont été satisfaites

Note 1 à l'article: Les preuves objectives nécessaires pour la VERIFICATION peuvent être le résultat d'un contrôle ou d'autres formes de détermination, telles que la réalisation de calculs ou la revue de documents.

Note 2 à l'article: Les ACTIVITES réalisées pour la VERIFICATION sont parfois appelées PROCESSUS de qualification.

Note 3 à l'article: Le terme "vérifié" est utilisé pour désigner l'état correspondant.

[SOURCE: ISO 81001-1:2021[17], 3.2.16]

3.47
VULNÉRABILITÉ
faille ou POINT FAIBLE dans la conception, la mise en œuvre ou le fonctionnement et la gestion d'un système qui peuvent être exploités pour enfreindre la stratégie de SURETE du système

[SOURCE: ISO 81001-1:2021[17], 3.4.22]

3.48
POINT FAIBLE
type d'insuffisance

Note 1 à l'article: Un POINT FAIBLE peut entraîner un risque de SURETE.

[SOURCE: ISO 81001-1:2021[17], 3.4.23, modifié – Suppression de "et/ou des risques pour la vie privée" dans la Note 1 à l'article.]

4 Exigences générales

4.1 Management de la qualité

4.1.1 Système de management de la qualité

Le FABRICANT doit réaliser les ACTIVITES DE SURETE du CYCLE DE VIE DU PRODUIT sur la base d'un système de management de la qualité établi et documenté.

Le système de management de la qualité peut être mis en œuvre conformément à l'ISO 13485 ou à d'autres normes de management de la qualité équivalentes.

Dans l'ensemble du présent document "établir une ACTIVITE (ou des ACTIVITES)" signifie que le FABRICANT doit documenter cette ACTIVITE (ou ces ACTIVITES) et doit assurer leur réalisation de manière efficace et exhaustive.

4.1.2 Identification des responsabilités

Le FABRICANT doit désigner et documenter les rôles organisationnels et le personnel en charge de chacune des ACTIVITES et de chacun des PROCESSUS exigés par le présent document.

NOTE L'identification du personnel peut s'effectuer par l'intermédiaire des rôles fonctionnels plutôt que des noms.

4.1.3 Identification de l'applicabilité

Le FABRICANT doit identifier les PRODUITS ou parties de PRODUITS auxquels le CYCLE DE VIE sécurisé s'applique.

NOTE 1 Pour les LOGICIELS DE SANTE, certaines capacités d'exposition, de mise en réseau ou d'interfaces de données TI sont définies par hypothèse, et un CYCLE DE VIE sécurisé du logiciel est suivi.

NOTE 2 Cette exigence ne concerne pas les instances de PRODUITS (et leur identification), mais les types de PRODUITS ou leurs parties –par exemple, les ELEMENTS LOGICIELS. Réaliser cette ACTIVITE (ou ces ACTIVITES) signifie que le FABRICANT dispose de critères d'identification des parties de ses PRODUITS qui sont développées, maintenues et prises en charge au moyen des ACTIVITES décrites par le présent document.

4.1.4 Expertise en matière de SÛRETÉ

Le FABRICANT doit établir une ACTIVITE (ou des ACTIVITES) destinées à identifier et à fournir des programmes de formation à la SURETE et d'évaluation de la sûreté de manière à vérifier que le personnel affecté aux rôles et devoirs organisationnels spécifiés en 4.1.2 a démontré une expertise en SURETE appropriée à ces PROCESSUS. Les résultats de cette ACTIVITE (ou ces ACTIVITES) incluent les descriptions de rôles, ainsi que les profils et les registres de formation.

NOTE Cette ACTIVITE (ou ces ACTIVITES) peuvent être mises en œuvre par exemple comme partie intégrante du 6.2 de l'ISO 13485:2016.

4.1.5 ÉLEMENTS LOGICIELS provenant de fournisseurs tiers

Le FABRICANT doit vérifier que les fournisseurs tiers réalisent les ACTIVITES applicables du CYCLE DE VIE DE SURETE pour chaque ELEMENT LOGICIEL lorsqu'il satisfait aux deux critères suivants:

a) l'ELEMENT LOGICIEL est développé principalement plus particulièrement pour le FABRICANT et pour un objet spécifique; et

b) l'ELEMENT LOGICIEL peut influer sur la SURETE.

Le FABRICANT doit communiquer les exigences liées à la SURETE pour chaque ELEMENT LOGICIEL développé plus particulièrement par une partie tierce pour le FABRICANT et pour un objet spécifique.

NOTE Cette exigence s'applique lorsque le FABRICANT sous-traite à une partie tierce le développement spécifique d'un ELEMENT LOGICIEL qui peut influer sur la SURETE. La MODELISATION D'UNE MENACE sert habituellement à déterminer quel ELEMENT LOGICIEL influe sur la SURETE.

4.1.6 Amélioration continue

Le FABRICANT doit établir une ACTIVITE (ou des ACTIVITES) d'amélioration continue du CYCLE DE VIE de développement de la SURETE. Cette ACTIVITE (ou ces ACTIVITES) doivent inclure l'analyse des défauts de SURETE des ELEMENTS LOGICIELS/LOGICIELS DE SANTE/PRODUITS déployés sur site – en raison d'ACTIVITES insuffisantes ou absentes.

NOTE 1 Cette ACTIVITE (ou ces ACTIVITES) peuvent être mises en œuvre par exemple comme partie intégrante du 8.5 de l'ISO 13485:2016.

NOTE 2 Cette ACTIVITE (ou ces ACTIVITES) assurent que le FABRICANT améliore la rigueur de ses ACTIVITES DE SURETE dans la durée. Dans le cas de défauts de SURETE dépendant du PROCESSUS, il est important que le FABRICANT facilite la compensation de cette dépendance par une amélioration continue de ses ACTIVITES DE SURETE.

4.1.7 Divulgation des problèmes liés à la SURETE

Le FABRICANT doit établir une ACTIVITE (ou des ACTIVITES) destinées à informer dans un délai convenable les organes de réglementation et les utilisateurs de PRODUITS de l'existence de VULNERABILITES (identifiées par le biais d'ACTIVITES comme cela est spécifié en 9.5) constatées dans les PRODUITS pris en charge. Cette ou ces activités d'information comprennent entre autres les informations suivantes:

a) description des VULNERABILITES et notation de celles-ci selon un système CVSS ou un système analogue de classement des VULNERABILITES, et de la ou des versions de PRODUITS affectées; et

b) description de la résolution.

NOTE 1 La description de la résolution peut inclure des références à l'installation de mises à jour de SURETE –voir l'Article 12 de l'IEC 62443-4-1:2018[11].

NOTE 2 Le respect des délais est géré par les autorités, la législation applicable, la politique de réglementation, la SECURITE des PRODUITS et les forces du marché. La stratégie de traitement des VULNERABILITES de composants tiers déterminées par le développeur de PRODUITS tient compte de la possibilité d'une divulgation publique par le fournisseur des composants tiers.

NOTE 3 Cette ACTIVITE (ou ces ACTIVITES) peuvent être mises en œuvre par exemple comme partie intégrante de l'ISO 13485:2016, 7.2.3.

NOTE 4 Voir 4.1.9, 4.2 et 6.2.

4.1.8 Revue périodique de la gestion des défauts de SURETE

Le FABRICANT doit établir une ACTIVITE (ou des ACTIVITES) destinées à mener des revues périodiques du PROCESSUS de résolution des problèmes logiciels.

Les revues périodiques des ACTIVITES doivent au moins examiner les problèmes liés à la SURETE gérés par le PROCESSUS depuis la dernière revue périodique destinée à déterminer si le PROCESSUS de gestion était complet, efficace et a permis de résoudre les problèmes liés à la SURETE.

Des revues périodiques du PROCESSUS de gestion des problèmes liés à la SURETE doivent être menées au moins une fois par an ou comme partie intégrante de la surveillance, du mesurage et de l'analyse des PROCESSUS définis au 4.1.3 de l'ISO 13485:2016.

NOTE Cette ACTIVITE (ou ces ACTIVITES) peuvent être mises en œuvre par exemple comme partie intégrante du 5.6 de l'ISO 13485:2016.

4.1.9 Revue de la DOCUMENTATION D'ACCOMPAGNEMENT

Le FABRICANT doit établir une ACTIVITE (ou des ACTIVITES) destinées à identifier, caractériser et établir le suivi des erreurs liées à la SURETE et des omissions dans la DOCUMENTATION D'ACCOMPAGNEMENT y compris les lignes directrices relatives à la SURETE.

NOTE Cette ACTIVITE (ou ces ACTIVITES) peuvent être mises en œuvre par exemple comme partie intégrante du 7.3 de l'ISO 13485:2016.

4.2 GESTION DES RISQUES DE SÛRETÉ

Le FABRICANT doit établir un PROCESSUS DE GESTION DES RISQUES associés à la SURETE. Ce PROCESSUS doit utiliser la MODELISATION D'UNE MENACE pour identifier les VULNERABILITES, estimer et évaluer les MENACES associées, surveiller ces MENACES, et contrôler l'efficacité des mesures (de SURETE) de MAITRISE DES RISQUES, compte tenu de l'EMPLOI PREVU et de l'ENVIRONNEMENT D'UTILISATION du LOGICIEL DE SANTE.

NOTE 1 Un dispositif médical conçu selon une approche de DEFENSE EN PROFONDEUR par couches ne repose pas sur des contrôles de SURETE dans l'environnement d'exploitation. Néanmoins, dans le cadre de cette approche de DEFENSE EN PROFONDEUR par couches, il existe des attentes par rapport à l'environnement d'exploitation prévu. Les attentes relatives à l'environnement d'exploitation peuvent inclure des caractéristiques de protection et de performance et peuvent constituer des éléments d'entrée pour la MODELISATION D'UNE MENACE.

Le FABRICANT doit établir les critères d'acceptabilité des risques qui doivent être appliqués pour déterminer la méthode appropriée de traitement de chaque VULNERABILITE.

Il convient que la GESTION DES RISQUES DE SURETE intègre les résultats de l'ACTIVITE (ou des ACTIVITES) de MODELISATION D'UNE MENACE et suive les lignes directrices et les meilleures pratiques du secteur.

Les étapes détaillées du PROCESSUS sont décrites à l'Article 7.

NOTE 2 Ce PROCESSUS peut faire partie intégrante d'un PROCESSUS général de GESTION DES RISQUES. La GESTION DES RISQUES DE SURETE peut être réalisée dans le cadre de l'ISO 14971 avec un relevé approprié des termes de VULNERABILITE, de MENACE et autres termes liés à la SURETE, ainsi que l'ajout des ACTIVITES pertinentes pour la SURETE. (Voir l'ISO TR 24971:2020 pour un relevé potentiel.)

Le FABRICANT doit documenter tout RISQUE RESIDUEL associé à une VULNERABILITE qui demeure dans le système et doit également documenter les contrôles compensatoires respectifs appliqués.

Voir l'Annexe C relative à la MODELISATION D'UNE MENACE.

4.3 Classification de l'ELEMENT LOGICIEL relatif au transfert de risque

Le FABRICANT doit documenter quel ELEMENT LOGICIEL est

a) le LOGICIEL MAINTENU;

b) le LOGICIEL PRIS EN CHARGE; ou

c) le LOGICIEL EXIGÉ.

NOTE Cette ACTIVITE (ou ces ACTIVITES) peuvent être mises en œuvre par exemple comme partie intégrante du 7.4 de l'ISO 13485:2016.

5 PROCESSUS de développement logiciel

5.1 Planification du développement logiciel

5.1.1 ACTIVITES du PROCESSUS DU CYCLE DE VIE

Le FABRICANT doit établir les ACTIVITES générales du CYCLE DE VIE – de la conception à la mise hors service – qui sont cohérentes et intégrées à un PROCESSUS communément accepté de développement des PRODUITS, y compris entre autres:

a) la GESTION DE LA CONFIGURATION avec maîtrise et historique des modifications;

b) la description du ou des PRODUITS et la définition des exigences avec leur TRAÇABILITE;

c) les pratiques de conception et de mise en œuvre des logiciels et des matériels, comme la conception modulaire;

d) un PROCESSUS reproductible de VERIFICATION et de VALIDATION des essais;

e) la revue et l'approbation de tous les enregistrements de PROCESSUS de développement;

f) le service après-vente; et

g) les mises à jour et les correctifs de SURETE pour les LOGICIELS DE SANTE.

NOTE Le service après-vente désigne la fourniture d'informations, ainsi que d'une assistance et d'une formation afin d'installer et de rendre opérationnel le LOGICIEL DE SANTE dans son environnement prévu, et également d'offrir de meilleures capacités aux utilisateurs. Voir l'ISO/IEC/IEEE 24765:2017.

Le FABRICANT doit documenter la justification de non mise en œuvre des exigences du présent document dans le cadre d'un projet de LOGICIEL DE SANTE donné sur la base d'une revue et de l'approbation du personnel doté de l'expertise appropriée en matière de SURETE.

5.1.2 SÛRETÉ de l'environnement de développement

Le FABRICANT doit établir des contrôles de procédure et techniques fondés sur les risques destinés à protéger l'infrastructure TI de développement, de fourniture et de maintenance des produits contre tout accès, toute corruption et toute suppression non autorisés. Ce processus comprend la protection du LOGICIEL DE SANTE pendant la conception, la mise en œuvre, les mises à jour, les essais et la diffusion.

5.1.3 Normes de codage sécurisé

Le FABRICANT doit établir et maintenir des normes de codage sécurisé conformes aux meilleures pratiques actuelles liées à la conception et à la mise en œuvre de systèmes logiciels sécurisés.

Voir l'Annexe A.

5.2 Analyse des exigences relatives aux LOGICIELS DE SANTE

5.2.1 Exigences de SURETE relatives aux LOGICIELS DE SANTE

Le FABRICANT doit établir une ACTIVITE (ou des ACTIVITES) destinées à vérifier la documentation des exigences de SURETE pour les LOGICIELS DE SANTE, y compris les exigences relatives aux CAPACITES DE SURETE liées à l'installation, à l'exploitation, à la maintenance et à la mise hors service.

NOTE 1 L'IEC TR 60601-4-5 fournit des recommandations concernant la spécification des CAPACITES DE SURETE et la preuve de leur existence dans la DOCUMENTATION D'ACCOMPAGNEMENT, ainsi qu'une méthode de détermination des exigences à partir du niveau de CAPACITE DE SURETE.

NOTE 2 L'IEC TR 80001-2-2 spécifie les besoins, les risques et les contrôles liés à la SURETE sous forme de recommandations concernant la divulgation et la communication entre le FABRICANT et l'ORGANISME DE PRESTATION DE SOINS DE SANTE.

NOTE 3 Le PROCESSUS de spécification des exigences concernant les PRODUITS établit une interface avec les exigences relatives aux LOGICIELS DE SANTE. Certains contrôles techniques peuvent être mis en œuvre au niveau du PRODUIT (par exemple, par le matériel). Voir E.2.1.

5.2.2 Revue des exigences de SÛRETÉ

Le FABRICANT doit établir une ACTIVITE (ou des ACTIVITES) destinées à vérifier que les exigences de SURETE

a) mettent en œuvre les exigences concernant les PRODUITS, y compris celles relatives à la MAITRISE DES RISQUES;
b) ne se contredisent pas mutuellement;
c) sont exprimées en des termes qui évitent toute ambiguïté; et
d) sont énoncées en des termes qui permettent d'établir des critères d'essai et de réaliser des essais.

Le FABRICANT doit documenter le niveau d'indépendance des réviseurs. Chacune des disciplines représentatives suivantes doit participer à cette ACTIVITE (ou à ces ACTIVITES):

a) architectes/développeurs (ceux qui mettent en œuvre les exigences);
b) contrôleurs (ceux qui valident la satisfaction aux exigences);
c) experts interfonctionnels (peuvent inclure ceux dotés d'une expertise clinique); et
d) conseiller(s) en SÛRETÉ.

NOTE 1 Une seule personne peut être chargée de plusieurs disciplines. Il n'est pas recommandé qu'une seule personne soit chargée de toutes les disciplines.

NOTE 2 La liste des disciplines est documentée au moins une fois par projet.

NOTE 3 Un système de management de la qualité comme celui défini dans l'ISO 13485 implique la prise en considération de l'indépendance des réviseurs.

5.2.3 Risques de SURETE pour les LOGICIELS EXIGES

Le FABRICANT doit établir une ACTIVITE (ou des ACTIVITES) qui identifient et gèrent les risques de SURETE de tous les LOGICIELS EXIGES.

NOTE 1 Cette ACTIVITE (ou ces ACTIVITES) permettent de vérifier que les exigences relatives aux LOGICIELS DE SANTE tiennent compte des besoins de SURETE des LOGICIELS EXIGES.

NOTE 2 Cette ACTIVITE (ou ces ACTIVITES) peuvent faire partie intégrante des ACTIVITES DE SURETE de la chaîne d'approvisionnement.

5.3 Conception architecturale des logiciels

5.3.1 ARCHITECTURE/conception de la DEFENSE EN PROFONDEUR

Le FABRICANT doit établir une ACTIVITE (ou des ACTIVITES) destinées à spécifier une ARCHITECTURE de SURETE.

À chaque phase de développement, il convient que le FABRICANT prenne en considération la DEFENSE EN PROFONDEUR et attribue des exigences techniques à chaque couche de défense.

Lors de l'identification des mesures techniques de MAITRISE DES RISQUES de SURETE, le FABRICANT doit tenir compte des exigences relatives à la SECURITE ou aux performances des LOGICIELS DE SANTE.

NOTE La DEFENSE EN PROFONDEUR peut inclure les exigences de SURETE dans la DOCUMENTATION D'ACCOMPAGNEMENT à mettre en œuvre par le HDO.

5.3.2 Meilleures pratiques de conception sécurisée

Le FABRICANT doit établir une ACTIVITE (ou des ACTIVITES) d'identification, de mise en œuvre et de maintien de pratiques de conception sécurisée. Il doit documenter les meilleures pratiques de conception sécurisée dont il convient qu'elles incluent entre autres:

a) la documentation de toutes les LIMITES DE CONFIANCE comme partie intégrante de la conception;

b) le moindre privilège (octroi aux utilisateurs/logiciels uniquement des privilèges nécessaires pour réaliser les opérations prévues);

c) l'utilisation d'ELEMENTS/conceptions LOGICIELS sécurisés éprouvés dans toute la mesure possible;

d) le développement d'une économie de mécanisme (œuvrant pour des conceptions simples);

e) l'utilisation de modèles de conception sécurisés;

f) la réduction de la SURFACE D'ATTAQUE;

g) le retrait des portes dérobées, la suppression de l'accès et des informations de débogage utilisés en cours de développement ou la documentation de leur présence, ainsi que la nécessité de les protéger contre tout accès non autorisé; et

h) la protection des informations de débogage restantes éventuelles contre tout accès non autorisé.

Le FABRICANT doit définir une ARCHITECTURE de SURETE en tant que partie intégrante de la DEFENSE EN PROFONDEUR, ainsi que les pratiques énumérées ci-dessus, s'il y a lieu.

NOTE Voir l'Annexe B.

5.3.3 Revue de conception architecturale de SURETE

Le FABRICANT doit mettre en œuvre une revue architecturale du LOGICIEL DE SANTE par rapport au comportement dans des conditions défavorables:

a) séparation efficace des ELEMENTS LOGICIELS;

b) meilleures pratiques de conception sécurisée (voir 5.3.2); et

c) failles de SURETE potentielles introduites par l'ARCHITECTURE.

Le FABRICANT doit documenter et mettre en œuvre la revue de conception architecturale.

NOTE La séparation utilise des contrôles techniques de conception et de mise en œuvre afin de vérifier que des ELEMENTS LOGICIELS ne peuvent être influencés de manière involontaire par d'autres ELEMENTS LOGICIELS du LOGICIEL DE SANTE.

5.4 Conception logicielle

5.4.1 Meilleures pratiques de conception logicielle

Le FABRICANT doit établir une ACTIVITE (ou des ACTIVITES) de développement et de documentation d'une conception sécurisée des LOGICIELS DE SANTE, et maintenir l'utilisation des meilleures pratiques pour la conception sécurisée, compte tenu des éléments suivants:

a) technologie des logiciels au niveau de l'application (par exemple, algorithmes, méthodes);

b) technique de programmation employée (par exemple, langage de programmation);

c) meilleures pratiques de conception sécurisée (spécifiées en 5.3.2).

5.4.2 Conception sécurisée

La conception des LOGICIELS DE SANTE doit inclure des mesures pour faire face aux MENACES identifiées dans le MODELE DE MENACE.

NOTE LE CONTEXTE DE SURETE des LOGICIELS DE SANTE est issu de l'ENVIRONNEMENT D'UTILISATION PREVU au niveau du PRODUIT, compte tenu également de la configuration et de l'intégration du LOGICIEL DE SANTE.

5.4.3 Interfaces sécurisées des LOGICIELS DE SANTE

La conception des LOGICIELS DE SANTE doit identifier et caractériser chaque interface des LOGICIELS DE SANTE, y compris les interfaces physiques et logiques. Le cas échéant, le FABRICANT identifie comme partie intégrante de la conception:

a) l'accessibilité externe (par d'autres PRODUITS) ou interne de l'interface – entre les ELEMENTS LOGICIELS du LOGICIEL DE SANTE – ou les deux types d'accessibilité;

b) les implications de la SURETE du CONTEXTE DE SURETE des LOGICIELS DE SANTE sur l'interface externe;

c) les utilisateurs potentiels de l'interface et les ACTIFS auxquels les interfaces permettent un accès (direct ou indirect);

d) l'inclusion éventuelle dans la conception statique d'un accès aux interfaces par le biais des LIMITES DE CONFIANCE;

e) les considérations, hypothèses et/ou contraintes de SURETE associées à l'utilisation de l'interface dans le CONTEXTE DE SURETE des LOGICIELS DE SANTE, y compris les menaces applicables;

f) les rôles de SURETE, privilèges/droits et autorisations de contrôle d'accès nécessaires pour utiliser l'interface et pour accéder aux ACTIFS définis en c);

g) les CAPACITES DE SURETE et/ou mécanismes de compensation utilisés pour la protection de l'interface et des ACTIFS identifiés en c) y compris la validation du temps d'exécution des éléments d'entrée, ainsi que le traitement des éléments de sortie et des erreurs;

h) l'utilisation d'ELEMENTS LOGICIELS tiers pour la mise en œuvre de l'interface et leurs CAPACITES DE SURETE;

i) la documentation de description de la méthode d'utilisation de l'interface avec un accès externe; et

j) la description de la manière dont la conception atténue les MENACES identifiées dans le MODELE DE MENACE.

NOTE LE CONTEXTE DE SURETE des LOGICIELS DE SANTE est issu de l'ENVIRONNEMENT D'UTILISATION PREVU au niveau du PRODUIT, compte tenu également de la configuration et de l'intégration du LOGICIEL DE SANTE.

5.4.4 VERIFICATION de conception détaillée pour la SURETE

Le FABRICANT doit établir une ACTIVITE (ou des ACTIVITES) de réalisation des revues de conception destinées à identifier, caractériser et établir le suivi des POINTS FAIBLES associés à chaque révision significative de la conception sécurisée, y compris entre autres:

a) les exigences de SURETE non correctement traitées par la conception;

b) les MENACES et leur capacité à exploiter les VULNERABILITES des interfaces de PRODUITS, des LIMITES DE CONFIANCE et des ACTIFS;

c) l'identification, la documentation et la caractérisation des meilleures pratiques de conception détaillée non suivies (5.3.2 et 5.4.1).

NOTE Les revues de conception tiennent également compte de chaque service logiciel utilisé par le LOGICIEL DE SANTE pour atteindre sa fonctionnalité prévue, par exemple: en nuage, logiciel/infrastructure/plateforme en tant que service.

5.5 Mise en œuvre et VERIFICATION des unités logicielles

5.5.1 Normes de codage sécurisé

Le FABRICANT doit établir une ACTIVITE (ou des ACTIVITES) de mise en œuvre qui suivent les normes de codage sécurisé.

Voir l'Article A.4.

5.5.2 Revue de mise en œuvre de la SURETE

Le FABRICANT doit établir une ACTIVITE (ou des ACTIVITES) destinées à vérifier que les revues de mise en œuvre sont réalisées afin d'identifier, de caractériser et d'intégrer au PROCESSUS de résolution des problèmes, tous les problèmes liés à la SURETE qui sont associés à la mise en œuvre de la conception sécurisée, y compris:

a) l'identification des exigences de SURETE (voir 5.2) non correctement traitées par la mise en œuvre;

NOTE L'attribution des exigences, y compris les exigences de SURETE, fait partie des PROCESSUS de conception types.

b) l'identification des normes de codage sécurisé utilisées et la documentation des parties de ces normes qui n'ont pas été suivies (par exemple, utilisation des fonctions exclues ou défaut d'application du principe du moindre privilège);

c) l'analyse de code statique (SCA - *static code analysis*) applicable au code source afin de déterminer les erreurs de codage sécurisé au moyen de la norme de codage sécurisé dédiée au langage de programmation pris en charge, comme cela est établi en 5.1.3; la SCA est souvent prise en charge par des outils, mais peut être réalisée par l'intermédiaire de contrôles et de révisions de codes;

d) la revue de la mise en œuvre et de sa TRAÇABILITE par rapport aux CAPACITES DE SURETE définies pour prendre en charge la conception de la SURETE (voir 5.3 et 5.4); et

e) l'examen des MENACES et de leur capacité à exploiter les interfaces de mise en œuvre, les LIMITES DE CONFIANCE et les ACTIFS (voir 5.3 et 5.4).

5.6 Essais d'intégration logicielle

Le FABRICANT peut réaliser certains des essais de systèmes logiciels comme partie intégrante des essais d'intégration logicielle (voir 5.7).

Il convient que le FABRICANT prenne en considération les différences de politique de SURETE par l'intermédiaire des LIMITES DE CONFIANCE, comme partie intégrante des essais d'intégration des LOGICIELS DE SANTE.

5.7 Essais des systèmes logiciels

5.7.1 Vérification par essai des exigences de SURETE

Le FABRICANT doit établir une ACTIVITE (ou des ACTIVITES) destinées à vérifier que les fonctions de SURETE des LOGICIELS DE SANTE satisfont aux exigences de SURETE et que le LOGICIEL DE SANTE traite les scénarii d'erreurs et les éléments d'entrée non valides. Les types d'essais, fondés sur l'ENVIRONNEMENT D'UTILISATION PREVU, doivent inclure:

a) les essais de fonctionnement des exigences de SURETE;

b) les essais de performances et de mise à l'échelle;

c) les conditions aux limites, les contraintes et les essais d'entrée malformés ou non prévus avec des conséquences potentielles pour la SURETE; et

d) la vérification par essai de chaque service logiciel utilisé par le LOGICIEL DE SANTE pour atteindre sa fonctionnalité prévue, dans le contexte d'accords de responsabilité parmi les fournisseurs de service, les FABRICANTS et les opérateurs, par exemple, services en nuage, logiciel en tant que service, infrastructure en tant que service, plateforme en tant que service.

NOTE Voir B.5.7.1.

5.7.2 Essais d'atténuation des MENACES

Le FABRICANT doit établir une ACTIVITE (ou des ACTIVITES) destinées à vérifier par essai l'efficacité de l'atténuation des MENACES identifiées et validées dans le MODELE DE MENACE. Ces ACTIVITÉS doivent inclure:

a) la création et l'exécution d'essais appropriés pour chaque mesure d'atténuation mise en œuvre pour traiter une MENACE spécifique, afin de vérifier que cette mesure fonctionne telle qu'elle a été conçue;

b) la création et l'exécution de plans qui visent à contrecarrer chaque mesure d'atténuation; et

c) la vérification pour assurer que la mesure d'atténuation n'introduit pas d'autres VULNERABILITES dans la conception.

5.7.3 Essais de VULNÉRABILITÉS

Le FABRICANT doit établir une ACTIVITE (ou des ACTIVITES) destinées à réaliser des essais qui ciblent l'identification et la caractérisation des VULNERABILITES potentielles de SURETE des LOGICIELS DE SANTE. Les essais de VULNERABILITES connues doivent être fondés, au moins, sur le contenu récent d'une source publique établie reconnue par le secteur industriel, qui traite des VULNERABILITES connues. Le cas échéant, les essais doivent inclure:

a) les cas d'abus pour les essais d'entrée malformés ou non prévus qui ne ciblent pas le traitement des problèmes de SURETE. Ces essais doivent inclure les essais de cas d'abus manuels ou automatisés, ainsi que les types spécialisés d'essais de cas d'abus sur toutes les interfaces et tous les protocoles externes. Les exemples d'essais de cas d'abus incluent les essais de distorsion, ainsi que les essais de charge de trafic sur le réseau et les essais de capacité;

b) les essais de SURFACE D'ATTAQUE destinés à déterminer toutes les issues vers l'intérieur et vers l'extérieur du système, les VULNERABILITES courantes y compris entre autres les listes de contrôle d'accès (LCA) faible, les accès exposés et les services dont le fonctionnement utilise des privilèges élevés;

c) l'analyse en "boîte fermée" des VULNERABILITES connues, qui cible la détection de ces VULNERABILITES (le cas échéant) dans le matériel, l'hôte, les interfaces ou les ELEMENTS LOGICIELS;

NOTE 1 Il peut s'agir, par exemple, d'une analyse des VULNERABILITES connues qui est fondée sur le réseau.

d) une ANALYSE DE COMPOSITION LOGICIELLE de tous les fichiers exécutables binaires y compris les micrologiciels intégrés, à utiliser avec les LOGICIELS DE SANTE et proposés par un fournisseur tiers. Cette analyse peut être utilisée pour détecter:

1) les VULNERABILITES connues dans les ELEMENTS LOGICIELS;
2) la mise en relation avec les bibliothèques de vulnérabilités;
3) les violations des règles de SURETE;
4) les configurations de compilateur qui peuvent entraîner des VULNERABILITES; et
5) la comparaison entre le logiciel concerné et la nomenclature des logiciels.

NOTE 2 Les outils peuvent prendre en charge l'ANALYSE DE COMPOSITION LOGICIELLE par la création d'une liste des progiciels inclus.

e) les essais dynamiques de SURETE (par exemple, les essais de distorsion) qui détectent les failles non visibles dans le cadre de l'analyse de code statique, y compris entre autres les conditions de refus de service dues à la non-diffusion de pseudonymes d'exécution, aux fuites de mémoires et aux accès autorisés à une mémoire partagée sans authentification. Ces essais doivent être appliqués lorsque de tels outils sont disponibles.

NOTE 3 Les essais exhaustifs d'exécution ne peuvent être réalisés de manière efficace sans l'aide d'outils.

5.7.4 Essais de pénétration

Le FABRICANT doit établir une ACTIVITE (ou des ACTIVITES) destinées à identifier et caractériser les POINTS FAIBLES par l'intermédiaire d'essais qui ciblent la détermination et l'exploitation des VULNERABILITES de SURETE des LOGICIELS DE SANTE.

Voir B.5.7.4.

5.7.5 Gestion des conflits d'intérêts entre les contrôleurs et les développeurs

Le fabricant doit documenter les moyens permettant de garantir l'objectivité de l'effort d'essai pour les essais suivants:

a) l'analyse de la SURFACE D'ATTAQUE;
b) la vérification par essai des exigences de SURETE;
c) les essais d'atténuation des MENACES;
d) les essais de VULNÉRABILITÉS;
e) l'analyse des VULNÉRABILITÉS connues; et
f) les essais de pénétration.

NOTE L'objectivité vise à soutenir la reproductibilité des résultats fondés sur des faits.

Voir l'Article A.1 et le paragraphe B.5.7.5.

5.8 Diffusion des logiciels

5.8.1 Résolution des constatations préalablement à la diffusion

Le FABRICANT doit établir une ACTIVITE (ou des ACTIVITES) destinées à vérifier que toutes les constatations issues des essais ont été traitées par le PROCESSUS de résolution des problèmes (Article 9).

5.8.2 Documentation de diffusion

Le FABRICANT doit établir des exigences relatives à la DOCUMENTATION D'ACCOMPAGNEMENT comme partie intégrante de l'ACTIVITE (ou des ACTIVITES) de diffusion des logiciels:

a) lignes directrices pour un fonctionnement sécurisé;

b) caractère rigoureux des PROCESSUS et documentation de conformité y compris le cadrage (Article 4), la personnalisation (Article 5) et les informations sur le champ d'application de la documentation (Annexe E);

NOTE Ces documents permettent de satisfaire aux obligations réglementaires ou contractuelles.

c) lignes directrices applicables à la gestion des comptes (le cas échéant); et

d) informations appropriées concernant les RISQUES RESIDUELS pertinents pour la SURETE auxquels sont soumis les LOGICIELS DE SANTE.

Voir l'Annexe E pour une spécification informative du contenu de la documentation.

5.8.3 Intégrité des FICHIERS

Le FABRICANT doit établir une ACTIVITE (ou des ACTIVITES) destinées à fournir un mécanisme de VERIFICATION d'INTEGRITE pour tous les scripts, fichiers exécutables et autres fichiers de SURETE utilisés avec un LOGICIEL DE SANTE.

Cette ACTIVITE (ou ces ACTIVITES) sont exigées pour assurer que les utilisateurs du PRODUIT peuvent vérifier que les fichiers exécutables, les scripts et les autres fichiers importants transmis par le FABRICANT n'ont pas été altérés. Les méthodes habituelles qui permettent de satisfaire à cette exigence incluent les empreintes numériques et les signatures numériques (qui prouvent également l'origine).

5.8.4 Contrôles dédiés aux clés privées

Le FABRICANT doit prévoir des contrôles procéduraux et techniques qui permettent de protéger les clés privées utilisées pour la signature de code contre les accès ou modifications non autorisé(e)s.

NOTE Ce processus fait référence à la chaîne d'approvisionnement logicielle et cible la signature de code afin de prendre en charge la distribution et la fourniture sécurisées des LOGICIELS DE SANTE.

5.8.5 Évaluation et traitement des problèmes liés à la SURETE

Le FABRICANT doit établir une ACTIVITE (ou des ACTIVITES) destinées à vérifier la non-diffusion d'un LOGICIEL DE SANTE ou l'absence de mise à jour tant que les problèmes liés à sa SURETE n'ont pas été traités et n'ont pas fait l'objet d'un suivi (voir 9.5). Ce processus inclut les problèmes associés:

a) aux exigences (voir 5.2);

b) à la SURETE par conception (voir 5.3 et 5.4);

c) à la mise en œuvre (voir 5.5);

d) à la VERIFICATION/VALIDATION (voir 5.5, 5.6 et 5.7); et

e) à la gestion des défauts de SURETE (voir 9.4).

5.8.6 Réalisation des ACTIVITÉS

Le FABRICANT doit établir une ACTIVITE (ou des ACTIVITES) destinées à vérifier que, préalablement à la diffusion des LOGICIELS DE SANTE, tous les PROCESSUS relatifs à la SURETE applicables exigés par le présent document ont été réalisés avec des enregistrements qui documentent la réalisation de l'ACTIVITE (ou des ACTIVITES) ou l'exécution du PROCESSUS.

5.8.7 Lignes directrices applicables à la mise hors service sécurisée des LOGICIELS DE SANTE

Le FABRICANT doit établir une ACTIVITE (ou des ACTIVITES) destinées à générer une documentation pour les utilisateurs de PRODUITS qui comprend les lignes directrices applicables à la mise hors service des LOGICIELS DE SANTE.

6 PROCESSUS DE MAINTENANCE DU LOGICIEL

6.1 Établissement d'un plan de MAINTENANCE DU LOGICIEL

6.1.1 Mises à jour de SURETE ponctuelles

Le FABRICANT doit établir – comme partie intégrante des ACTIVITES de mise à jour – une politique qui définit les délais de qualification et de fourniture des mises à jour de SURETE aux utilisateurs de PRODUITS. Cette politique doit au moins prendre en considération les facteurs suivants:

a) l'impact potentiel (aspect technique, SECURITE, efficacité, SURETE) de la VULNERABILITE;

b) la notoriété publique de la VULNERABILITE;

c) la détermination d'EXPLOITS publiés éventuels relatifs à la VULNERABILITE;

d) le volume des PRODUITS déployés atteints; et

e) la DISPONIBILITE d'un contrôle externe efficace en l'absence de mise à jour des LOGICIELS DE SANTE.

NOTE 1 Certains organes de réglementation peuvent avoir des exigences de délais spécifiques.

NOTE 2 Le FABRICANT peut catégoriser les mises à jour de SURETE (par exemple, par impact potentiel) et définir des délais appropriés. Voir l'IEC TR 60601-4-5.

NOTE 3 Au cours d'un intervalle de temps acceptable dans lequel le FABRICANT développe un contrôle technique, les mesures d'atténuation et contraintes documentées éventuelles relatives à l'EMPLOI PREVU peuvent être fondées sur la GESTION DES RISQUES. Il est recommandé de développer et déployer une mesure d'atténuation technique dans les LOGICIELS DE SANTE.

NOTE 4 L'IEC TR 60601-4-5 définit des performances minimales (terme "Fonction essentielle" tel qu'il est utilisé dans la série IEC 62443) à associer aux dispositifs médicaux dans le cas d'ATTAQUES de CYBERSECURITE correspondantes sur le réseau TI d'un ORGANISME DE PRESTATION DE SOINS DE SANTE (HDO). Ces performances minimales assurent une fonctionnalité de base jusqu'à la disponibilité d'une mise à jour de SURETE vérifiée dans les situations dans lesquelles tous les dispositifs médicaux du même type dans le HDO peuvent être affectés simultanément par une ATTAQUE de CYBERSECURITE donnée. Par conséquent, les ACTIVITES du CYCLE DE VIE d'un logiciel, dans le cas des dispositifs médicaux, vérifient que:

a) les "fonctions essentielles" restent sécurisées pendant l'intervalle donné jusqu'à l'installation d'une mise à jour de SURETE, et

b) les mises à jour de SURETE rétablissent toujours la CAPACITE DE SURETE comme cela est spécifié dans la DOCUMENTATION D'ACCOMPAGNEMENT.

Des recommandations supplémentaires sont fournies par l'IEC TR 60601-4-5.

6.2 Analyse des problèmes et des modifications

6.2.1 Contrôle des rapports publics d'incidents

Le FABRICANT doit établir une ACTIVITE (ou des ACTIVITES) destinées à recueillir et à revoir de manière active les sources pertinentes d'information concernant les VULNERABILITES des LOGICIELS PRIS EN CHARGE.

NOTE Ce processus inclut les LOGICIELS DE SANTE.

6.2.2 VERIFICATION des mises à jour de SURETE

Le FABRICANT doit établir une ACTIVITE (ou des ACTIVITES) destinées à vérifier que les mises à jour de SURETE qu'il a créées traitent des VULNERABILITES de SURETE prévues.

Le FABRICANT doit établir une ACTIVITE (ou des ACTIVITES) destinées à vérifier que les mises à jour de SURETE n'influent pas de manière inattendue sur les attributs fonctionnels ou de qualité des LOGICIELS DE SANTE. Ces mises à jour de SURETE incluent entre autres les mises à jour créées par:

a) le FABRICANT du LOGICIEL DE SANTE,

b) les fournisseurs des ELEMENTS LOGICIELS utilisés dans le LOGICIEL DE SANTE, et

c) les fournisseurs des ELEMENTS LOGICIELS ou des plateformes dont dépend le LOGICIEL DE SANTE.

Le FABRICANT peut définir une responsabilité partagée pour ce type de VERIFICATION dans le cas de certains ELEMENTS LOGICIELS ou de certaines plateformes.

NOTE Voir aussi l'Article 9.

6.3 Mise en œuvre des modifications

6.3.1 Documentation des mises à jour de SURETE des LOGICIELS PRIS EN CHARGE

Le FABRICANT doit établir une politique destinée à informer les utilisateurs de PRODUITS de la disponibilité de mises à jour des LOGICIELS PRIS EN CHARGE. Ces informations doivent inclure:

a) l'indication de la compatibilité du LOGICIEL DE SANTE avec la mise à jour de SURETE du logiciel pris en charge; et
b) les mesures d'atténuation qui peuvent se substituer à la mise à jour dans le cas des mises à jour de SURETE non agréées par le FABRICANT du LOGICIEL DE SANTE.

6.3.2 Mise à disposition des mises à jour de SURETE des LOGICIELS MAINTENUS

Le FABRICANT doit établir une ACTIVITE (ou des ACTIVITES) destinées à vérifier que les mises à jour de SURETE des LOGICIELS MAINTENUS sont à disposition des utilisateurs de PRODUITS.

Voir E.2.5.

6.3.3 INTEGRITE des mises à jour de SURETE des LOGICIELS MAINTENUS

Le FABRICANT doit établir une ACTIVITE (ou des ACTIVITES) destinées à vérifier que chaque mise à jour applicable des LOGICIELS MAINTENUS est à disposition des utilisateurs de PRODUITS selon un mode qui facilite la VERIFICATION de l'INTEGRITE de la mise à jour de SURETE.

Cette ACTIVITE (ou ces ACTIVITES) doivent garantir que les utilisateurs des LOGICIELS DE SANTE peuvent obtenir des correctifs de SURETE applicables aux LOGICIELS MAINTENUS, et afin de réduire toute possibilité de correctifs frauduleux. La mise en place de cette ACTIVITE (ou ces ACTIVITES) signifie que le FABRICANT prévoit un mécanisme ou une technique qui permet aux utilisateurs de LOGICIELS DE SANTE de vérifier l'authenticité des correctifs. Une diffusion concurrente des correctifs pour tous les LOGICIELS MAINTENUS peut réduire la fenêtre de temps entre la prise de conscience de la VULNERABILITE et la DISPONIBILITE des correctifs.

7 PROCESSUS DE GESTION DES RISQUES DE SURETE

7.1 Contexte de GESTION DES RISQUES

7.1.1 Généralités

Le FABRICANT doit établir et maintenir un PROCESSUS DE GESTION DES RISQUES DE SURETE liés aux LOGICIELS DE SANTE comme partie intégrante de son approche de GESTION DES RISQUES DE PRODUITS. Il convient que ce PROCESSUS comprenne les étapes suivantes décrites en 7.1.2, 7.2, 7.3, 7.4 et 7.5.

Voir l'Annexe C.

7.1.2 CONTEXTE DE SÛRETÉ DES PRODUITS

Le FABRICANT doit établir une ACTIVITE (ou des ACTIVITES) destinées à vérifier la documentation effective du CONTEXTE DE SURETE prévu des PRODUITS. Cette ACTIVITE (ou ces ACTIVITES) doivent assurer la documentation des exigences minimales de l'environnement et des hypothèses

relatives à cet environnement afin d'atteindre le niveau de SURETE de conception pour lequel le PRODUIT a été conçu.

La définition de ces informations a pour objet de permettre tant aux développeurs du LOGICIEL DE SANTE qu'aux utilisateurs du PRODUIT de comprendre dans une même mesure la manière dont le PRODUIT est destiné à être utilisé. Ce processus permet aux développeurs de prendre des décisions appropriées en matière de conception, tout comme il permet aux utilisateurs d'employer le PRODUIT comme cela est prévu.

Le CONTEXTE DE SURETE peut inclure:

a) l'emplacement dans le réseau;

b) la SURETE physique ou la CYBERSECURITE assurée par l'environnement dans lequel le PRODUIT est amené à être déployé;

c) l'isolation (du point de vue d'un réseau);

d) lorsqu'il est connu, l'impact potentiel sur la SECURITE dû à la dégradation de la SURETE;

e) les contrôles de la SURETE mis en œuvre dans le matériel dédié avec lequel le LOGICIEL DE SANTE est destiné à être utilisé.

Par exemple, il est important de documenter l'exigence éventuelle d'une SURETE physique. Si aucune SURETE physique n'est prévue, le PRODUIT peut faire l'objet d'un certain nombre d'exigences connexes telles que l'interdiction d'une configuration à bouton-poussoir. Autre exemple: lorsque le PRODUIT (sans diminuer sa SECURITE et ses performances) ne peut vraisemblablement mettre en œuvre son propre pare-feu, il peut être protégé par un pare-feu fourni par l'utilisateur qui assure sa connexion au réseau TI de santé.

La documentation de ces caractéristiques de SURETE externes du PRODUIT (son CONTEXTE DE SURETE) permet aux développeurs de concevoir une stratégie de DEFENSE EN PROFONDEUR qui complète ce CONTEXTE DE SURETE, et permet aux contrôleurs de valider et de vérifier la SURETE d'un PRODUIT dans un environnement similaire à celui dans lequel il est amené à être déployé.

La mise en place de ce PROCESSUS signifie que l'environnement de déploiement dans lequel le PRODUIT est destiné à être utilisé est correctement représenté dans tous les PROCESSUS impliqués dans le développement et les essais de ce PRODUIT. Cette mise en place signifie également la documentation de cet environnement.

7.2 Identification des VULNERABILITES, MENACES et effets défavorables associés

Le FABRICANT doit établir une ACTIVITE (ou des ACTIVITES) qui identifient et documentent les vulnérabilités, MENACES et effets défavorables associés éventuels qui affectent la CONFIDENTIALITE, l'INTEGRITE et la DISPONIBILITE des ACTIFS des LOGICIELS DE SANTE. Cette ACTIVITE (ou ces ACTIVITES) doivent prendre en considération l'EMPLOI PREVU et l'ENVIRONNEMENT D'UTILISATION PREVU par rapport au CONTEXTE DE SURETE.

Cette ACTIVITE (ou ces ACTIVITES) doivent permettre de vérifier que tous les PRODUITS doivent avoir un MODELE DE MENACE spécifique au domaine de développement actuel du PRODUIT avec les caractéristiques suivantes (le cas échéant):

a) flux correct des informations catégorisées dans l'ensemble du système;

b) LIMITES DE CONFIANCE;

c) PROCESSUS;

d) dépôts de données;

e) entités externes interactives;

f) protocoles de communication interne et externe mis en œuvre dans le PRODUIT;

g) ports physiques à accès externe y compris ports de débogage;

h) connexions de cartes de circuits telles que les connexions du Joint Test Action Group (JTAG) ou les socles de débogage qui peuvent être utilisés pour les ATTAQUES du matériel;

i) vecteurs potentiels d'ATTAQUE y compris l'ATTAQUE du matériel (prévu);

j) MENACES potentielles;

k) problèmes liés à la SURETE identifiés; et

l) éléments dépendants externes sous la forme de pilotes ou d'applications tierces (code non développé par le fournisseur) associés à l'application.

Le MODELE DE MENACE doit être revu et vérifié par l'équipe de développement afin d'établir son caractère.

Le MODELE DE MENACE doit faire l'objet d'une revue périodique (au moins annuelle) pour les PRODUITS diffusés, et d'une mise à jour lorsque cela est exigé en réponse à l'émergence de nouvelles MENACES pour le PRODUIT même en cas de non-modification de la conception.

Tous les problèmes identifiés dans le MODELE DE MENACE doivent être traités comme cela est défini en 9.4 et 9.5.

7.3 Estimation et évaluation du risque de SURETE

Le FABRICANT doit établir une ACTIVITE (ou des ACTIVITES) destinées à:

a) estimer le risque des VULNERABILITES identifiées ci-dessus. L'estimation du risque est réalisée compte tenu de l'effet défavorable de la VULNERABILITE sur la CYBERSECURITE. Cette estimation peut être soutenue par une notation des VULNERABILITES, comme le Système commun de notation des VULNERABILITES (CVSS - *common vulnerability scoring system*) ou la Rubrique de notation MITRE[30] pour les dispositifs médicaux. Le système de notation peut également être fondé sur un programme de probabilité/gravité utilisé par le FABRICANT pour les autres risques (voir par exemple le Guide ISO/IEC 51 ou l'ISO 14971);

b) évaluer les risques estimés et – sur la base d'une notation – déterminer si le risque est acceptable ou non; et

c) informer le PROCESSUS de GESTION DES RISQUES DE PRODUITS concernant les mises à jour du MODELE de MENACE.

7.4 MAÎTRISE DES RISQUES de SÛRETÉ

Le FABRICANT doit déterminer si les mesures de MAITRISE DES RISQUES de SURETE sont appropriées pour réduire les risques de SURETE à un niveau acceptable fondé sur les politiques d'acceptation des risques de SURETE. Lorsque les mesures de MAITRISE DES RISQUES sont considérées comme appropriées, le FABRICANT doit:

- choisir les mesures d'atténuation appropriées;
- déterminer si ces mesures entraînent de nouveaux risques ou accroissent d'autres risques;
- mettre en œuvre les mesures d'atténuation choisies; et
- vérifier par essai l'efficacité des mesures mises en œuvre.

Le FABRICANT doit documenter les résultats de ces ACTIVITES.

Le traitement des RISQUES RESIDUELS pour la SURETE doit être effectué en collaboration avec la GESTION DES RISQUES DE PRODUITS.

NOTE L'appréciation des risques de SURETE est influencée par le CONTEXTE DE SURETE. L'acceptabilité des risques de SURETE est fondée sur la notation respective et le seuil d'acceptabilité applicable à ces RISQUES. Voir aussi 4.2.

7.5 Contrôle de l'efficacité des mesures de MAITRISE DES RISQUES

Le FABRICANT doit contrôler l'efficacité des mesures de MAITRISE DES RISQUES par la collecte et la revue d'informations pendant la phase post-diffusion des produits.

Cette ACTIVITE (ou ces ACTIVITES) doivent également informer les autres ACTIVITES et PROCESSUS de l'existence du problème concerné ou du ou des problèmes associés y compris les PROCESSUS applicables à d'autres PRODUITS/révisions. Cette ACTIVITE (ou ces ACTIVITES) doivent également informer les parties tierces (par exemple, fournisseurs) de la constatation de problèmes au niveau du code source tiers à utiliser avec le LOGICIEL DE SANTE.

Les problèmes éventuels identifiés dans le MODELE DE MENACE du LOGICIEL DE SANTE diffusé sont traités comme cela est défini en 9.4 et 9.5.

8 PROCESSUS de GESTION DE LA CONFIGURATION logicielle

Le FABRICANT doit établir un PROCESSUS général de développement/maintenance/service après-vente du PRODUIT qui inclut la GESTION DE LA CONFIGURATION avec maîtrise et historique des modifications.

Au titre des obligations de SURETE dans le cas des LOGICIELS DE SANTE déjà diffusés ou mis sur le marché, la GESTION DE LA CONFIGURATION doit prévoir la capacité de reproduire une liste des composants externes inclus qui sont ou peuvent devenir sensibles aux VULNERABILITES.

9 PROCESSUS de résolution des problèmes logiciels

9.1 Présentation

Les ACTIVITES définies par le présent article sont destinées à traiter les problèmes liés à la SURETE des LOGICIELS DE SANTE.

9.2 Réception des notifications concernant les VULNERABILITES

Le FABRICANT doit établir une ACTIVITE (ou des ACTIVITES) qui permettent de lui signaler les informations relatives aux VULNERABILITES, que ces informations proviennent d'une entité interne, d'une entité externe ou d'un système de traitement des réclamations.

Cette ACTIVITE (ou ces ACTIVITES) de réception doivent collecter et établir le suivi des rapports relatifs aux problèmes liés à la SURETE propres aux LOGICIELS DE SANTE, lesdits rapports provenant des sources suivantes, y compris au moins:

a) les contrôleurs de VERIFICATION et de VALIDATION de la SURETE;

b) les fournisseurs des composants tiers utilisés dans le PRODUIT;

c) les développeurs et contrôleurs de PRODUITS;

d) les utilisateurs de PRODUITS y compris les intégrateurs, les opérateurs, les administrateurs et le personnel de maintenance;

e) les données fournies par les informations des journaux d'événements d'audit;

f) les chercheurs du domaine de la SURETE (déclarants de VULNERABILITES de SURETE), voir aussi l'ISO/IEC 29147; et

g) les données ou notifications portant sur les VULNERABILITES réparties qui peuvent affecter les LOGICIELS DE SANTE – Voir 6.2.

NOTE Généralement, ces informations proviennent de publications, de rapports, de recherches indépendantes dans le domaine de la SURETE; d'enquêtes internes, de CERT et d'organismes de partage et d'analyse de l'information (ISAO - *information sharing and analysis organizations*).

9.3 Revue des VULNÉRABILITÉS

Le FABRICANT doit établir une ACTIVITE (ou des ACTIVITES) qui permettent l'analyse des VULNERABILITES dans un délai convenable afin de déterminer leur:

a) applicabilité au PRODUIT;

b) vérifiabilité; et

c) MENACES associées.

NOTE 1 Le respect des délais est géré par les autorités, la législation applicable, la politique de réglementation et les forces du marché.

NOTE 2 Ce PROCESSUS peut être mis en œuvre par exemple comme partie intégrante des PROCESSUS conformes aux 8.2.1, 8.2.2 et 8.2.3 de l'ISO 13485:2016.

9.4 Analyse des VULNÉRABILITÉS

Le FABRICANT doit établir une ACTIVITE (ou des ACTIVITES) destinées à analyser les VULNERABILITES du PRODUIT qui comprennent:

a) l'évaluation de leur effet par rapport:
   1) au CONTEXTE DE SURETE technique dans lequel elles ont été découvertes (voir l'Article 6 de l'IEC 62443-4-1:2018[11]);
   2) à l'ENVIRONNEMENT D'UTILISATION PREVU, du PRODUIT, et
   3) à la stratégie de DEFENSE EN PROFONDEUR DU PRODUIT;
b) l'influence telle qu'elle est définie par un système de notation des VULNERABILITES (par exemple CVSS);
c) l'identification de tous les autres PRODUITS/toutes les autres versions de PRODUITS qui comportent tous les problèmes liés à la SURETE (le cas échéant);
d) l'identification de la cause initiale du problème;
e) l'identification des problèmes de SURETE associés (c'est-à-dire au sein du même PRODUIT); et
f) l'influence sur la SECURITE et l'efficacité du produit.

NOTE 1 Une approche méthodique de l'analyse de cause initiale, comme celle décrite dans l'IEC 62740, peut être appliquée.

NOTE 2 Une cause initiale constitue le premier événement d'une séquence de facteurs de causalité qui s'écarte de la séquence prévue.

NOTE 3 Les causes initiales ne peuvent pas être toutes déterminées par des mesures techniques des LOGICIELS DE SANTE.

NOTE 4 Ce PROCESSUS peut être mis en œuvre par exemple comme partie intégrante des 8.5.2 et 8.5.3 de l'ISO 13485:2016.

9.5 Traitement des problèmes liés à la SURETE

Le FABRICANT doit établir une ACTIVITE (ou des ACTIVITES) destinées à traiter les problèmes liés à la SURETE et à déterminer s'il y a lieu de les divulguer (en 4.1.7) sur la base des résultats de l'évaluation des effets et du niveau acceptable de RISQUE RESIDUEL.

Le FABRICANT doit établir une ACTIVITE (ou des ACTIVITES) destinées à déterminer si, et de quelle façon, les risques de SURETE sont traités par l'intermédiaire du PROCESSUS de résolution des problèmes ou par le biais de spécifications actualisées concernant l'ENVIRONNEMENT D'UTILISATION PREVU.

Le FABRICANT doit établir une ACTIVITE (ou des ACTIVITES) destinées à examiner les modifications éventuelles de conception ou de mise en œuvre par rapport à leur effet sur la SECURITE, la SURETE et l'efficacité.

Le FABRICANT doit faire état du problème concerné ou d'un ou de plusieurs problèmes associés dans d'autres PROCESSUS, y compris les PROCESSUS applicables à d'autres PRODUITS/révisions de PRODUITS. Cette démarche peut être effectuée par l'intégration de rapports de signalement de problèmes ou de documents analogues dans d'autres PROCESSUS.

Le FABRICANT doit informer les parties tierces de la détection de problèmes dans leur code source à utiliser avec les LOGICIELS DE SANTE PRIS EN CHARGE. Dans le cas de logiciels libres, la plateforme de publication peut servir à informer de l'existence du problème constaté ou de sa résolution.

Cette ACTIVITE doit inclure une revue périodique des problèmes en suspens liés à la SURETE afin d'assurer le traitement approprié des problèmes. Cette revue périodique doit avoir lieu au moins lors de chaque diffusion de PRODUIT; voir 4.1.6 et 4.1.8.

NOTE 1 Cette revue périodique peut être mise en œuvre par exemple comme partie intégrante de l'ISO 13485:2016, 8.2.6.

NOTE 2 À titre d'exemple, une fonction prévue qui inclut la transmission d'informations personnelles identifiables par un réseau externe peut susciter la nécessité du chiffrement des données.

NOTE 3

- L'atténuation de certaines MENACES par des mesures techniques internes aux LOGICIELS DE SANTE peut ne pas être réalisable, parce que ces menaces peuvent être liées à l'EMPLOI PREVU ou aux fonctions essentielles.
  - Exemple: L'accès console aux dispositifs de soins d'urgence/de courte durée est empêché par des procédures d'authentification excessivement complexes et peut retarder la prestation des soins urgents.
  - Exemple: Des algorithmes de cryptographie puissants dédiés au chiffrement des données et utilisés pour la transmission en champ proche recourent en principe à une puissance de calcul considérable et peuvent appeler le courant de batterie lorsqu'ils sont mis en œuvre dans des dispositifs mobiles plus petits.
- Certaines MENACES peuvent être mieux traitées par des mesures d'atténuation dans l'ENVIRONNEMENT D'UTILISATION PREVU, qui sont exprimées par la DOCUMENTATION D'ACCOMPAGNEMENT (voir l'Annexe E).
- Certaines VULNERABILITES ne peuvent pas être exploitées en raison des mesures intrinsèques à la conception des LOGICIELS DE SANTE.

NOTE 4 Du fait de la complexité de détermination de la probabilité liée aux MENACES, le concept de probabilité est mieux adapté et utilisé couramment pour la SURETE TI. La probabilité d'occurrence de MENACES identifiées est exprimée généralement au moyen de systèmes de notation structurés comme les Systèmes communs de notation des VULNERABILITES (CVSS), qui peuvent également tenir compte du gain du pirate par rapport à l'effort applicable.

NOTE 5 La GESTION DES RISQUES pour la SECURITE des dispositifs médicaux – comme dans l'ISO 14971 – peut être prise en charge par une méthode de MODELISATION DES MENACES afin de couvrir les MENACES POUR LA SURETE.

NOTE 6 L'IEC TR 63069 explique la relation entre les PROCESSUS de SECURITE/SURETE.

Annexe A
(informative)

Justification

A.1 Relation avec l'IEC 62443

L'IEC 62443 constitue une série de spécifications de SECURITE pour les systèmes d'automatisation et de commande industrielles. Cette série, qui succède aux normes ISA-99, constitue un ensemble reconnu de normes de SURETE pour la technologie opérationnelle. Les parties de la série IEC 62443 sont reconnues par la FDA. Par ailleurs, le document "MDCG 2019-16 Guidance on Cybersecurity for medical devices" (MDCG 2019-16 Recommandations concernant la cybersécurité des dispositifs médicaux) de l'UE et les recommandations CS 132 du BSI allemand font référence aux spécifications de l'IEC 62443.

Les systèmes d'automatisation et de commande industrielles (IACS - *industrial automation and controls systems*) reconnaissent la SURETE, ainsi que la SECURITE et l'efficacité. Il s'agit de propriétés clés qui peuvent également être appliquées dans le domaine des LOGICIELS DE SANTE.

Le terme "risque" est utilisé pour décrire le potentiel de dommages par rapport à certains objectifs de protection. Par exemple, pour les dispositifs médicaux, ces objectifs sont le fonctionnement sûr et performant des dispositifs. Dans les normes relatives aux dispositifs médicaux, le risque est défini, selon 3.9 du Guide ISO/IEC 51:2014 ou 3.10 du Guide ISO/IEC 63, comme la "combinaison de la probabilité de la survenue d'un dommage et de sa gravité" (le dommage étant défini comme une atteinte à des ACTIFS *externes* tels que la santé, l'environnement ou les biens), tandis que les normes de la série IEC 62443 utilisent le terme "risque" pour décrire le potentiel de réduction de la CONFIDENTIALITE, de l'INTEGRITE et de la DISPONIBILITE d'ACTIFS plutôt internes au système. Cependant, la perspective de l'IEC 62443 inclut les risques qui ont le potentiel de causer des dommages *externes* au sens du Guide ISO/IEC 51 ou du Guide ISO/IEC 63. Puisque le présent document utilise principalement le concept plus large de risque (de SURETE), ce terme n'a pas fait l'objet de définition afin d'éviter toute confusion avec une utilisation plus spécifique du terme.

Il est difficile de définir un ensemble spécifique de contrôles de SURETE du fait du large spectre de techniques et d'applications propres aux LOGICIELS DE SANTE. La pratique dans le secteur industriel a démontré que des mesures de SURETE intrinsèques aux PROCESSUS DU CYCLE DE VIE permettaient d'obtenir des PRODUITS sécurisés. Le présent document traite par conséquent des PROCESSUS DU CYCLE DE VIE dont le FABRICANT a la charge et prend en considération les exigences de l'IEC 62443-4-1[11], qui par ailleurs sont les suivantes:

- elles sont appropriées aux LOGICIELS DE SANTE;
- elles spécifient des exigences liées aux PROCESSUS;
- elles concernent le FABRICANT;
- elles ne spécifient pas de capacités de PRODUITS;
- elles ne définissent pas de contenu pour la DOCUMENTATION D'ACCOMPAGNEMENT – ledit contenu sera défini par l'IEC TR 60601-4-5.

La satisfaction aux exigences du présent document favorise la démarche de conformité à l'IEC62443-4-1[11]. Le présent document contient toutefois certaines adaptations au secteur des soins de santé, ainsi que certaines clarifications à son intention.

Les FABRICANTS qui s'efforcent de se conformer totalement à l'IEC 62443-4-1[11] prennent en considération les dispositions supplémentaires suivantes concernant l'indépendance par rapport aux développeurs "qui ont conçu et mis en œuvre le PRODUIT" selon le Tableau A.1.

Tableau A.1 – Niveau d'indépendance exigé des contrôleurs par rapport aux développeurs

Type d'essai	Référence	Niveau d'indépendance
Vérification par essai des exigences de SURETE	SVV-1 Essais des exigences de SECURITE	Service indépendant
Essais d'atténuation des MENACES	SVV-2 Essais d'atténuation des MENACES	Service indépendant
Essais de VULNÉRABILITÉS	SVV-3 Essais de VULNÉRABILITÉS	Personne indépendante
Analyse de code statique	SI-1 Revue de mise en œuvre de la SURETE	Aucun
Analyse de la SURFACE D'ATTAQUE	SVV-3 Essais de VULNÉRABILITÉS	Personne indépendante
Analyse des VULNÉRABILITÉS connues	SVV-3 Essais de VULNÉRABILITÉS	Personne indépendante
ANALYSE DE COMPOSITION LOGICIELLE	SVV-3 Essais de VULNÉRABILITÉS	Aucun
Essais de pénétration	SVV-4 Essais de pénétration	Service indépendant ou organisme indépendant
SOURCE: IEC 62443-4-1:2018[11], SVV-5, 9.6.1.		

Le FABRICANT peut mettre en place une équipe d'essai interne (semi-)indépendante et/ou faire recours à un organisme d'essai de SURETE tiers. Il convient que les individus indépendants des développeurs qui ont conçu et mis en œuvre les caractéristiques de SURETE réalisent les essais de SURETE. Les niveaux d'indépendance peuvent être les suivants:

- Aucun – aucune indépendance exigée. Le développeur peut réaliser les essais.
- Personne indépendante – la personne qui réalise les essais ne peut pas être l'un des développeurs du PRODUIT.
- Service indépendant – la personne qui réalise les essais ne peut pas rendre compte au même responsable en chef comme le font les développeurs du PRODUIT. En variante, ces personnes peuvent être membres d'un service d'assurance qualité (AQ).
- Organisme indépendant – la personne qui réalise les essais ne peut pas faire partie du même organisme que les développeurs du PRODUIT. Un organisme peut être une entité juridique distincte, une division ou un service d'une entreprise qui rend compte à un cadre différent tel qu'un vice-président ou un cadre de niveau similaire.

Pour l'utilisation du présent document, "Cas d'abus" dans l'IEC 62443-4-1:2018[11], SVV-5, 9.6.1 a été modifié en "VULNERABILITE"

A.2 Relation avec l'IEC 62304

Pour une extension des PROCESSUS DU CYCLE DE VIE existants des LOGICIELS DE SANTE, ces exigences ont été disposées dans une structure qui reflète celle de l'IEC 62304[8].

Il n'est pas exigé d'appliquer l'IEC 62304[8] pour la mise en œuvre des PROCESSUS spécifiés dans le présent document. Toutefois, l'identification dans les PROCESSUS d'un FABRICANT des ACTIVITES spécifiées dans l'IEC 62304[8] facilite la détermination de l'ACTIVITE (ou des ACTIVITES) associées pour la CYBERSECURITE spécifiée dans le présent document.

L'IEC 62304[8] définit les ACTIVITES sur la base de la classification de SECURITE des logiciels. Les ACTIVITES exigées sont indiquées dans la partie normative de l'IEC 62304[8] sous la forme "[Classe A, B, C]", "[Classe B, C]" ou "[Classe C]", avec précision de l'exigence de leur choix selon la classification du logiciel auquel elles s'appliquent. Les exigences spécifiées de l'Article 4 à l'Article 9 du présent document concernent particulièrement la CYBERSECURITE et

ne suivent donc pas le concept des classes de SECURITE. Pour la conformité au présent document, le choix des ACTIVITES est indépendant des classes de SECURITE.

A.3 Transfert de risque

A.3.1 Présentation

L'utilisation sécurisée des LOGICIELS DE SANTE relève de responsabilités partagées. Une partie du risque lié à un fonctionnement sécurisé est transférée lors de la mise à disposition d'un LOGICIEL DE SANTE à un client, tandis qu'une autre partie de ce risque demeure de la responsabilité du FABRICANT.

L'IEC 62443-4-1 ne définit pas clairement les termes ou les concepts de transfert de risque, car elle note simplement que des exigences différentes s'appliquent aux "composants fournis par des prestataires externes", aux "composants dépendants" et aux "composants développés à la demande par des fournisseurs tiers". Par conséquent, le présent document introduit des catégories applicables aux ELEMENTS LOGICIELS qui déclarent différents niveaux de transfert de responsabilité et de risque du FABRICANT au client.

Le FABRICANT identifie les catégories suivantes de transfert de risque qu'exige chaque LOGICIEL DE SANTE pour atteindre sa DESTINATION PREVUE.

A.3.2 LOGICIEL MAINTENU

Par hypothèse, le FABRICANT est responsable du risque lié à la SURETE du LOGICIEL MAINTENU (6.3.2, 6.3.3). Ainsi, le FABRICANT fournit des mises à jour de SURETE pour tous les logiciels qui relèvent de cette catégorie.

Les exemples de LOGICIELS MAINTENUS incluent

- les logiciels provenant d'une partie tierce, développés spécifiquement pour une utilisation avec un LOGICIEL DE SANTE;
- les logiciels prêts à l'emploi intégrés; et
- les LOGICIELS DE SANTE y compris ceux développés préalablement à la publication du présent document.

A.3.3 LOGICIEL PRIS EN CHARGE

Le FABRICANT informe le client des risques connus liés à la SURETE de ce type de logiciel (6.3.1).

Les exemples de LOGICIELS PRIS EN CHARGE incluent

- les logiciels prêts à l'emploi généralement disponibles;
- les logiciels provenant d'une partie tierce, également destinés à d'autres utilisations qu'avec un LOGICIEL DE SANTE; et
- les LOGICIELS MAINTENUS.

A.3.4 LOGICIEL EXIGÉ

Par hypothèse, le FABRICANT est responsable des risques connus liés à la SURETE (5.2.1, 5.2.3) identifiés préalablement à la diffusion du logiciel.

Ce processus signifie que toutes les exigences de SURETE pour chaque ELEMENT LOGICIEL exigé par un LOGICIEL DE SANTE pour atteindre sa DESTINATION PREVUE sont considérées comme partie intégrante de la spécification des exigences de ce LOGICIEL DE SANTE.

Les exemples de LOGICIELS EXIGES incluent

- les logiciels pour lesquels aucune mise à jour ne peut être fournie;
- les logiciels tiers obsolètes; et
- les LOGICIELS PRIS EN CHARGE.

A.4 Meilleures pratiques de codage sécurisé

Il convient que les meilleures pratiques de codage sécurisé des LOGICIELS DE SANTE incluent au moins les éléments suivants:

a) l'évitement de constructions de mise en œuvre potentiellement exploitables – modèles de conception de mise en œuvre identifiés comme présentant des POINTS FAIBLES de SURETE,

b) l'évitement des fonctions et constructions de codage/modèles de conception interdits – fonctions logicielles et modèles de conception qu'il convient de ne pas utiliser en raison de leurs POINTS FAIBLES de SURETE connus.

NOTE 1 Les meilleures pratiques de codage évitent de coder sur la base d'un comportement non spécifié ou non défini de l'environnement de programmation.

NOTE 2 Il existe des listes publiques des fonctions interdites pour les bibliothèques et les langages de programmation courants. Selon les meilleures pratiques de codage sécurisé, le FABRICANT peut décider de ne pas utiliser ces fonctions ou un plus grand nombre de fonctions.

NOTE 3 Les normes de codage, fournisseurs de bibliothèques, outils et autres sources fournissent des informations sur les mauvaises pratiques.

c) l'utilisation et la configuration d'outils automatisés (par exemple, pour les outils d'analyse statique),

d) les meilleures pratiques générales de codage sécurisé,

NOTE 4 Les meilleures pratiques de codage sécurisé peuvent être fondées sur des spécifications publiées, par exemple, ISO/IEC TR 24772, normes de codage MISRA-C ou SEI CERT C et SEI CERT C++.

e) la vérification de validité de tous les éléments d'entrée qui interfèrent avec une LIMITE DE CONFIANCE,

f) le traitement des erreurs.

Il convient que le FABRICANT évalue chaque type d'alerte issu de l'analyse statique afin d'établir s'il justifie une modification de code.

L'application des normes de codage sécurisé peut être fondée sur l'ARCHITECTURE de SURETE, la technique de programmation et le contexte.

Annexe B
(informative)

Recommandations concernant la mise en œuvre des ACTIVITÉS DU CYCLE DE VIE DE SÛRETÉ

B.1 Présentation

La CYBERSECURITE d'un PRODUIT qui comprend un logiciel peut être prise en charge par les CAPACITES DE SURETE de ce logiciel – qui mettent généralement en œuvre la protection contre les incidents, la détection de ces incidents, la réponse à ces mêmes incidents et le rétablissement par suite d'incidents qui peuvent compromettre la CONFIDENTIALITE, l'INTEGRITE ou la DISPONIBILITE des ACTIFS du produit.

B.2 Tâches connexes

Bien que le présent document cible les logiciels, il convient que toutes les ACTIVITES DE PROCESSUS intègrent des considérations de SURETE supplémentaires relatives au dispositif physique sur lequel le logiciel fonctionne. Exemples de considérations de SURETE: réduction des ports d'interface physique, tels que les ports JTAG ou les ports USB inutilisés, similaire à la limitation des accès par les réseaux ouverts au niveau du logiciel. De la même façon, le dispositif prévoit des mesures d'atténuation, comme des verrous physiques qui permettent un contrôle d'accès aux supports internes.

Les rapports techniques IEC TR 60601-4-5 et IEC TR 80001-2-2 fournissent des recommandations pour l'identification et la communication de ce type de CAPACITES DE SURETE. Bien que ces rapports techniques traitent des dispositifs médicaux, leurs concepts et leurs mesures peuvent être facilement transférés aux LOGICIELS DE SANTE.

Un autre aspect est lié au CYCLE DE VIE: les FABRICANTS de LOGICIELS DE SANTE peuvent établir des PROCESSUS qui évitent ou atténuent les VULNERABILITES, voire réduisent leur effet sur la DESTINATION PREVUE des PRODUITS. Certains PROCESSUS – par exemple, l'application technique des exigences et l'ANALYSE DES MENACES/RISQUES (TRA - *threat/risk analysis*) – associent la perspective des aspects du PRODUIT avec l'observation des PROCESSUS. Il est important de comprendre que seule la combinaison des capacités de PRODUITS et des mesures internes aux PROCESSUS DU CYCLE DE VIE peut assurer une CYBERSECURITE efficace.

B.3 ANALYSE DES MENACES/RISQUES

Les incidents de SURETE peuvent affecter la SECURITE ou l'efficacité du produit. La relation spécifique entre les VULNERABILITES et les risques relatifs à la SECURITE ou à l'efficacité dépend de la conception, de la mise en œuvre et de l'objet du PRODUIT respectif. Une analyse des risques de PRODUITS en matière de SECURITE doit par conséquent prendre en considération les effets des VULNERABILITES sur les fonctions clés du PRODUIT. Partie intégrante de cette ACTIVITE (ou ces ACTIVITES), la TRA est effectuée pour le PRODUIT.

La SECURITE est définie comme l'absence de risque inacceptable, le risque constituant la combinaison de la gravité et de la probabilité d'un dommage potentiel. Le dommage est exprimé en tant que blessure physique ou atteinte à la santé des personnes, ou atteinte aux biens ou à l'environnement (voir le Guide ISO/IEC 51). Lorsque l'EMPLOI PREVU est connu, l'effet des incidents de SURETE peut enfin être exprimé en tant que gravité du dommage respectif. Dans ce cas, la GESTION DES RISQUES DE SURETE peut être intégrée dans un processus général de GESTION DES RISQUES comme cela est appliqué par le FABRICANT sur la base du Guide ISO/IEC 51 ou de l'ISO 14971 pour les dispositifs médicaux. Lorsque ce type d'approche intégrée est suivie, il faut prendre en considération le fait que la gestion des risques issus d'activités non autorisées (c'est-à-dire risques liés à la SURETE) exige l'application de méthodes

et de techniques spécifiques différentes de celles applicables pour les risques issus par exemple d'un logiciel non fiable, de défaillances électriques, de rayonnements, d'une contamination biologique ou d'erreurs d'utilisation. Ces méthodes et techniques spécifiques à la SURETE incluent la TRA et d'autres méthodes et techniques comme cela est décrit dans le présent document. La TRA a pour objectif d'identifier et d'évaluer les scénarii d'intrusion et les POINTS FAIBLES résultants. Les scénarii que la TRA prend en considération sont fondés sur le contexte d'utilisation réel, qui ne se limite pas à l'EMPLOI PREVU du PRODUIT. Toutefois, la TRA tient compte de l'ENVIRONNEMENT D'UTILISATION. Ces scénarii d'exploitation d'une VULNERABILITE connue par un pirate peuvent être considérés comme "prévisibles" par rapport à la GESTION DES RISQUES DE PRODUITS et font également partie intégrante du contexte d'utilisation réel.

NOTE 1 L'EMPLOI PREVU peut généralement être déterminé au niveau du PRODUIT.

NOTE 2 L'ISO 14971 indique comment prendre en considération la mauvaise utilisation raisonnablement prévisible.

Dans le cas où l'ENVIRONNEMENT D'UTILISATION ou d'autres mesures de contrôle d'atténuation peuvent ne pas empêcher un certain type d'ATTAQUE, ce scénario devient "prévisible" selon la perspective du FABRICANT. La TRA identifie et évalue de tels scénarii de MENACE – compte tenu:

a) du matériel dédié avec lequel le LOGICIEL DE SANTE est destiné à être utilisé,

b) du contexte opérationnel prévu, et

c) des flux potentiels de données/commande entre des acteurs externes et le LOGICIEL DE SANTE.

B.4 GESTION DES MENACES et DES RISQUES

Un résultat d'application de la GESTION DES MENACES et des RISQUES consiste à évaluer les VULNERABILITES connues qui peuvent affecter les ACTIFS du LOGICIEL DE SANTE (données, fonctions logicielles, services logiciels) par rapport à la CONFIDENTIALITE, l'INTEGRITE ou la DISPONIBILITE, ainsi que par rapport au mode d'association de ces éléments avec la SECURITE, la SURETE et l'efficacité globales du PRODUIT dans son ensemble.

Les possibilités de contrôle du risque de SURETE avec les VULNERABILITES restantes incluent un ou plusieurs des éléments suivants:

a) résolution du problème par un ou plusieurs des facteurs suivants:
   1) stratégie de DEFENSE EN PROFONDEUR ou modification de conception;
   2) ajout d'une ou plusieurs exigences de SURETE et/ou CAPACITES DE SECURITE;
   3) application de mécanismes de compensation; et/ou
   4) désactivation ou suppression de fonctionnalités par rapport à l'utilisation sûre et efficace du LOGICIEL DE SANTE;

b) création d'un plan de réhabilitation afin de résoudre le problème;

c) report du problème en vue d'une résolution future (nouvelle application de cette exigence ultérieurement) et précision de la ou des raisons et du ou des risques associés; et

d) non-résolution du problème lorsque le RISQUE RESIDUEL satisfait aux critères d'acceptation.

Lorsque la décision de résolution consiste à résoudre le problème lié à la SURETE dans le cadre de la mise en œuvre du PRODUIT, la synchronisation de la version de résolution peut entraîner le report d'une mise à jour de SURETE jusqu'à la prochaine version.

B.5 Planification du développement logiciel

B.5.1 Développement

B.5.1.1 PROCESSUS de développement logiciel

Il convient qu'un PROCESSUS de développement approprié des LOGICIELS DE SANTE mette en œuvre un PROCESSUS de développement/maintenance/prise en charge comme cela est exigé dans l'IEC 62304[8] et mette par ailleurs en œuvre les éléments de la liste spécifiés en 5.1.1.

B.5.1.2 SÛRETÉ de l'environnement de développement

Les LOGICIELS DE SANTE doivent être protégés contre les compromis éventuels par l'intermédiaire de l'environnement de développement. Par exemple, l'introduction d'un logiciel malveillant ou le vol d'identifiants tels que les certificats de signature logicielle.

B.5.2 Analyse des exigences relatives aux LOGICIELS DE SANTÉ

B.5.2.1 Exigences de SÛRETÉ relatives aux LOGICIELS DE SANTÉ

Dans certaines circonstances, un système à un niveau supérieur a déjà défini un niveau de SURETE pour ce (sous-)système. Cette situation est décrite de manière générale selon l'IEC 62443-3-2 et par l'IEC TR 60601-4-5 pour les systèmes électromédicaux programmables (SEMP).

B.5.2.2 Revue des exigences de SÛRETÉ

La mise en œuvre des CAPACITES DE SURETE peut avoir une influence sur la SECURITE ou l'efficacité du produit. Cette revue peut déterminer une exigence appropriée relative à la mise en œuvre équilibrée des CAPACITES DE SURETE.

B.5.3 Conception architecturale des logiciels

B.5.3.1 ARCHITECTURE/conception de la DÉFENSE EN PROFONDEUR

La DEFENSE EN PROFONDEUR est une approche de la CYBERSECURITE dans laquelle une série de mécanismes de défense est présentée sous forme de couches afin de protéger les ACTIFS informationnels. En cas de défaillance d'un mécanisme, une autre couche contrecarre une ATTAQUE. Cette approche multicouche avec redondances délibérées accroît la SURETE d'un système dans son ensemble et traite de nombreux vecteurs d'ATTAQUE différents. La DEFENSE EN PROFONDEUR est couramment appelée "approche du château" parce qu'elle reflète les défenses disposées en couches d'un château médiéval.

La DEFENSE EN PROFONDEUR réduit la probabilité de réussite des ATTAQUES, ainsi que leur effet, et permet au système cible de prendre des mesures de compensation.

B.5.3.2 Principes de conception sécurisée

Les principes décrits dans cette exigence s'appliquent à la conception de tout système, qu'il s'agisse des applications, du client ou du serveur, des services en nuage ou des dispositifs de l'Internet des objets (IDO). Les spécificités de leur application varient – un service en nuage peut exiger plusieurs rôles administratifs, chaque rôle avec son propre moindre privilège, alors qu'un dispositif IDO exige de prendre particulièrement en considération la nécessité de mises à jour de SURETE, ainsi que la nécessité d'une SURETE et d'une SECURITE intrinsèques.

Toutefois, les principes sont généraux et fournissent des recommandations de SURETE précieuses à l'intention des concepteurs et des architectes de toutes les classes de systèmes. Les éléments de ce type de PROCESSUS nécessitent des spécifications supplémentaires qui dépendent de l'environnement de programmation et des technologies de l'information utilisées. Il existe des spécifications produites par des organismes d'élaboration de normes (OEN) ou

des associations qui comportent des spécifications plus détaillées (dépendance potentielle à l'égard de la technologie ou du contexte).

B.5.3.3 Revue de conception architecturale de SÛRETÉ

La capacité d'une ARCHITECTURE à assurer un comportement stable et prévisible est importante, parce que des conditions défavorables peuvent survenir de manière délibérée ou non (par l'intermédiaire d'appels/données défavorables lors de l'emploi du LOGICIEL DE SANTE dans son ENVIRONNEMENT D'UTILISATION).

B.5.4 Mise en œuvre et VÉRIFICATION des unités logicielles

Il convient que les normes de codage sécurisé intègrent les principes suivants:

- établir des normes et des conventions de codage;
- utiliser uniquement des fonctions sûres (c'est-à-dire des fonctions fiables);
- utiliser les versions actuelles de compilation et de chaînes d'outils, ainsi que des options de compilation sécurisée;
- traiter les éléments d'entrée et autres données en toute sécurité (c'est-à-dire de manière prudente et restrictive…);
- utiliser des outils d'analyse de code statique afin de détecter rapidement les problèmes de SURETE;
- traiter les erreurs.

NOTE 1 Les meilleures pratiques de codage évitent de coder sur la base d'un comportement non spécifié ou non défini de l'environnement de programmation.

NOTE 2 L'analyse de code statique (SCA) détecte le potentiel d'occurrence d'erreurs comme les débordements de la mémoire tampon, le déréférencement de pointeur null et phénomènes analogues.

NOTE 3 La SCA peut être réalisée au moyen d'un outil lorsque celui-ci est disponible pour le langage utilisé. De plus, une analyse de code statique peut être réalisée pour toutes les modifications de code source y compris un nouveau code source.

B.5.5 Mise en œuvre sécurisée

Le FABRICANT peut mettre en œuvre une ARCHITECTURE et une conception qui permettent la mise à jour ou le remplacement des composants matériels et des ELEMENTS LOGICIELS – par exemple, modules cryptographiques. L'objectif dans le cas présent est une mise en œuvre qui valorise la souplesse technologique: par exemple, les algorithmes de chiffrement peuvent potentiellement être divisés à tout moment, même s'ils sont considérés comme représentant les meilleures pratiques actuelles, et les bibliothèques de chiffrement peuvent comporter des VULNERABILITES qui nuisent à des algorithmes par ailleurs fiables. Dans l'exemple donné, il convient qu'une mise en œuvre sécurisée assure qu'une certaine stratégie de chiffrement précise comment il convient que les applications et services mettent en œuvre leur chiffrement afin de permettre une transition vers de nouveaux mécanismes, de nouvelles bibliothèques et de nouvelles clés cryptographiques en cas de nécessité avérée. La description ci-dessus constitue simplement un exemple: un remplacement interne à l'ARCHITECTURE permet également la prise en charge des mises à jour et des améliorations de SURETE nécessaires.

B.5.6 Non utilisé

B.5.7 Essais des systèmes logiciels

B.5.7.1 Vérification par essai des exigences de SÛRETÉ

Le paragraphe 5.7 qui traite des essais des systèmes logiciels fournit les exigences et de plus amples informations liées aux essais de SURETE.

Une présentation de certaines techniques d'essai automatisées et manuelles inclut les techniques décrites de B.5.7.2 à B.5.7.5.

B.5.7.2 Essais d'atténuation des MENACES

Il s'agit par exemple de l'essai de VALIDATION des éléments d'entrée qui joue un rôle important dans l'atténuation des MENACES.

Les essais de VALIDATION des éléments d'entrée visent à détecter un comportement système non souhaité lors de la transmission de données incorrectes ou d'une charge de données excessive à une interface système. Des outils automatisés sont souvent utilisés et plus l'outil est spécialisé pour un certain protocole d'interface, plus les résultats d'essai sont exacts. Les essais de distorsion, ainsi que les essais de débordement de la mémoire tampon et d'erreurs de format en constituent des exemples. Il existe des techniques spécialisées d'essai par injection pour les protocoles tels que SQL, LDAP, XML et le script intersites.

B.5.7.3 Analyse des VULNÉRABILITÉS

L'analyse des VULNERABILITES consiste en une détection automatisée des VULNERABILITES connues. Les scanneurs détectent les logiciels installés, les accès par les réseaux ouverts, la configuration des systèmes d'exploitation et d'autres informations pertinentes pour la SURETE. De nombreux scanneurs des VULNERABILITES permettent à la fois des analyses authentifiées et non authentifiées. Une analyse authentifiée signifie que l'outil comporte des identifiants de système administratifs afin de contourner certaines protections et qu'il est capable d'évaluer la configuration des systèmes de manière bien plus détaillée et exacte. La fondation OWASP (Open Web Application SECURITY Project) maintient une liste des outils d'analyse des VULNERABILITES.

B.5.7.4 Essais de pénétration

Les essais de pénétration, également appelés "pen-testing" en anglais, ciblent spécifiquement la remise en cause de la CONFIDENTIALITE, de l'INTEGRITE ou de la DISPONIBILITE. Il peut s'agit de compromettre plusieurs aspects de la conception de la DEFENSE EN PROFONDEUR. Par exemple: contourner l'authentification pour accéder au PRODUIT, utiliser l'élévation de privilèges pour obtenir un accès administratif et compromettre la CONFIDENTIALITE en piratant le chiffrement. Comme le démontre cet exemple, les essais de pénétration impliquent de se présenter comme pirate et souvent d'exploiter les VULNERABILITES en chaîne dans un PRODUIT au moyen d'outils et de compétences manuelles. Les résultats de l'analyse des VULNERABILITES et d'autres essais peuvent fournir un élément d'entrée précieux afin de développer des scénarii d'ATTAQUE manuelle.

Il convient que les essais de pénétration incluent la participation d'un individu non impliqué dans le développement du LOGICIEL DE SANTE.

B.5.7.5 Gestion des conflits d'intérêts entre les contrôleurs et les développeurs

L'objectivité vise à prendre des décisions en appliquant aux faits les méthodes établies, de sorte que tout autre contrôleur puisse reproduire la décision ultérieurement. L'indépendance peut favoriser l'objectivité. Le FABRICANT peut mettre en place une équipe d'essai interne (semi-)indépendante et/ou faire recours à un organisme d'essai de SURETE.

L'analyse de code statique et l'ANALYSE DE COMPOSITION LOGICIELLE (analyse binaire) dépendent généralement de l'utilisation d'outils automatisés. Ces essais sont mentionnés dans l'IEC 62443-4-1, toutefois le présent document ne spécifie pas les exigences d'indépendance. La méthode d'application des outils automatisés et d'interprétation de leurs résultats nécessite également de l'objectivité. Cependant, l'étalonnage exigé pour les différents outils (et les différents environnements de programmation) ne garantit pas toujours la cohérence des résultats entre les outils. Il est donc recommandé de mettre en œuvre la reproductibilité au sein d'une chaîne d'outils donnée[41].

Annexe C
(informative)

MODÉLISATION D'UNE MENACE

C.1 Généralités

La MODELISATION D'UNE MENACE est une approche systématique d'analyse structurelle de la SURETE d'un élément de manière à pouvoir identifier, énumérer et hiérarchiser par ordre de priorité toutes les VULNERABILITES, et ce, du point de vue d'un attaquant hypothétique. La MODELISATION D'UNE MENACE peut être appliquée à une large plage d'objets, y compris les logiciels, les dispositifs, les systèmes, les réseaux, les systèmes répartis et les PROCESSUS opérationnels. La MODELISATION D'UNE MENACE applique généralement une approche systématique qui permet d'identifier les vecteurs d'ATTAQUE et les ACTIFS les plus souhaités par les différents acteurs de MENACES. Cette démarche entraîne une décomposition de l'élément (logiciel, dispositif, système, etc.) afin d'observer de manière individuelle chaque vecteur d'ATTAQUE et chaque ACTIF potentiels, et de déterminer le type d'ATTAQUES auquel ils sont vulnérables. Sur cette base, une liste des VULNERABILITES peut être générée et ordonnée par rapport au risque, au potentiel d'influence sur la SECURITE, à l'efficacité ou à d'autres critères éventuels considérés comme appropriés (comme le respect de la vie privée).

Il existe différentes approches de création d'un modèle de MENACE (de la constitution d'une liste des VULNERABILITES connues à l'adoption d'un cadre), dont certains exemples sont décrits de l'Article C.2 à l'Article C.10.

Un acteur de MENACES ou un acteur malveillant est une personne, un groupe ou une organisation qui attaque un organisme avec le potentiel d'influence sur la SECURITE ou la SURETE des systèmes. Les acteurs de MENACES ont des motivations différentes pour attaquer certains organismes ou systèmes, telles que le gain financier, le vol de données, le vol de propriété intellectuelle ou simplement la rupture de la confiance dont jouit l'organisme ciblé. Un acteur de MENACES peut avoir des compétences et des ressources limitées (pirates adolescents) ou importantes (cyberterroristes et acteurs étatiques). Les acteurs de MENACES sont souvent classés en acteurs intentionnels et non intentionnels (erreurs d'utilisation) et peuvent être externes ou internes à l'organisme. Les acteurs types de MENACES qui peuvent être pris en considération lors de la MODELISATION D'UNE MENACE sont les initiés (utilisateurs cliniques, administrateurs système), les pirates adolescents, les cybercriminels, les hacktivistes et les acteurs étatiques.

C.2 Arbres d'ATTAQUE-défense

Un arbre d'ATTAQUE-défense (AD Tree - *attack-defense tree*) est un arbre enraciné avec étiquettes de nœuds, qui décrit les mesures qu'un pirate peut appliquer pour ATTAQUER un système, ainsi que les défenses qu'un défenseur peut utiliser pour protéger le système.

C.3 CAPEC/OWASP/SANS

Une approche fondamentale consiste à utiliser des listes de MENACES élevées connues telles que la menace OWASP Top 10 ou la menace CWE/SANS Top 25. L'approche "Énumération et classification des motifs d'attaque communs" (CAPEC - *common attack pattern enumeration and classification*) comporte un dictionnaire plus exhaustif des motifs d'ATTAQUE connus utilisés par des adversaires pour exploiter des POINTS FAIBLES connus.

C.4 CWSS

Le Système de notation des POINTS FAIBLES communs (CWSS - *common weakness scoring system*) identifie à la fois les VULNERABILITES et prévoit un système de notation pour leur

hiérarchisation par ordre de priorité. Il s'agit d'un effort communautaire collaboratif qui cible l'analyse des logiciels et des bogues signalés afin de déterminer l'importance relative des POINTS FAIBLES détectés.

C.5 DREAD

DREAD est un programme de classification qui permet de quantifier, de comparer et de hiérarchiser par ordre de priorité le niveau de risque présenté par chaque MENACE évaluée. La modélisation DREAD cible l'évaluation des risques. L'algorithme DREAD sert à calculer une valeur de risque qui constitue une valeur moyenne de la totalité des cinq catégories suivantes: **D**amage, (**D**ommage), **R**eproducibility (**R**eproductibilité), **E**xploitability (**E**xploitabilité), **A**ffected users (**U**tilisateurs affectés) et **D**iscoverability (**D**écouvrabilité).

C.6 Liste des VULNÉRABILITÉS potentielles connues

Une liste de toutes les VULNERABILITES susceptibles d'affecter un système peut être établie. Bien qu'il soit impossible d'établir la liste de toutes les VULNERABILITES potentielles, il convient de se concentrer sur les VULNERABILITES qui peuvent être développées par les MENACES connues.

C.7 OCTAVE

OCTAVE est une approche méthodologique d'envergure des risques, développée par le Software Engineering Institute (SEI) de la Carnegie Mellon University en collaboration avec un CERT. OCTAVE cible le risque organisationnel et non le risque technique.

C.8 STRIDE

STRIDE est un modèle de décomposition d'un système, par la caractérisation des MENACES connues selon les types d'EXPLOITS utilisés. L'acronyme STRIDE représente chacune des catégories: **S**poofing (**U**surpation), **T**ampering (**A**ltération), **R**epudiation (**R**épudiation), **I**nformation disclosure (**D**ivulgation de renseignements), **D**enial of service (Refus de service) et **E**levation of Privilege (**É**lévation de privilège). STRIDE n'inclut pas de système de notation.

C.9 Trike

Trike est un cadre de MODELISATION D'UNE MENACE qui présente des similitudes avec les PROCESSUS de même nature STRIDE et DREAD. Trike est différent en ce sens qu'il utilise une approche fondée sur le risque avec des modèles distincts de mise en œuvre, de MENACES et de risques, et non le MODELE de MENACE agrégé STRIDE/DREAD (ATTAQUES, MENACES et POINTS FAIBLES).

C.10 VAST

L'acronyme VAST (Visual, Agile, Simple Threat) désigne la MODELISATION D'UNE MENACE Visual (Visuelle), Agile (Flexible) et Simple (Simple). Le principe de cette approche est la nécessité d'une mise à l'échelle du PROCESSUS de MODELISATION D'UNE MENACE au sein de l'infrastructure et du CYCLE DE VIE complet de développement des logiciels. Cette approche s'intègre dans une méthodologie de développement flexible de logiciels. La méthodologie fournit un programme d'application et de visualisation d'infrastructure de telle sorte que la création et l'utilisation de MODELEs de MENACE n'exigent aucune expertise spécifique dans le domaine de la SURETE.

Annexe D
(informative)

Relation avec les pratiques spécifiées dans l'IEC 62443-4-1:2018

D.1 IEC 81001-5-1 avec IEC 62443-4-1:2018

IEC 81001-5-1	IEC 62443-4-1:2018		IEC 81001-5-1	IEC 62443-4-1:2018
4.1.1	Pas dans l'IEC 62443-4-1		5.7.4	SVV-4
4.1.2	SM-2		5.7.5	SVV-5
4.1.3	SM-3		5.8.1	SM-11
4.1.4	SM-4		5.8.2	SG-5, SG-6
4.1.5	SM-10		5.8.3	SM-6
4.1.6	SM-13		5.8.4	SM-8
4.1.7	DM-5		5.8.5	SM-11
4.1.8	DM-6		5.8.6	SM-12
4.1.9	SG-7		5.8.7	SG-4
4.2	Pas dans l'IEC 62443-4-1		6.1.1	SUM-5
5.1.1	SM-1, SM-5		6.2.1	DM-1
5.1.2	SM-7		6.2.2	SUM-1
5.1.3	SI-2		6.3.1	SUM-3
5.2.1	SR-3, SR-4		6.3.2	SUM-2, SUM-4
5.2.2	SR-5		6.3.3	SM-6
5.2.3	SM-9		7.1	SR-1
5.3.1	SD-2		7.2	SR-2
5.3.2	SD-4		7.3	Pas dans l'IEC 62443-4-1
5.3.3	SD-3		7.4	Pas dans l'IEC 62443-4-1
5.4.1	SD-4		7.5	Pas dans l'IEC 62443-4-1
5.4.2	SD-2		8	SM-1
5.4.3	SD-1		9.1	Pas dans l'IEC 62443-4-1
5.4.4	SD-3		9.2	DM-1
5.5.1	SI-2		9.3	DM-2
5.5.2	SI-1		9.4	DM-3
5.6	Pas dans l'IEC 62443-4-1		9.5	DM-4
5.7.1	SVV-1		A.4	SI-2
5.7.2	SVV-2		E.2	SG-1, SG-2, SG-3
5.7.3	SVV-3		E.3	SG-4

D.2 IEC 62443-4-1:2018 avec IEC 81001-5-1

Noter que les exigences SG-1,2,3 ne sont pas spécifiées de manière normative comme cela est expliqué à l'Annexe A (justification). C'est la raison pour laquelle les parties normatives du présent document excluent les exigences du contenu de la DOCUMENTATION D'ACCOMPAGNEMENT.

IEC 62443-4-1:2018	IEC 81001-5-1		IEC 62443-4-1:2018	IEC 81001-5-1
SM-1	5.1.1, 8		SVV-1	5.7.1
SM-2	4.1.2		SVV-2	5.7.2
SM-3	4.1.3		SVV-3	5.7.3
SM-4	4.1.4		SVV-4	5.7.4
SM-5	5.1.1		SVV-5	5.7.5
SM-6	5.8.3, 6.3.3		DM-1	6.2.1, 9.2
SM-7	5.1.2		DM-2	9.3
SM-8	5.8.4		DM-3	9.4
SM-9	5.2.3		DM-4	9.5
SM-10	4.1.5		DM-5	4.1.7
SM-11	5.8.1, 5.8.5		DM-6	4.1.8
SM-12	5.8.6		SUM-1	6.2.2
SM-13	4.1.6		SUM-2	6.3.2
SR-1	7.1		SUM-3	6.3.1
SR-2	7.2		SUM-4	6.3.2
SR-3	5.2.1		SUM-5	6.1.1
SR-4	5.2.1		SG-1	E.2
SR-5	5.2.2		SG-2	E.2
SD-1	5.4.3		SG-3	E.2
SD-2	5.3.1, 5.4.2		SG-4	5.8.7, E.3
SD-3	5.3.3, 5.4.4		SG-5	5.8.2
SD-4	5.3.2, 5.4.1		SG-6	5.8.2
SI-1	5.5.2		SG-7	4.1.9
SI-2	5.1.3, 5.5.1, A.4			

Annexe E
(informative)

Documents spécifiés dans l'IEC 62443-4-1

E.1 Présentation

La présente annexe spécifie les documents liés au PRODUIT qui viennent à l'appui de l'utilisation sécurisée des LOGICIELS DE SANTE.

Pour une conformité totale à l'IEC 62443-4-1[11], le FABRICANT a besoin de démontrer la conformité au présent document, y compris la présente annexe dédiée à la documentation liée au PRODUIT.

Les PROCESSUS spécifiés par la présente annexe permettent de fournir une documentation qui décrit comment intégrer, configurer et maintenir la stratégie de DEFENSE EN PROFONDEUR des LOGICIELS DE SANTE conformément à leur CONTEXTE DE SURETE. L'application et le maintien de la stratégie de DEFENSE EN PROFONDEUR pour une installation spécifique de LOGICIEL DE SANTE traitent généralement des points suivants:

1) politiques et procédures associées au CONTEXTE DE SURETE des LOGICIELS DE SANTE;
2) considérations architecturales, telles que l'installation de pare-feu et l'utilisation de mécanismes de compensation y compris des mesures de SURETE;
3) configuration des paramètres/options de SURETE tels que la configuration des règles d'installation de pare-feu et la gestion des comptes utilisateurs; et
4) utilisation d'outils qui facilitent le renforcement des LOGICIELS DE SANTE.

E.2 Documentation de diffusion

E.2.1 Documentation liée au PRODUIT

Il convient que le FABRICANT inclue dans les exigences relatives au PRODUIT, les éléments suivants:

a) privilèges de SURETE exigés pour l'installation, l'exploitation et la maintenance du PRODUIT;
b) options de SURETE, y compris la suppression des mots de passe par défaut, utilisés pour l'installation, la configuration, l'exploitation et la maintenance du PRODUIT; et
c) considérations/actions de SURETE associées au retrait du PRODUIT (par exemple, suppression des données sensibles).

NOTE 1 Les spécifications en 5.2.1 couvrent la documentation relative aux exigences de SURETE au niveau du LOGICIEL DE SANTE. La documentation de diffusion du PRODUIT traite également des spécifications de SURETE.

Il convient que le FABRICANT inclue dans les exigences de SURETE les informations suivantes:

a) le domaine d'application et les limites des ELEMENTS LOGICIELS du PRODUIT, tant physiques que logiques;
b) l'identification du LOGICIEL EXIGE y compris sa version;
c) les informations concernant les interfaces: les capacités d'intégration de la gestion de l'identité du PRODUIT et de son accès avec celles de l'infrastructure de déploiement; et les capacités d'intégration du PRODUIT dans l'environnement de déploiement;
d) les contrôles internes au PRODUIT; et
e) la conception d'une mise à jour de SURETE du PRODUIT y compris la mise à jour du ou des logiciels incorporés provenant de sources externes. Voir l'ISO/IEC 30111.

NOTE 2 Ces informations sont destinées à couvrir le concept de niveaux de CAPACITE DE SURETE.

E.2.2 Documentation relative à la DÉFENSE EN PROFONDEUR des LOGICIELS DE SANTÉ

Il convient que le FABRICANT établisse une ACTIVITE destinée à produire une documentation relative aux LOGICIELS DE SANTE qui décrit les contrôles compensatoires dédiés aux LOGICIELS DE SANTE, afin de venir à l'appui de l'installation, de l'exploitation et de la maintenance. Il est prévu que cette documentation inclue:

a) les CAPACITES DE SURETE mises en œuvre par les LOGICIELS DE SANTE et leur rôle dans la stratégie de DEFENSE EN PROFONDEUR;

b) les MENACES traitées par la stratégie de DEFENSE EN PROFONDEUR;

c) les stratégies d'atténuation des utilisateurs des LOGICIELS DE SANTE applicables aux risques de SURETE connus associés à ces mêmes LOGICIELS DE SANTE, y compris les risques associés aux LOGICIELS EXIGES; et

d) les informations appropriées concernant les RISQUES RESIDUELS pertinents pour la SURETE auxquels sont soumis les LOGICIELS DE SANTE.

NOTE 1 L'IEC TR 60601-4-5 fournit des recommandations concernant la spécification des CAPACITES DE SURETE et la preuve de leur existence dans la DOCUMENTATION D'ACCOMPAGNEMENT, ainsi qu'une méthode de détermination des exigences à partir du niveau de CAPACITE DE SURETE.

NOTE 2 L'IEC TR 80001-2-2 spécifie les besoins, les risques et les contrôles liés à la SURETE sous forme de recommandations concernant la divulgation et la communication entre le FABRICANT et l'ORGANISME DE PRESTATION DE SOINS DE SANTE.

NOTE 3 La documentation relative à la DEFENSE EN PROFONDEUR des LOGICIELS DE SANTE peut servir à expliquer la relation entre les VULNERABILITES des composants et la SECURITE.

E.2.3 Mesures de DÉFENSE EN PROFONDEUR et environnement

Un LOGICIEL DE SANTE peut comporter des VULNERABILITES pour lesquelles les contrôles techniques peuvent altérer la SECURITE et l'efficacité du PRODUIT dans sa DESTINATION PREVUE.

Il convient que le PRODUIT anticipe à un certain degré son ENVIRONNEMENT D'UTILISATION PREVU. Une déclaration des contrôles externes prévus peut être utilisée pour définir les responsabilités partagées – par exemple, comme cela est spécifié dans les normes IEC TR 60601-4-5 et IEC TR 80001-2-2 pour lesquelles des recommandations en bonne et due forme sont publiées en tant que document HIMSS/NEMA "MDS2".

Il convient que le FABRICANT établisse une ACTIVITE destinée à produire une documentation liée au PRODUIT qui déclare les contrôles de SURETE externes à prévoir ou à mettre en œuvre par l'environnement externe.

E.2.4 Lignes directrices pour un renforcement de la SÛRETÉ

Il convient que le FABRICANT établisse une ACTIVITE destinée à produire une documentation relative aux LOGICIELS DE SANTE qui comprend des lignes directrices applicables au renforcement des LOGICIELS DE SANTE lors de leur déploiement, leur installation et leur maintenance. Le cas échéant, il convient que les lignes directrices incluent entre autres des instructions, une justification et des recommandations applicables aux éléments suivants:

a) intégration du LOGICIEL DE SANTE, y compris des ELEMENTS LOGICIELS tiers, dans son CONTEXTE DE SURETE;

b) intégration des interfaces/protocoles de programmation d'application du LOGICIEL DE SANTE avec les applications utilisateurs;

c) application et maintien de la stratégie de DEFENSE EN PROFONDEUR du LOGICIEL DE SANTE;

d) configuration et utilisation des options de SURETE et des CAPACITES DE SURETE à l'appui des politiques de SURETE locales, et pour chaque option de SURETE/CAPACITE DE SURETE:

   1) sa contribution à la stratégie de DEFENSE EN PROFONDEUR DU LOGICIEL DE SANTE;

2) les descriptions des valeurs configurables et par défaut qui indiquent comment chaque option/capacité affecte la SURETE, ainsi que l'effet potentiel de chacune de cette même option/capacité sur les pratiques de travail; et

3) la configuration/modification/suppression de la valeur de cette option/capacité;

e) instructions et recommandations pour l'utilisation de tous les outils et services liés à la SURETE qui viennent à l'appui de l'administration, de la surveillance, du traitement des incidents et de l'évaluation de la SURETE du LOGICIEL DE SANTE;

f) instructions et recommandations pour les ACTIVITES périodiques de maintenance de la SURETE;

g) instructions de signalement au FABRICANT des incidents de SURETE qui impliquent le LOGICIEL DE SANTE; et

h) description des meilleures pratiques de SURETE pour la maintenance et l'administration du LOGICIEL DE SANTE.

NOTE La nomenclature des logiciels (SBOM - *software bill of material*) constitue une documentation qui assure la traçabilité de tous les logiciels incorporés. La SBOM constitue une documentation à l'intention du client non exigée par l'IEC 62443-4-1[11], mais en revanche par l'IEC TR 60601-4-5. Les SBOM permettent aux clients de contrôler l'environnement du risque de SURETE et de communiquer ce risque au FABRICANT, à titre d'exemple relatif aux correctifs de SURETE associés dédiés aux logiciels énumérés.

E.2.5 Informations relatives aux mises à jour de SÛRETÉ

Le FABRICANT doit établir une ACTIVITE (ou des ACTIVITES) destinées à vérifier que la DOCUMENTATION relative aux mises à jour de SURETE du PRODUIT est mise à disposition des utilisateurs dudit PRODUIT. Cette documentation comporte entre autres:

a) le ou les numéros de version du PRODUIT auxquels le correctif de SURETE s'applique;

b) les instructions portant sur le mode d'application manuel et automatisé des correctifs agréés;

c) la description des effets éventuels que peut avoir l'application du correctif au PRODUIT, y compris une réinitialisation;

d) les instructions portant sur la méthode de vérification de l'application effective d'un correctif agréé;

e) les risques (effet potentiel sur la SECURITE, l'efficacité, la SURETE) liés à la non-application de la mise à jour et des mesures d'atténuation qui peuvent être utilisées pour les mises à jour non agréées ou non mises en œuvre par le propriétaire des ACTIFS;

f) la possibilité de porter atteinte à la CONFIDENTIALITE, l'INTEGRITE et la DISPONIBILITE en l'absence de mise à jour; et

g) des recommandations qui visent à réduire la possibilité de porter atteinte à la CONFIDENTIALITE, l'INTEGRITE et la DISPONIBILITE.

E.3 Documents relatifs à la mise hors service des LOGICIELS DE SANTÉ

Il convient que les lignes directrices applicables à la mise hors service des LOGICIELS DE SANTE incluent, entre autres, des instructions et des recommandations pour les tâches suivantes:

a) retrait du LOGICIEL DE SANTE de son ENVIRONNEMENT D'UTILISATION PREVU (voir l'Article 6 de l'IEC 62443-4-1:2018[11]);

b) élimination des données du patient et de configuration stockées dans l'environnement;

c) transfert, migration, archivage et suppression sécurisés des données stockées dans le LOGICIEL DE SANTE; et

d) mise au rebut sécurisée du LOGICIEL DE SANTE afin d'empêcher toute divulgation potentielle des données contenues dans ce dernier et qui n'ont pu être éliminées comme cela est écrit en c) ci-dessus.

Annexe F
(normative)

LOGICIEL DE SANTÉ TRANSITOIRE

F.1 Présentation

La présente annexe définit un certain nombre d'ACTIVITES destinées à améliorer la SURETE du LOGICIEL DE SANTE TRANSITOIRE développé sans suivre toutes les ACTIVITES définies de l'Article 4 à l'Article 9 du présent document. Les résultats sont documentés sous la forme d'une "Déclaration de conformité aux activités relatives aux LOGICIELS DE SANTE TRANSITOIRES de l'Annexe F".

Deux options se présentent pour les LOGICIELS DE SANTE dont le processus du fabricant ne satisfait pas à toutes les exigences spécifiées dans la partie normative des Articles 4 à 9 du présent document:

1) redévelopper le LOGICIEL DE SANTE conformément aux parties normatives du présent document;
2) améliorer la SURETE des LOGICIELS DE SANTE existants par des ACTIVITES telles que la mise à jour des lignes directrices pour un fonctionnement sécurisé, la mise en place de contrôles compensatoires ou la réécriture partielle du LOGICIEL DE SANTE. Il s'agit des ACTIVITES décrites de l'Article F.2 à l'Article F.4.

Les résultats des ACTIVITES décrites de l'Article F.2 à l'Article F.4 sont documentés sous la forme d'une "Déclaration de conformité aux ACTIVITES relatives aux LOGICIELS DE SANTE TRANSITOIRES de l'IEC 81001-5-1:2021, Annexe F".

Du fait de l'application de l'Annexe F, le FABRICANT peut conserver le LOGICIEL DE SANTE TRANSITOIRE non modifié ou peut décider de réexécuter les ACTIVITES spécifiées à l'Article 5 pour les ELEMENTS LOGICIELS sélectionnés.

NOTE 1 Le concept de "logiciel hérité", comme cela est défini dans l'IEC 62304[8], ne peut pas être appliqué directement au domaine de la SURETE. Les principales raisons sont les suivantes:

– L'évaluation de "tout retour d'informations, y compris les informations de postproduction, sur le "logiciel hérité" concernant les incidents et/ou les quasi-incidents" (IEC 62304:2006/AMD1:2015, 4.4.2 a)) ne peut pas constituer un support de fiabilité qui permet de rester à la pointe de l'état de l'art en matière de CYBERSECURITE.
– La "validité continue des mesures de MAITRISE DU RISQUE" (IEC 62304:2006/AMD1:2015, 4.4.2 b)) ne peut pas constituer un support de fiabilité qui permet d'assurer une protection dans l'environnement de la CYBERSECURITE qui évolue rapidement.

NOTE 2 Un LOGICIEL DE SANTE TRANSITOIRE peut être partiellement conforme aux Articles 4 à 9 du présent document. Les PROCESSUS pour les LOGICIELS DE SANTE TRANSITOIRES peuvent mettre en œuvre un sous-ensemble des exigences normatives du présent document.

NOTE 3 Les LOGICIELS DE SANTE TRANSITOIRES font partie intégrante de l'ensemble des LOGICIELS EXIGES.

F.2 Activités d'évaluation du développement et de comblement des lacunes

Le FABRICANT des LOGICIELS DE SANTE TRANSITOIRES doit mettre en œuvre les ACTIVITES spécifiées à l'Article 4.

Le FABRICANT doit effectuer une analyse des lacunes des consommables disponibles par rapport à ceux exigés selon 5.2, 5.7, 7.1.1, 7.2 et 7.3 comme cela est décrit ci-dessous.

Le FABRICANT doit exécuter les activités de comblement des lacunes suivantes:

a) documentation des exigences de SURETE au niveau du système, comme cela est décrit en 5.2.1;

b) réalisation et documentation d'essais (exhaustifs) au niveau du système, comme cela est décrit en 5.7 (essais des systèmes logiciels);

c) évaluation et estimation du risque de SURETE. Cette opération doit documenter le CONTEXTE DE SURETE et le MODELE DE MENACE décrits en 7.1.1, 7.2 et 7.3;

d) maîtrise du risque de SURETE comme cela est décrit en 7.4. Dans certains exemples, le risque de SURETE résiduel impose des contrôles compensatoires – externes aux LOGICIELS DE SANTE – qui sont documentés dans les lignes directrices pour un fonctionnement sécurisé;

e) production de lignes directrices, ou mise à jour des lignes directrices existantes pour un fonctionnement sécurisé et pour une gestion des comptes, comme cela est décrit en 5.8.2; et

NOTE 1 Voir E.2.1 (documentation relative à la DEFENSE EN PROFONDEUR des LOGICIELS DE SANTE pour les recommandations de divulgation).

f) évaluation du risque de SURETE résiduel global et détermination, sur la base de cette évaluation, du caractère adapté du LOGICIEL DE SANTE TRANSITOIRE pour une utilisation continue.

NOTE 2 Le FABRICANT peut également choisir de remettre en œuvre certaines parties du LOGICIEL DE SANTE selon le présent document, par exemple, composants d'interface de réseau.

F.3 Justification de l'utilisation des LOGICIELS DE SANTÉ TRANSITOIRES

Le FABRICANT doit documenter la version du LOGICIEL DE SANTE TRANSITOIRE ainsi qu'une justification de son utilisation continue sur la base des résultats des activités de comblement des lacunes.

Le FABRICANT doit établir et diffuser un plan de migration des LOGICIELS DE SANTE TRANSITOIRES afin qu'ils soient conformes aux Articles 6 à 9.

Dans les cas pour lesquels une mise à niveau de certains composants n'est pas appropriée, le plan doit documenter la version respective et la justification d'une utilisation continue de ces composants. Selon l'Article F.2, les composants non mis à jour sont pris en considération dans la GESTION DES RISQUES et le RISQUE RESIDUEL résultant, ainsi que les contrôles compensatoires appropriés doivent être clairement communiqués comme partie intégrante de la documentation de diffusion décrite en 5.8.2 ou à l'Annexe E.

NOTE 1 Le terme "certains composants" peut comprendre l'ensemble du LOGICIEL DE SANTE.

NOTE 2 La réalisation complète de ces activités permet au FABRICANT de documenter un référentiel du niveau de CYBERSECURITE mis en œuvre dans les LOGICIELS DE SANTE TRANSITOIRES.

F.4 ACTIVITÉS post-diffusion

Les ACTIVITES post-diffusion décrites de l'Article 6 à l'Article 9 doivent être accomplies pour les LOGICIELS DE SANTE TRANSITOIRES afin de revendiquer la conformité à l'Annexe F.

Annexe G
(normative)

Identificateurs d'objet

Conformément à l'ISO 9834-1:2012, 6.1.3, "l'enregistrement (des éléments et de leurs identificateurs d'objet (OID) associés) peut être effectué par une Recommandation UIT-T et/ou une Norme internationale, en publiant dans la Recommandation UIT-T et/ou la Norme internationale les noms et les définitions correspondantes de l'objet".

Par conséquent, la présente annexe spécifie les OID pour les concepts de conformité définis dans le présent document.

Le Tableau G.1 spécifie les identificateurs d'objet et les noms symboliques pour l'organisme d'enregistrement UIT-T/ISO/IEC (voir actuellement oid-info.com), et ce afin obtenir des références stables et données par version pour ces concepts de conformité.

Tableau G.1 – Identificateurs d'objet pour les concepts de conformité du présent document

OID	Définition du concept	Nom symbolique
1.0.81001	Série ISO/IEC 81001, *Logiciels de santé et sécurité, efficacité et sûreté des systèmes TI de santé*	health-software (logiciel de santé)
1.0.81001.5	ISO/IEC 81001-5, *Logiciels de santé et sécurité, efficacité et sûreté des systèmes TI de santé – Partie 5: Sûreté*	security (sûreté)
1.0.81001.5.1	IEC 81001-5-1, *Logiciels de santé et sécurité, efficacité et sûreté des systèmes TI de santé – Partie 5-1: Sûreté – Activités du cycle de vie du produit*	lifecycle (cycle de vie)
1.0.81001.5.1.2021	IEC 81001-5-1:2021	edition1 (édition1)
1.0.81001.5.1.2021.1	Conformité aux Articles 4 à 9	full (totale)
1.0.81001.5.1.2021.2	Conformité de la documentation	documentation
1.0.81001.5.1.2021.3	Conformité du LOGICIEL DE SANTE TRANSITOIRE	transitional-sw (logiciel transitoire)

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

_____

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

3, rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland

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