# FINAL DRAFT

# INTERNATIONAL STANDARD

# IEC/FDIS 81001-5-1

ISO/TC **215** 

Secretariat: ANSI

Voting begins on: **2021-09-10** 

Voting terminates on: 2021-11-05

# Health software and health IT systems safety, effectiveness and security —

Part 5-1:

Security — Activities in the product life cycle

# iTeh STANDARD PREVIEW (standards.iteh.ai)

IEC/FDIS 81001-5-1 https://standards.iteh.ai/catalog/standards/sist/227a3148-4206-42e3-ad21-05f80dda507a/iec-fdis-81001-5-1

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNO-LOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STAN-DARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS. This draft is submitted to a parallel vote in ISO and in IEC.



Reference number IEC/FDIS 81001-5-1:2021(E)

# iTeh STANDARD PREVIEW (standards.iteh.ai)

IEC/FDIS 81001-5-1 https://standards.iteh.ai/catalog/standards/sist/227a3148-4206-42e3-ad21-05f80dda507a/iec-fdis-81001-5-1 – 2 – IEC FDIS 81001-5-1 © IEC 2021

# CONTENTS

FOREWORD						
INTRODUCTION						
	0.1	Structure	7			
	0.2	Field of application	8			
	0.3	Conformance	8			
1	Scop	e	. 10			
2	Norm	ative references	.10			
3	Terms and definitions11					
4	General requirements1					
	4.1	Quality management	.18			
	4.1.1	Quality management system	. 18			
	4.1.2	Identification of responsibilities	.18			
	4.1.3	Identification of applicability	.18			
	4.1.4	SECURITY expertise	. 18			
	4.1.5	SOFTWARE ITEMS from third-party suppliers	.19			
	4.1.6	Continuous improvement	.19			
	4.1.7	Disclosing SECURITY-related issues	.19			
	4.1.8	Periodic review of SECURITY defect management	.19			
	4.1.9	ACCOMPANYING DOCUMENTATION REVIEW	.20			
	4.2	SECURITY RISK MANAGENENTING Ards.iteh.ai)	.20			
	4.3	SOFTWARE ITEM classification relating to risk transfer	.20			
5	Softw	/are development PROCESS… <u>IEC/FDIS 81001-5-1</u>	.21			
	5.1	Software development plantalog/standards/sist/227a3148-4206-42e3-ad21-	.21			
	5.1.1	ACTIVITIES in the LIFE CYCLE PROCESS	.21			
	5.1.2	Development environment SECURITY	.21			
	5.1.3	Secure coding standards	.21			
	5.2	HEALTH SOFTWARE requirements analysis	.21			
	5.2.1	HEALTH SOFTWARE SECURITY requirements	.21			
	5.2.2	SECURITY requirements review	.22			
	5.2.3	SECURITY risks for REQUIRED SOFTWARE	.22			
	5.3	Software architectural design	.22			
	5.3.1	DEFENSE-IN-DEPTH ARCHITECTURE/design	.22			
	5.3.2	Secure design best practices	.22			
	5.3.3	SECURITY architectural design review	.23			
	5.4	Software design	.23			
	5.4.1	Software design best practices	.23			
	5.4.2	Secure design	.23			
	5.4.3	Secure HEALTH SOFTWARE interfaces	.23			
	5.4.4	Detailed design VERIFICATION for SECURITY	.24			
	5.5	Software unit implementation and VERIFICATION	.24			
	5.5.1	Secure coding standards	.24			
	5.5.2	SECURITY implementation review	.24			
	5.6	Software integration testing	.25			
	5.7	Sottware system testing	.25			
	5.7.1	SECURITY requirements testing	.25			
	5.7.2	THREAT mitigation testing	.25			

# IEC FDIS 81001-5-1 © IEC 2021

	5.7.3	;	VULNERABILITY testing	25
	5.7.4		Penetration testing	26
	5.7.5	5	Managing conflicts of interest between testers and developers	26
	5.8	Sof	tware release	26
	5.8.1		Resolve findings prior to release	26
	5.8.2		Release documentation	27
	5.8.3	5	File INTEGRITY	27
	5.8.4		Controls for private keys	27
	5.8.5	;	Assessing and addressing SECURITY-related issues	27
	5.8.6	;	ACTIVITY completion	27
	5.8.7		SECURE decommissioning guidelines for HEALTH SOFTWARE	27
6	SOFT	WAR	E MAINTENANCE PROCESS	28
	6 1	Est	ablish SOFTWARE MAINTENANCE plan	28
	611	200	Timely delivery of SECURITY undates	28
	6.2	Pro	hlem and modification analysis	28
	621	110	Monitoring public incident reports	28
	622	,		28
	63		dification implementation	20
	631	WIOC	SUPPORTED SOFTWARE SECURITY undate documentation	29
	632	,	MAINTAINED SOFTWARE SECURITY update delivery	23
	633	- !	MAINTAINED SOFTWARE SECURITY Update NEEDITY	20
7	0.3.3 SECI			20
'	JECC		(standards.iten.ai)	29
	7.1	RIS		29
	7.1.1		General	29
	7.1.2		PRODUCTstSECURITYLCONTEXTtandards/sist/227a3148-4206-42e3-ad21-	29
	7.2	Idei	ntification of VULNERABILITIES, THREATS and associated adverse impacts	30
	7.3	Esti	mation and evaluation of SECURITY risk	31
	7.4	Cor	Itrolling SECURITY risks	31
	7.5	Mor	hitoring the effectiveness of RISK CONTROLS	31
8	Softv	vare	CONFIGURATION MANAGEMENT PROCESS	32
9	Softv	vare	problem resolution PROCESS	32
	9.1	Ove	erview	32
	9.2	Rec	eiving notifications about VULNERABILITIES	32
	9.3	Rev	iewing VULNERABILITIES	32
	9.4	Ana	Ilysing VULNERABILITIES	33
	9.5	Add	Iressing SECURITY-related issues	33
Aı	nnex A (	info	mative) Rationale	35
	Δ 1	Rel	ationship to IEC 62443	35
	Δ 2	Rel	ationship to IEC 62304	36
	Δ3	Riel	<pre>/ transfer</pre>	37
	Δ31	11131		37
	A.3.1	) )	MAINTAINED SOETWARE	
	A 3 3	2	SUDDODTED SOFTWARE	
	A.3.3	, I		
	A.3.4	+ جمع	NEQUIRED SUFTWARE	ა <i>ი</i> იი
۸.		JeC (info:	me county pest practices	00
AI	mex B (			39
	B.1	Öve	erview	39
	B.2	Rel	ated work	39

– 4 –

IEC FDIS 81001-5-1 © IEC 2021

B.3	THREAT / RISK ANALYSIS	
B.4	THREAT and RISK MANAGEMENT	40
B.5	Software development planning	40
B.5.1	Development	40
B.5.2	HEALTH SOFTWARE requirements analysis	41
B.5.3	Software architectural design	41
B.5.4	Software unit implementation and VERIFICATION	41
B.5.5	Secure implementation	42
B.5.6	Not used	42
B.5.7	Software system testing	42
Annex C (	informative) THREAT MODELLING	44
C.1	General	44
C.2	ATTACK-defense trees	44
C.3	CAPEC / OWASP / SANS	44
C.4	CWSS	44
C.5	DREAD	45
C.6	List known potential VULNERABILITIES	45
C.7	OCTAVE	45
C.8	STRIDE	45
C.9		45
C.10	VAST IIEN SIANDARD PREVIEW	45
Annex D (	informative) Relation to practices in IEC 62443-4-1.2018	46
D.1	IEC 81001-5-1 to IEC 62443-4-1:2018	46
D.2	IEC 62443-4-1 2018 to IEC 81001-5-1	17
	<u>TEO 02110 1 1.2010 10 120 <u>TEO 101-3-1</u></u>	
Annex E (	informative)s;Documents.specified.inalECi62443-4814206-42e3-ad21	
Annex E( E.1	informative)s:Documents specified inalECi62443-4814206-42e3-ad21- Overview	
Annex E( E.1 E.2	informative)s:Documents.specified.inalEGi62443-4814206-42c3-ad21- Overview	
Annex E ( E.1 E.2 E.2.1	informative)s:Documents specified in ECi62443-4814206-42e3-ad21- Overview	
Annex E ( E.1 E.2 E.2.1 E.2.2	informative)s:Documents specified in EG 62443-4814206-42c3-ad21- Overview	48 48 48 48 48 48 48 48
Annex E ( E.1 E.2 E.2.1 E.2.2 E.2.3	informative)s:Documents specified in ECi62443-4-14206-42e3-ad21- Overview	48 48 48 48 48 48 49 49
Annex E ( E.1 E.2 E.2.1 E.2.2 E.2.3 E.2.4	informative)s:Documents specified inalEGi62443-4814206-42e3-ad21- Overview	48 48 48 48 48 48 49 49 49
Annex E ( E.1 E.2 E.2.1 E.2.2 E.2.3 E.2.4 E.2.5	informative)s:Documents specified inalECi62443-4-14206-42e3-ad21- Overview	48 48 48 48 48 48 49 49 49 50
Annex E ( E.1 E.2 E.2.1 E.2.2 E.2.3 E.2.4 E.2.5 E.3	informative)s:Documents specified inalECi62443-4814206-42e3-ad21- Overview	48 48 48 48 48 49 49 49 50 50
Annex E ( E.1 E.2 E.2.1 E.2.2 E.2.3 E.2.4 E.2.5 E.3 Annex F (	informative)s:Documents specified in IEG 62443-4814206-42c3-ad21- Overview. 05f80dda507a/icc-fdis-81001-5-1 Release documentation. PRODUCT documentation HEALTH SOFTWARE DEFENSE-IN-DEPTH documentation DEFENSE-IN-DEPTH measures expected in the environment. SECURITY hardening guidelines SECURITY update information Documents for decommissioning HEALTH SOFTWARE mormative) TRANSITIONAL HEALTH SOFTWARE.	48 48 48 48 48 49 49 49 50 50 50 51
Annex E ( E.1 E.2 E.2.1 E.2.2 E.2.3 E.2.4 E.2.5 E.3 Annex F ( F.1	informative)s:Documents specified in IEC 62443-4814206-42e3-ad21- Overview. 05f80dda507a/iec-fdis-81001-5-1 Release documentation. PRODUCT documentation. HEALTH SOFTWARE DEFENSE-IN-DEPTH documentation. DEFENSE-IN-DEPTH measures expected in the environment. SECURITY hardening guidelines SECURITY update information Documents for decommissioning HEALTH SOFTWARE normative) TRANSITIONAL HEALTH SOFTWARE.	48 48 48 48 48 49 49 49 49 50 50 50 51 51
Annex E ( E.1 E.2 E.2.1 E.2.2 E.2.3 E.2.4 E.2.5 E.3 Annex F ( F.1 F.2	informative)s:Documents specified in IEG 62443-4814206-42c3-ad21- Overview. 05f80dda507a/icc-fdis-81001-5-1 Release documentation. PRODUCT documentation. HEALTH SOFTWARE DEFENSE-IN-DEPTH documentation. DEFENSE-IN-DEPTH measures expected in the environment. SECURITY hardening guidelines. SECURITY update information. Documents for decommissioning HEALTH SOFTWARE . normative) TRANSITIONAL HEALTH SOFTWARE. Overview. Development assessment and gap closure activities.	48 48 48 48 48 49 49 49 50 50 50 51 51 51
Annex E ( E.1 E.2 E.2.1 E.2.2 E.2.3 E.2.4 E.2.5 E.3 Annex F ( F.1 F.2 F.3	informative)s:Documents specified in IEC 62443-4814206-42e3-ad21- Overview. 05f80dda507a/iec-fdis-81001-5-1 Release documentation. PRODUCT documentation. HEALTH SOFTWARE DEFENSE-IN-DEPTH documentation. DEFENSE-IN-DEPTH measures expected in the environment. SECURITY hardening guidelines. SECURITY update information. Documents for decommissioning HEALTH SOFTWARE . normative) TRANSITIONAL HEALTH SOFTWARE. Overview. Development assessment and gap closure activities. Rationale for use of TRANSITIONAL HEALTH SOFTWARE .	48 48 48 48 48 49 49 49 49 50 50 50 51 51 51 51 52
Annex E ( E.1 E.2 E.2.1 E.2.2 E.2.3 E.2.4 E.2.5 E.3 Annex F ( F.1 F.2 F.3 F.4	informative): Documents specified in IEC 62443-4814206-42e3-ad21- Overview	48 48 48 48 48 49 49 49 50 50 50 50 51 51 51 51 52 52
Annex E ( E.1 E.2 E.2.1 E.2.2 E.2.3 E.2.4 E.2.5 E.3 Annex F ( F.1 F.2 F.3 F.4 Annex G (	informative): Documents specified in IEC 62443-4814206-42e3-ad21- Overview. 05f80dda507a/iec-fdis-81001-5-1 Release documentation PRODUCT documentation HEALTH SOFTWARE DEFENSE-IN-DEPTH documentation DEFENSE-IN-DEPTH measures expected in the environment SECURITY hardening guidelines SECURITY update information Documents for decommissioning HEALTH SOFTWARE normative) TRANSITIONAL HEALTH SOFTWARE Overview Development assessment and gap closure activities Rationale for use of TRANSITIONAL HEALTH SOFTWARE Post-release ACTIVITIES normative) Object identifiers	48 48 48 48 48 49 49 49 49 50 50 50 50 51 51 51 51 52 52 52 53
Annex E ( E.1 E.2 E.2.1 E.2.2 E.2.3 E.2.4 E.2.5 E.3 Annex F ( F.1 F.2 F.3 F.4 Annex G ( Bibliograp	informative)s: Documents specified in IEC 62443-4814206-42e3-ad21- Overview. 05f80dda507a/icc-fdis-81001-5-1 Release documentation. PRODUCT documentation. HEALTH SOFTWARE DEFENSE-IN-DEPTH documentation. DEFENSE-IN-DEPTH measures expected in the environment. SECURITY hardening guidelines SECURITY update information. Documents for decommissioning HEALTH SOFTWARE . normative) TRANSITIONAL HEALTH SOFTWARE. Overview. Development assessment and gap closure activities. Rationale for use of TRANSITIONAL HEALTH SOFTWARE . Post-release ACTIVITIES . normative) Object identifiers. hy.	48 48 48 48 48 49 49 49 50 50 50 50 51 51 51 51 52 52 52 52 52 53 54
Annex E ( E.1 E.2 E.2.1 E.2.2 E.2.3 E.2.4 E.2.5 E.3 Annex F ( F.1 F.2 F.3 F.4 Annex G ( Bibliograp	informative): Documents specified in IEC 62443 4814206-42e3-ad21- Overview. OSt80dda507a/icc-fdis-81001-5-1 Release documentation. PRODUCT documentation HEALTH SOFTWARE DEFENSE-IN-DEPTH documentation. DEFENSE-IN-DEPTH measures expected in the environment. SECURITY hardening guidelines SECURITY update information Documents for decommissioning HEALTH SOFTWARE normative) TRANSITIONAL HEALTH SOFTWARE Overview. Development assessment and gap closure activities Rationale for use of TRANSITIONAL HEALTH SOFTWARE Post-release ACTIVITIES normative) Object identifiers. hy.	48 48 48 48 49 49 49 49 50 50 50 50 51 51 51 51 52 52 52 52 53 54
Annex E ( E.1 E.2 E.2.1 E.2.2 E.2.3 E.2.4 E.2.5 E.3 Annex F ( F.1 F.2 F.3 F.4 Annex G ( Bibliograp	informative): Documents specified in IECi62443:4814206-42e3-ad21- Overview	48 48 48 48 48 49 49 49 50 50 50 50 50 51 51 51 51 52 52 52 52 52 53 53 54
Annex E ( E.1 E.2 E.2.1 E.2.2 E.2.3 E.2.4 E.2.5 E.3 Annex F ( F.1 F.2 F.3 F.4 Annex G ( Bibliograp Figure 1 – Figure 2 –	informative): Documents specified in IEC 62443:14:14206-42c3-ad21. Overview. 05f80dda507a/icc-fdis-81001-5-1 Release documentation. PRODUCT documentation. HEALTH SOFTWARE DEFENSE-IN-DEPTH documentation. DEFENSE-IN-DEPTH measures expected in the environment. SECURITY hardening guidelines. SECURITY update information. Documents for decommissioning HEALTH SOFTWARE. normative) TRANSITIONAL HEALTH SOFTWARE. Overview. Development assessment and gap closure activities. Rationale for use of TRANSITIONAL HEALTH SOFTWARE. Post-release ACTIVITIES. normative) Object identifiers. hy.	48 48 48 48 49 49 49 50 50 50 50 51 51 51 51 51 52 52 52 52 53 53 54 54
Annex E ( E.1 E.2 E.2.1 E.2.2 E.2.3 E.2.4 E.2.5 E.3 Annex F ( F.1 F.2 F.3 F.4 Annex G ( Bibliograp Figure 1 – Figure 2 –	informative): Documents specified in IEC 62443-4814206-42e3-ad21. Overview	48 48 48 48 49 49 49 50 50 50 50 50 51 51 51 51 52 52 52 52 52 52 53 53 54 8 10
Annex E ( E.1 E.2 E.2.1 E.2.2 E.2.3 E.2.4 E.2.5 E.3 Annex F ( F.1 F.2 F.3 F.4 Annex G ( Bibliograp Figure 1 – Figure 2 –	<ul> <li>Informative): Documents specified in IEC 62443 4414206-42c3-ad21.</li> <li>Overview.</li> <li>Osf80dda507a/icc-fdis-81001-5-1</li> <li>Release documentation.</li> <li>PRODUCT documentation.</li> <li>HEALTH SOFTWARE DEFENSE-IN-DEPTH documentation.</li> <li>DEFENSE-IN-DEPTH measures expected in the environment.</li> <li>SECURITY hardening guidelines.</li> <li>SECURITY update information</li> <li>Documents for decommissioning HEALTH SOFTWARE</li> <li>Overview.</li> <li>Development assessment and gap closure activities.</li> <li>Rationale for use of TRANSITIONAL HEALTH SOFTWARE</li> <li>Post-release ACTIVITIES</li> <li>normative) Object identifiers.</li> <li>hy.</li> </ul>	48 48 48 48 49 49 49 50 50 50 50 51 51 51 51 52 52 52 52 52 53 54 8 
Annex E ( E.1 E.2 E.2.1 E.2.2 E.2.3 E.2.4 E.2.5 E.3 Annex F ( F.1 F.2 F.3 F.4 Annex G ( Bibliograp Figure 1 – Figure 2 – Table A.1 Table G 1	<ul> <li>Informative): Documents specified in IEC i62443-4414206-42c3-ad21.</li> <li>Overview.</li> <li>Osf80dda507a/icc-fdis-81001-5-1</li> <li>Release documentation.</li> <li>PRODUCT documentation.</li> <li>HEALTH SOFTWARE DEFENSE-IN-DEPTH documentation.</li> <li>DEFENSE-IN-DEPTH measures expected in the environment.</li> <li>SECURITY hardening guidelines.</li> <li>SECURITY update information</li> <li>Documents for decommissioning HEALTH SOFTWARE</li> <li>Overview.</li> <li>Development assessment and gap closure activities.</li> <li>Rationale for use of TRANSITIONAL HEALTH SOFTWARE</li> <li>Post-release ACTIVITIES</li> <li>normative) Object identifiers.</li> <li>hy.</li> <li>HEALTH SOFTWARE field of application</li> <li>HEALTH SOFTWARE LIFE CYCLE PROCESSES.</li> <li>Okiect identifiers for conformance concepts of this document</li> </ul>	48 48 48 48 49 49 49 50 50 50 50 50 50 51 51 51 51 52 52 52 52 53 53 54 8 

IEC FDIS 81001-5-1 © IEC 2021

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 conformitys 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.

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

Draft	Report on voting
62A/XX/FDIS	62A/XX/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.

- 6 -

IEC FDIS 81001-5-1 © IEC 2021

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 **iTeh STANDARD PREVIEW**
- amended.

# (standards.iteh.ai)

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.

IEC FDIS 81001-5-1 © IEC 2021

# 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]<sup>1</sup> 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; **iTeh STANDARD PREVIEW**

• 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 rds.iteh.ai/catalog/standards/sist/227a3148-4206-42e3-ad21-

### 05f80dda507a/iec-fdis-81001-5-1

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.

<sup>&</sup>lt;sup>1</sup> Numbers in square brackets refer to the Bibliography.

- 8 -

IEC FDIS 81001-5-1 © IEC 2021

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.

IEC FDIS 81001-5-1 © IEC 2021 - 9 -

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.

# iTeh STANDARD PREVIEW (standards.iteh.ai)

IEC/FDIS 81001-5-1 https://standards.iteh.ai/catalog/standards/sist/227a3148-4206-42e3-ad21-05f80dda507a/iec-fdis-81001-5-1 – 10 –

IEC FDIS 81001-5-1 © IEC 2021

# 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.

IEC FDIS 81001-5-1 © IEC 2021 - 11 -

# 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

# (standards.iteh.ai)

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

#### IEC/FDIS 81001-5-1

05f80dda507a/iec-fdis-81001-5-1

3.4 https://standards.iteh.ai/catalog/standards/sist/227a3148-4206-42e3-ad21-

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  $\ensuremath{\mathsf{ASSET}}$ 

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

- 12 -

IEC FDIS 81001-5-1 © IEC 2021

# 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

iTeh STANDARD PREVIEW [SOURCE: IEC 62304:2006[8], 3.5]

# 3.10

# **CONFIGURATION MANAGEMENT**

IEC/FDIS 81001-5-1 PROCESS ensuring consistency of CONFIGURATION JTEMS by using mechanisms for identifying, controlling and tracking versions of CONFIGURATION ITEMS 5-1

(standards.iteh.ai)

# 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]

IEC FDIS 81001-5-1 © IEC 2021 - 13 -

# 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] (standards.iteh.ai)

# 3.16

# HEALTHCARE DELIVERY ORGANIZATION IEC/FDIS 81001-5-1

HDO https://standards.iteh.ai/catalog/standards/sist/227a3148-4206-42e3-ad21facility or enterprise such as a clinic of 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  $\ensuremath{\mathsf{HEALTH}}$  SOFTWARE – as specified by the  $\ensuremath{\mathsf{MANUFACTURER}}$ 

### 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".]

IEC FDIS 81001-5-1 © IEC 2021

- 14 -

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

# (standards.iteh.ai)

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

https://standards.iteh.ai/catalog/standards/sist/227a3148-4206-42e3-ad21-

[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]