

INTERNATIONAL STANDARD

NORME INTERNATIONALE



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

**Logiciels de santé et sécurité, efficacité et sûreté des systèmes TI de santé –
Partie 5-1: Sûreté – Activités du cycle de vie du produit**

IEC 81001-5-1:2021

<https://standards.iteh.ai/catalog/standards/iso/227a3148-4206-42e3-ad21-05f80dda507a/iec-81001-5-1-2021>





THIS PUBLICATION IS COPYRIGHT PROTECTED
Copyright © 2021 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester. If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'IEC ou du Comité national de l'IEC du pays du demandeur. Si vous avez des questions sur le copyright de l'IEC ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de l'IEC de votre pays de résidence.

IEC Central Office
3, rue de Varembe
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 It also gives information on projects, replaced and withdrawn publications.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



**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](https://standards.iteh.ai/catalog/standards/iso/227a3148-4206-42e3-ad21-05f80dda507a/iec-81001-5-1-2021)

<https://standards.iteh.ai/catalog/standards/iso/227a3148-4206-42e3-ad21-05f80dda507a/iec-81001-5-1-2021>

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 11.040.01; 35.240.80

ISBN 978-2-8322-1053-7

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

CONTENTS

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

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

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

INTERNATIONAL ELECTROTECHNICAL COMMISSION

**HEALTH SOFTWARE AND HEALTH IT SYSTEMS SAFETY,
EFFECTIVENESS AND SECURITY –****Part 5-1: Security –
Activities in the product life cycle**

FOREWORD

- 1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as “IEC Publication(s)”). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
- 2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
- 3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
- 4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
- 5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
- 6) All users should ensure that they have the latest edition of this publication.
- 7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
- 8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
- 9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 81001-5-1 has been prepared by a Joint Working Group of IEC subcommittee 62A: Common aspects of electrical equipment used in medical practice, of IEC technical committee 62: Electrical equipment in medical practice, and ISO technical committee 215: Health informatics.

It is published as a double logo standard.

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

Draft	Report on voting
62A/1458/FDIS	62A/1466/RVD

Full information on the voting for its approval can be found in the report on voting indicated in the above table.