

# IEC 81001-5-1:2021-12 (E/F)

## 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 logiciels de santé et des systèmes TI de santé - Partie 5-1: Sûreté - Activités du cycle de vie du produit

---

#### Contents

	Page
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
	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
	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
	Software CONFIGURATION MANAGEMENT PROCESS.....	32
	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

## SOMMAIRE

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

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

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

E.3 Documents relatifs à la mise hors service des LOGICIELS DE SANTÉ .....	108
Annexe F (normative) LOGICIEL DE SANTÉ TRANSITOIRE .....	109
F.1 Présentation .....	109
F.2 Activités d'évaluation du développement et de comblement des lacunes .....	109
F.3 Justification de l'utilisation des LOGICIELS DE SANTÉ TRANSITOIRES.....	110
F.4 ACTIVITÉS post-diffusion .....	110
Annexe G (normative) Identificateurs d'objet.....	111
Bibliographie.....	112
Figure 1 – Champ d'application des LOGICIELS DE SANTE.....	65
Figure 2 – PROCESSUS DU CYCLE DE VIE DES LOGICIELS DE SANTE .....	67
Tableau A.1 – Niveau d'indépendance exigé des contrôleurs par rapport aux développeurs .....	94
Tableau G.1 – Identificateurs d'objet pour les concepts de conformité du présent document.....	111