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).

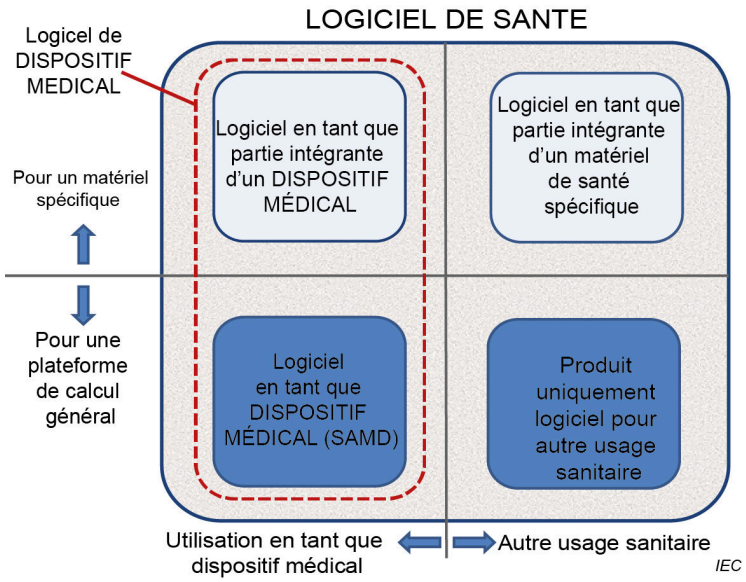
0.2 Champ d'application

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].

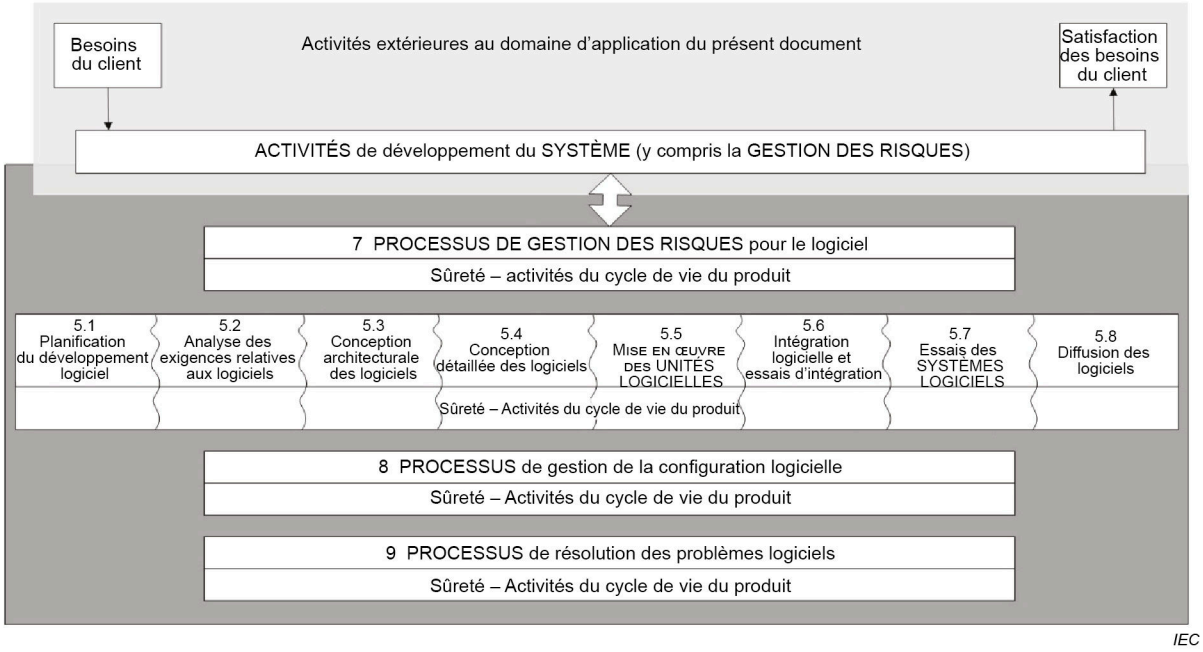
Les Articles 4 à 9 du présent document exigent l'établissement d'un ou plusieurs PROCESSUS comprenant des ACTIVITES identifiées. Selon les parties normatives du présent document, les PROCESSUS DU CYCLE DE VIE mettent en œuvre ces ACTIVITES. Aucune exigence définie dans le présent document n'impose la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