NORME INTERNATIONALE

INTERNATIONAL STANDARD

CEI
IEC
60601-1-4

1996

AMENDEMENT 1
AMENDMENT 1
1999-10

Amendement 1

Appareils électromédicaux –

Partie 1-4: Règles générales de sécurité – Norme collatérale: Systèmes électromédicaux programmables

Amendment 1

Medical electrical equipment –

Part 1-4: General requirements for safety – Collateral standard: Programmable electrical medical systems

International Electrotechnical Commission 3, rue de Varembé Geneva, Switzerland
Telefax: +41 22 919 0300 e-mail: inmail@iec.ch IEC web site http://www.iec.ch

Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

CODE PRIX
PRICE CODE H

Pour prix, voir catalogue en vigueur
For price, see current catalogue

AVANT-PROPOS

Le présent amendement a été établi par le comité d'études 62 de la CEI: Equipements électriques dans la pratique médicale.

Le texte de cet amendement est issu des documents suivants:

FDIS	Rapport de vote
62/114/FDIS	62/120/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à l'approbation de cet amendement.

_____

Page 2

SOMMAIRE

Remplacer le titre de l'annexe DDD par ce qui suit:

Page 8

INTRODUCTION

Remplacer le troisième tiret par ce qui suit:

– méthodes assurant la SÉCURITÉ;

Page 14

2.201.12 SÉCURITÉ ABSOLUE:

Remplacer cette définition par ce qui suit:

2.201.12 Non utilisé.

Page 16

6 Identification, marquage et documentation

6.8 DOCUMENTS D'ACCOMPAGNEMENT

Remplacer 6.8.201 par ce qui suit:

6.8.201 Toutes les informations importantes relatives au RISQUE RÉSIDUEL significatif, informations comprenant la description des DANGERS et les actions à entreprendre par L'OPÉRATEUR ou L'UTILISATEUR pour les éviter/les réduire, doivent être reportées à la fois dans les INSTRUCTIONS D'UTILISATION et dans le FICHIER DE GESTION DES RISQUES.

FOREWORD

This amendment has been prepared by IEC technical committee 62: Electrical equipment in medical practice.

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

FDIS	Report of voting
62/114/FDIS	62/120/RVD

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

_____

Page 3

CONTENTS

Replace title of annex DDD by the following:

Page 9

INTRODUCTION

Replace the third dash by the following:

– methods by which SAFETY is assured;

Page 15

2.201.12 SAFETY INTEGRITY:

Replace this definition by the following:

2.201.12 Not used.

Page 17

6 Identification, marking and documents

6.8 ACCOMPANYING DOCUMENTS

Replace 6.8.201 by the following:

6.8.201 All relevant information regarding significant RESIDUAL RISK including descriptions of the HAZARDS and any actions by the OPERATOR or the USER necessary to avoid/mitigate them shall be placed in both the INSTRUCTIONS FOR USE and the RISK MANAGEMENT FILE.

Ajouter le nouveau paragraphe 6.8.202 suivant:

6.8.202 LES DOCUMENTS D'ACCOMPAGNEMENT pour le SEMP doivent identifier, au minimum, le CONSTRUCTEUR et un unique identificateur tel que l'indice de révision et la date de mise en circulation/publication.

NOTE Les informations concernant tout ÉQUIPEMENT avec lequel un logiciel est destiné à être utilisé, ainsi que les moyens grâce auxquels le CONSTRUCTEUR peut être contacté, peuvent être donnés sur l'emballage ou dans les INSTRUCTIONS D'UTILISATION de telle façon qu'ils soient disponibles pour L'UTILISATEUR indépendamment de l'usage du logiciel.

52 Fonctionnement anormal et conditions de défaut

52.201.3c)

Remplacer 52.201.3 c) par ce qui suit:

c) référence aux mesures de SÉCURITÉ utilisées pour éliminer ou maîtriser le RISQUE de DANGER;

Page 18

Figure 201

Modifier la case «Méthodes et résultats de la VALIDATION 52.210.6» *en* «Méthodes et résultats de la VALIDATION 52.210.7».

Correction ne concernant que le texte anglais.

Modifier, en bas à droite de la figure, le texte «Méthodes et résultats de la VÉRIFICATION 52.209.3» *en* «Méthodes, techniques et résultats de la VÉRIFICATION 52.209.4».

Page 20

52.203 CYCLE DE DÉVELOPPEMENT

Ajouter le nouveau paragraphe 52.203.6 suivant:

52.203.6 Le cas échéant, un système défini pour la résolution des problèmes pendant et entre toutes les phases et tâches du CYCLE DE DÉVELOPPEMENT doit être développé et maintenu en tant qu'une partie du FICHIER DE GESTION DES RISQUES. Selon le problème, le système peut avoir les caractéristiques suivantes:

– être défini en tant que partie du CYCLE DE DÉVELOPPEMENT;
– permettre de rendre compte de problèmes potentiels ou existants de SÉCURITÉ;
– inclure une évaluation de chaque problème pour les RISQUES associés;
– identifier les critères (SÉCURITÉ et/ou performance) à satisfaire pour prononcer une conclusion;
– identifier les actions à entreprendre pour résoudre chaque problème;
– identifier les méthodes de VALIDATION pour chaque action;
– identifier les mesures prises pour vérifier, de façon continue, la conformité.

Add the following new subclause 6.8.202:

6.8.202 ACCOMPANYING DOCUMENTS for the PEMS shall identify, as a minimum, the MANUFACTURER and a unique identifier such as revision level and date of release/issue.

NOTE Information pertaining to any specific EQUIPMENT that software is intended to be used in conjunction with, and a means by which the MANUFACTURER can be contacted, can be located on the package or in the INSTRUCTIONS FOR USE so that it is available to the USER independently of the software operation.

52 Abnormal operation and fault conditions

52.201.3c)

Replace 52.201.3 c) by the following:

c) reference to the SAFETY measures, used to eliminate or control the RISK of the HAZARD;

Page 19

Figure 201

Amend the box "VALIDATION methods and results 52.210.6" *to* "VALIDATION methods and results 52.210.7".

Amend the box "VERIFICATION plan 52.210.2" *to* "VALIDATION plan 52.210.2".

Amend, within the lower right-hand corner of the figure, the text "VERIFICATION methods and results 52.209.3" *to* "Methods, techniques and results of the VERIFICATION 52.209.4".

Page 21

52.203 DEVELOPMENT LIFE-CYCLE

Add the following new subclause 52.203.6:

52.203.6 Where appropriate, a defined system for problem resolution within and between all phases and tasks of the DEVELOPMENT LIFE CYCLE shall be developed and maintained as part of the RISK MANAGEMENT FILE. Depending upon the problem, the system may have the following characteristics:

– be defined as a part of the DEVELOPMENT LIFE-CYCLE;
– allow the reporting of potential or existing SAFETY and/or performance problems;
– include an assessment of each problem for associated RISKS;
– identify the criteria (SAFETY and/or performance) that have to be met for the issue to be closed;
– identify the action to be taken to resolve each problem;
– identify VALIDATION methods for each action;
– identify the steps taken for VERIFICATION of continuing compliance.

Page 20

52.204.3.1 ANALYSE DES DANGERS

Remplacer à la page 22, dans le paragraphe 52.204.3.1.5, le premier tiret par le suivant:

– les facteurs humains, y compris les servitudes ergonomiques;

Page 24

52.204.4 Maîtrise des RISQUES

Ajouter au paragraphe 52.204.4.3 la nouvelle phrase suivante:

La probabilité pour que les mesures prises pour réduire les RISQUES soient efficaces doit être spécifiée quantitativement ou qualitativement; voir annexe CCC.

52.206 Spécification des prescriptions

Remplacer 52.206.3 par le nouveau paragraphe 52.206.3 suivant:

52.206.3 La spécification des prescriptions doit contenir les informations utiles en vue de s'assurer que les mesures prises pour la maîtrise des RISQUES réduisent de façon satisfaisante les RISQUES identifiés.

Page 26

52.207 Architecture

Remplacer 52.207.3 par le nouveau paragraphe 52.207.3 suivant:

52.207.3 Le cas échéant, la spécification de l'architecture d'un SEMP et de ses sous-systèmes doit aborder les prescriptions de la MAÎTRISE DU RISQUE par la diminution de la probabilité correspondante du DANGER ou par la diminution de la SÉVÉRITÉ des conséquences du DANGER ou les deux.

Ajouter les nouveaux paragraphes 52.207.4 et 52.207.5 suivants:

52.207.4 Le cas échéant, pour diminuer la probabilité des DANGERS, la spécification de l'architecture doit recommander d'utiliser ce qui suit:

a) des composants hautement fiables;
b) des fonctions à sécurité positive;
c) la redondance;
d) la diversité;
e) une conception défensive;
f) des limitations de conséquences potentiellement dangereuses, par exemple en réduisant la puissance de sortie et/ou en introduisant des moyens de limiter le déplacement pour les organes de manoeuvres.

Page 21

52.204.3.1 HAZARD ANALYSIS

Replace on page 23, in subclause 52.204.3.1.5, the first dash by the following:

– human factors including ergonomic limitations;

Page 25

52.204.4 RISK control

Add, in subclause 52.204.4.3, the following new sentence:

The likelihood that the means for RISK reduction will perform correctly shall be specified quantitatively or qualitatively; see annex CCC.

52.206 Requirement specification

Replace 52.206.3 by the following new subclause 52.206.3:

52.206.3 The requirement specification shall include the information necessary to assure that RISK control measures satisfactorily reduce the identified RISKS.

Page 27

52.207 Architecture

Replace 52.207.3 by the following new subclause 52.207.3:

52.207.3 Where appropriate, the architecture specification of a PEMS and its subsystems shall address the RISK CONTROL requirements by reducing the corresponding likelihood of the HAZARD or by reducing the SEVERITY of the HAZARD or both.

Add the following new subclauses 52.207.4 and 52.207.5:

52.207.4 Where appropriate, to reduce the likelihood of the HAZARD, the architecture specification shall make use of:

a) highly reliable components;

b) fail-safe functions;

c) redundancy;

d) diversity;

e) defensive design;

f) limits on potentially hazardous effects, for example by restricting the available output power and/or by introducing means to limit the travel of actuators.

52.207.5 La spécification de l'architecture doit prendre en compte ce qui suit:

a) l'allocation des mesures de la maîtrise des RISQUES aux sous-systèmes et aux éléments du SEMP.

NOTE Les sous-systèmes et les éléments comprennent les capteurs, les dispositifs de commande, le SSEP et les interfaces.

b) les types de pannes et leurs conséquences;

c) les pannes ayant les mêmes causes;

d) les pannes systématiques;

e) l'intervalle de temps entre les essais, la durée des essais et la couverture du diagnostic;

f) la maintenabilité;

g) la protection contre les erreurs humaines intentionnelles ou non.

52.208 Conception et réalisation

Remplacer 52.208.2 par le nouveau paragraphe 52.208.2 suivant:

52.208.2 Les données descriptives pour l'environnement de la conception doivent être comprises dans le FICHIER DE GESTION DES RISQUES.

NOTE Voir en annexe DDD des exemples d'éléments d'environnement de la conception.

52.209 VÉRIFICATION

Remplacer 52.209.2 par le nouveau paragraphe 52.209.2 suivant:

52.209.2 Un plan de VÉRIFICATION doit être établi pour indiquer comment les prescriptions de SÉCURITÉ sont vérifiées à chaque phase du CYCLE DE DÉVELOPPEMENT. Ce plan doit comprendre

a) le choix et la documentation des stratégies, activités et techniques de VÉRIFICATION;

b) la sélection et l'utilisation des outils de VÉRIFICATION;

c) les critères de couverture pour la VÉRIFICATION.

NOTE Méthodes et techniques sont par exemple

– lectures croisées et examens;
– analyses statiques/dynamiques;
– essais boîte blanche/boîte noire.

Supprimer le paragraphe 52.209.3 et ajouter les nouveaux paragraphes 52.209.3 et 52.209.4 suivants:

52.209.3 La VÉRIFICATION doit être conduite conformément au plan de VÉRIFICATION. Les résultats des activités de VÉRIFICATION doivent être documentés, analysés et évalués.

52.209.4 Une référence aux méthodes, techniques et résultats de la VÉRIFICATION doit figurer dans le RELEVÉ DE GESTION DES RISQUES.

52.210 VALIDATION

Changer le paragraphe 52.210.1 comme suit:

La VALIDATION de la SÉCURITÉ des SEMP doit être faite dans les conditions d'usage prévues.

52.207.5 The architecture specification shall take the following into consideration:

a) allocation of RISK control measures to subsystems and components of the PEMS;

NOTE Subsystems and components include sensors, actuators, PESS and interfaces.

b) failure modes of components and their effects;

c) common cause failures;

d) systematic failures;

e) test interval, test duration and diagnostic coverage;

f) maintainability;

g) protection from human intentional or unintentional causes.

52.208 Design and implementation

Replace 52.208.2 by the following new subclause 52.208.2:

52.208.2 Descriptive data regarding the design environment shall be included in the RISK MANAGEMENT FILE.

NOTE See annex DDD for examples of design environment elements.

52.209 VERIFICATION

Replace 52.209.2 by the following new subclause 52.208.2:

52.209.2 A VERIFICATION plan shall be produced to show how the SAFETY requirements for each DEVELOPMENT LIFE-CYCLE phase will be verified. The plan shall include

a) the selection and documentation of VERIFICATION strategies, activities and techniques;

b) the selection and utilization of VERIFICATION tools;

c) coverage criteria for VERIFICATION.

NOTE Examples of methods and techniques are

– walkthroughs and inspections;
– static/dynamic analyses;
– white/black box testing.

Delete former subclause 52.209.3 and add the following new subclauses 52.209.3 and 52.209.4:

52.209.3 The VERIFICATION shall be performed according to the VERIFICATION plan. The results of the VERIFICATION activities shall be documented, analyzed and assessed.

52.209.4 A reference to the methods, techniques and results of the VERIFICATION shall be included in the RISK MANAGEMENT SUMMARY.

52.210 VALIDATION

Replace 52.210.1 by the following:

VALIDATION of the SAFETY of PEMS under the conditions of the intended use shall be carried out.

Page 28

Insérer le nouveau paragraphe 52.210.3 comme suit:

52.210.3 La VALIDATION doit être conduite conformément au plan de VALIDATION. Les résultats des activités de VALIDATION doivent être documentés, analysés et évalués.

Renuméroter les paragraphes 52.210.3 en 52.210.4, 52.210.4 en 52.210.5, 52.210.5 en 52.210.6 avec le nouveau texte suivant:

52.210.6 L'équipe de conception ne doit pas être entièrement responsable de la VALIDATION de son propre produit.

Renuméroter l'ancien paragraphe 52.210.6 en 52.210.7.

Page 30

Annexe AAA

Supprimer la ligne suivante:

SÉCURITÉ ABSOLUE 2.201.12

Page 32

Annexe BBB

Ajouter, entre Terminologie et Définitions *et* Documentation, *le nouveau texte suivant:*

Identification, marquage et documentation

La prescription pour l'identification du SEMP est destinée à s'assurer que les UTILISATEURS ne peuvent utiliser par mégarde un mauvais logiciel ou une version obsolète de logiciel. L'information sur le RISQUE RÉSIDUEL est incluse, car il n'est pas toujours possible, ou pratique, d'éliminer tous les DANGERS. Dans ce cas, la responsabilité minimale du CONSTRUCTEUR est de prévenir les UTILISATEURS de ces DANGERS et de fournir les informations qui peuvent aider à les éviter/les minimiser.

CYCLE DE DEVELOPPEMENT

Ajouter les nouvelles phrases suivantes:

Un système défini est exigé pour la résolution des problèmes car les approches particulières peuvent générer leurs propres problèmes. Les problèmes envisagés comprennent des éléments tels que prescriptions contradictoires ou ambiguës, spécifications manquantes et «bugs» apparus lors des évaluations.

Traitement de la gestion des RISQUES

Ajouter, après la première phrase, la nouvelle phrase suivante:

La conception de base est la suivante: plus grand est le RISQUE prévisible, plus l'analyse est rigoureuse et plus grande est l'intégrité des mesures de maîtrise du RISQUE.

Page 29

Insert a new subclause 52.210.3 as follows:

52.210.3 The VALIDATION shall be performed according to the VALIDATION plan. The results of VALIDATION activities shall be documented, analyzed and assessed.

Renumber subclauses 52.210.3 to 52.210.4, 52.210.4 to 52.210.5, 52.210.5 to 52.210.6 with the following new text:

52.210.6 No member of a design team shall be responsible for the VALIDATION of his own design.

Renumber former subclause 52.210.6 to 52.210.7.

Page 31

Annex AAA

Delete the following line:

SAFETY INTEGRITY 2.201.12

Page 33

Annex BBB

Add between Terminology and definitions *and* Documentation *the following new text:*

Identification, marking and documents

The requirement to identify the PEMS is intended to ensure that USERS do not inadvertently use the wrong software or an obsolete version of the software. Information on RESIDUAL RISK is included, because it may not be possible or practical to eliminate all HAZARDS. Where this is the case, it is the MANUFACTURER'S minimum responsibility to make the USERS aware of those HAZARDS and provide information that may help avoid/mitigate them.

DEVELOPMENT LIFE-CYCLE

Add the following new sentences:

A defined system for problem resolution is required because ad hoc approaches can bring problems of their own. Anticipated problems include such things as inconsistent or ambiguous requirements, missing specifications and "bugs" found during evaluations.

RISK management process

Add, after the first sentence, the following new sentence:

The basic concept is that the greater the foreseeable RISK, the more rigorous the analysis and the greater the integrity of the RISK control measures are.

Page 36

Annexe CCC

Remplacer, aux pages 44 et 46, les textes de «SÉCURITÉ ABSOLUE», «Intégrité du matériel» et «Intégrité systématique» par ce qui suit:

Probabilité pour un fonctionnement correct

Le paragraphe 52.204.4.3 prescrit que la probabilité doit être spécifiée quantitativement ou qualitativement. Ci-dessous sont donnés des conseils pour ce faire.

Probabilité quantitative

Si la probabilité de défaillance peut être calculée ou démontrée (par exemple un calcul basé sur une panne aléatoire pour un système électronique du matériel), cette valeur peut être utilisée pour spécifier la probabilité d'un fonctionnement correct. Typiquement celle-ci peut être exprimée en temps moyen entre défaillances ou comme une probabilité de défaillance.

Probabilité qualitative

Si les défaillances sont systématiques, comme dans le cas d'un logiciel, il est souvent impossible de démontrer ou calculer une probabilité de défaillance. Si c'est le cas, une méthode qualitative peut être utilisée pour spécifier et vérifier la probabilité.

Cette norme ne prescrit aucune méthode particulière pour déterminer une mesure qualitative de la probabilité pour les défaillances systématiques. L'approche décrite est donnée à titre d'information.

Cette approche est basée sur l'idée que plus les processus utilisés pour créer un SSEP sont rigoureux et de bonne qualité, plus il y a de chances pour que celui-ci assure les fonctions prévues. De tels processus comprennent ce qui suit:

– techniques et méthodes de développement;
– sélection de l'architecture;
– assurance de la qualité;
– gestion de projet.

Avec les technologies les plus répandues il n'y a pas de moyen absolu de déterminer les processus adaptés à chaque cas particulier. Il est recommandé pour les utilisateurs de la norme de faire appel à leur jugement, basé sur ce qui est raisonnablement faisable et prenant en compte les principes ALARP.

Des indications supplémentaires pour la détermination de la relation entre processus utilisés et probabilité attendue de réduction des risques pour le logiciel peuvent être trouvées dans les références [5] et [7] de l'annexe FFF. Dans la référence [5], l'expression «sécurité absolue» est utilisée pour spécifier la probabilité que le SSEP assure les fonctions prévues.