SLOVENSKI PREDSTANDARD

oSIST prEN 62304:2005

februar 2005

Programska oprema za medicinske aparate – Procesi v življenjskem ciklu programske opreme

Medical device software - Software life-cycle processes

ICS 13.020.60; 35.240.80

Referenčna številka
oSIST prEN 62304:2005(en)

62A/474/CDV

COMMITTEE DRAFT FOR VOTE (CDV)
PROJET DE COMITÉ POUR VOTE (CDV)

	Project number / Numéro de projet: IEC 62304 Ed. 1.0	
IEC/TC or SC: **62A** / CEI/CE ou SC:	Date of circulation / Date de diffusion: **2004-12-03**	Closing date for voting (Voting mandatory for P-members) / Date de clôture du vote (Vote obligatoire pour les membres (P)): **2005-05-06**
Titre du CE/SC: Aspects généraux des équipments utilisés en pratique médicale	TC/SC Title: Common aspects of electrical medical equipment used in medical practice	
Secretary: USA / Secrétaire:		
Also of interest to the following committees / Intéresse également les comités suivants: TC 62, SC 62B/C/D, TC 66, ISO/TC 106/SC 6, ISO/TC 121/SC 3, ISO/TC 150/SC 6, ISO/TC 210, CENELEC TC 62	Supersedes document / Remplace le document: 62A/446/CD and 62A/456A/CC	

Functions concerned / Fonctions concernées

- ☒ Safety / Sécurité
- ☐ EMC / CEM
- ☐ Environment / Environnement
- ☐ Quality assurance / Assurance qualité

CE DOCUMENT EST TOUJOURS À L'ÉTUDE ET SUSCEPTIBLE DE MODIFICATION. IL NE PEUT SERVIR DE RÉFÉRENCE.

LES RÉCIPIENDAIRES DU PRÉSENT DOCUMENT SONT INVITÉS À PRÉSENTER, AVEC LEURS OBSERVATIONS, LA NOTIFICATION DES DROITS DE PROPRIÉTÉ DONT ILS AURAIENT ÉVENTUELLEMENT CONNAISSANCE ET À FOURNIR UNE DOCUMENTATION EXPLICATIVE.

THIS DOCUMENT IS STILL UNDER STUDY AND SUBJECT TO CHANGE. IT SHOULD NOT BE USED FOR REFERENCE PURPOSES.

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

Titre :

Logiciels de dispositifs médicaux - Processus du cycle de vie du logiciel

Title :

Medical device software – Software life-cycle processes

Note d'introduction

Introductory note

This Committee Draft for Vote was developed by IEC/SC 62A – ISO/TC 210 JWG 3 and is being circulated in both committees for comment.

Please note the line number of the text that your comment addresses and include this as the first line in the column headed "Paragraph/Figure/ Table" in the comment form.

ATTENTION	ATTENTION
CDV soumis en parallèle au vote (CEI) et à l'enquête (CENELEC)	Parallel IEC CDV/CENELEC Enquiry

CONTENTS

FIGURES

TABLES

INTERNATIONAL ELECTROTECHNICAL COMMISSION

Medical device software – Software life-cycle processes

Foreword

1) The IEC (International Electrotechnical Commission) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of the 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, the IEC publishes International Standards. 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. The 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 the 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 National Committees.

3) The documents produced have the form of recommendations for international use and are published in the form of standards, technical specifications, technical reports or guides and they are accepted by the National Committees in that sense.

4) In order to promote international unification, IEC National Committees undertake to apply IEC International Standards transparently to the maximum extent possible in their national and regional standards. Any divergence between the IEC Standard and the corresponding national or regional standard shall be clearly indicated in the latter.

5) The IEC provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with one of its standards.

6) Attention is drawn to the possibility that some of the elements of this International Standard may be the subject of patent rights. The IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 62304 has been prepared by a joint working group of 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 210, *Quality management and corresponding general aspects for* MEDICAL DEVICES.

It is published as a dual logo standard.

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

FDIS	Report on voting
XX/XX/FDIS	XX/XX/RVD

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

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

In this standard the following print types are used:

- Requirements and definitions: in 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 USED THROUGHOUT THIS STANDARD THAT HAVE BEEN DEFINED IN CLAUSE 3 AND ALSO GIVEN IN THE INDEX: IN SMALL CAPITALS.

An asterisk (*) as the first character of a title or at the beginning of a paragraph indicates that there is guidance related to that item in Annex B.

The committee has decided that the contents of this publication will remain unchanged until _____. At this date, the publication will be

- reconfirmed;
- withdrawn;
- replaced by a revised edition, or
- amended.

Annexes A to D of this International Standard are for information only.

Introduction

Software is often an integral part of MEDICAL DEVICE technology. Establishing the SAFETY and effectiveness of a MEDICAL DEVICE containing software requires knowledge of what the software is intended to do and demonstration that the use of the software fulfils those intentions without causing any unacceptable RISKS.

This standard provides a framework of life-cycle PROCESSES with ACTIVITIES and TASKS necessary for the safe design and maintenance of MEDICAL DEVICE SOFTWARE. This standard provides requirements for each life-cycle PROCESS. Each life-cycle PROCESS is further divided into a set of ACTIVITIES, with most ACTIVITIES further divided into a set of TASKS.

As a basic foundation it is assumed that MEDICAL DEVICE SOFTWARE is developed and maintained within a quality management system (see 4.1) and a RISK MANAGEMENT system (see 4.2). The RISK MANAGEMENT PROCESS is already very well addressed by the International Standard ISO 14971. Therefore IEC 62304 makes use of this advantage simply by a normative reference to ISO 14971. Some minor additional RISK MANAGEMENT requirements are needed for software, especially in the area of identification of contributing software factors related to HAZARDS. These requirements are summarized and captured in Clause 7 as the software RISK MANAGEMENT PROCESS.

Whether software is a contributing factor to a HAZARD is determined during the HAZARD identification ACTIVITY of the RISK MANAGEMENT PROCESS. HAZARDS that could be indirectly caused by software (for example, by providing misleading information that could cause inappropriate treatment to be administered) need to be considered when determining whether software is a contributing factor. The decision to use software to control RISK is made during the RISK CONTROL ACTIVITY of the RISK MANAGEMENT PROCESS. The software RISK MANAGEMENT PROCESS required in this standard has to be embedded in the device RISK MANAGEMENT PROCESS according to ISO 14971.

The software development PROCESS consists of a number of ACTIVITIES. These ACTIVITIES are shown in Figure 1 and described in Clause 5. Because many incidents in the field are related to service or maintenance of MEDICAL DEVICE SYSTEMS including inappropriate software updates and upgrades, the software maintenance PROCESS is considered to be as important as the software development PROCESS. The software maintenance PROCESS is very similar to the software development PROCESS. It is shown in Figure 2 and described in Clause 6.

This standard identifies two additional PROCESSES considered essential for developing safe MEDICAL DEVICE SOFTWARE. They are the software configuration management PROCESS (Clause 8) and the software problem resolution PROCESS (Clause 9).

This standard does not specify an organizational structure for the MANUFACTURER or which part of the organization is to perform which PROCESS, ACTIVITY, or TASK. This standard requires only that the PROCESS, ACTIVITY, or TASK be completed to establish compliance with this standard.

This standard does not prescribe the name, format, or explicit content of the documentation to be produced. This standard requires documentation of TASKS, but the decision of how to package this documentation is left to the user of the standard.

This standard does not prescribe a specific life-cycle model. The users of this standard are responsible for selecting a life-cycle model for the software project and for mapping the PROCESSES, ACTIVITIES, and TASKS in this standard onto that model.

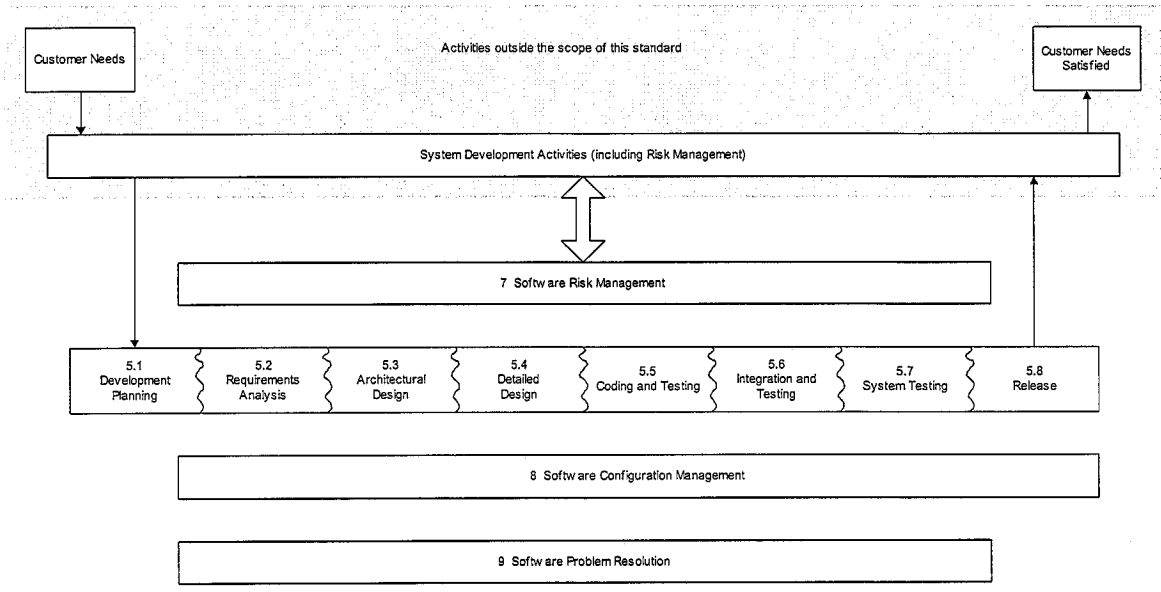

Figure 1 – Overview of software development PROCESSES and ACTIVITIES

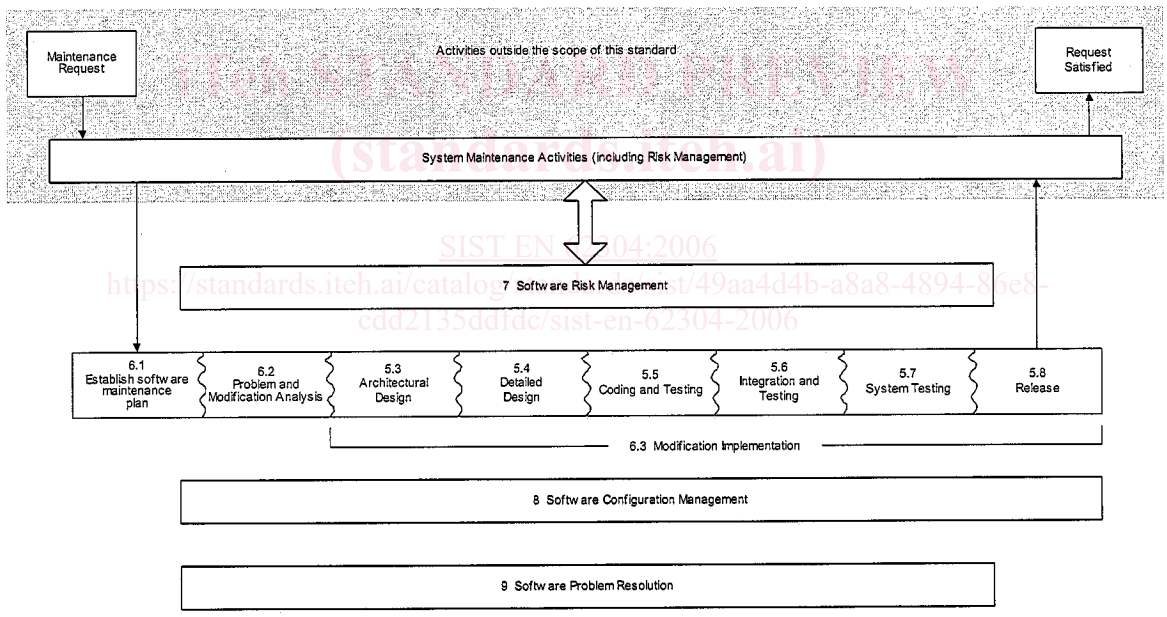

Figure 2 – Overview of software maintenance PROCESSES and ACTIVITIES

Annex A provides rationale for the clauses of this standard. Annex B provides guidance on the provisions of this standard.

For the purposes of this standard:

- "shall" means that compliance with a requirement is mandatory for compliance with this standard;
- "should" means that compliance with a requirement is recommended but is not mandatory for compliance with this standard;
- "may" is used to describe a permissible way to achieve compliance with a requirement;
- "establish" means to define, document, and implement; and

54 – Where this standard uses the term "as appropriate" in conjunction with a required PROCESS,
55 ACTIVITY, TASK or output, the intention is that the MANUFACTURER shall use the PROCESS, ACTIVITY,
56 TASK or output unless the MANUFACTURER can document a justification for not so doing.

INTERNATIONAL ELECTROTECHNICAL COMMISSION

MEDICAL DEVICE SOFTWARE – SOFTWARE LIFE-CYCLE PROCESSES

1 Scope

1.1 * Purpose

This standard defines the life-cycle requirements for MEDICAL DEVICE SOFTWARE. The set of PROCESSES, ACTIVITIES, and TASKS described in this standard establishes a common framework for MEDICAL DEVICE SOFTWARE life-cycle PROCESSES.

1.2 * Field of application

This standard applies to the development and maintenance of MEDICAL DEVICE SOFTWARE.

This standard may be used when software is itself a MEDICAL DEVICE or when software is an embedded or integral part of the final MEDICAL DEVICE.

1.3 Relationship to other standards

The scope of this standard is the MEDICAL DEVICE SOFTWARE. This standard is to be used together with other appropriate standards when developing a MEDICAL DEVICE. Annex C shows the relationship between this standard and other relevant standards.

1.4 Compliance

Compliance with this standard is defined as implementing all of the PROCESSES, ACTIVITIES, and TASKS identified in this standard in accordance with the software safety class of the SOFTWARE ITEM.

Compliance is determined by inspection of the RISK MANAGEMENT FILE, and assessment of the PROCESSES, ACTIVITIES and TASKS required for the software safety class. See Annex D.

NOTE 1 This assessment could be carried out by internal or external audit.

NOTE 2 Although the specified PROCESSES, ACTIVITIES, and TASKS are performed, flexibility exists in the methods of implementing these PROCESSES and performing these ACTIVITIES and TASKS.

NOTE 3 Where any requirements contain "as appropriate" and were not performed, documentation for the justification is necessary for this assessment.

2 * Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 13485:2003, *Medical devices – Quality management systems – Requirements for regulatory purposes.*

ISO 14971:2000, *Medical devices – Risk management – Application of risk management to medical devices.*

3 * Definitions

3.1
ACTIVITY
a set of one or more interrelated or interacting TASKS

3.2
ANOMALY
Any condition that deviates from the expected based on requirements specifications, design documents, standards, etc. or from someone's perceptions or experiences. ANOMALIES may be found during, but not limited to, the review, text, analysis, compilation, or use of SOFTWARE PRODUCTS or applicable documentation.

[IEEE 1064.1:1995]

3.3
ARCHITECTURE
organizational structure of a SYSTEM or component

[IEEE 610.12:1990]

3.4
CHANGE SPECIFICATION
a documented specification of a change to be made to a SOFTWARE PRODUCT.

3.5
CONFIGURATION ITEM
entity within a configuration that can be uniquely identified at a given reference point

3.6
DELIVERABLE
required result or output (includes documentation) of an ACTIVITY or TASK

3.7
HARM
physical injury, damage, or both to the health of people or damage to property or to the environment

[ISO/IEC Guide 51:1999]

3.8
HAZARD
potential source of HARM

[ISO/IEC Guide 51:1999]

3.9
MANUFACTURER
natural or legal person with responsibility for designing, manufacturing, packaging, or labelling a MEDICAL DEVICE; assembling a SYSTEM; or adapting a MEDICAL DEVICE before it is placed on the market and/or put into service, regardless of whether these operations are carried out by that person or by a third party on that person's behalf

[ISO 14971:2000]

3.10
MEDICAL DEVICE
any instrument, apparatus, implement, machine, appliance, implant, in vitro reagent or calibrator, software, material or other similar or related article, intended by the MANUFACTURER to be used, alone or in combination, for human beings for one or more of the specific purpose(s) of

- diagnosis, prevention, monitoring, treatment or alleviation of disease,
- diagnosis, monitoring, treatment, alleviation of or compensation for an injury,
- investigation, replacement, modification, or support of the anatomy or of a physiological PROCESS,
- supporting or sustaining life,
- control of conception,
- disinfection of medical devices,
- providing information for medical purposes by means of in vitro examination of specimens derived from the human body,

and which does not achieve its primary intended action in or on the human body by pharmacological, immunological or metabolic means, but which may be assisted in its function by such means

NOTE 1 This definition has been developed by the Global Harmonization Task Force (GHTF). See bibliographic reference [15] (in ISO 13485:2003).

[ISO 13485:2003]

NOTE 2 Some differences can occur in the definitions used in regulations of each country.

3.11
MEDICAL DEVICE SOFTWARE
SOFTWARE SYSTEM that has been developed for the purpose of being incorporated into the MEDICAL DEVICE being developed or that is intended for use as a MEDICAL DEVICE in its own right.

3.12
MODIFICATION REQUEST
A proposal for SOFTWARE PRODUCT improvement or enhancement from a user or other interested person.

NOTE 1 This standard does not require that every MODIFICATION REQUEST results in a change to the SOFTWARE PRODUCT. A MANUFACTURER can reject a MODIFICATION REQUEST.

NOTE 2 A MODIFICATION REQUEST can relate to a released SOFTWARE PRODUCT or to a SOFTWARE PRODUCT that is still under development.

NOTE 3 This standard requires the MANUFACTURER to perform extra decision making steps (see Clause 6) for a MODIFICATION REQUEST relating to a released product to ensure that regulatory actions are identified and implemented.

3.13
PROBLEM REPORT
a record of actual or potential behaviour of a SOFTWARE PRODUCT that a user or other interested person believes to be unsafe, inappropriate for the intended use or contrary to specification

NOTE 1 This standard does not require that every PROBLEM REPORT results in a change to the SOFTWARE PRODUCT. A MANUFACTURER can reject a PROBLEM REPORT as a misunderstanding, error or insignificant event.

NOTE 2 A PROBLEM REPORT can relate to a released SOFTWARE PRODUCT or to a SOFTWARE PRODUCT that is still under development.

NOTE 3 This standard requires the MANUFACTURER to perform extra decision making steps (see Clause 6) for a PROBLEM REPORT relating to a released product to ensure that regulatory actions are identified and implemented.

3.14
PROCESS
a set of interrelated or interacting ACTIVITIES that transform inputs into outputs

NOTE The term "ACTIVITIES" covers use of resources.

[ISO 9000:2000]

3.15
RISK
combination of the probability of occurrence of HARM and the severity of that HARM

[ISO/IEC Guide 51:1999]

3.16
RISK ANALYSIS
systematic use of available information to identify HAZARDS and to estimate the RISK

[ISO/IEC Guide 51:1999]

3.17
RISK CONTROL
PROCESS in which decisions are made and RISKS are reduced to, or maintained within, specified levels

[ISO 14971:2000]

3.18
RISK MANAGEMENT
systematic application of management policies, procedures, and practices to the TASKS of analyzing, evaluating, and controlling RISK

[ISO 14971:2000]

3.19
RISK MANAGEMENT FILE
set of records and other documents, not necessarily contiguous, that are produced by a RISK MANAGEMENT PROCESS

[ISO 14971:2000]

3.20
SAFETY
freedom from unacceptable RISK

[ISO/IEC Guide 51:1999]

3.21
SECURITY
protection of information and data so that unauthorized people or SYSTEMS cannot read or modify them and so that authorized persons or SYSTEMS are not denied access to them

[ISO/IEC 12207:1995]

3.22
SERIOUS INJURY
injury or illness that:

a) is life threatening,

b) results in permanent impairment of a body function or permanent damage to a body structure, or

c) necessitates medical or surgical intervention to prevent permanent impairment of a body function or permanent damage to a body structure

NOTE Permanent impairment means an irreversible impairment or damage to a body structure or function excluding trivial impairment or damage.

3.23
SOFTWARE PRODUCT
set of computer programs, procedures, and possibly associated documentation and data

[ISO/IEC 12207:1995]

3.24
SOFTWARE ITEM
any identifiable part of a computer program

[ISO/IEC 90003:2003]

NOTE Three terms identify the software decomposition. The top level is the SOFTWARE SYSTEM. The lowest level that is not further decomposed is the SOFTWARE UNIT. All levels of composition, including the top and bottom levels, can be called SOFTWARE ITEMS. A SOFTWARE SYSTEM, then, is composed of one or more SOFTWARE ITEMS, and each SOFTWARE ITEM is composed of one or more SOFTWARE UNITS or decomposable SOFTWARE ITEMS. The responsibility is left to the MANUFACTURER to provide the definition and granularity of the SOFTWARE ITEMS and SOFTWARE UNITS. Leaving these terms vague allows one to apply them to the many different development methods and types of software used in MEDICAL DEVICES.

3.25
SOFTWARE DEVELOPMENT LIFE-CYCLE MODEL
framework containing the PROCESSES, ACTIVITIES, and TASKS involved in the development of a SOFTWARE PRODUCT, spanning the life of the software from the definition of its requirements to its release for manufacturing

NOTE The framework:

- identifies the PROCESSES to be used;
- describes the sequence of, and dependency between, ACTIVITIES and TASKS; and
- identifies milestones at which the completeness of specified DELIVERABLES is VERIFIED.

3.26
SOFTWARE SYSTEM
integrated collection of SOFTWARE ITEMS organized to accomplish a specific function or set of functions

3.27
SOFTWARE UNIT
SOFTWARE ITEM that is not subdivided into other items

NOTE SOFTWARE UNITS can be used for the purpose of software configuration management or testing.

3.28
SOUP
Software Of Unknown Provenance
SOFTWARE ITEM that has not been developed for the purpose of being incorporated into the MEDICAL DEVICE being developed and for which the development PROCESS is not known

NOTE This can be a SOFTWARE ITEM that is already developed and generally available and that has not been developed for the purpose of being incorporated into the MEDICAL DEVICE (which can be called off-the-shelf software) or it can be legacy software previously developed for another MEDICAL DEVICE.

3.29
SYSTEM
integrated composite consisting of one or more of the PROCESSES, hardware, software, facilities, and people that provides a capability to satisfy a stated need or objective

[ISO/IEC 12207:1995]

3.30
TASK
element of an ACTIVITY

3.31
TRACEABILITY
degree to which a relationship can be established between two or more products of the development PROCESS

[IEEE 610.12:1990]