EESTI STANDARD EVS-EN 80001-1:2011

Riskijuhtimise rakendamine meditsiiniseadmeid sisaldavates IT-võrkudes. Osa 1: Rollid, vastutus ja tegevused

Application of risk management for IT-networks incorporating medical devices - Part 1: Roles, responsibilities and activities

EESTI STANDARDIKESKUS
ESTONIAN CENTRE FOR STANDARDISATION
EVS

EESTI STANDARDI EESSÕNA	NATIONAL FOREWORD
Käesolev Eesti standard EVS-EN 80001-1:2011 sisaldab Euroopa standardi EN 80001-1:2011 ingliskeelset teksti.	This Estonian standard EVS-EN 80001-1:2011 consists of the English text of the European standard EN 80001-1:2011.
Standard on kinnitatud Eesti Standardikeskuse 31.03.2011 käskkirjaga ja jõustub sellekohase teate avaldamisel EVS Teatajas.	This standard is ratified with the order of Estonian Centre for Standardisation dated 31.03.2011 and is endorsed with the notification published in the official bulletin of the Estonian national standardisation organisation.
Euroopa standardimisorganisatsioonide poolt rahvuslikele liikmetele Euroopa standardi teksti kättesaadavaks tegemise kuupäev on 18.03.2011.	Date of Availability of the European standard text 18.03.2011.
Standard on kättesaadav Eesti standardiorganisatsioonist.	The standard is available from Estonian standardisation organisation.

ICS 11.040.01, 35.240.80

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 80001-1

March 2011

ICS 11.040.01; 35.240.80

English version

Application of risk management for IT-networks incorporating medical devices - Part 1: Roles, responsibilities and activities (IEC 80001-1:2010)

Application de la gestion des risques aux réseaux des technologies de l'information contenant des dispositifs médicaux - Partie 1: Fonctions, responsabilités et activités (CEI 80001-1:2010)

Anwendung des Risikomanagements für IT-Netzwerke, die Medizinprodukte beinhalten - Teil 1: Aufgaben, Verantwortlichkeiten und Aktivitäten (IEC 80001-1:2010)

This European Standard was approved by CENELEC on 2011-02-01. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the Central Secretariat or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the Central Secretariat has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and the United Kingdom.

CENELEC

European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

Management Centre: Avenue Marnix 17, B - 1000 Brussels

Foreword

The text of document 62A/703/FDIS, future edition 1 of IEC 80001-1, prepared by SC 62A, Common aspects of electrical equipment used in medical practice, of IEC TC 62, Electrical equipment in medical practice, was submitted to the IEC-CENELEC parallel vote and was approved by CENELEC as EN 80001-1 on 2011-02-01.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN and CENELEC shall not be held responsible for identifying any or all such patent rights.

The following dates were fixed:

– latest date by which the EN has to be implemented at national level by publication of an identical national standard or by endorsement (dop) 2011-11-01

– latest date by which the national standards conflicting with the EN have to be withdrawn (dow) 2014-02-01

Terms defined in Clause 2 of this standard are printed in SMALL CAPITALS.

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; and

— "establish" means to define, document, and implement.

Endorsement notice

The text of the International Standard IEC 80001-1:2010 was approved by CENELEC as a European Standard without any modification.

In the official version, for Bibliography, the following notes have to be added for the standards indicated:

[1] IEC 60601-1:2005	NOTE	Harmonized as EN 60601-1:2006 (not modified).
[2] IEC 61907:2009	NOTE	Harmonized as EN 61907:2010 (not modified).
[3] IEC 62304:2006	NOTE	Harmonized as EN 62304:2006 (not modified).
[4] ISO 14971:2007	NOTE	Harmonized as EN ISO 14971:2009 (not modified).
[7] ISO 16484-2:2004	NOTE	Harmonized as EN ISO 16484-2:2004 (not modified).
[8] ISO 9000:2005	NOTE	Harmonized as EN ISO 9000:2005 (not modified).

CONTENTS

INTRODUCTION

An increasing number of MEDICAL DEVICEs are designed to exchange information electronically with other equipment in the user environment, including other MEDICAL DEVICES. Such information is frequently exchanged through an information technology network (IT-NETWORK) that also transfers data of a more general nature.

At the same time, IT-NETWORKS are becoming increasingly vital to the clinical environment and are now required to carry increasingly diverse traffic, ranging from life-critical patient data requiring immediate delivery and response, to general corporate operations data and to email containing potential malicious content (e.g. viruses).

For many jurisdictions, design and production of MEDICAL DEVICES is subject to regulation, and to standards recognized by the regulators. Traditionally, regulators direct their attention to MEDICAL DEVICE manufacturers, by requiring design features and by requiring a documented PROCESS for design and manufacturing. MEDICAL DEVICES cannot be placed on the market in these jurisdictions without evidence that those requirements have been met.

The use of the MEDICAL DEVICES by clinical staff is also subject to regulation. Members of clinical staff have to be appropriately trained and qualified, and are increasingly subject to defined PROCESSES designed to protect patients from unacceptable RISK.

In contrast, the incorporation of MEDICAL DEVICES into IT-NETWORKS in the clinical environment is a less regulated area. IEC 60601-1:2005 [1][1)] requires MEDICAL DEVICE manufacturers to include some information in ACCOMPANYING DOCUMENTS if the MEDICAL DEVICE is intended to be connected to an IT-NETWORK. Standards are also in place covering common information technology activities including planning, design and maintenance of IT-NETWORKS, for instance ISO 20000-1:2005 [9]. However, until the publication of this standard, no standard addressed how MEDICAL DEVICES can be connected to IT-NETWORKS, including general-purpose IT-NETWORKS, to achieve INTEROPERABILITY without compromising the organization and delivery of health care in terms of SAFETY, EFFECTIVENESS, and DATA AND SYSTEM SECURITY.

There remain a number of potential problems associated with the incorporation of MEDICAL DEVICES into IT-NETWORKS, including:

- lack of consideration for RISK from use of IT-NETWORKS during evaluation of clinical RISK;
- lack of support from manufacturers of MEDICAL DEVICES for the incorporation of their products into IT-NETWORKS, (e.g. the unavailability or inadequacy of information provided by the manufacturer to the OPERATOR of the IT-NETWORK);
- incorrect operation or degraded performance (e.g. incompatibility or improper configuration) resulting from combining MEDICAL DEVICES and other equipment on the same IT-NETWORK;
- incorrect operation resulting from combining MEDICAL DEVICE SOFTWARE and other software applications (e.g. open email systems or computer games) in the same IT-NETWORK;
- lack of security controls on many MEDICAL DEVICES; and
- the conflict between the need for strict change control of MEDICAL DEVICES and the need for rapid response to the threat of cyberattack.

When these problems manifest themselves, unintended consequences frequently follow.

This standard is addressed to RESPONSIBLE ORGANIZATIONS, to manufacturers of MEDICAL DEVICES, and to providers of other information technology.

[1)] Numbers in square brackets refer to the Bibliography.

This standard adopts the following principles as a basis for its normative and informative sections:

– The incorporation or removal of a MEDICAL DEVICE or other components in an IT-NETWORK is a task which requires design of the action; this might be out of the control of the manufacturer of the MEDICAL DEVICE.

– RISK MANAGEMENT should be used before the incorporation of a MEDICAL DEVICE into an IT-NETWORK takes place, and for any changes during the entire life cycle of the resulting MEDICAL IT-NETWORK, to avoid unacceptable RISKS, including possible RISK to patients, resulting from the incorporation of the MEDICAL DEVICE into the IT-NETWORK. Many things are part of a RISK decision, such as liability, cost, or impact on mission. These should be considered in determining acceptable RISK in addition to the requirements described in this standard.

– Aspects of removal, maintenance, change or modification of equipment, items or components should be addressed adequately in addition to the incorporation of MEDICAL DEVICES.

– The manufacturer of the MEDICAL DEVICE is responsible for RISK MANAGEMENT of the MEDICAL DEVICE during the design, implementation, and manufacturing of the MEDICAL DEVICE. This standard does not cover the RISK MANAGEMENT PROCESS for the MEDICAL DEVICE.

– The manufacturer of a MEDICAL DEVICE intended to be incorporated into an IT-NETWORK might need to provide information about the MEDICAL DEVICE that is necessary to allow the RESPONSIBLE ORGANIZATION to manage RISK according to this standard. This information can include, as part of the ACCOMPANYING DOCUMENTS, instructions specifically addressed to the person who incorporates a MEDICAL DEVICE into an IT-NETWORK.

– Such ACCOMPANYING DOCUMENTS should convey instructions about how to incorporate the MEDICAL DEVICE into the IT-NETWORK, how the MEDICAL DEVICE transfers information over the IT-NETWORK, and the minimum IT-NETWORK characteristics necessary to enable the INTENDED USE of the MEDICAL DEVICE when it is incorporated into the IT-NETWORK. The ACCOMPANYING DOCUMENTS should warn of possible hazardous situations associated with failure or disruptions of the IT-NETWORK, and the misuse of the IT-NETWORK connection or of the information that is transferred over the IT-NETWORK.

– RESPONSIBILITY AGREEMENTS can establish roles and responsibilities among those engaged in the incorporation of a MEDICAL DEVICE into an IT-NETWORK, all aspects of the life cycle of the resulting MEDICAL IT-NETWORK and all activities that form part of that life cycle.

– The RESPONSIBLE ORGANIZATION is required to appoint people to certain roles defined in this standard. This standard defines the responsibilities of those roles. The most important of those roles is the MEDICAL IT-NETWORK RISK MANAGER. This role can be assigned to someone within the RESPONSIBLE ORGANIZATION or to an external contractor.

– The MEDICAL IT-NETWORK RISK MANAGER is responsible for ensuring that RISK MANAGEMENT is included during the PROCESSES of:

  - planning and design of new incorporations of MEDICAL DEVICES or changes to such incorporations;
  - putting the MEDICAL IT-NETWORK into use and the consequent use of the MEDICAL IT-NETWORK; and
  - CHANGE-RELEASE MANAGEMENT and change management of the IT-NETWORK during the IT-NETWORK'S entire life cycle.

– RISK MANAGEMENT should be applied to address the following KEY PROPERTIES appropriate for the IT-NETWORK incorporating a MEDICAL DEVICE:

  - SAFETY (freedom from unacceptable RISK of physical injury or damage to the health of people or damage to property or the environment);

- EFFECTIVENESS (ability to produce the intended result for the patient and the RESPONSIBLE ORGANIZATION); and

- DATA AND SYSTEM SECURITY (an operational state of a MEDICAL IT-NETWORK in which information assets (data and systems) are reasonably protected from degradation of confidentiality, integrity, and availability).

APPLICATION OF RISK MANAGEMENT FOR IT-NETWORKS INCORPORATING MEDICAL DEVICES –

Part 1: Roles, responsibilities and activities

1 Scope

Recognizing that MEDICAL DEVICES are incorporated into IT-NETWORKS to achieve desirable benefits (for example, INTEROPERABILITY), this international standard defines the roles, responsibilities and activities that are necessary for RISK MANAGEMENT of IT-NETWORKS incorporating MEDICAL DEVICES to address SAFETY, EFFECTIVENESS and DATA AND SYSTEM SECURITY (the KEY PROPERTIES). This international standard does not specify acceptable RISK levels.

NOTE 1 The RISK MANAGEMENT activities described in this standard are derived from those in ISO 14971 [4]. The relationship between ISO 14971 and this standard is described in Annex A.

This standard applies after a MEDICAL DEVICE has been acquired by a RESPONSIBLE ORGANIZATION and is a candidate for incorporation into an IT-NETWORK.

NOTE 2 This standard does not cover pre-market RISK MANAGEMENT.

This standard applies throughout the life cycle of IT-NETWORKS incorporating MEDICAL DEVICES.

NOTE 3 The life cycle management activities described in this standard are very similar to those of ISO/IEC 20000-2 [10]. The relationship between ISO/IEC 20000-2 and this standard is described in Annex D.

This standard applies where there is no single MEDICAL DEVICE manufacturer assuming responsibility for addressing the KEY PROPERTIES of the IT-NETWORK incorporating a MEDICAL DEVICE.

NOTE 4 If a single manufacturer specifies a complete MEDICAL DEVICE that includes a network, the installation or assembly of the MEDICAL DEVICE according to the manufacturer's ACCOMPANYING DOCUMENTS is not subject to the provisions of this standard regardless of who installs or assembles the MEDICAL DEVICE.

NOTE 5 If a single manufacturer specifies a complete MEDICAL DEVICE that includes a network, additions to that MEDICAL DEVICE or modification of the configuration of that MEDICAL DEVICE, other than as specified by the manufacturer, is subject to the provisions of this standard.

This standard applies to RESPONSIBLE ORGANIZATIONS, MEDICAL DEVICE manufacturers and providers of other information technology for the purpose of RISK MANAGEMENT of an IT-NETWORK incorporating MEDICAL DEVICES as specified by the RESPONSIBLE ORGANIZATION.

This standard does not apply to personal use applications where the patient, OPERATOR and RESPONSIBLE ORGANIZATION are one and the same person.

NOTE 6 In cases where a MEDICAL DEVICE is used at home under the supervision or instruction of the provider, that provider is deemed to be the RESPONSIBLE ORGANIZATION. Personal use where the patient acquires and uses a MEDICAL DEVICE without the supervision or instruction of a provider is out of scope of this standard.

This standard does not address regulatory or legal requirements.

2 Terms and definitions

For the purposes of this document, the following terms and definitions apply: