SEK Teknisk rapport 80001-2-1

Utgiven	Utgåva	Sida	Ansvarig kommitté
2014-02-19	1	1 (1+62)	SEK TK 62

Application of risk management for IT-networks incorporating medical devices – Part 2-1: Step-by-step risk management of medical IT-networks – Practical applications and examples

(IEC Technical Report 80001-2-1:2012)

Denna publikation ingår i en serie med tekniska rapporter som ansluter till standarden SS-EN 80001-1, Riskhantering tillämpad på IT-nätverk som innehåller eller är kopplade till medicintekniska produkter – Del 1: Roller, ansvar och aktiviteter. Den är avsedd att ge vägledning steg för steg till den riskhanteringsprocess som beskrivs i standarden.

För närvarande finns fyra tekniska rapporter i serien. De är:

Part 2-1: Step-by-step risk management of medical IT-networks – Practical applications and examples

Part 2-2: Guidance for the disclosure and communication of medical device security needs, risks and controls

Part 2-3: Guidance for wireless networks

Part 2-4: Application guidance – General implementation guidance for healthcare delivery organizations

ISSN 1651-1417

ICS 11.040.01; 35.240.80

Upplysningar om **sakinnehållet** i rapporten lämnas av
SEK Svensk Elstandard.
Postadress: SEK, Box 1284, 164 29 KISTA
Telefon: 08 - 444 14 00. *Telefax*: 08 - 444 14 30
E-post: sek@elstandard.se. *Internet*: www.elstandard.se

Standarder underlättar utvecklingen och höjer elsäkerheten

Det finns många fördelar med att ha gemensamma tekniska regler för bl a säkerhet, prestanda, dokumentation, utförande och skötsel av elprodukter, elanläggningar och metoder. Genom att utforma sådana standarder blir säkerhetskraven tydliga och utvecklingskostnaderna rimliga samtidigt som marknadens acceptans för produkten eller tjänsten ökar.

Många standarder inom elområdet beskriver tekniska lösningar och metoder som åstadkommer den elsäkerhet som föreskrivs av svenska myndigheter och av EU.

SEK är Sveriges röst i standardiseringsarbetet inom elområdet

SEK Svensk Elstandard svarar för standardiseringen inom elområdet i Sverige och samordnar svensk medverkan i internationell och europeisk standardisering. SEK är en ideell organisation med frivilligt deltagande från svenska myndigheter, företag och organisationer som vill medverka till och påverka utformningen av tekniska regler inom elektrotekniken.

SEK samordnar svenska intressenters medverkan i SEKs tekniska kommittéer och stödjer svenska experters medverkan i internationella och europeiska projekt.

Stora delar av arbetet sker internationellt

Utformningen av standarder sker i allt väsentligt i internationellt och europeiskt samarbete. SEK är svensk nationalkommitté av International Electrotechnical Commission (IEC) och Comité Européen de Normalisation Electrotechnique (CENELEC).

Standardiseringsarbetet inom SEK är organiserat i referensgrupper bestående av ett antal tekniska kommittéer som speglar hur arbetet inom IEC och CENELEC är organiserat.

Arbetet i de tekniska kommittéerna är öppet för alla svenska organisationer, företag, institutioner, myndigheter och statliga verk. Den årliga avgiften för deltagandet och intäkter från försäljning finansierar SEKs standardiseringsverksamhet och medlemsavgift till IEC och CENELEC.

Var med och påverka!

Den som deltar i SEKs tekniska kommittéarbete har möjlighet att påverka framtida standarder och får tidig tillgång till information och dokumentation om utvecklingen inom sitt teknikområde. Arbetet och kontakterna med kollegor, kunder och konkurrenter kan gynnsamt påverka enskilda företags affärsutveckling och bidrar till deltagarnas egen kompetensutveckling.

Du som vill dra nytta av dessa möjligheter är välkommen att kontakta SEKs kansli för mer information.

SEK Svensk Elstandard
Box 1284
164 29 Kista
Tel 08-444 14 00
www.elstandard.se

CONTENTS

INTRODUCTION

This technical report is a step-by-step guide to help in the application of RISK MANAGEMENT when creating or changing a MEDICAL IT-NETWORK. It provides easy to apply steps, examples, and information helping in the identification and control of RISKS. All relevant requirements in IEC 80001-1:2010 are addressed and links to other clauses and subclauses of IEC 80001-1 are addressed where appropriate (e.g. handover to release management and monitoring).

This technical report focuses on practical RISK MANAGEMENT. It is not intended to provide a full outline or explanation of all requirements that are satisfactorily covered by IEC 80001-1.

This step-by-step guidance follows a 10-step PROCESS that follows subclause 4.4 of IEC 80001-1:2010, which *specifically* addresses RISK ANALYSIS, RISK EVALUATION and RISK CONTROL. These activities are embedded within the full life cycle RISK MANAGEMENT PROCESS. They can never be the first step, as RISK MANAGEMENT follows the general PROCESS model which sets planning before any action.

For the purpose of this technical report, "prerequisites" as stated in subclause 1.3 are considered to be in place before execution of the 10 steps. Also, it is well understood that all steps outlined in this technical report should have been performed before any new MEDICAL IT-NETWORK can go live or before proceeding with a change to an existing MEDICAL IT-NETWORK. It is emphasized that subclause 4.5 of IEC 80001-1:2010 "CHANGE RELEASE MANAGEMENT and CONFIGURATION MANAGEMENT" explicitly includes and applies to new MEDICAL IT-NETWORKS, as well as changes to existing networks.

This technical report will be useful to those responsible for or part of a team executing RISK MANAGEMENT when changing or creating (as the ultimate change) a MEDICAL IT-NETWORK. MEDICAL DEVICES in the context of IEC 80001 refer to those MEDICAL DEVICES that connect to a network.

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

Part 2-1: Step-by-step risk management of medical IT-networks – Practical applications and examples

1 Scope

This technical report provides step-by-step information to aid RESPONSIBLE ORGANIZATIONS in implementation of the RISK MANAGEMENT PROCESS required by IEC 80001-1. Specifically, it details the steps involved in executing subclause 4.4 of IEC 80001-1:2010 and provides guidance in the form of a study of RISK MANAGEMENT terms, RISK MANAGEMENT steps, an explanation of each step, step-by-step examples, templates, and lists of HAZARDS and causes to consider.

The steps outlined within this technical report are considered to be universally applicable. Application of these steps can be scaled as described within this document.

2 Normative references

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

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