

© Copyright SEK. Reproduction in any form without permission is prohibited.

## **Application of risk management for IT-networks incorporating medical devices – Part 2-3: Guidance for wireless networks**

*(IEC Technical Report 80001-2-3:2012)*

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 vårdgivaren vägledning beträffande helt eller delvis trådlösa IT-nätverk.

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](mailto:sek@elstandard.se). Internet: [www.elstandard.se](http://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](http://www.elstandard.se)

## CONTENTS

INTRODUCTION.....	6
1 Scope and object.....	9
1.1 Scope.....	9
1.2 Objective.....	9
1.3 HDO scalability .....	10
2 Normative references .....	10
3 Terms and definitions .....	11
4 Wireless MEDICAL IT-NETWORK: An introduction .....	21
4.1 Basics .....	21
4.2 Enterprise MEDICAL IT-NETWORK.....	22
4.3 Use of VLANs and SSIDs .....	22
4.4 Wide area MEDICAL IT-NETWORK .....	23
4.5 Smart phone applications .....	24
4.5.1 General .....	24
4.5.2 Application clinical functionality .....	24
4.5.3 Cellular networks.....	24
4.5.4 Smart phone coexistence .....	25
4.5.5 Wireless data security .....	25
4.6 DISTRIBUTED ANTENNA SYSTEMS .....	25
5 Wireless MEDICAL IT-NETWORKS: Planning and design.....	26
5.1 Clinical systems and their impact on the wireless network .....	26
5.1.1 Defining the clinical SLA.....	26
5.1.2 Creating partnerships .....	26
5.1.3 Geographical location.....	26
5.1.4 Clinical use case .....	27
5.2 MEDICAL DEVICE wireless capabilities .....	27
5.3 MEDICAL DEVICE capabilities and networking traffic profile.....	27
5.4 Network performance requirements .....	27
5.5 QoS mechanisms .....	28
5.6 Receiver capabilities .....	28
5.7 Received signal strength and SNR versus data rates .....	29
5.8 Capacity versus coverage versus AP density.....	30
5.9 Deterministic versus non-deterministic wireless access protocol.....	31
5.10 Planning and design summary.....	31
6 Wireless MEDICAL IT-NETWORKS: Deployment and configuration.....	31
6.1 RISKS versus benefit of a wireless communications system .....	31
6.2 Licensed versus unlicensed spectrum .....	31
6.3 Interference sources.....	32
6.4 Spectrum usage and allocation.....	32
6.4.1 Device coexistence.....	32
6.4.2 Spectrum management.....	32
6.4.3 Capacity management .....	33
6.5 Wireless network configuration (802.11 specific).....	33
6.5.1 General .....	33

6.5.2	VLAN and SSID .....	33
6.5.3	Authentication and encryption.....	33
6.5.4	Vendor proprietary extensions .....	34
6.5.5	Cellular and proprietary networks .....	34
6.5.6	Network availability.....	34
6.6	VERIFICATION testing .....	35
6.6.1	General .....	35
6.6.2	Pre GO-LIVE VERIFICATION testing.....	35
6.6.3	GO-LIVE VERIFICATION testing.....	35
7	Wireless MEDICAL IT-NETWORKS: Management and support.....	36
7.1	General .....	36
7.2	Network and application management .....	36
7.3	Policies and procedures .....	36
7.4	Change control.....	36
8	General RISK CONTROL measures .....	37
8.1	General .....	37
8.2	Determining baseline networking performance .....	37
8.3	Designing for coverage signal strength.....	37
8.4	Segregating traffic and data types .....	38
8.5	Environmental and physical changes.....	38
8.6	Maintaining a clean RF environment.....	38
8.7	Capacity planning.....	38
8.7.1	General .....	38
8.7.2	5 GHz and DYNAMIC FREQUENCY SELECTION (DFS) .....	39
8.7.3	Security measures and planning .....	39
8.8	RF spectrum use .....	40
8.9	Device and application classification .....	40
8.10	Guest or smart phone access .....	40
8.11	WLAN infrastructure configuration .....	41
8.12	External partnering with both MEDICAL DEVICE and networking manufacturer.....	41
8.13	Redundancy .....	41
	Annex A (informative) Clinical use cases and network traffic profiles .....	42
	Annex B (informative) Questions to consider.....	44
	Bibliography.....	48
	Figure 1 – Focus of technical report.....	8
	Figure 2 – HDO MEDICAL IT-NETWORK .....	23
	Figure 3 – Wireless WAN connectivity.....	24
	Figure 4 – SIGNAL TO NOISE RATIO .....	29
	Table A.1 – Example clinical use cases and network traffic profiles .....	43
	Table A.2 – Network profile parameters .....	43

## INTRODUCTION

### 0.1 Background

Wireless communications has been a key technology enabling the connectivity of MEDICAL DEVICES for decades. Early examples of the use of wireless technologies and MEDICAL DEVICES include ambulatory cardiac monitoring systems in hospitals and telemetry systems used by paramedics over wide area wireless networks. While these solutions were based on proprietary technology, the advent of off-the-shelf standards-based approaches has resulted in increasingly ubiquitous wireless communications systems both indoors and outdoors. These provide and enable compelling and varied use cases for connection between MEDICAL DEVICES and information systems. Wireless technology has great benefits; however, as with any technology, certain RISKS are introduced that can affect the three KEY PROPERTIES of SAFETY, EFFECTIVENESS, and DATA AND SYSTEMS SECURITY. This document will review the challenges associated with wireless technologies and provide guidance regarding the safe, effective, and secure use of MEDICAL DEVICES on a wireless MEDICAL IT-NETWORK. This is done in a framework that follows the RISK MANAGEMENT PROCESS as defined by the IEC 80001-1 standard.

The targeted audience for this technical report is the HDO IT department, biomedical and clinical engineering departments, risk managers, and the people responsible for design and operation of the wireless IT network.

For the purposes of this technical report, “should” is used to indicate that amongst several possibilities to meet a requirement, one is recommended as being particularly suitable without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required. This term is not to be interpreted as indicating requirement.

### 0.2 Organization of the technical report

This technical report is divided into five main clauses, a bibliography and two annexes. Clause 4 provides an overview of a wireless MEDICAL IT-NETWORK and reviews varying types of wireless technologies and their applicability to healthcare. The next three clauses focus on the high level steps involved with understanding and defining the networking performance characteristics, requirements and associated RISK CONTROL measures regarding the creation a MEDICAL IT-NETWORK, namely:

- a) planning and design;
- b) deployment and implementation; and
- c) operational management.

Clause 8 provides general RISK CONTROL measures that might be applicable to an HDO's unique MEDICAL IT-NETWORK. Finally, a bibliography is included that lists references for further exploration. Annex A offers a table that suggests a mapping between MEDICAL DEVICE data types and associated networking QUALITY OF SERVICE priorities. Annex B is a checklist questionnaire for assistance in performing a RISK ANALYSIS.

### 0.3 Clinical functionality and use case

One of the fundamental concepts that this technical report emphasizes is that MEDICAL DEVICES have networking characteristics that are similar to other types of general purpose devices and applications; yet the repercussions of not properly designing and managing the network to ensure the SERVICE LEVEL AGREEMENT of the MEDICAL DEVICES could negatively impact clinical functionality. This can lead to erroneous diagnostics and/or missed treatment that can ultimately affect patient health outcome. In this technical report, clinical functionality and the clinical use case are interchangeable; they are a reference to the means by which a clinician

(nurse, physician, etc.) performs their clinical duties across the wireless network, and includes the component of patient care and SAFETY. These are components in the overall context as it is referred to in the step-by-step technical report, IEC 80001-2-1, and this information is required for a complete RISK ANALYSIS. A typical example is a nurse who is remotely monitoring a patient from the nursing central station using a patient monitor at the bedside that is wirelessly connected to the network. The clinical functionality is the remote monitoring of a patient's health.

#### 0.4 Wireless guidance and RISK MANAGEMENT

The wireless link between a patient and the remote clinician is now a component of the clinical functionality and may impact the KEY PROPERTIES of SAFETY and DATA AND SYSTEMS SECURITY. While the benefits of wireless access are well known and documented, typically the wireless link between a MEDICAL DEVICE and a clinician is more likely, or has a higher probability, of experiencing a loss of connectivity versus that of a wired connection. This is a motivation behind the creation and focus of this technical report.

Because the definitions of HAZARD, HAZARDOUS SITUATIONS, HARM and causes are use case specific to each HDO, this document should be used in conjunction with both the IEC 80001-1 and IEC/TR 80001-2-1 at a minimum.

Figure 1 provides an overview of the RISK MANAGEMENT aspect of this technical report. The column of boxes on the left of the figure is an overview (for this technical report's purpose) of the 10 steps of RISK MANAGEMENT as defined in the IEC/TR 80001-2-1. The center boxes show the steps of the RISK MANAGEMENT PROCESS that this technical report is focused on. They are the following in terms of the RISK MANAGEMENT PROCESS:

- The cause is an event that can turn a HAZARD into a HAZARDOUS SITUATION. Examples of causes in a wireless network are RF interference, wireless network misconfiguration, or networking device failure.
- A HAZARD associated in the context of wireless connectivity is the loss or impairment of connectivity in a medical system. This disruption in connectivity can negatively impact the ability of a MEDICAL DEVICE or clinical system to perform its intended function.
- A HAZARDOUS SITUATION is a circumstance in which the MEDICAL DEVICE or clinical functionality is exposed to a HAZARD. For example, a clinician is monitoring a patient at the nursing station (clinical functionality is remote monitoring). If RF interference *causes* the wireless network to be disabled (loss of connectivity is the HAZARD), then the patient is no longer being remotely monitored (HAZARDOUS SITUATION).
- The RISK CONTROL measures as used in this technical report are the steps taken to reduce the probability of the occurrence of a HAZARDOUS SITUATION (referred to as P1 in IEC/TR 80001-2-1), or the steps taken to reduce the probability of HARM once the HAZARDOUS SITUATION has occurred (referred to as P2 in IEC/TR 80001-2-1). A P1 RISK CONTROL measure example might be RF redundancy or networking change control procedures. A P2 RISK CONTROL measure example might be the sequence of actions that a nurse would take if notified that the connectivity is lost between a patient monitor and central station.

The majority of this technical report focuses on the design and RISK CONTROL measures associated with wireless technologies. However, and this is another motivation for engaging with the clinicians early in the planning phase, the role of the clinicians in mitigating against Patient HARM should be clearly reviewed. In the example used in the bulleted steps above, the clinician might have a documented procedure to follow during network outages; when the network experiences loss of connectivity the clinician can follow a procedure where they need to attend to the patient directly.

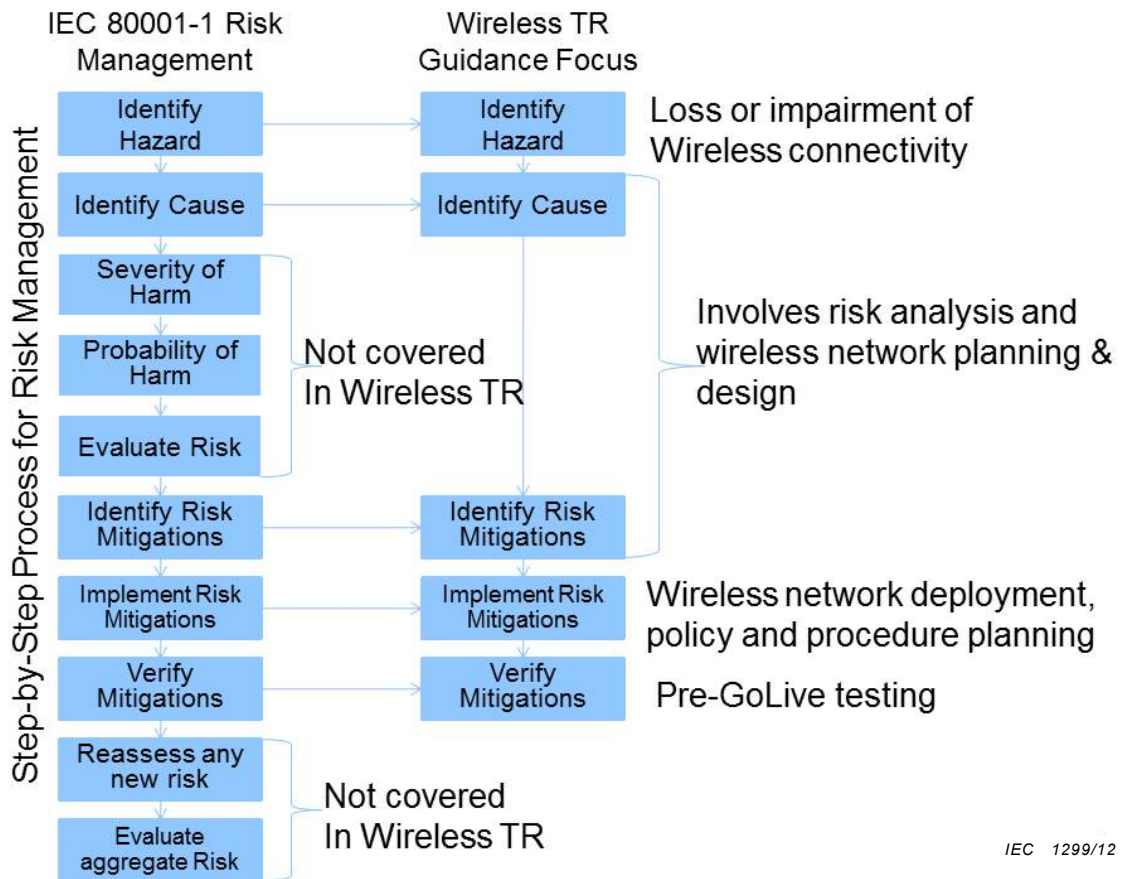


Figure 1 – Focus of technical report

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

## Part 2-3: Guidance for wireless networks

### 1 Scope and object

#### 1.1 Scope

This part of IEC 80001 supports the HDO in the RISK MANAGEMENT of MEDICAL IT-NETWORKS that incorporate one or more wireless links. The report provides technical background concerning wireless technology and examples of HAZARDS to be considered when wireless technology is used in MEDICAL IT-NETWORKS and suggests RISK CONTROL measures to reduce the probability of UNINTENDED CONSEQUENCES.

#### 1.2 Objective

This Technical Report, as part of IEC 80001 considers the use of wirelessly networked MEDICAL DEVICES on a MEDICAL IT-NETWORK and offers practical techniques to address the unique RISK MANAGEMENT requirements of operating wirelessly enabled MEDICAL DEVICES in a safe, secure and effective manner.

This technical report is focused on wireless technologies from an agnostic viewpoint; however, there are particular wireless technologies that are predominant in HDOs (e.g. 802.11) and are discussed in more detail. Where appropriate, these differences are pointed out and discussed. In addition, while it does not focus on a single wireless technology, it is assumed that the attached wired infrastructure is an Ethernet-based IP network.

It is not the intent of this document to propose a regimented step-by-step PROCESS for implementing a wireless MEDICAL IT-NETWORK or mitigating the RISK associated with a particular wireless technology. There are many reasons which conspire against such an effort and chief among them are:

- There are many different wireless technologies available, each with their PHY, MAC and upper layer characteristics with varying degrees of control available to the HDO.
- Many wireless technologies are in an evolving stage of development and are still subject to frequent and significant changes.
- HDOs, depending on their needs, might utilize varying combinations of wireless technologies to meet their particular requirements. Each technology should require its own independent RISK ANALYSIS and RISK CONTROL measures that should be reviewed systemically (aggregate RISKS ANALYSIS).
- Each HDO will have their own unique clinical use cases and network topologies and will perform their own unique RISK ANALYSIS and management that will differ from other HDOs.

Instead, this technical report acknowledges a generalized or high level approach relative to a step-by-step PROCESS review that both inherently and intentionally considers HAZARDS, the causes leading to HAZARDOUS SITUATIONS, and RISK CONTROL measures. The general approach that this technical report follows is the following:

- a) Pose the question: does the use case of the device require wireless connectivity? This is not a trivial question but this technical report assumes the answer is “yes”.
- b) Define the clinical use-cases/functionality by bringing together the clinicians, biomedical engineering staff and whoever else might be involved in the use and support of the MEDICAL DEVICES.



- c) Review the wireless specifications and capabilities of the MEDICAL DEVICE(S) and systems and create baseline networking performance requirements.
- d) Create the clinical SLA by mapping the networking performance requirements to the clinical functionality. See Table A.1 for examples regarding this mapping.
- e) Match the wireless networking performance requirements of the MEDICAL DEVICES and systems to the existing capabilities of the general purpose IT-NETWORK and identify gaps or incompatibilities. Take into consideration the wireless network configurations and networking performance requirements of all existing or planned wireless non-MEDICAL DEVICES.
- f) Complete the RISK MANAGEMENT PROCESS, including identification and implementation of RISK CONTROL measures relative to the KEY PROPERTIES. Many RISK CONTROL measures are very much like 'best design practices', but are documented, applied, and VERIFIED as part of the RISK MANAGEMENT PROCESS.
- g) Design and configure the network(s) to match the SLAs of all devices (medical and non-medical).
- h) Perform pre-GO-LIVE network testing to VERIFY that all devices properly coexist while maintaining their particular SLA.
- i) Use operational measures to monitor and manage the live network such that SLAs are continuously being met.

### 1.3 HDO scalability

The scope of this document is targeted at all HDOs regardless of network size. Large networks might have to deal with many devices and complex application mixes using both wired and wireless networks. They might or might not have life critical patient data traversing the network. Other networks can be smaller in scale, simpler in the number of devices and applications operating on the network, but also might have life critical data on the network. The complexity of the networks and the patient SAFETY aspect of the network traffic drive the extent of HAZARD analysis and RISK MANAGEMENT required. The patient SAFETY aspect requires that a RISK MANAGEMENT plan be completed while the network complexity translates into the level of complexity in the RISK CONTROL measures.

One can certainly argue that a small network (e.g. physician office) that uses wireless technology does not need to go through the same level of RISK ANALYSIS as a hospital. For example, there are small catheterization laboratories and small cosmetic surgery practices that might have small scale networks, yet have patient data on the network. All HDOs have to manage the security of their networks and evaluate their clinical functionality for patient SAFETY implications. HDOs need to manage their network wireless technology deployments with an appropriate and scaled attention to RISK MANAGEMENT.

While this document focuses on deployment issues for complex wireless deployments, its guidance, appropriately applied, can be used in many different networked environments, both large and small.

## 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*