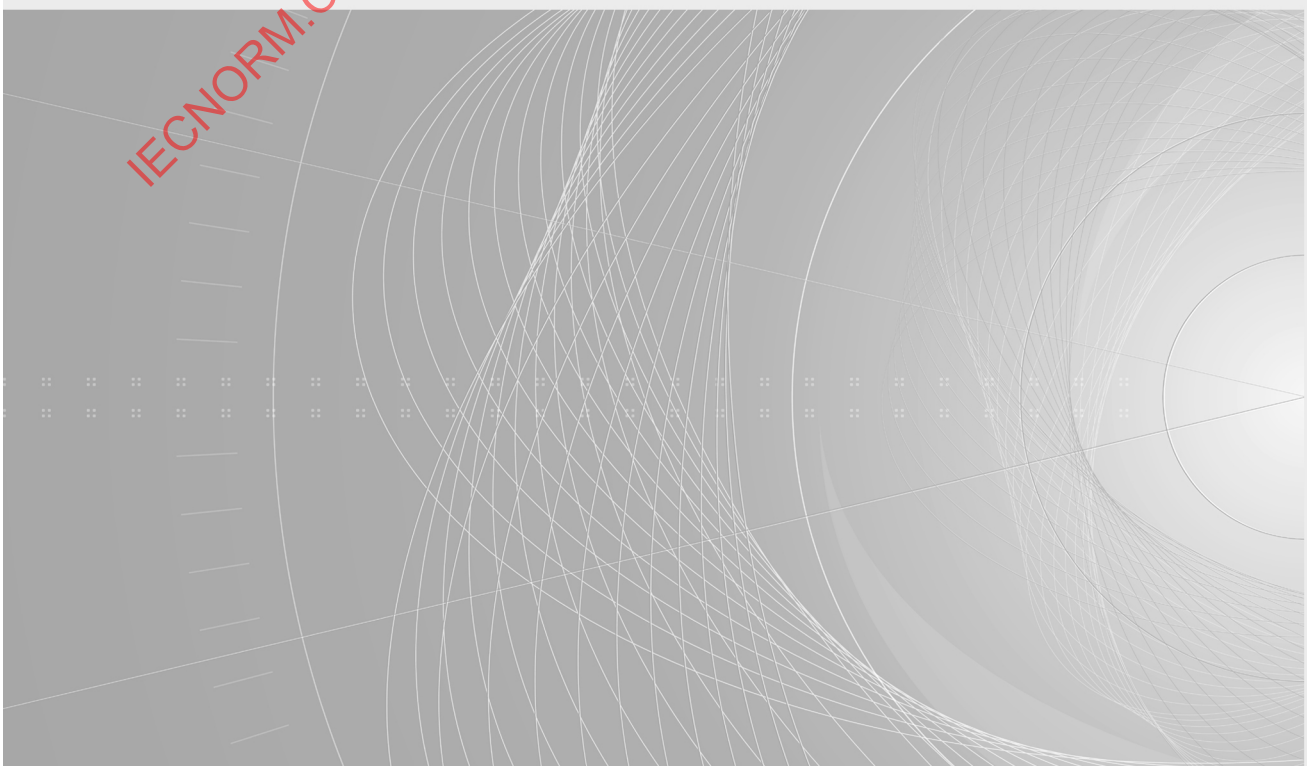
IEC/TR 80001-2-3

Edition 1.0 2012-07

TECHNICAL REPORT

colour inside

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



IEC/TR 80001-2-3:2012(E)

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
info@iec.ch
www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

Useful links:

IEC publications search - www.iec.ch/searchpub

The advanced search enables you to find IEC publications by a variety of criteria (reference number, text, technical committee,…).
It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

Stay up to date on all new IEC publications. Just Published details all new publications released. Available on-line and also once a month by email.

Electropedia - www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 30 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary (IEV) on-line.

Customer Service Centre - webstore.iec.ch/csc

If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: csc@iec.ch.

IEC/TR 80001-2-3

Edition 1.0 2012-07

TECHNICAL REPORT

colour inside

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

INTERNATIONAL ELECTROTECHNICAL COMMISSION

PRICE CODE X

ICS 11.040.01; 35.240.80

ISBN 978-2-83220-203-6

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

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

Part 2-3: Guidance for wireless networks

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of 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, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). 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. 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 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 IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

The main task of IEC technical committees is to prepare International Standards. However, a technical committee may propose the publication of a technical report when it has collected data of a different kind from that which is normally published as an International Standard, for example "state of the art".

IEC 80001-2-3, which is a technical report, 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 215: Health informatics.

The text of this technical report is based on the following documents:

Enquiry draft	Report on voting
62A/784/DTR	62A/804/RVC

Full information on the voting for the approval of this technical report 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.

Terms used throughout this technical report that have been defined in Clause 3 appear in SMALL CAPITALS.

The committee has decided that the contents of this publication will remain unchanged until the stability date indicated on the IEC web site under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

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

A bilingual version of this publication may be issued at a later date.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

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.

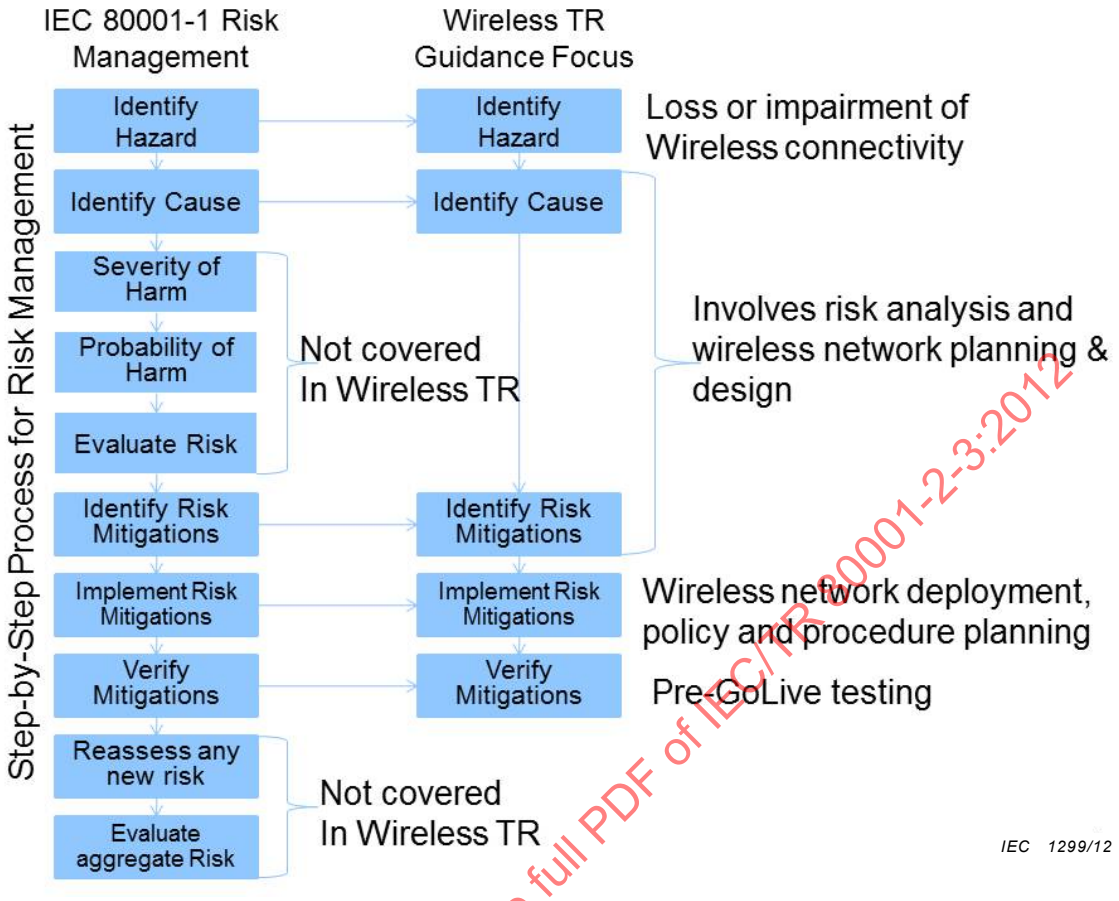


Figure 1 – Focus of technical report

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*

3 Terms and definitions

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

3.1
ACCESS POINT
AP
bridge from a wireless medium to a wired medium

3.2
ACCOMPANYING DOCUMENT
document accompanying a MEDICAL DEVICE or an accessory and containing information for the RESPONSIBLE ORGANIZATION or OPERATOR, particularly regarding SAFETY

[SOURCE: IEC 80001-1:2010, definition 2.1]

3.3
ADVANCED ENCRYPTION STANDARD
AES
a symmetric-key encryption standard

Note 1 to entry: One of its uses is for the WPA2 wireless encryption standard.

3.4
BASIC SERVICE SET IDENTIFIER
BSSID
an 802.11 term for the MAC address of an AP

3.5
BOOTSTRAP PROTOCOL
BOOTP
network protocol used by a network client to obtain an IP address from a configuration server

3.6
BROADCAST ADDRESSING
technology for delivering a message to all destinations on a network simultaneously

3.7
CHANGE PERMIT
an outcome of the RISK MANAGEMENT PROCESS consisting of a document that allows a specified change or type of change without further RISK MANAGEMENT Activities subject to specified constraints

[SOURCE: IEC 80001-1:2010, definition 2.3]

3.8
CHANGE-RELEASE MANAGEMENT
PROCESS that ensures that all changes to the IT-NETWORK are assessed, approved, implemented and reviewed in a controlled manner and that changes are delivered, distributed, and tracked, leading to release of the change in a controlled manner with appropriate input and output with CONFIGURATION MANAGEMENT

[SOURCE: IEC 80001-1:2010, definition 2.2]

3.9
CONFIGURATION MANAGEMENT
PROCESS that ensures that configuration information of components and the IT-NETWORK are defined and maintained in an accurate and controlled manner, and provides a mechanism for identifying, controlling and tracking versions of the IT-NETWORK

[SOURCE: IEC 80001-1:2010, definition 2.4]

3.10
DATA AND SYSTEMS SECURITY
operational state of a MEDICAL IT-NETWORK in which information assets (data and systems) are reasonably protected from degradation of confidentiality, integrity, and availability

[SOURCE: IEC 80001-1:2010, definition 2.5, modified – two notes integral to understanding the scope of the original definition have been deleted.]

3.11
DIGITAL ENHANCED CORDLESS TELECOMMUNICATIONS
DECT
digital communication standard which is primarily used for creating cordless phone system

3.12
DISTRIBUTED ANTENNA SYSTEM
DAS
antenna system that collects wireless signals and routes them to centralized locations

3.13
DYNAMIC FREQUENCY SELECTION
DFS
mechanism for dynamically selecting frequencies to avoid interference sources – usually used in conjunction with the mechanism 802.11a based systems use to avoid frequencies used by radar systems

3.14
DYNAMIC HOST CONFIGURATION PROTOCOL
DHCP
method to allocate IP addresses to client devices upon request by the client

3.15
EFFECTIVENESS
ability to produce the intended result for the patient and the RESPONSIBLE ORGANIZATION

[SOURCE: IEC 80001-1:2010, definition 2.6]

3.16
ELECTRONIC MEDICAL RECORD
EMR
computerized medical record created in an HDO

3.17
ENCODER/DECODER
CODEC
module that can encode data and decode data

3.18
EVENT MANAGEMENT
PROCESS that ensures that all events that can or might negatively impact the operation of the IT-NETWORK are captured, assessed, and managed in a controlled manner

[SOURCE: IEC 80001-1:2010, definition 2.7]

3.19
EXTENDED SERVICE SET IDENTIFIER
ESSID
term that describes a logical grouping of multiple BSSIDs

Note 1 to entry: This term is sometimes used in place of SSID.

3.20
EXTENSIBLE AUTHENTICATION PROTOCOL
EAP
authentication framework frequently used in wireless networks and point-to-point connections

Note 1 to entry: It is defined in RFC 3748 and was updated by RFC 5247.

3.21
EXTENSIBLE AUTHENTICATION PROTOCOL – TRANSPORT LAYER SECURITY
EAP-TLS
specific authentication method using the EAP authentication framework (RFC 5216)

3.22
GO-LIVE
point at which a system transitions from the installation phase to the active use phase

3.23
HARM
physical injury or damage to the health of people, or damage to property or the environment, or reduction in EFFECTIVENESS, or breach of DATA AND SYSTEMS SECURITY

[SOURCE: IEC 80001-1:2010, definition 2.8]

3.24
HAZARD
potential source of HARM

[SOURCE: IEC 80001-1:2010, definition 2.9]

3.25
HAZARDOUS SITUATION
circumstance in which people, property, or the environment are exposed to one or more HAZARD (S)

[SOURCE: ISO 14971:2007, definition 2.4]

3.26
HEALTH DATA
PRIVATE DATA that indicates physical or mental health

Note 1 to entry: This generically defines PRIVATE DATA and it subset, HEALTH DATA, within this document to permit users of this document to adapt it easily to different privacy compliance laws and regulations. For example, in Europe, the requirements might be taken and references changed to “Personal Data” and “Sensitive Data”; in the USA, HEALTH DATA might be changed to “Protected Health Information (PHI)” while making adjustments to text as necessary.

[SOURCE: IEC 80001-2-2:2012, definition 3.7]

3.27
HEALTHCARE DELIVERY ORGANIZATION
HDO
facility or enterprise such as a clinic or hospital that provides healthcare services

3.28
HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT
HIPAA
legislation enacted in the USA that among its provisions requires the protection of protected HEALTH DATA

3.29
INDUSTRIAL, SCIENTIFIC AND MEDICAL BAND
ISM BAND
radio bands that were originally reserved internationally for the use of RADIO FREQUENCY (RF) energy for industrial, scientific and medical purposes

3.30
INFORMATION TECHNOLOGY
IT
technology (computer systems, networks, software) used to PROCESS, store, acquire and distribute information

3.31
INFORMATION TECHNOLOGY NETWORK
IT-NETWORK
system or systems composed of communicating nodes and transmission links to provide physically linked or wireless transmission between two or more specified communication nodes

[SOURCE: IEC 80001-1:2010, definition 2.12, modified – the two notes to the original definition have not been retained.]

3.32
INTENDED USE
INTENDED PURPOSE
use for which a product, PROCESS or service is intended according to the specifications, instructions and information provided by the manufacturer

[SOURCE: IEC 80001-1:2010, definition 2.10]

3.33
INTENSIVE CARE UNIT
ICU
area of the hospital where a PATIENT will be monitored closely for a critical medical condition

3.34
INTERNET GROUP MULTICAST PROTOCOL
IGMP
communications protocol used by hosts and adjacent routers on IP networks to establish MULTICAST group memberships

3.35
INTEROPERABILITY
a property permitting diverse systems or components to work together for a specified purpose

[SOURCE: IEC 80001-1:2010, definition 2.11]

3.36
INTRUSION DETECTION SYSTEM
IDS
system that monitors the wireless environment and detects unauthorized uses such as “rogue” ACCESS POINTS, viruses, worms, etc.

3.37
INTRUSION PROTECTION SYSTEM
IPS
system that includes an IDS and actively attempts to block system intrusions

3.38
KEY PROPERTIES
three RISK managed characteristics (SAFETY, EFFECTIVENESS, and DATA AND SYSTEMS SECURITY) of MEDICAL IT-NETWORKS

[SOURCE: IEC 80001-1:2010, definition 2.13]

3.39
LOCAL AREA NETWORK
LAN
computer network covering a small physical area, such as a home or office, or small group of buildings, such as a school or an airport

Note 1 to entry: In 802.3 parlance, a LAN is a set of devices that share a BROADCAST domain.

3.40
MEDIA ACCESS CONTROL
MAC
part of the Link Layer in the Open System Interconnection Reference Model

3.41
MEDICAL DEVICE
any instrument, apparatus, implement, machine, appliance, implant, *in vitro* reagent or calibrator, software, material or other similar or related article:

a) 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 or diagnostic purposes by means of in vitro examination of specimens derived from the human body; and
b) 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 intended function by such means.

Note 1 to entry: The definition of a device for *in vitro* examination includes, for example, reagents, calibrators, sample collection and storage devices, control materials, and related instruments or apparatus. The information provided by such an *in vitro* diagnostic device may be for diagnostic, monitoring or compatibility purposes. In some jurisdictions, some *in vitro* diagnostic devices, including reagents and the like, may be covered by separate regulations.

Note 2 to entry: Products which may be considered to be MEDICAL DEVICES in some jurisdictions but for which there is not yet a harmonized approach, are:

– aids for disabled/handicapped people;
– devices for the treatment/diagnosis of diseases and injuries in animals;
– accessories for MEDICAL DEVICES (see Note 3 to entry);
– disinfection substances;
– devices incorporating animal and human tissues which may meet the requirements of the above definition but are subject to different controls.

Note 3 to entry: Accessories intended specifically by manufacturers to be used together with a 'parent' MEDICAL DEVICE to enable that MEDICAL DEVICE to achieve its intended purpose should be subject to the same GHTF procedures as apply to the MEDICAL DEVICE itself. For example, an accessory will be classified as though it is a MEDICAL DEVICE in its own right. This may result in the accessory having a different classification than the 'parent' device.

Note 4 to entry: Components to MEDICAL DEVICES are generally controlled through the manufacturer's quality management system and the conformity assessment procedures for the device. In some jurisdictions, components are included in the definition of a 'MEDICAL DEVICE'.

[SOURCE: IEC 80001-1:2010, definition 2.14]

3.42
MEDICAL DEVICE MANUFACTURER
MDM
manufacturer of MEDICAL DEVICES

3.43
MEDICAL DEVICE SOFTWARE
software system that has been developed for the purpose of being incorporated into the MEDICAL DEVICE or that is intended for use as a MEDICAL DEVICE in its own right

[SOURCE: IEC 80001-1:2010, definition 2.15]

3.44
MEDICAL IT-NETWORK
an IT-NETWORK that incorporates at least one MEDICAL DEVICE

[SOURCE: IEC 80001-1:2010, definition 2.16]

3.45
MEDICAL IT-NETWORK RISK MANAGER
person accountable for RISK MANAGEMENT of a MEDICAL IT-NETWORK

[SOURCE: IEC 80001-1:2010, definition 2.17]

3.46
MULTIPLE-IN MULTIPLE-OUT
MIMO
use of multiple antennas at both the transmitter and receiver to improve communication performance

3.47
MULTICAST ADDRESSING
technology for delivering a message to a group of destinations on a network simultaneously

3.48
OPERATOR
person handling equipment

[SOURCE: IEC 80001-1:2010, definition 2.18]

3.49
PERSONAL AREA NETWORK
PAN
computer network used for communication among computer devices, including telephones and personal digital assistants, in proximity to an individual's body

3.50
PHYSICAL INTERFACE
PHY
layer of a communication controller that interfaces to the physical world

3.51
PORTABLE DIGITAL ASSISTANT
PDA
small computing device used for applications such as maintaining a personal diary or schedule

3.52
PRE-SHARED KEY
PSK
shared secret which was previously shared between the two parties to be used for the encryption of data to be communicated between them

3.53
PRIVATE DATA
any information relating to an identified or identifiable person

[SOURCE: IEC 80001-2-2:—[1)], definition 3.15]

3.54
PROCESS
set of interrelated or interacting activities which transforms inputs into outputs

[SOURCE: IEC 80001-1:2010, definition 2.19]

3.55
QUALITY OF SERVICE
QoS
the capability or means of providing differentiated levels of networking performance in terms of traffic engineering (packet delay, loss, jitter, bit rate) to different data flows

RADIO FREQUENCY
RF
frequency in the portion of the electromagnetic spectrum that is between the audio-frequency portion and the infrared portion; frequency useful for radio transmission

[IEC 60601-1-2:2007, definition 3.25]

3.56
RADIO FREQUENCY IDENTIFICATION
RFID
identification of objects or persons using special tags that contain information (such as demographics, serial number, etc.) that can be read using RF-based readers

3.57
RECEIVED SIGNAL STRENGTH INDICATOR
RSSI
measure, typically in dBm, of the RF power detected by a receiver

3.58
RESIDUAL RISK
RISK remaining after RISK CONTROL measures have been taken

[SOURCE: IEC 80001-1:2010, definition 2.20]

3.59
RESPONSIBILITY AGREEMENT
one or more documents that together fully define the responsibilities of all relevant stakeholders

Note 1 to entry: This agreement can be a legal document, e.g. a contract.

[SOURCE: IEC 80001-1:2010, definition 2.21]

3.60
RESPONSIBLE ORGANIZATION
RO
entity accountable for the use and maintenance of a MEDICAL IT-NETWORK

Note 1 to entry: The accountable entity can be, for example, a hospital, a private clinician or a telehealth organization.

Note 2 to entry: Adapted from IEC 60601-1:2005 definition 3.101.

[SOURCE: IEC 80001-1:2010, definition 2.22]

3.61
RISK
combination of the probability of occurrence of HARM and the severity of that HARM

[SOURCE: IEC 80001-1:2010, definition 2.23]

3.62
RISK ANALYSIS
systematic use of available information to identify HAZARDS and to estimate the RISK

[SOURCE: IEC 80001-1:2010, definition 2.24]

3.63
RISK ASSESSMENT
overall PROCESS comprising a RISK ANALYSIS and a RISK EVALUATION

[SOURCE: IEC 80001-1:2010, definition 2.25]

3.64
RISK CONTROL
PROCESS in which decisions are made and measures implemented by which RISKS are reduced to, or maintained within, specified levels

[SOURCE: IEC 80001-1:2010, definition 2.26]

3.65
RISK EVALUATION
PROCESS of comparing the estimated RISK against given RISK criteria to determine the acceptability of the RISK

[SOURCE: IEC 80001-1:2010, definition 2.27]

3.66
RISK MANAGEMENT
systematic application of management policies, procedures and practices to the tasks of analyzing, evaluating, controlling, and monitoring RISK

[SOURCE: IEC 80001-1:2010, definition 2.28]

3.67
RISK MANAGEMENT FILE
set of records and other documents that are produced by RISK MANAGEMENT

[SOURCE: IEC 80001-1:2010, definition 2.29]

3.68
SAFETY
freedom from unacceptable RISK of physical injury or damage to the health of people or damage to property or the environment

[SOURCE: IEC 80001-1:2010, definition 2.30]

3.69
SERVICE LEVEL AGREEMENT
SLA
the network performance required by a device or class of devices for proper operation

Note 1 to entry: A typical network services SLA covers metrics such as availability, latency and throughput. It can also include specifications for mean time to respond, mean time to repair and problem notification/escalation guarantees. In wireless systems, examples include data rate, signal strength, jitter, and latency.

3.70
SIMPLE NETWORK MANAGEMENT PROTOCOL
SNMP
Internet-standard protocol for managing devices on IP networks

3.71
SIGNAL TO NOISE RATIO
SNR
comparison of signal power to noise power

3.72
SERVICE SET IDENTIFIER
SSID
802.11 term that describes a logical grouping of multiple BSSIDs

Note 1 to entry: Sometimes referred to as an ESSID or network name.

3.73
TCP
one of the core protocols within the Internet protocol suite

Note 1 to entry: Differs from UDP in that TCP is acknowledged and connection oriented.

3.74
TEMPORAL KEY INTEGRITY PROTOCOL
TKIP
interim security solution that legacy hardware could support when WEP was found vulnerable

Note 1 to entry: Also known under the 802.11 branding as WPA.

3.75
TOP MANAGEMENT
person or group of people who direct(s) and control(s) the RESPONSIBLE ORGANIZATION accountable for a MEDICAL IT-NETWORK at the highest level

[SOURCE: IEC 80001-1:2010, definition 2.31]

3.76
UNICAST ADDRESSING
technology for delivering a message to a single destination on a network

3.77
UNLICENSED NATIONAL INFORMATION INFRASTRUCTURE
U-NII
unlicensed spectrum in the 5 GHz range used by IEEE-802.11an devices and wireless ISPs

3.78
USER DATAGRAM PROTOCOL
UDP
one of the core protocols within the Internet protocol suite

Note 1 to entry: Differs from TCP in that UDP is not acknowledged and connectionless oriented.

3.79
VERIFICATION
confirmation through provision of objective evidence that specified requirements have been fulfilled

[SOURCE: IEC 80001-1:2010, definition 2.32, modified – three notes to the original definition have not been retained.]

3.80
VIRTUAL LAN
VLAN
group of hosts that communicate as if they were attached to the same BROADCAST domain, regardless of their physical location or physical attachment to the same network switch

3.81
VOICE OVER INTERNET PROTOCOL
VoIP
technology that allows telephone calls to be made over computer networks

Note 1 to entry: A typical CODEC, the G.711 consumes a network bandwidth of 64 kbps comprised in 50 packets per second.

3.82
WIDE AREA NETWORK
WAN
communication network that spans a large geographical area, providing data transmission across metropolitan, regional or national boundaries

3.83
WIRED EQUIVALENT PRIVACY
WEP
original security mechanism of 802.11 which has been superseded by TKIP (aka WPA) for legacy devices and AES (aka WPA2) for all 802.11 certified devices since 2006

3.84
WIRELESS FIDELITY
WI-FI™
trademark of the Wi-Fi Alliance

3.85
WIRELESS LOCAL AREA NETWORK
WLAN
a LOCAL AREA NETWORK that uses RF signals to transmit and receive data

3.86
WIRELESS MEDICAL TELEMETRY SERVICE
WMTS
wireless service (set of RF bands) specifically defined in the United States by the Federal Communications Commission (FCC) for transmission of data related to a patient's health (biotelemetry)

3.87
WI-FI MULTI-MEDIA
WMM
subset of the 802.11e standard that provides a differentiated QUALITY OF SERVICE for delivery of messages for some traffic classes

3.88
WI-FI PROTECTED ACCESS
WPA
interim security solution that fixed many of the weaknesses in WEP and could be implemented on legacy hardware designed to implement WEP

3.89
WI-FI PROTECTED ACCESS 2
WPA2
long-term security solution put in place to replace WEP and WPA

Note 1 to entry: WPA2 uses the ADVANCED ENCRYPTION STANDARD and adds security features such as a message integrity check.

4 Wireless MEDICAL IT-NETWORK: an introduction

4.1 Basics

A basic understanding of the challenges presented by wireless connectivity as it relates to MEDICAL DEVICES is critical to the successful operation of a MEDICAL IT-NETWORK. The following are some of the high level challenges faced in implementing a wireless medical IT network:

– the introduction of smart phones and tablet devices running apps from social networks to cardiology viewers;
– lack of RF and wireless competency in the hospital IT, biomedical and clinical engineering staff;
– use of crowded unlicensed spectrum;
– proprietary functions on top of standards (e.g. 802.11);
– securing data on wireless devices as well as over the air;
– formal organizational engagement between IT, biomedical and clinical engineering staff.

Typically these challenges are addressed using the concept of ‘best practices’ in designing and managing a wireless network. Many of the best practices used to address these challenges are categorized as RISK CONTROL measures in the vernacular of IEC 80001-1:2010.

This technical report proposes to integrate these and other best practices into the PROCESS of applying RISK MANAGEMENT to the development of a wireless MEDICAL IT-NETWORK.

The challenges associated with meeting the SLA needs of many varied devices are compounded by the fact that MEDICAL DEVICES can have multiple levels of RISK in a single device. This technical report will emphasize that the same type of traffic in a clinical device can have varying clinical importance depending on the clinical use case or functionality. As an example, physiological data generally do not have a real time requirement when transferred into an EMR. However, if the data is going to a clinician and includes real time information about a patient's current status, then a delay in delivering this same data has now an increased HAZARD severity and might require stronger RISK CONTROL measure. Thus it is not enough to use the performance characteristics of a MEDICAL DEVICE to design and configure the network, but the clinical aspects of how the device is used and maintained are also a part of the network design solution.

4.2 Enterprise MEDICAL IT-NETWORK

Design of hospital networks is very challenging in wireless environments because of the complex physical environment and its impact on the propagation of RF signals, as well as the large number of disparate devices that operate on the network. The RF environment is typically complicated by mobile metal equipment (e.g. metal food or drug cart), walls comprised of building materials with varying RF propagation characteristics, and floor plans that change from one department to the next. The types of devices on a healthcare network include multiple types of general purpose, non-MEDICAL DEVICES as well as MEDICAL DEVICES. Some examples of these devices are guest access devices, workstations on wheels running various applications, infusion pumps, handheld data entry devices such as PDAs or tablet PCs, VoIP communication devices, RFID tags, and patient monitors. Each of these devices has its own data and traffic characteristics using various communication protocols (TCP, UDP, etc.) and with its own network performance requirements (which can vary with the clinical functionality as in the lab test results mentioned above). A device can have multiple clinical functions that include patient mobility; large image files transfers, real time clinical alerts and alarms, and transfer of physiological data into an EMR. These clinical functions, along with the device network performance requirements and data traffic profiles, define the clinical SLA. Clinical functionality maps into networking use cases, where mobility, security, low latency, high availability and other networking performance metrics need to be met. Succinctly, the differences between meeting the networking performance requirements of a general purpose wireless device compared to that of a MEDICAL DEVICE, is that the consequences of not meeting the SLA of a general purposes computer is the inconvenience of a slow network connection. A HAZARD caused by not meeting the SLA of a MEDICAL DEVICE could result in a HAZARDOUS SITUATION and potential HARM to a patient.

The diagram in

Figure 2 below shows a simplified example of a wired and wireless MEDICAL IT-NETWORK carrying traffic from both MEDICAL DEVICES and general purpose devices. The use of VLANs to logically separate traffic types is common in wired networking technology and is extended to the wireless technology at the network edge by various means (e.g. SSIDs are often mapped to a specific VLAN). In addition to the many types of traffic and associated SLAs, multiple communication paths between MEDICAL DEVICES and nursing central stations or through the data center into a centralized monitoring room can exist across a MEDICAL IT-NETWORK.

4.3 Use of VLANs and SSIDs

The use of VLANs is common in wired networks, but every additional VLAN and subsequent SSID comes with a certain overhead of BROADCAST/MULTICAST traffic that can negatively affect available capacity on the wireless link. Care needs to be used in simply using VLANs and SSIDs to segment traffic. Other mechanisms to logically separate traffic should also be explored in order to minimize overhead of BROADCAST/MULTICAST traffic associated with using multiple VLANs. These other options might include using multiple frequencies or bands with differing SSIDs and proprietary mechanisms provided by a WLAN infrastructure provider. Isolating devices using unique VLANs and ESSIDs is not considered a best practice,

especially if the group of devices that need to be isolated grows large, since every additional ESSID and VLAN brings with it an additional overhead on the wireless channel.

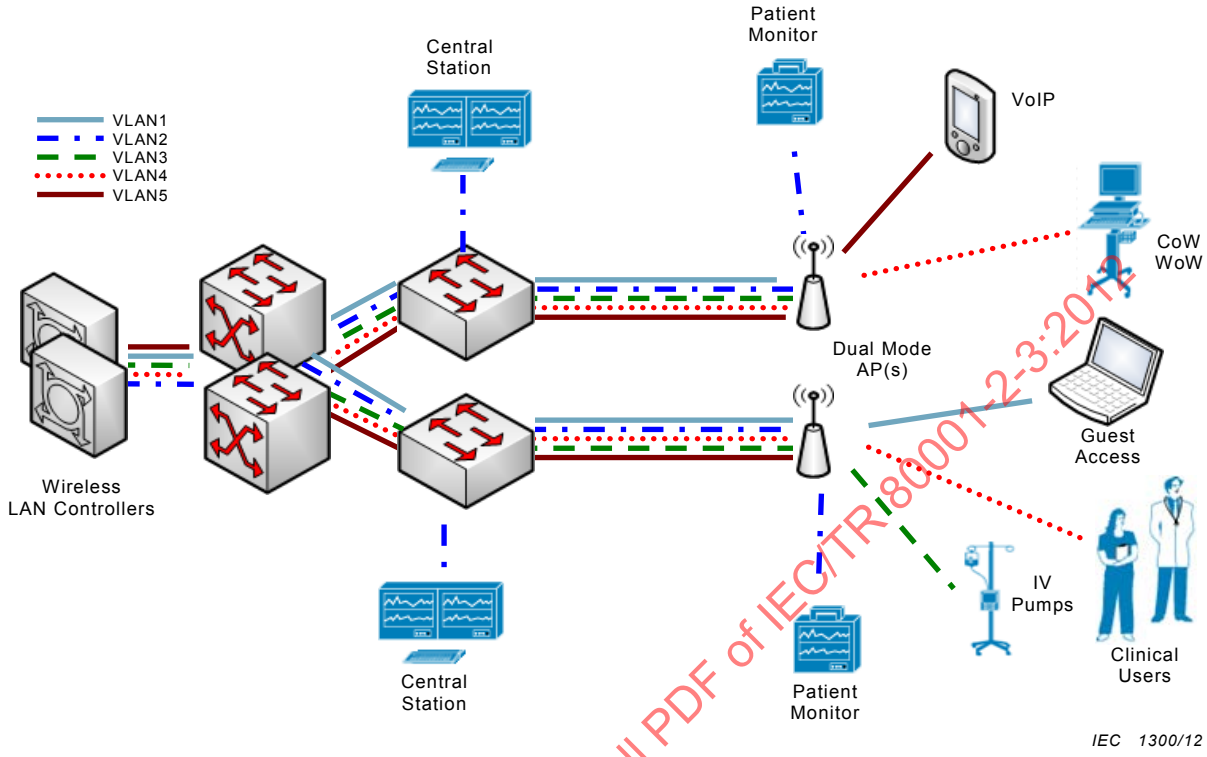


Figure 2 – HDO MEDICAL IT-NETWORK

4.4 Wide area MEDICAL IT-NETWORK

Figure 3 shows a model where MEDICAL DEVICES communicate across WIDE AREA NETWORKS, both wired and wireless, to deliver medical traffic for remote clinical access. This could be the gathering of data from remotely monitored patients at home or more advanced capabilities where video feeds allow a physician real-time, interactive access to patient data in their home. Many of the intermediate networks in the wide-area use case have components that belong to different administrative domains making it difficult to assure end-to-end SLAs. As such, these large network components make it difficult to ensure the performance required for real-time patient alarms and response where patient SAFETY is dependent on the overall network performance.

The return on the benefits for the use of a particular infrastructure, such as cellular, needs to be weighed against the RISKS. For example, for patients remote to the hospital, clinical expertise assistance across a wireless WAN, such as a cellular network, would be beneficial, even if the physician is sometimes unavailable due to a WAN outage.

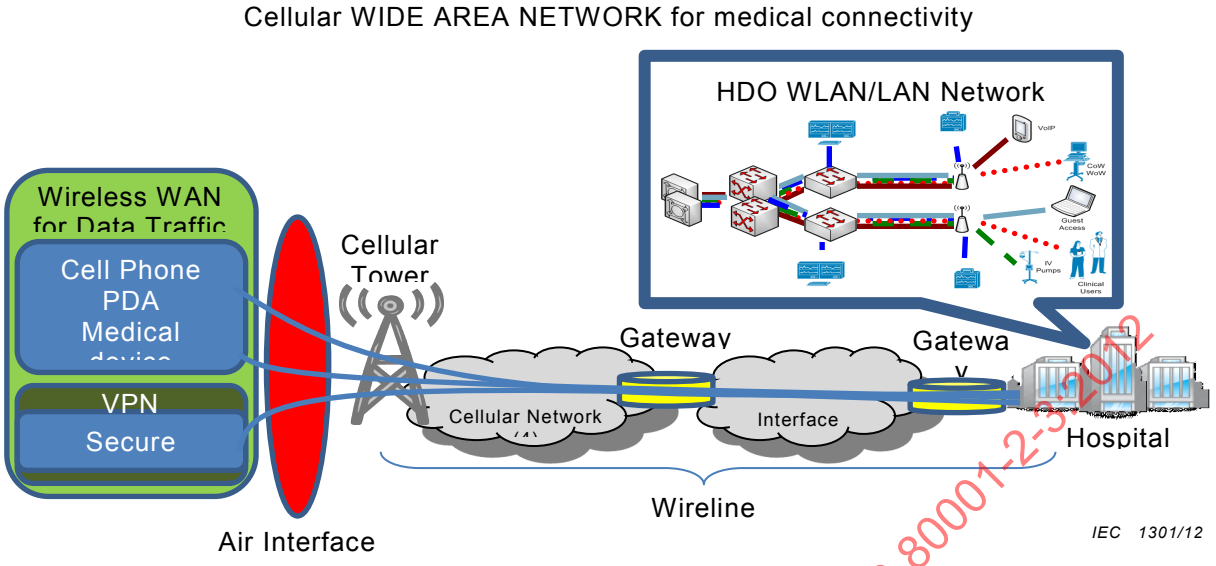


Figure 3 – Wireless WAN connectivity

4.5 Smart phone applications

4.5.1 General

The increasing use of smart phones for voice, video and data services has led to a significant amount of application development for these devices. Some of these applications are, or will be, targeted at healthcare. The use of these devices and their healthcare applications will reach both into the hospital as well as medical office buildings, clinics and homes. Just like any MEDICAL DEVICE, how the application is used clinically as well as the expected performance capabilities of the network(s) that the healthcare data transverses, should be used in the RISK ANALYSIS.

4.5.2 Application clinical functionality

While the smart phone hardware is generally not operated as a MEDICAL DEVICE, the use of healthcare applications and their intended clinical functionality will determine whether or not RISK CONTROL measures are warranted. The challenge to the IT department in an HDO lies in the fact that the network can be a WAN that is not under the configuration and control of the HDO IT administration. This does not mean that RISK CONTROL measures are not possible, just that the performance of the external network has to be understood and defined in terms of the clinical functionality and expectations of the user. It is important that the end user, whether it is a physician or patient, understand the performance capabilities of the underlying network and that some RISK CONTROL measures might need to be managed at the device by the user.

For example, the reliability of a cellular or wireless broadband networks might be acceptable for the use case of a physician remotely reviewing patient health records using a smart phone. However, the physician would need to be prepared for the circumstance that the wireless data connection could be unavailable at a given place and time.

4.5.3 Cellular networks

The advent of 4th generation (4G) networks and devices with much higher data rates, the introduction of femto cells for localized wireless deployment, and the continued evolution and advancement of smart phones will have an impact on the HDO and its ability to safely manage its network. In order to accommodate the increasing demand for bandwidth by both medical and non-medical applications and devices, it is necessary to consider the use of all networks. For example, a smart phone that includes both 802.11 and 3G/4G radios, often defaults to the 802.11 network. This can place an unnecessary burden on the 802.11 WLAN. In this case,

forcing the device to operate on the 3G/4G network is an example of a RISK CONTROL measure.

4.5.4 Smart phone coexistence

Smart phones generally include an 802.11 radio (in addition to a cellular radio) that is used for broadband access when available. If there are many smart phones in use in an HDO enterprise with demanding broadband network access requirements (e.g. wireless video, voice, etc.), then the devices can overload the capacity of the network and cause network outages that affect all devices attached to the 802.11 WLAN. Even though the smart phones might or might not be used for medical purposes, they will impact the security and performance of all devices on the network if not properly provisioned. Properly provisioning the network such that smart phones, regardless of the application, do not overload the network is a design and configuration RISK CONTROL measure that should be considered. See 6.4 for general guidance on RISK CONTROL measures.

4.5.5 Wireless data security

The transfer of patient HEALTH DATA requires that strong mechanisms be in place for securing that data. RISK CONTROL measures to prevent the loss or theft of PRIVATE DATA or HEALTH DATA includes the use of technologies preventing the storage of PRIVATE DATA or HEALTH DATA and/or remote wiping/destruction of data from the device. Security measures related to encryption and user authorization on networks are covered in the remaining clauses of this technical report. Additional information can be found in the security technical report (*see bibliography)*

4.6 DISTRIBUTED ANTENNA SYSTEMS

Some HDOs consider DISTRIBUTED ANTENNA SYSTEMS (DAS) to extend cellular, paging, public SAFETY and other RF signals through the building over a shared antenna infrastructure. The infrastructure can include active and passive technologies and many infrastructures include a hybrid of both. A passive system uses splitters, couplers, and coaxial cable to carry the signals in the form of RF energy to radiators/antennas that distribute the signal throughout the desired area. An active system communicates digital data to remote electronics that convert the digital signal to/from RF and amplify both the received and transmitted RF signals. A hybrid fiber/coax system adds passive distribution after the remote electronics.

If designed, deployed, provisioned, and validated correctly, DAS can provide operational benefits versus deploying a separate in-building antenna system for multiple WSPs, because a single DAS can provide coverage for each WSP throughout the enterprise facility. This is especially true when carrying cellular signals into an enterprise. The HDO should recognize that this wide-coverage feature causes each WSP device to receive noise from the entire coverage area, and this affects the system SNR. Similarly, benefit of DAS increasing the coverage area increases the number of users that are supported by a specific piece of WSP hardware, and this increased user load should be considered in the DAS deployment.

It is important to understand the challenges and solutions when using 802.11 technologies over a DAS. Some DAS vendors support integrating 802.11 over DAS, others do not. At this time, 802.11 infrastructure vendors do not certify their equipment in conjunction with DAS. Many of the add-on functions that 802.11 vendors promote and market such as IDS, IPS, location services, and coherent use of multipath propagation to improve RF performance are designed for use with a discrete WLAN architecture and might be compatible, though typically the AP vendors do not guarantee RF performance when using antennas other than those they test and recommend. The use of 802.11n with MIMO offers further challenge to DAS deployments as each input/output stream requires an additional antenna to operate as designed. Some features of 802.11n, such as beam forming, will require additional engineering of the DAS. Consulting with both the DAS vendor, device manufacturer, and the 802.11 infrastructure vendor is critical prior to deploying 802.11 over a DAS.

5 Wireless MEDICAL IT-NETWORKS: planning and design

5.1 Clinical systems and their impact on the wireless network

Clinical systems and their impact on the wireless network are defined in the early planning and design phase of the MEDICAL IT-NETWORK. From the IT perspective, clinicians could be viewed as new customers of the WLAN who bring to the network clinical systems and MEDICAL DEVICES that have unique and varying network performance requirements.

5.1.1 Defining the clinical SLA

Understanding how clinicians will use MEDICAL DEVICES in their work flow, as defined in this technical report as clinical functionality, is a first step in the early planning stages of applying RISK MANAGEMENT to wireless networks. It is a challenging task to support, ensure and manage the many SLAs that exist on a MEDICAL IT-NETWORK some of which will have life-critical aspects. From general purpose guest internet access to mission-critical business applications to patient monitoring devices, the networking performance requirements are varied and diverse.

The clinical SLA is comprised of both the device level network performance requirements and the clinical helpdesk-type support and procedural systems. Following is a list of typical components of a clinical SLA:

– device level network performance requirements (packet loss, delay, etc.);
– helpdesk support response times;
– network uptime or availability;
– wireless coverage areas, signal levels and bandwidth availability;
– security;
– communication protocol support & configuration;
– disaster recovery procedures;
– device maintenance scheduling.

Compiling and documenting the baseline clinical SLA is a key deliverable in the planning and design of the MEDICAL IT-NETWORK. This is accomplished by engaging with the clinicians and biomedical engineering staff during the planning and design phase to understand the PROCESSES and clinical functionality associated with the networked devices.

5.1.2 Creating partnerships

With the introduction of MEDICAL DEVICES and clinical systems to a general purpose wireless IT network, one of the initial considerations is the inclusion of the clinicians, the biomedical engineers, and the IT engineering team in the planning PROCESS. The network designer gains insight into the network performance requirements of a clinical system by reviewing with the clinicians and supporting staff how and where each type of MEDICAL DEVICE will be used. Without this understanding it is not possible to define the clinical SLA of the MEDICAL DEVICE(S) or systems.

Please refer to the table in Annex A for an example overview of MEDICAL DEVICES and their clinical and networking traffic requirements. The table in Annex A illustrates the different data types that might be encountered in a wireless MEDICAL DEVICE and their associated network profiles. Annex B provides a list of questions to consider when defining the networking performance requirements of MEDICAL DEVICES on a wireless network.

5.1.3 Geographical location

An input to defining the clinical functionality includes identifying the geographical area where the clinicians will use the MEDICAL DEVICES, applications and systems. Devices that support

mobility across the enterprise can require one or both internal and external handover support across wireless networks. Devices that are used in a specific area (e.g., ICU) might best be supported through using an isolated wireless infrastructure dedicated to MEDICAL DEVICES. These are all considerations that should be evaluated during the planning phase to choose the appropriate wireless technology.

5.1.4 Clinical use case

Asking the clinicians 'how' they expect to use the devices will help in defining the networking priority that is attached to the device and/or clinical system. For example, does it involve archiving data, or is there a real time aspect that includes life critical information such as patient alarms? Engage with the biomedical engineers who support the clinical systems to understand how they support the systems. What are their maintenance plans including the upgrading of devices, and seek a partnership where PROCESSES and procedures are jointly managed when the network is involved. Determine how the devices are configured for network access. The outcome of these efforts will be a clear understanding of the networking priority that needs to be applied to the MEDICAL DEVICE and systems and jointly defined rules of engagement regarding the management of the devices and network related clinical support models.

5.2 MEDICAL DEVICE wireless capabilities

Accompanying the investigation of the clinical functionality is a need to understand the wireless capabilities and performance characteristics of the MEDICAL DEVICES, applications and systems. Engaging with the MDM to fully understand the MEDICAL DEVICE capabilities regarding wireless performance is an important early step in the design and configuration of the wireless network. The combination of understanding the clinical functionality along with the device level wireless performance characteristics allows for the establishment of the baseline requirements for wireless networking design.

5.3 MEDICAL DEVICE capabilities and networking traffic profile

The wireless technology defines the networking characteristics that provide the boundaries for the wireless performance of the MEDICAL DEVICE. Some examples include but are not limited to:

– PHY (physical radio interface); receiver performance specifications, supported modulation and coding types, data rates, frequencies, and transmit power levels;

– MAC (link layer component): deterministic vs. non-deterministic network access, QoS capabilities, security, AP handover for roaming, and power saving mechanisms;

– network (IP layer): DHCP or BOOTP, subnet or layer 3 roaming, BROADCAST and MULTICAST data type usage;

– transport protocol: TCP (connection oriented), UDP (connectionless);

– application/device layer: traffic types (real-time, non-real-time), bandwidth, power saving mechanisms, higher layer acknowledgments.

Once the capabilities and traffic profile of the MEDICAL DEVICES, systems, and/or application types are understood from a wireless technology perspective, the network designer can begin to design and configure the wired and wireless network to properly support the MEDICAL DEVICES and systems.

5.4 Network performance requirements

A MEDICAL IT-NETWORK has to support the performance requirements of the MEDICAL DEVICE systems determined during the planning and design phase; otherwise the clinical system(s) might not be safe, secure or effective. The network performance requirements of all devices once known should be documented to provide a reference baseline for testing before and during installation, and when changes are made that might impact system performance. Changes that can affect device performance include actual network configuration changes,

RF environment modifications, and adding devices to the network. The network performance requirements of every device need to be accommodated in the network topology and configuration. The network should be designed to ensure the network performance requirement for the most sensitive application/device on the network is met while the network maximum load is in place. A listing of some device performance requirements to consider is included in Annex B.

A good rule of thumb is to determine the MEDICAL DEVICE performance requirements from the device specification, noting the most restrictive performance requirements. Match these to the performance capabilities (as specified and measured) of the network (wireless and wired). As an example, one manufacturer specifies a maximum network load and maximum number of users on the AP. To ensure these maximums are not reached, the HDO decides to add extra APs in the location where the devices will be used. This RISK CONTROL measure also tends to provide a higher signal strength (and SNR – see Figure 4) since APs are closer to clients. Because of decreased contention for airtime, bandwidth, latency, packet loss and transceiver performance requirements are all mitigated by this design decision. The use of network monitoring tools to monitor the network performance characteristics, with generation of alerts when conditions degrade, is a further RISK CONTROL measure against failure to maintain device-specific SLAs.

5.5 QoS mechanisms

QUALITY OF SERVICE (QoS) mechanisms provide preferential access to the network within a technology. This can be used to assist in ensuring that the network is able to meet the clinical SLAs required by clients with high priority data by giving these clients favored access to the network than low priority clients. Wireless technologies have differing methods of providing QoS, and vendors supporting the same standards can implement the QoS mechanism differently. For example, in an 802.11 network, WMM provides four classes of service as a standard option. In addition to this, some vendors might provide traffic shaping and/or reserved airtime via proprietary schemes. The HDO should VERIFY that the wireless clients and the wireless network have compatible and consistent QoS solutions. Furthermore, ensure the QoS policies are effectively applied end-to-end across the network. This includes any QoS mapping between the wired and wireless networks.

An example scenario is that an HDO decides to provide wireless guest access and wants assurance that guest access to the WLAN doesn't interfere with patient data. The HDO already uses 802.11e QoS to segment traffic on the WLAN. Voice devices and MEDICAL DEVICES share the voice QoS category, while video traffic is assigned to the video category. The guest access SSID and associated devices are assigned to the best effort category and hence have a lower priority of access to the WLAN.

If a device or group of devices does not support QoS, the HDO segments non-compliant devices into a separate band or subset of channels to provide a separation at the physical layer.

5.6 Receiver capabilities

The SNR of a received signal is the ratio of the received signal power to the RF noise power at the receiver (see Figure 4). The minimum SNR for a device to operate at a certain data rate is the lowest SNR that enables reception and decoding of the received packet at a specified or maximum allowable packet error rate. Many factors are involved in determining a device's SNR requirements, but, all other things being equal, the lower the SNR requirements of a device, the better it performs in degraded RF signal conditions. The minimum received signal strength of a device is a measure of the received signal power required for the device to properly decode the signal at a specified packet error rate. In the case of SNR, it is the "S" (desired signal strength) in SNR. In Figure 4, AP1 has received signal strength of -65 dBm and an SNR of 30 dB. AP2 has received signal strength of -55 dBm and an SNR of 40 dB.

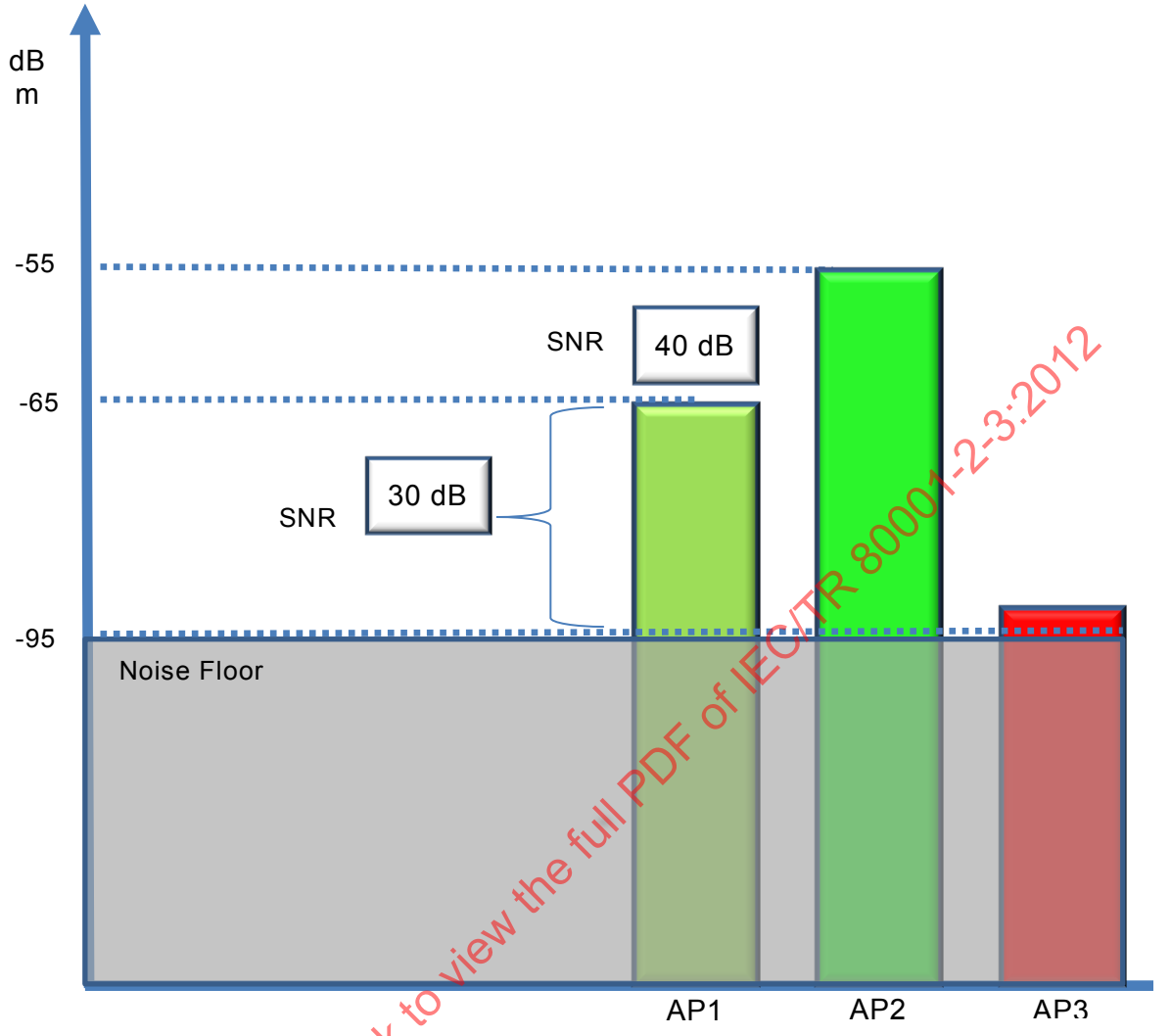


Figure 4 – SIGNAL TO NOISE RATIO

5.7 Received signal strength and SNR versus data rates

As the received signal strength (RSSI) and attendant SNR decreases, the maximum data rate at which the receiver can successfully decode the signal also decreases. The SNR is the amount, or margin, of signal level above the receiver sensitivity threshold or noise floor (whichever is higher). Assuming a noise floor and receiver sensitivity of -88 dBm, for 802.11, an RSSI of -65 dBm and consequent SNR of 23 dB (88 – 65 = 23) generally allow a 36 Mbps data rate. At an RSSI of -82 dBm and same receiver sensitivity of -88 dBm, the consequent SNR of 6 means that the receiver might only support a data rate of 6 Mbps. However, a low data rate channel can allow successful reception of data with a weaker signal at longer distances from the AP. Similarly, a high density of devices, especially devices that require high data rates or very low error rates, require a high SNR. This is why applications or devices that use a lot of bandwidth (video streams) or require low packet error rates (real time traffic such as VoIP or streaming patient waveform data) has to be deployed in a high SNR environment. The RISK CONTROL measure of over-provisioning the network capacity is aligned with the concept of delivering the SNR required for the most effective data rate possible while simultaneously minimizing the effect of high AP signal levels on the overall background RF noise.

MEDICAL DEVICES support various communication protocols based on their design and purpose. Some of the common layer protocols that are encountered in a MEDICAL DEVICE are IP, TCP, UDP, and lower MAC layer protocols. Traffic types that can have differing impacts on the wireless performance and requirements are the various uses of UNICAST, MULTICAST and

BROADCAST. A MEDICAL DEVICE can use multiple types of protocols, traffic types and other networking traffic functions in a single device. For example, a patient monitoring network can use BROADCAST traffic for communications setup, UNICAST traffic to talk between devices, and MULTICAST traffic to talk between multiple devices. Some vendors deliver BROADCAST/MULTICAST traffic as multiple UNICAST messages (one for each associated client) at an AP. This type of conversion can consume higher amounts of wireless network bandwidth. Vendors can also enhance the delivery of UNICAST messages only to clients that need to receive this message thereby limiting the amount of wireless channel bandwidth used while gaining reliable delivery of such messages at the same time. On the other hand, by default, BROADCAST and UNICAST messages are not acknowledged, so message delivery is not confirmed. It is important to understand and design the network to support the delivery of all traffic types required by a MEDICAL DEVICE while ensuring that the medical traffic will coexist with network traffic from other network devices. The design needs to include the consideration of all data types and their communication protocol.

For example, in an 802.11 network a specific MEDICAL DEVICE requires the use of MULTICAST, while a second MEDICAL DEVICE type specifies that MULTICAST traffic be minimized. When MULTICAST traffic is required, for example, if some devices or applications make use of MULTICAST traffic, the network designer should understand and enable proper IGMP versions and support across the network path. Because many times these devices have different MULTICAST requirements, the network design should logically isolate the devices appropriate methods. As mentioned earlier, the segmenting of traffic by SSID/VLAN is not considered best practice beyond a small amount of devices and SSIDs. Other vendor specific mechanisms should be explored to isolate traffic on the wireless link.

5.8 Capacity versus coverage versus AP density

Capacity, coverage and density are inter-related considerations in the design of a wireless network:

– Capacity relates the available bandwidth to a specific geographical location. Capacity is affected not only by the density of wireless ACCESS POINTS, but also by the signal strength which is directly related to data rate.

– Coverage typically is used to indicate that a wireless device can connect to the wireless network, without any connotation regarding available bandwidth.

– Density of the AP deployment relates to both capacity and coverage, because the denser the deployment, the higher the available capacity (channel planning dependency aside) and RF signal coverage.

Specifying the signal strength for a given coverage area is no longer sufficient for wireless network design. The capacity requirements for that area have to be considered and addressed by providing the required density of ACCESS POINTS. For example, a nursing station can have many wireless users in a small physical area. If these users and associated application(s) require the aggregate peak bandwidth of 45 Mbps, and a single 802.11 AP can deliver a 'real world' throughput of approximately 15 Mbps, then a minimum of 3 ACCESS POINTS would be required in this physical area to support the application without considering the need to overprovision in terms of available capacity.

An example of coverage compared to capacity is a DISTRIBUTED ANTENNA SYSTEM connected to an 802.11 AP such that it provides extended coverage to an entire floor. If this is done with the use of multiple antennas and/or radiating coax, it can expose that AP to a large population of devices and users. In this example, it is likely that the capacity of that AP will be exceeded. Regardless of whether a DAS is used or the AP manufacturer's recommended antennas are used, it is important to correctly provision the number of APs in an area to achieve proper load balancing. Alternately, simply install the APs in a standard discrete deployment independent of the DAS.

For the case of cellular coverage vs. capacity, the cellular service provider should review the quantity of devices to be enabled in the facility and plan accordingly with micro-cell or pico-

cell installation(s). The HDO should work with a cellular provider in reviewing the types of devices and applications that will be operating on their network to ensure that sufficient capacity exists to support peak load conditions.

5.9 Deterministic versus non-deterministic wireless access protocol

Deterministic access is such that devices are a-priori granted access to the network in predefined time slots, (i.e. allotted a dedicated fraction of total capacity). Non deterministic access means that devices have to contend for the medium, and access to the network is not guaranteed. A deterministic protocol uses fixed time slots, making them inflexible regarding timing, so a burst of data has to wait for its time slot to transmit even if no other devices are using the medium.

Proprietary protocols have the advantage of a turnkey solution managed by the vendor but this can also be a disadvantage, since an HDO might be locked into a particular vendor. Standards-based protocols generally have multiple vendors to choose from but require a higher degree of design, deployment and network management competency by the HDO.

The use of deterministic versus non deterministic protocols, standards based vs. proprietary, or other unique attributes of protocols is dependent on both the available wireless technologies and the device requirements. A deterministic solution can provide a higher level of assurance in packet delivery, but less efficient use of the time domain. In a non-deterministic system, over-provisioning the network capacity is required.

5.10 Planning and design summary

Defining the networking performance requirements of the MEDICAL DEVICE as used by the clinician and matching them to the capabilities of the wireless technologies available are key deliverables of the planning phase. Adhering to the guidelines as reviewed in this clause provides a strong foundation of RISK CONTROL measure for the actual design of a wireless MEDICAL IT-NETWORK.

6 Wireless MEDICAL IT-NETWORKS: Deployment and configuration

6.1 RISKS versus benefit of a wireless communications system

The RISKS for wireless communications systems have to be considered against the benefits, such as increased mobility of patients, devices and clinicians with faster access to data. Many RISKS are independent of which wireless solution is in place; rather, all wireless systems have inherent RISK due to relying upon a medium which is not constrained by a physical boundary. For example, while user authentication is required for both wired and wireless systems, the inability to ensure that an unauthorized user cannot access wireless data requires a different technical approach than would be taken on a wired LAN. Connections to wired LANs are generally unaffected by nearby construction and other electronic devices, while connections to wireless LANs can be greatly affected when signals are blocked by newly erected walls or other wireless devices create interference.

One should consider that many wireless technologies exist beyond the wireless LAN. These include multiple WAN, PAN, and proprietary technologies, each of which exhibit desirable characteristics that a facility might wish to employ with networked MEDICAL DEVICES.

6.2 Licensed versus unlicensed spectrum

Generally speaking, licensed spectrum is regulated by governing bodies that set laws dictating what or who is allowed to use a particular band of spectrum. Cellular systems operate in licensed spectrum and are allowed to operate relatively interference-free from other sources. Unlicensed spectrum is governed by specific regulatory rules regarding interference from unintentional radiators, but the spectrum is neither limited to specific devices nor to wireless technologies. Devices that operate in unlicensed spectrum need to be

able to co-exist with other types of devices, and accept a certain threshold of interference. All potential candidate bands of spectrum, regardless of licensed or unlicensed, should be evaluated at the HDOs facility for levels of interference from all sources. Additionally, the devices ability to operate in the presence of interference is a consideration during the wireless networks RISK ANALYSIS.

6.3 Interference sources

Applicable to both licensed and unlicensed spectrum usage, identifying interference sources (e.g. microwave ovens, two way radios, neighbor WLANs) is a challenging and critical factor to the performance of a wireless network; challenging in that identifying and managing an interfering source is difficult at best, and critical in that these interfering sources can cause a portion or the whole wireless network to fail for extended periods of time. Generally speaking, the use of unlicensed spectrum has a higher probability of interference. While interference sources are more likely in unlicensed spectrum, licensed spectrum is not immune from interference. A common source of interference in the 2,4 GHz band is microwave ovens. A policy of evaluating placement of microwave ovens near clinical areas where MEDICAL DEVICES operate is a RISK CONTROL measure. This evaluation includes testing for interference and using new model microwave ovens that have reduced RF emissions. More generally, the interference sources in and around an HDO should be known and considered as part of the wireless network RISK ANALYSIS.

6.4 Spectrum usage and allocation

6.4.1 Device coexistence

If devices are coexisting in the same spectrum but using different wireless technologies, the systems have to have inherent mechanisms to avoid the impact of RF collisions (e.g. using RF energy detection and avoidance methods). Preferably the ability to segregate disparate wireless technologies sharing the same spectrum by means of physical location is preferred. Devices can coexist in the same physical space by operating in different parts of the spectrum (e.g. cellular bands versus WMTS versus unlicensed bands). However, many times this is impractical as many devices can operate in the same spectral band.

If devices needs to coexist in the same physical space and the same spectral band (e.g. U-NII bands), then the next area to evaluate for proper deployment is the spectrum availability and usage. This might or might not require separate infrastructures. For coexistence on the same infrastructure, frequency separation by proper channel planning is a means of providing higher capacity without interference. Proper frequency planning, or channel management is essential to increasing capacity in a physical space. Advanced functions such as MIMO, beam-forming and smart antennas can provide more efficient spectral reuse and less interference, and if available should be evaluated in context of the requirements for the specific physical areas of deployment. The wireless network vendor and device manufacturers should be consulted to determine if they have validated these solutions.

6.4.2 Spectrum management

Proper use of available spectrum is a cornerstone of successful wireless MEDICAL IT-NETWORK deployment. Preferably, the allocation of spectrum would be based on the network access priority and criticality of the device's clinical requirements. For example, if two applications on the network degrade the RF performance of each other, the HDO should consider giving spectral preference to the higher priority application. An example is the deployment of 802.11 devices. Using the U-NII bands (5,150 – 5,875 GHz) in addition to using the 2,4 GHz bands and coherently separating devices across these bands based on priority and clinical use cases is a proper mechanism for deploying across all available spectra.

Spectrum management requires an understanding of which wireless technologies are available and their characteristics. It also requires understanding which of these wireless technologies is in use within and around the HDO facility. With this understanding the HDO can properly determine where interference can exist. Using this information the physical and/or frequency separation of the clinical devices can be managed to mitigate the RISK of RF

interference. If the devices need to coexist in the same physical space and share the same spectral bands, then the spectrum and channelization has to be properly deployed to provide adequate performance for meeting their INTENDED USE.

Sometimes the use of different slices of spectrum around the HDO facility, especially by those that are not within the administrative control of the HDO, can change with time. Adapting to such changes in spectrum usage requires continuous monitoring of the RF environment, and taking corrective action when necessary to maintain unused or less-used slices of spectrum for critical HDO applications.

6.4.3 Capacity management

Wireless spectrum is a finite resource that has to be shared amongst devices. As each device consumes spectrum and airtime to transmit and receive information, other devices have to wait their turn. Capacity management's goal is to ensure that all devices can access the wireless infrastructure per their SLA. Some important examples of techniques for achieving required capacity are installing a sufficient number of wireless ACCESS POINTS and frequency reuse through proper channel planning. Managing and metering airtime for channel access across different traffic classes is another method to manage capacity and ensure SLAs are met. Exploring these types of options (some of which are proprietary) with the wireless networking vendor is an important part of the planning and design phase.

6.5 Wireless network configuration (802.11 specific)

6.5.1 General

The configuration of the wireless LAN components determines the network's ability to provide safe and effective communications.

6.5.2 VLAN and SSID

The logical separation of devices using VLANs can provide isolation on the wired segment of the network. VLANs are mapped to the wireless network using SSIDs to extend the logical isolation to the wireless devices. This concept is a common practice with MEDICAL DEVICES to mitigate against undesirable and potentially incompatible network traffic, and to prevent unnecessary client power consumption that can result from receiving unwanted MULTICAST or BROADCAST traffic.

Using SSIDs to logically separate devices is a means to provide unique services (e.g. security policy) to groups of devices, but has other consequences that needs to be understood during network design. The number of possible SSIDs is limited, especially when compared with the number of possible VLANs. Increasing the number of SSIDs on the same physical infrastructure increases the idle load (i.e. due to multiple beacon transmissions, etc.) on the wireless channels, decreasing the available capacity for critical data, and increasing complexity in WLAN management.

As mentioned earlier, VLANs do not have additional cost on wired networks, but do present additional overhead on wireless links when VLANS are mapped, and thus require a unique SSID, to each WLAN on the wireless link. Each SSID will present additional idle load in the form of beacons. Best practice dictates that they are both minimized and other methods of traffic separation, such as assigning WLANs to specific bands of spectrum (e.g. U-NII and ISM).

6.5.3 Authentication and encryption

Wireless security provides protection from eavesdropping and from unauthorized network access. Ensure the minimum acceptable level of security is supported by the wireless technology and implement the highest level of security available. For example, due to a number of well-known vulnerabilities, it would not be recommended to use WEP as the security mechanism for patient data transport in an 802.11 network. TEMPORAL KEY INTEGRITY

PROTOCOL (TKIP), the mechanism employed by the original WI-FI PROTECTED ACCESS (WPA) protocol, addresses the key shortcomings of WEP, however newer more preferred methods are now available. The Wi-Fi Alliance now recommends WPA2 / 802.11i, which uses ADVANCED ENCRYPTION STANDARD (AES) [1], as the minimum security capability. WPA2-Personal, which uses a PRE-SHARED KEY (PSK) requires the same key be used for all users, which can be limiting and logistically challenging. By contrast, WPA2-Enterprise allows a variety of flexible authentication mechanisms based on 802.1X EXTENSIBLE AUTHENTICATION PROTOCOL (EAP) that can be different for each user or device. For an 802.11 deployment, WPA2-Enterprise provides a greater level of security and access control than WPA2-PSK. There are a large number of specific EAP types that could be implemented in different devices, as well as supported on the network. Using an EAP solution that supports bi-directional certificates (server and client side) such as EAP-TLS is considered a stronger solution than username/password for client-side authentication, but imposes a potentially difficult challenge related to generating and maintaining a large number of client-side certificates. A RISK ANALYSIS should be used to determine if the actual use case requires the additional complexity of implementing bi-directional certificates.

6.5.4 Vendor proprietary extensions

Many standards-based wireless technologies such as 802.11 have proprietary components. These proprietary functions might not be compatible with all devices and can have both positive and negative impact on performance of MEDICAL DEVICES. It is important to understand the operation of these functions as it relates to the networking performance characteristics of the MEDICAL DEVICES. Examples include mechanisms to support asset tracking and algorithms to set AP channel and transmit power. Engage with the wireless networking vendor to understand the impact of these proprietary functions so that the configuration of the network can optimally use proprietary extensions.

6.5.5 Cellular and proprietary networks

Cellular and proprietary wireless networks are either managed by service providers or pre-configured where minimal or no networking oversight is required of the HDO. This includes the configuration and technical characteristics of wired networking devices such as switches (core, distribution and edge), routers (directing packets between LANs, or to a WAN, or to the Internet and/or to a cellular network), the security levels within the network and number of MEDICAL DEVICES that are part of the wired network. This technical report does not directly address the RISKS of a wired network, but they are related in that most or all wireless MEDICAL DEVICES eventually connect to the wired network for server access that typically have a wired network connection. As such, the wired network is part of the overall medical network system and should be considered systemically in overall network planning and design for ensuring the networks support clinical SLA of MEDICAL DEVICES.

Although the HDO cannot be responsible for the detailed design, implementation and management of cellular and proprietary wireless networks, it should work with the network and service provider to define and ensure that the network meets an appropriate SLA.

6.5.6 Network availability

If data availability is critical, then the network has to be designed to quickly recover from component failures. Building in redundancy and resiliency to increase network availability can ensure that no single-fault failure stops the flow of data. For example, in a critical continuous patient monitoring application, if a router or WLAN controller fails, there should be an alternate path for data to flow from the patient to the clinician. Due to different RISK levels, the requirement for recovery speed might be different for life-critical data compared with general purpose data. Recovery times for different backup solutions can vary from several seconds to several minutes. The best backup solution to use depends on cost of implementation and probability of occurrence of a HAZARDOUS SITUATION (e.g. patient experiences an arrhythmia

[1] http://www.wi-fi.org/files/kc/WPA-WPA2_Implementation_2-27-05v2.pdf

during the time required for network recovery). A RISK ANALYSIS is used to determine if a faster and more expensive backup recovery solution should be put in place.

In the wireless or RF space, the use of overlapping coverage provides a mechanism for high network availability. As discussed in 6.4, proper use of RF channels allows for use of RF redundancy. For example, the 2,4 GHz ISM BAND has 83 MHz of spectrum, while the 5 GHz U-NII bands provide up to 555 MHz of spectrum. In the case of 802.11 in the USA, this translates to 3 available non-overlapping channels in the 2,4 GHz spectrum and up to 24 non-overlapping channels in the U-NII spectrum. Due to the small number of distinct channels in the 2,4 GHz band, it is not feasible to overlap coverage in a large physical space where high capacity is required using 2,4 GHz. The higher number of available channels in the 5 GHz U-NII bands allows for RF coverage overlap and thus RF redundancy, which translates into high wireless network availability.

6.6 VERIFICATION testing

6.6.1 General

The use of network VERIFICATION testing is an industry best practice that is directly applicable to successfully deploying and operating a wireless network. Network testing discovers errors not only in 1) the network hardware or firmware, or 2) INTEROPERABILITY between the device and the infrastructure, but also in 3) the design, topology, and configuration of the network which is owned by the network designer/maintainer. There will always be variance from one network to another, and neither the MDM nor the IT equipment manufacturer has complete visibility into the design and day-to-day operation of a hospital-unique network. In terms of the design, deployment and configuration of a wireless MEDICAL IT-NETWORK, VERIFICATION testing is a necessary task.

Many HDOs do not have the facilities to support the creation of a lab network to perform VERIFICATION testing. Segmenting a portion of the live network so that it can serve as a test bed without connecting devices to actual patients can be an appropriate alternative. Providing full access to the implementation team (IT, biomed, clinicians, etc.) during the VERIFICATION testing is important, and the ability to test devices and systems on the actual network is of great value.

6.6.2 Pre GO-LIVE VERIFICATION testing

The use of a lab environment to emulate and VERIFY the performance of both MEDICAL DEVICES and non-MEDICAL DEVICES on a WLAN is an important component of RISK CONTROL measures. While the lab testing will give a good indication of overall performance, it cannot replace testing on the actual MEDICAL IT-NETWORK environment, as the lab environment only approximates the actual environment. In addition, VERIFICATION should also include testing to confirm that the network is available as designed when individual network components go off-line.

6.6.3 GO-LIVE VERIFICATION testing

After isolated VERIFICATION testing, the network changes are tested in the actual environment. Preparation for testing involves creating an installation plan to move to the new solution which includes a personnel support plan (e.g. extra staff available) in case the upgrade fails or includes network downtime[2)]. This involves the support of IT, clinicians and biomedical engineering to trial the MEDICAL DEVICES on the live network. Device and network configurations, expected down time, extra support personnel and actual use by clinicians should all be part of the installation plan for GO-LIVE VERIFICATION testing. For large deployments, a staged release after successful testing might be warranted. For example, a multi-floor system might be rolled out one floor at a time.

---

2) The 10-step RISK ANALYSIS process described in IEC 80001-2-1:2012 provides a template that can be used to define roles and responsibilities during network upgrades.

7 Wireless MEDICAL IT-NETWORKS: Management and support

7.1 General

This clause provides an overview of RISK CONTROL measures and best practices associated with managing a MEDICAL IT-NETWORK after deployment and configuration.

7.2 Network and application management

Once the MEDICAL IT-NETWORK is planned, deployed, and VERIFIED, use network and application management tools to monitor and mitigate wireless network performance degradation events and outages. A RISK ANALYSIS should be used to define the required scope and scale of network monitoring tools or capabilities. Simple RISK CONTROL measures such as SNMP traps to large scale third party enterprise tools should be considered. The goal should be to identify performance degradation before it actually manifests as a HAZARDOUS SITUATION or HARM.

The use of network monitoring on the wireless and wired infrastructure(s) combined with application layer monitoring can provide insight into the real time performance of the network. Monitoring can also provide alerts of low capacity or other issues that might degrade the network's ability to meet the required SLAs

7.3 Policies and procedures

Define, document and distribute strong policies and procedures regarding the use of both the wireless network and RF environment. Policies should focus on the restricted (by location perhaps) use of wireless or other devices that might interfere with devices on the HDO wireless network.

Examples include:

– the location of where personal communication devices, such as cellular phones, Bluetooth headsets, DECT or other cordless phones can be used;

– the prohibition of individual or group use of rogue wireless network devices such as 802.11 APs;

– determining the physical placement and/or replacement (e.g. with models that generate lower levels of RF emissions/interference) of HDO assets that might be interference sources such as microwave ovens, electrosurgery equipment, etc.

Document the procedures that outline the PROCESS of approving the connection of a wireless device to the network. A policy should define the requirement that any purchases of wireless devices include the review of IT staff as part of the RESPONSIBLE ORGANIZATION before the purchase is made. Policies should be clearly posted for guest users as well as internally distributed.

7.4 Change control

Awareness and understanding of the potential impact on the performance of MEDICAL DEVICES from changes in a MEDICAL IT-NETWORK allows RISK MANAGEMENT to be applied to the change control PROCESS. Examples of changes include changing the wireless controller software versions, applying software patches, or changing the configuration of a networking component (note that some wireless network management systems will automatically change networking device parameters.) As an example, updating wireless controller firmware to support a security patch might fix an issue with security, but cause problems elsewhere in the network as a result of the introduction of a software defect in the new controller software. A hardware example would be the upgrade of an AP from 802.11abg to 802.11abgn. In all of these instances, the use of pre GO-LIVE VERIFICATION testing as part of a change control PROCESS, as described in 6.6, is recommended.

Upgrading to a release of network infrastructure hardware or software without consulting with the MDM is not recommended. Early releases of software have a higher probability of performance issues. It is recommended to check with the MDM to determine if any VERIFICATION testing of their devices and the wireless infrastructure software version in review has been completed. It is important to note that with the proliferation of hardware and software versions available from both the network infrastructure vendors as well as the MDM, it is probable that not all combinations will be tested prior to the roll-out of a specific combination at an HDO. If the desired combination has not yet been tested, the HDO should complete their own VERIFICATION.

As the release of some hardware, software and firmware updates by wireless network vendors is generally not scheduled (e.g. security updates), the MDM might not be able to complete validation in a time requested by the HDO. The HDO should consider in their RISK ANALYSIS the RISKS of running wireless networking software that has not been tested for INTEROPERABILITY by MDMs. If neither is acceptable, the HDO should complete testing for VERIFICATION.

Changes to the physical environment will affect the RF coverage. The use of site surveys or RF management tools to validate the RF coverage after any environmental changes is a key RISK CONTROL measure. Examples include the renovation of units or floor plans where wireless is used for MEDICAL DEVICES.

Adding new applications, medical or non-medical, can impact the performance of existing networked devices in a shared wireless environment with finite available bandwidth. Examples are enabling WLAN guest access and the addition of asset tracking / location devices.

8 General RISK CONTROL measures

8.1 General

The previous clauses outlined a PROCESS by which a wireless MEDICAL IT-NETWORK can be planned, designed, deployed and managed. Clearly every network is different including the use of different technologies and vendor solutions. This final clause will review some RISK CONTROL measures that can be applicable to a specific technology or HDO. It also provides a summary of some of the inherent best design practices covered in previous clauses. When determining the list of unique causes unique to an HDO, this clause's listing of RISK CONTROL measures should be reviewed for applicability and might assist in filling RISK ANALYSIS gaps.

8.2 Determining baseline networking performance

Understanding the performance characteristics of a wireless technology and matching them to the performance requirements of the networked devices are vital to ensuring the proper deployment of MEDICAL DEVICES on a wireless infrastructure.

A grouping of devices is one where all the devices share the same network performance capabilities and requirements. Categorizing each grouping of performance requirements into specific wireless performance characteristics, including WLAN configurations, is a recommended method of defining each group. One should design the wireless network to match the requirements of the most stringent performance characteristics of the devices for each grouping, thus inherently meeting the SLA of less demanding devices in terms of networking performance.

8.3 Designing for coverage signal strength

It is a good rule of thumb when using wireless technologies such as 802.11 to deploy the wireless infrastructure such that its minimum RSSI and SNR in the intended coverage area is above the MEDICAL DEVICE'S specified receiver sensitivity and SNR for its highest supported data rate. RF signals in a real-world environment such as a hospital can vary in signal strength by 10 dB while standing still and experience fading (reduced signal due to multipath

effects) of 20 dB or more. Thus if a devices receiver sensitivity for the highest data rate possible is -75 dBm (or 20 dB SNR if noise floor equals -95 dBm), then the wireless network design might need to provide coverage at -65 dBm.

Another view is to measure the RF noise floor in the wireless coverage area over a period of time to identify worst case scenarios, and reduce the transmit power of the wireless APs, and/or space the APs closer, such that the received signal strength of the MEDICAL DEVICE exceeds the highest data rate receiver sensitivity by a margin of at least 10 dB. Refer to Figure 4 for a graphical representation of SNR.

8.4 Segregating traffic and data types

As a typical best practice, networks are logically segmented to isolate (e.g. use of VLANs) BROADCAST traffic to its intended domain or subnet. This same best practice, when traffic types can be clearly identified, can be used to separate life-critical data from general purpose IT traffic. After identification of the clinical use of a MEDICAL DEVICE and associated traffic (e.g. life critical, data archiving, etc.), determine the MEDICAL DEVICE supported communication protocols, addressing modes (UNICAST, MULTICAST, BROADCAST), and other protocol usage information. Create VLAN(s) on the wired link for different classes of MEDICAL DEVICES and clinical data and then map the wireless MEDICAL DEVICES to the proper VLAN (e.g. for WI-FI the SSID is mapped to a specific VLAN).

8.5 Environmental and physical changes

Physical changes in the wireless environment (e.g. floor plan changes) will impact the RF performance of wireless devices. Obstructing or altering the RF signal path can have a significant performance impact on a device's wireless link. A potential RISK CONTROL measure would be to evaluate all physical structure changes in a MEDICAL IT-NETWORK environment for adequate RSSI and SNR and test after any changes. Move or install additional wireless infrastructure (e.g. APs) as determined by an RF site survey or other means.

8.6 Maintaining a clean RF environment

It is a challenge for the HDO to keep the RF environment clean on its existing and managed wireless network(s). Outside interference from neighboring networks, microwave ovens, other users of unlicensed spectrum (Bluetooth, DECT phones, Zigbee, etc.) can intermittently appear in the HDOs managed RF space. Periodic surveys of the coverage area using spectrum analysis tools to scan and identify sources of interference is one way to mitigate against unknown and unmanaged interferers. Define and document policies that remove or restrict the use of interfering sources (by location if possible). Another potential way to mitigate against interference is to dedicate the least congested channels to MEDICAL DEVICES, whether they be in licensed or unlicensed bands.

8.7 Capacity planning

8.7.1 General

Designing a wireless network that always maintains a specific amount of capacity above the user load is a difficult task because quantifying usage of the network from many disparate devices over time is nearly impossible. In terms of probability, usage is typically a Poisson-distributed random PROCESS and can also include spatial-temporal variance. The difficulty in quantifying the precise load is part of the reason for provisioning the network with significant margin (e.g. designing with fifty percent more capacity than required for the expected usage). If the network is a proprietary network, management of capacity might be built-in (e.g. in a channelized wireless telemetry system).

A RISK CONTROL measure against an overloaded network is to test and VERIFY the actual impact introduced by changes to networking equipment and wireless network clients. Gather both the MDM and wireless infrastructure provider's performance specifications to understand capacity requirements of devices and applications versus coverage area capacity. One way to

envision coverage area capacity is to think of the available bandwidth (Mbps) per unit area of floor space.

As an example, consider a 1 000 m^2 hospital floor. During the planning and design phase it is determined that the combined peak capacity requirements of all devices (medical and non-medical) is 100 Mbps, or 100 Kbps/m^2 (100 Mbps spread across entire floor equals 100 Kbps per square meter). It is also determined that the nursing station is considered the highest capacity user per physical area, and the nursing station area will require a peak capacity of 130 Kbps/m^2. During the planning phase, 802.11 is the chosen wireless technology, and the 802.11 dual band AP is expected to deliver a 'real world' capacity of 20 Mbps in the 802.11a 5 GHz U-NII bands, and 6 Mbps in the 802.11bg 2,4 GHz ISM BAND. The network designer chooses to deploy enough APs to meet the nursing station capacity requirements across the entire floor (an alternate plan would be to add additional AP(s) only in the nursing station area). Extending the 130 Kbps/m^2 requirement across the entire floor, and designing to overprovision the WLAN by 50 %, the WLAN coverage design requires an aggregate capacity of 260 Kbps/m^2, or 260 Mbps. The deployment meets this requirement with the use of 10 APs (200 Mbps for 802.11a and 60 Mbps in 802.11bg). Assuming that devices are deployed and configured (e.g. channel assignments, etc.) to utilize the two bands effectively and the RF coverage of the APs is confirmed with an RF survey tool, the deployment design is appropriate and would be ready for test and VERIFICATION.

8.7.2 5 GHz and DYNAMIC FREQUENCY SELECTION (DFS)

Each country has its own rules and regulations regarding the use of unlicensed spectrum. The channels available and secondary use of the spectrum can change from one country to another. For example, some of the 5 GHz channels are restricted in areas where they might interfere with radar systems that operate on a primary usage basis in the band. An HDO can investigate with the proper local government authorities to learn if there are any radar installations in the vicinity of the facility. Additionally, any infrastructure device such as an 802.11 AP that operates on a DFS channel is required to monitor for radar and avoid interfering transmissions if a radar source is detected. Most APs or WLANs will alert or provide logs showing that they have detected radar and activated their DFS system. Once it is known that there are radar installations in the vicinity, the affected 802.11 channels might need to be manually disabled. This is because DFS will cause the AP to cease operation on the affected channel, and any clients connected to the AP might be disassociated and experience a loss of connectivity for a significant period of time (seconds to minutes depending on the client behavior) until they can reconnect to the same or a neighboring AP on an unaffected channel.

8.7.3 Security measures and planning

For additional information on securing wireless communications, please refer to security RISK ASSESSMENT standards such as ISO/IEC 27001:2005, ISO/IEC 27002:2005, ISO/IEC 15408-2:2008, etc. Wireless communication technologies include many technical security controls, please refer to the specification for each technology, (e.g. 802.11, Bluetooth, etc.). For guidance regarding security RISKS in connecting MEDICAL DEVICES to IT-NETWORKS please see IEC/TR 80001-2-2 on of MEDICAL DEVICE security needs, RISKS and controls.

Security was already a strategic and important focus for IT NETWORKS before the introduction of MEDICAL DEVICES. Protected health information on any network demands strong security measures; this is especially true for wireless networks. As part of the design and planning of the WLAN, each link in the communication chain should be evaluated for security flaws and appropriate counter measures. Use strong encryption and authentication solutions such as AES and 802.1X. In addition, the use of IDS/IPS might be warranted to detect and protect against many of the wireless intrusion mechanisms. If legacy devices that support lesser levels of encryption have to be allowed on the network, the design should restrict the network access of these devices. For example, infusion pumps that have lesser means of security might only have access to a single formulary update server so that RISK of a network breach is restricted to the single server.

8.8 RF spectrum use

Although available spectrum is a limited and valuable resource, proper planning and use of the RF spectrum by the HDO is often overlooked. The RISK ANALYSIS should include consideration of all spectrum and associated wireless technologies available to the HDO. Considerations include the nature and probability of interference, the support for peak traffic loads, and the ability of the technology to operate in the presence of expected interference sources. In most locations, licensed spectrum has a lower probability of interference than unlicensed spectrum; however, some providers of licensed spectrum (e.g. cellular) design for average loads, not peak loads. In the case of unlicensed spectrum, the use of less crowded or higher bandwidth spectrum is recommended. For example, a capacity analysis might indicate use of the U-NII bands (5 GHz) with 555 MHz of bandwidth over the use of the ISM 2,4 GHz band with only 83 MHz of bandwidth. Each band of spectrum has pro's and con's that should be vetted against the wireless RF requirements.

For example, the RISK ANALYSIS should consider whether the HDO should use the U-NII band DFS channels as radar interfering events can lead to temporary loss of communications and other performance degradation due to secondary network perturbations when the affected APs all suddenly change channels.

8.9 Device and application classification

When disparate devices with varying performance requirements coexist on the same network, the use of classification on the network by security policy and performance requirements is helpful in managing network access. In the case of MEDICAL DEVICES where network performance and availability can have patient SAFETY implications, the ability to classify the wireless MEDICAL DEVICES as higher priority on the network at the access layer is even more important and vital. Selecting wireless technologies and infrastructure solutions that are able to distinguish and manage packet transmissions of different priorities should be considered. Such QUALITY OF SERVICE (QoS) mechanisms should be explored in the design and planning phases and implemented end-to-end on the network.

Mechanisms that also allow for detection and prevention of misuse of QoS tags to gain unfair access to wireless bandwidth should also be considered. For example, a low priority packet gets tagged as a high priority packet and gets preferred treatment that it doesn't deserve. This can impact SLAs for the high-priority traffic. Detection and prevention of such misuse can help meet SLAs. Consult with your wireless network infrastructure provider to explore these types of capabilities.

8.10 Guest or smart phone access

Most enterprise 802.11 networks employ some capability to enforce user bandwidth allocation. For example, guest users should be bandwidth limited such that their particular classes of devices only receive minimal bandwidth while reserving most of the bandwidth for mission and life critical applications. Even with MEDICAL DEVICES or medical smart phone applications, the clinical functionality of 'how' the application is used has to be considered as part of the system level design. If a physician wants to use his or her smart phone for non-medical use while in the HDO then the traffic from that device should be segregated either within the guest access SSID or a separate dedicated SSID to smart phone applications. Regardless, the device and the applications that reside on it need to be understood regarding the clinical functionality and properly accounted for in the RISK ANALYSIS and design. The use of limiting the bandwidth to a particular device or application needs to take into account the clinical functionality and not necessarily the user's preferences for broadband access. If higher levels of broadband access are needed to support guest access and smart phone applications, then other means of design RISK CONTROL measures might be necessary. Examples of such are considered in this technical report, such as the increase in the number of APs and expanded use of the 5 GHz spectrum.

8.11 WLAN infrastructure configuration

An HDO MEDICAL IT-NETWORK administrator can expect to have to alter or create some level of customization in the wireless infrastructure configuration. Most wireless infrastructure solutions include extensive manuals and sets of best practices. Appropriate personnel should undertake the necessary training to learn the capabilities of the wireless network and how to properly configure the system for peak performance and availability. Once the configurations are understood, they can be matched to the networking performance requirements of the devices on the MEDICAL IT NETWORK. This includes networking performance characteristics such as latency and packet loss, security posture and any configuration to enable compatibility between the MEDICAL DEVICES and the wireless network. Meeting the SLAs of all devices is a task that will require tradeoffs based on clinical priority, resources, and budgets, all of which should be considered as part of the RISK MANAGEMENT PROCESS.

8.12 External partnering with both MEDICAL DEVICE and networking manufacturer

Developing a relationship with the MDM as well as the MEDICAL IT-NETWORK provider is now an important aspect of designing and maintaining a MEDICAL IT-NETWORK. Work with both the wireless networking provider and MDM to understand the infrastructure and device level requirements and capabilities, and review device and WLAN network configurations with all interested parties. Ideally the parameters are formalized in the RESPONSIBILITY AGREEMENTS. After review and acceptance of a proposed configuration by all responsible parties, a testing of the WLAN and device(s) configurations in a laboratory environment to evaluate compatibility and measure performance is an integral part of the RISK ANALYSIS PROCESS.

Note that this is complementary with the internal partnering required within the HDO including biomedical engineers, safety officers, clinicians and risk managers.

8.13 Redundancy

Redundancy is a best practice implemented in wired networks and wireless networks. Deploying the wireless network so that each area is covered by at least two transceivers on different channels provides RF redundancy. This deployment strategy is only possible when sufficient channels are available. Further, if these transceivers are wired to different network switch fabrics, then a single switch failure will not result in loss of all wireless functionality.

For example, if using 802.11 operating in the 2,4 GHz ISM BAND, there are, at best depending on the regulatory domain, three distinct 802.11 frequency channels available. In a physical space where there are many overlapping AP coverage areas, lack of distinct channels can lead to increased co-channel interference. Implementing RF redundancy in this scenario will result in a decrease in overall capacity. A mitigation technique is to move critical traffic to the U-NII 5 GHz bands where up to twenty four distinct 802.11 channels are available. In conjunction with this larger number of distinct channels, physically overlapping AP coverage areas provide enhanced capacity as well as RF redundancy when properly deployed. As more APs are added, the AP and client transmit power can also be decreased to support extremely dense AP deployments.