Risikomanagement für medizinische Netzwerke in der Intensiv- und Notfallmedizin. Gemeinsames Positionspapier zur Norm IEC 80001-1

Risk management for medical networks in intensive care and emergency medicine – a joint position paper on IEC 80001-1

Abstract

IEC 80001-1 is an international standard and offers recommendations for a risk management process for medical information technology networks (MITs). MITs are defined as IT networks incorporating at least one medical device. The goal is to build and maintain reliable and secure MITs for hospitals of all kids. To achieve it, the standard suggests applying risk management and defines the roles involved as well as their responsibilities.

A central role is the medical IT-network risk manager, assigned by the top management of organizations. He communicates with and mediates between clinical, medical device and IT divisions and compiles risk relevant facts usually distributed among them. All identified risks are analyzed, evaluated and documented in the risk management file along with counter measures and a final assessment of acceptability.

We acknowledge that implementing the suggested process will create an overhead cost in documentation and – partly by extension – in personnel. However we believe that the investment at the start of projects is worthwhile, because it helps to prevent or solve problems in later stages. Especially consecutive projects can profit from the investment, reducing required effort and costs. Furthermore, a reliable and secure MIT forms the basis for frictionless routine operations and innovations for connected medical devices. Hence the investment is justified.

Applying risk management to the whole cooperation all at once is unrealistic. Focusing on parts of the network, which are crucial to a new project is more recommendable. With a smaller scope, risk management remains feasible and can later be expanded to other parts of the network.

IEC 80001-1 demands communication among involved employees from different specialties and divisions. This offers a chance for cooperation to find better decisions and solutions regarding an organization's medical IT network.

Keywords: patient safety, risk management, equipment failure, organization and administration

Janko Ahlbrandt[1,2]
Rainer Röhrig[1,2]
Johannes Dehm[3]
Christian Wrede[1,4,5]
Michael Imhoff[4,6]
Sektion IT & Medizintechnik der Deutschen Interdisziplinären Vereinigung für Intensiv- und Notfallmedizin e.V. Deutsche Gesellschaft für Biomedizinische Technik (DGBMT) im VDE e.V., Fachausschuss Methodik der Patientenüberwachung

1 Deutsche Interdisziplinäre Vereinigung für Intensiv- und Notfallmedizin (DIVI), Berlin, Deutschland

2 Justus-Liebig-Universität Gießen, Deutschland

3 Verband der Elektrotechnik Elektronik Informationstechnik e.V. (VDE), Initiative MikroMedizin, Frankfurt am Main, Deutschland

4 Deutsche Gesellschaft für Biomedizinische Technik im VDE (DGBMT), Frankfurt am Main, Deutschland

5 Helios-Klinikum Berlin-Buch, Berlin, Deutschland

Zusammenfassung

Die IEC 80001-1 ist eine Norm, die Empfehlungen für einen Risikomanagementprozess für medizinische IT-Netzwerke (MIT) – also Netzwerke mit angeschlossenen Medizinprodukten – gibt. Das Ziel ist der Aufbau und Betrieb von stabilen und sicheren IT-Netzwerken in Kliniken. Die Empfehlungen richten sich vor allem an die Betreiber von Krankenhäusern, weisen Verantwortlichkeiten innerhalb einer verantwortlichen Organisation (meist einer Klinik) zu und geben deren Interaktion vor. Eine zentrale Rolle ist der MIT Risiko-Manager, der von der Geschäftsführung beauftragt wird und die Anstrengungen in Richtung Risikomanagement

6 Ruhr Universität Bochum, Deutschland

koordiniert. Dazu steht er in Kontakt mit Mitarbeitern von klinischen Abteilungen, der Medizintechnik, der IT-Abteilung und auch den Herstellern der beteiligten Medizinprodukte. Auf diese Art wird Wissen, das oft nur an diesen verschiedenen Stellen vorhanden ist, gesammelt und in der Risikomanagement-Akte dokumentiert. Jede gefundene Bedrohungs-Situation wird analysiert und nach ihrer Wahrscheinlichkeit und ihren (geschätzten) Folgen bewertet. Danach wird festgelegt, ob ein bestehendes Restrisiko tragbar ist und wie Gegenmaßnahmen umgesetzt werden. Der Dialog, der während des Informationsaustausches entsteht, nützt allen Parteien und trägt maßgeblich dazu bei, MITs stabiler und sicherer zu machen.
Die Umsetzung der Norm erfordert einen Mehraufwand an Personal und Dokumentation. Nach Einschätzung der Autoren lohnt sich diese Investition am Anfang von Projekten, da sich dadurch Probleme im späteren Projektverlauf vermeiden oder zumindest reduzieren lassen. Spätestens bei Anschlussprojekten ist hier mit einer Aufwands- und damit Kostenersparnis zu rechnen. Ein stabiles und sicheres Netzwerk stellt die Basis für reibungslosen Routinebetrieb aber vor allem auch für Innovation im Bereich der vernetzten Medizingeräte dar.
Eine sofortige unternehmensweite Einführung der IEC 80001-1 ist ein unrealistischer Ansatz. Vielmehr ist zu empfehlen, sich zunächst auf bestimmte Subnetze zu konzentrieren, die innerhalb eines Projektes oder eines bestimmten Prozesses wichtig sind. In einem solchen kleineren Rahmen bleibt der Aufwand für das Risikomanagement beherrschbar und lässt sich danach auf weitere Bereiche ausdehnen.
Die IEC 80001-1 fordert alle Beteiligten zur Kommunikation auf und bietet so die Chance, aus einer Kooperation heraus die besten Entscheidungen im Sinne der verantwortlichen Organisation zu treffen.

1 Vorwort

Die Informationstechnologie spielt in der Krankenversorgung und speziell der stationären Versorgung eine große und immer noch wachsende Rolle. Systeme, die benötigt werden, um Daten zu erfassen, zu verwalten und aufzubereiten, werden durch eine systemübergreifende Prozessunterstützung immer komplexer und verlangen zunehmend die Integration von verschiedenen Datenquellen. Diese Integration ist nur über Vernetzung von IT-Systemen und Medizinprodukten (MP) zu erreichen. In der Vernetzung liegen also große Möglichkeiten und Chancen für die Informationsverarbeitung in der Medizin, aber auch damit verbundene Risiken. Ein Ausfall von Informationstechnologie, selbst wenn er auf einen Teilbereich eines Krankenhauses beschränkt bleibt, ist oft gleichbedeutend mit Stillstand des betrieblichen Ablaufs in klinischen Abteilungen. Und auch Zwischenfälle in technischen Systemen, die nicht zum Ausfall führen sind potentiell gefährdend.
Aus diesen Gründen braucht es ein klares Regelwerk, das die Vernetzung medizinischer Geräte zu einem sogenannten medizinischen IT-Netzwerk (MIT) für alle Beteiligten transparent macht. Die gegensätzlichen Zielsetzungen zwischen einerseits hohen Anforderungen an Verfügbarkeit und Sicherheit und andererseits dem Bedürfnis nach einem möglichst großen Funktionsumfang müssen bei der Einrichtung und dem Betrieb eines MIT abgewogen werden und bilden den Rahmen dieses Positionspapiers.

Am 13. Dezember 2010 fand in Gießen ein Workshop zur IEC 80001-1 („Anwendung des Risikomanagements für IT-Netzwerke mit Medizinprodukten; Teil 1: Aufgaben, Verantwortlichkeiten und Aktivitäten“) statt. Anwesend waren Vertreter des Verbandes der Elektrotechnik Elektronik Informationstechnik e.V. (VDE), der Deutschen Gesellschaft für Biomedizinische Technik im VDE (DGBMT), der Sektion IT und Medizintechnik der Deutschen Interdisziplinären Vereinigung für Intensiv- und Notfallmedizin (DIVI), von Medizin-Technik-Herstellern, Unternehmensberatungen und Kliniken für den Bereich Medizintechnik und Informationstechnologie (IT).
Dieses Positionspapier entstand durch Zusammenführen der Ergebnisse des Workshops, weiteren Beiträgen der Teilnehmer und anderer Organisationen, sowie Studien und Forschungsergebnissen zu den diskutierten Themen. Das vorliegende Positionspapier befasst sich mit dem Risikomanagement von vernetzten Medizinprodukten in der Intensiv- und Notfallmedizin. Er ist das Ergebnis einer Expertenrunde aus Sachverständigen des VDE, der DGBMT, der Sektion IT und Medizintechnik der DIVI, des Bundesverbandes Gesundheits-IT (BVITG) und der Deutschen Gesellschaft für Fachkrankenpflege (DGF). Dies geschieht in Bezug auf die 2010 in Kraft getretene Norm IEC 80001-1.

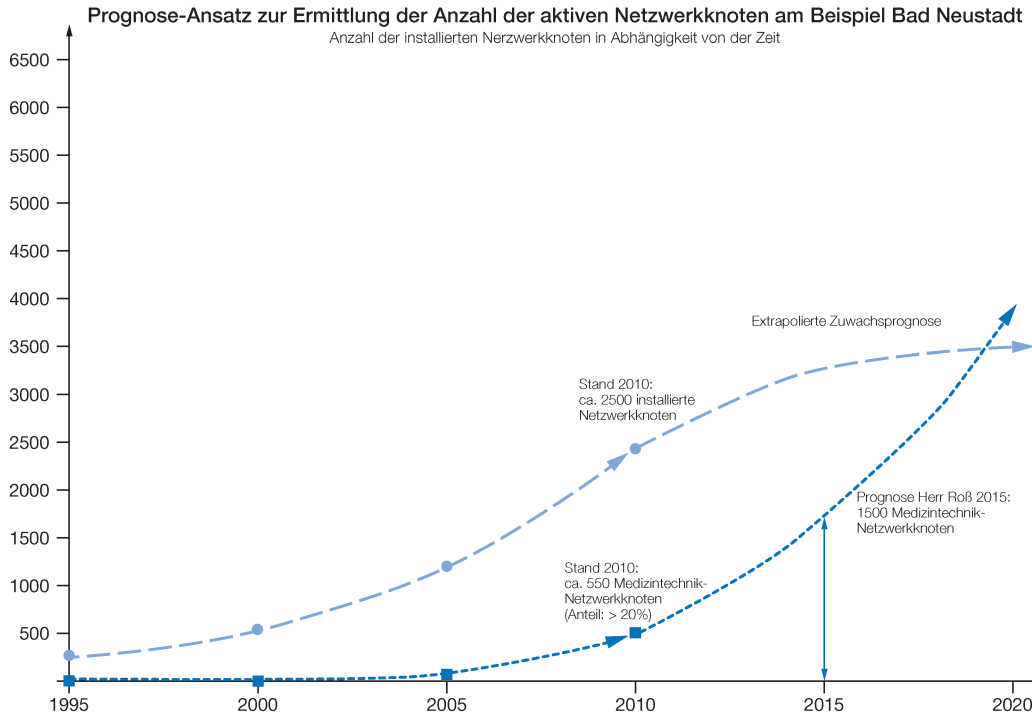

Abbildung 1: Entwicklung der aktiven Netzwerkknoten am Beispiel eines mittelgroßen Krankenhauses (Abbildung: Peter Roß)

2 Einführung

2.1 Entwicklung der IT-Netzwerkinfrastruktur in Krankenhäusern

In den letzten 15 Jahren hat in den deutschen Krankenhäusern eine rasante Entwicklung der IT-Infrastruktur stattgefunden. Dies ist zum einen in den durch die Einführung des fallpauschalen-basierten Entgeltsystems der Diagnosis Related Groups (DRG) zu begründen. Die Erfassung der DRGs erfordert eine detaillierte Dokumentation der Patientenbehandlung. Hinzu kommt der Kostendruck, der eine Prozessoptimierung, z.B. durch klinische Pfade, nach sich zieht. Beides ist ohne Informationstechnik auf den Stationen und am Krankenbett nicht wirtschaftlich durchführbar. Dementsprechend wird der Wertbeitrag der Informationstechnologie in deutschen Krankenhäusern hoch eingeschätzt [1].

Zum anderen hat eine technische Entwicklung stattgefunden: Beispielhaft ist hier die Einführung des digitalen Röntgen anzuführen und der damit verbundenen Implementierung von Picture Archive and Communication Systemen (PACS) zu nennen. Den technischen Möglichkeiten in der Bildverarbeitung steht die Notwendigkeit einer flächendeckenden Installation von Arbeitsplätzen am Behandlungsplatz, also auf Station, im Operationssaal, in der Ambulanz oder am Krankenbett gegenüber.

Dies hat zu einem Ausbau der IT-Infrastruktur geführt, der sich in einem sprunghaften Anstieg der Anzahl von PC-Arbeitsplätzen und damit der aktiven Netzwerkknoten im IT-Netzwerk darstellt. Hier ist in den nächsten Jahren, wenn alle Mitarbeiter und alle Patienten(-zimmer) über einen (Tablet-)PC verfügen, mit einer Verlangsamung der Zunahme an notwendigen Netzwerkknoten zu rechnen.

In den letzten Jahren hat auch in der Medizintechnik ein Wandel stattgefunden: Während früher Medizingeräte, wie z.B. Spritzenpumpen, (Narkose-) Beatmungsgeräte, Geräte für die Nieren- oder Leberdialyse einzelnstehende Geräte waren, bei denen Daten maximal über eine proprietäre serielle Schnittstelle ausgelesen werden konnten, verfügen sie heute über Schnittstellen in ein IT-Netzwerk. Durch die Nutzung der vorhandenen IT-Netzwerkstruktur können über diese Schnittstellen ortsunabhängig Behandlungsdaten ausgelesen, Software- und Wartungsstände abgefragt und Updates durchgeführt, sowie Gerätestandorte lokalisiert werden. Aufgrund der Vielzahl von Medizingeräten ist davon auszugehen, dass sowohl die absolute Anzahl als auch der relative Anteil von Medizingeräten an den aktiven Netzwerkknoten steigen wird. Nach einer internen Erhebung von Peter Roß (Rhön-Klinikum AG) ist zu erwarten, dass 2015 Medizingeräte 50% der Netzwerkknoten in einem mittelgroßen Krankenhaus ausmachen werden (s. Abbildung 1).

Im Gegensatz zur Medizintechnik gehört es zu den Grundzügen einer IT Infrastruktur auf technische und organisatorische Veränderungen zu reagieren und immer wieder neue Verfahren aufzunehmen. Deshalb gibt es für die IT Infrastruktur nie ein endgültiges Design aus dem alle Fragen entschieden werden können.

2.2 Entstehende Risiken in der Intensiv- und Notfallmedizin

Aus der Tatsache, dass für den Wertbeitrag der Informationstechnologie und der Medizinprodukte eine funktionierende Netzwerkstruktur essentiell ist, geht deren unternehmenskritische Bedeutung im ökonomischen Sinne hervor. Bei der Vernetzung von Medizinprodukten gilt es jedoch auch, mögliche Folgen für die Gesundheit des Patienten zu beachten.
Prinzipiell gibt es für die Anwendung von Medizingeräten am Menschen verschiedene Vorschriften und Normen, die den Schutz der Gesundheit und der Unversehrtheit des Patienten im Fokus haben:

- EU-Directive: Council Directive 2007/47/EC concerning medical devices
- MPG: Gesetz über Medizinprodukte [2]
- DIN EN 60601-1 (3. Ausgabe): Medizinische elektrische Geräte; Teil 1: Allgemeine Festlegungen für die Sicherheit einschließlich der wesentlichen Leistungsmerkmale
- DIN EN 60601-1-6: Medizinische elektrische Geräte – Teil 1-6: Allgemeine Festlegungen für die Sicherheit einschließlich der wesentlichen Leistungsmerkmale – Ergänzungsnorm: Gebrauchstauglichkeit, europäische, harmonisierte Fassung der internationalen Norm IEC 60601-1-6.
- DIN EN 62304: Medizingeräte-Software – Software-Lebenszyklus-Prozesse, europäische, harmonisierte Fassung der internationalen Norm IEC 62304
- DIN EN 62366: Anwendung der Gebrauchstauglichkeit auf Medizinprodukte, europäische, harmonisierte Fassung der internationalen Norm IEC 62366
- DIN EN 13485: Medizinprodukte – Qualitätsmanagementsysteme – Anforderungen für regulatorische Zwecke, europäische, harmonisierte Fassung der internationalen Norm ISO 13485
- DIN EN ISO 14971: Anwendung des Risikomanagements auf Medizinprodukte, europäische, harmonisierte Fassung der internationalen Norm ISO 14971

In Gesetzen und Verordnungen wird vor allem die Verantwortung der Hersteller für die „Sicherheit und Leistung der Medizinprodukte, sowie die Gesundheit und den erforderlichen Schutz der Patienten, Anwender und Dritter“ [2] geregelt. Voraussetzung für die Verantwortung und damit auch die Haftung des Herstellers ist die ordnungsgemäße Verwendung des Medizinproduktes.
Das „Errichten, Betreiben, Anwenden und Instandhalten von Medizinprodukten“ fällt gemäß der Medizinprodukte-Betreiberverordnung (MPBetreibV) [3] in die Verantwortung des Betreibers und damit der Kliniken. Der Betreiber hat sicherzustellen, dass Medizinprodukte nur entsprechend Ihrer Zweckbestimmung eingesetzt werden (§2(1) MPBetreibV)) [3].
Durch die Anbindung eines Medizinproduktes an ein anderes Gerät oder an eine Gruppe unterschiedlicher Produkte über ein IT-Netzwerk übernimmt der Betreiber gewissermaßen wie ein Hersteller Verantwortung für den ordnungsgemäßen Betrieb des Gesamtsystems einschließlich der Medizinprodukte. Schwierigkeiten, die sich aus dieser Vernetzung ergeben können, sollten mit folgenden – real stattgefundenen – Beispielen aufgezeigt werden:

- **Beispiel 1:**
  Ein Beatmungsgerät wurde an ein Intensivinformationsmanagementsystem (IMS) für die Datenübernahme angeschlossen. Nach einer unbestimmten Zeit schaltete sich das Beatmungsgerät ohne Fehlermeldung oder Alarmgebung aus. Ursache war, dass der Gerätetreiber des PDMS regelmäßig seine Datenanfrage wiederholte. Dabei wurde jedes Mal in dem Beatmungsgerät ein neuer Prozess generiert ohne den Speicherbereich des vorherigen freizugeben. Mit der Zeit kam es zu einem Speicherüberlauf und es wurden für den Betrieb des Beatmungsgerätes essentielle Speicherbereiche überschrieben, es kam zum Totalabsturz der Betriebssoftware des Beatmungsgeräts.
- **Beispiel 2:**
  Auf einer Intensivstation wird ein Programm installiert, welches Informationen und Alarmmeldungen von Spritzenpumpen in den Patientenzimmern ortsfern anzeigen kann. Von den Alarmmeldungen gehen mehrere nachweislich verloren. Da sich das Pflegepersonal auf die Meldungen verlässt, kommt es zu verzögerten Reaktionen auf die Alarmmeldungen.
- **Beispiel 3:**
  Eine defekte Netzwerkkomponente (Router) ist in einem IT-Netzwerk und sendet ununterbrochen auf bestimmte Ports und IP-Adressen. Dadurch wird die Funktion von einigen, im IT-Netzwerk eingebundenen Medizinprodukten gestört.
- **Beispiel 4:** Die Software auf Medizinprodukten darf vom Anwender nur in den vom Hersteller vorgegebenen Rahmen verändert werden. Dies lässt meist keine Updates des Betriebssystems, einer Firewall oder einer Malware Detection Software (Virenscanner) zu. Dies führt zu Konflikten, wenn z.B. auf einer Intensivstation die Zentrale des Patientenmonitorings mit dem IT-Netzwerk des Klinikums verbunden wird, um auch im Arztzimmer einen Einblick auf die Monitoringdaten zu erhalten. Auf der einen Seite kann die Funktionalität nicht ausreichend geschützt werden, auf der anderen Seite benötigt die Funktionalität die Integration in das IT-Netzwerk der Klinik. So kam es, dass bei einem Schädlingsbefall (Wurm) bei Wartungsarbeiten an einem PACS-System die Zentralen des Patientenmonitorings befallen wurden. In diesem Fall ist kein regelrechter Betrieb mehr zu gewährleisten.

Die Fallberichte der Autoren werden durch die Statistik des Bundesinstitut für Arzneimittel und Medizinprodukten (BfArM) gestützt: Im Zeitraum von 2005 bis 2010 wurden von 3.788 Risikomeldungen mit der Fehlerursache „Design-/Konstruktionsfehler“ 813 als Softwarefehler eingestuft (Abbildung 2, [4]), davon jedoch nur 310 als Softwareprobleme eigener Art (falsche Therapievorgaben, falsche Patientenzuordnung, Auswertungs- und Dokumen-

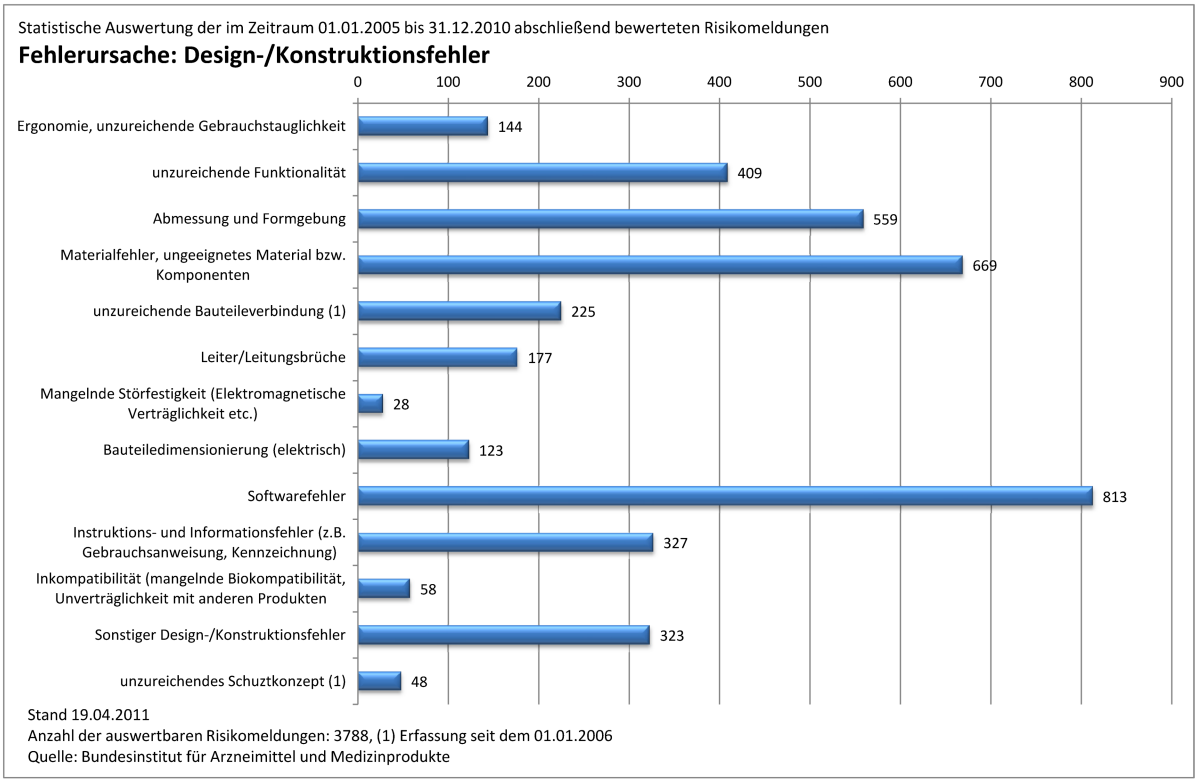

Abbildung 2: Fehlerursachen für Design-/Konstruktionsfehler bei Risikomeldungen an das BfArM (Quelle BfArM [4])

tationsfehler) eingestuft werden [5]. Auch wenn die Probleme, die aufgrund einer Vernetzung aufgetreten sind, nicht gesondert ausgewiesen werden, so ist doch von einem relevanten Anteil auszugehen. Hinzu kommt, dass Fehler, die durch die Integration eines Medizinproduktes in ein IT-Netzwerk auftreten, wahrscheinlich kaum gemeldet werden und somit eine sehr hohe Dunkelziffer existiert.

Mit dem zunehmenden Ausbau der Netzwerkinfrastruktur, der angeschlossenen Systeme und Medizinprodukte wächst auch die Komplexität des Gesamtsystems und damit die Fehleranfälligkeit einzelner angeschlossener Komponenten. Um ein solches Netzwerk sicher betreiben zu können, muss dieses auch einem Risikomanagement unterworfen werden.

Daher wurde nach langjähriger Abstimmungsarbeit im Oktober 2010 von der International Electrotechnical Commission (IEC) die Norm IEC 80001-1:2010 (Anwendung des Risikomanangements für IT-Netzwerke, die Medizinprodukte beinhalten – Teil 1: Aufgaben, Verantwortlichkeiten und Aktivitäten) für das Risikomanagement in der medizinischen Informationstechnologie veröffentlicht. Sie ist Teil einer Normenreihe und enthält neben Regelungen zur Zuständigkeit auch Handlungsempfehlungen für Betreiber von Medizinischen IT-Netzwerken (MITs). Dabei ist ein MIT ein Netzwerk, in dem mindestens ein Medizinprodukt angeschlossen ist. Im November 2011 ist die deutsche Fassung der Norm als DIN EN 80001-1 veröffentlicht worden [6]. Die Normenreihe wurde im September 2012 um die Technical Reports IEC/TR 80001-2-1 bis IEC/TR 80001-2-4 ergänzt.

Die IEC 80001-1 hat in vielen Kliniken für eine Verunsicherung bezüglich Verantwortlichkeiten und Haftungsrisiken gesorgt. Das Ziel des vorliegenden Positionspapiers ist, die IEC 80001-1 zu erläutern und deren Konsequenzen für Betreiber, Anwender und Hersteller darzustellen und Empfehlungen für die praktikable Umsetzung der Norm aufzuzeigen.

3 Die IEC 80001-1

3.1 Ziele der IEC 80001-1

Die IEC 80001-1 ist eine Norm zur Anwendung des Risikomanagements bei Planung, Umsetzung und Betrieb eines medizinischen IT-Netzes (MIT). Sie definiert Rollen und Verantwortlichkeiten und legt Aufgaben und Aktivitäten für den Prozess des Risiko-Managements fest. Sie ist kein rechtsverbindliches Dokument, stellt aber eine Empfehlung für die Betreiber von MIT dar.

3.2 Geltungsbereich

Der Fokus des Geltungsbereiches ist das medizinische IT-Netzwerk (MIT). Dieses ist definiert als ein IT-Netzwerk, das wenigstens ein MP enthält.

Nicht unter die Norm fallen

- Netzwerke, die ausschließlich Medizinprodukte enthalten und von einem Hersteller als Gesamtsystem betreut werden. (Abgeschlossenes Netzwerk Klasse C gemäß Anlage H, DIN EN 60601-1). Hierunter fällt in

Tabelle 1: Die wichtigsten Definitionen basierend auf der IEC 80001-1

Begriff	Definition
Medizinisches Netzwerk (MIT)	Ein Medizinisches Netzwerk (MIT) ist ein IT-Netzwerk mit mindestens einem Medizinprodukt.
IT-Netzwerk	System/Systeme, bestehend aus Kommunikationsknoten und Übertragungsverbindungen, um Übertragungen über Leitungen oder drahtlos zwischen zwei oder mehr festgelegten Übertragungsknoten zu ermöglichen.
Risiko	Eine Kombination aus der Einschätzung der Wahrscheinlichkeit des Vorkommens eines Schadens und dem Schweregrad dieses Schadens ergibt das Risiko.
Rest-Risiko (residual risk)	Das Risiko, das nach allen Risikokontroll-Maßnahmen verbleibt.
Risiko-Identifikation	Auffinden und Erfassen von Risiken unter Einsatz von Analysetechniken, wie Expertenbefragung, Checklisten und offene Kommunikation.
Risiko-Analyse	Hierunter versteht man den systematischen Einsatz der verfügbaren Informationen zur Identifikation von Gefährdungen (Risiko-Identifikation) und die Abschätzung des resultierenden Risikos.
Risiko-Bewertung	Prozess des Vergleichs des eingeschätzten Risikos mit gegebenen Risiko-Kriterien, um die Akzeptanz des Risikos zu bestimmen.
Risiko-Beurteilung	Prozess der Risiko-Analyse und der Risiko-Bewertung.
Risiko-Beherrschung	Ein Prozess, in dem Entscheidungen getroffen und Maßnahmen implementiert werden, durch die Risiken auf festgelegte Bereiche verringert oder auf diesen gehalten werden.
Schaden	Physikalische Verletzung oder Schaden an der Gesundheit von Menschen, der Umgebung, einer Reduzierung der Effektivität oder ein Bruch der Daten- oder Systemsicherheit.
Daten- und Systemsicherheit	Ein Zustand des MIT, in dem Informationen und Informationssysteme sinnvoll davor geschützt sind, an Vertraulichkeit, Integrität oder Erreichbarkeit zu verlieren.
Gefährdung	Potentielle Quelle eines Schadens.
Sicherheit	Abwesenheit von inakzeptablem Risiko für Schäden.
Effektivität	Fähigkeit, das beabsichtigte Ergebnis für den Patienten und die verantwortliche Organisation zu erzeugen. Anmerkung: Dieser Begriff wurde in der DIN EN 80001-1 eingeführt, um Wirksamkeit hinsichtlich unverfälschtem und rückwirkungsfreiem Datenflusses im IT-Netzwerk mit dem Ziel der angestrebten Abläufe zu beschreiben.

der Regel das Patientenmonitoring mit Zentrale auf der Intensivstation.
- Netzwerke, in die keine MP Integriert sind.

3.3 Definitionen

In der IEC 80001-1 werden einige Begriffe definiert, die zum Teil aus dem Bereich des klassischen Risikomanagements kommen. In Tabelle 1 finden Sie einige wichtige Definitionen.

3.4 Organisationsstruktur und Rollen

In Tabelle 2 sind die in der IEC80001-1 definierten Rollen, in Abbildung 3 ist die Organisationsstruktur dargestellt. Innerhalb der verantwortlichen Organisation findet das gesamte Risikomanagement statt. Dies umfasst alles von Planung und Design von MITs über deren Installation, Wartung und Anschluss von Medizingeräten bis hin zum Betrieb und der geregelten Außerbetriebnahme. Das verantwortliche Management gibt für die Durchführung des Risikomanagements Richtlinien vor, unter anderem für eine Bestimmung eines akzeptablen Restrisikos. Außerdem muss es sicherstellen, dass die benötigten Ressourcen und qualifiziertes Personal aus verschiedenen Fachabteilungen vorhanden sind (Abbildung 4).
Als Beauftragter der Obersten Leitung nimmt der MIT-Risiko-Manager dabei eine zentrale Rolle ein. Seine Aufgabe ist, nach Vorgaben der verantwortlichen Organisation die verschiedenen Perspektiven von Anwendern, Medizintechnik, IT-Abteilung und Herstellern zusammenzuführen und zu koordinieren (Abbildung 5). Er kooperiert dabei mit Mitarbeitern aus verschiedenen Fachabteilungen, die Experten für den Risikomanagement-Prozess entsenden. Außerdem steht er in Kontakt mit den Herstellern der beteiligten Medizinprodukte, die die Verantwortung haben, wichtige technische Informationen zu ihren Produkten zu liefern, die für eine Vernetzung der Geräte nötig sind. Ihm obliegt die Entscheidung, ob die Vernetzung

Tabelle 2: Rollen, wie sie in der IEC 80001-1 definiert sind

Begriff	Definition
Verantwortliche Organisation	Betreiber, der die Sachherrschaft über den Gebrauch und die Instandhaltung eines MIT besitzt. Oft auch als Betreiber (Krankenhaus) bezeichnet
Oberste Leitung	Person oder Personengruppe, die die verantwortliche Organisation leitet und überwacht, sowie für das MIT auf oberster Ebene verantwortlich ist. Anmerkung: Dies entspricht im Allgemeinen dem Vorstand, bzw. der Geschäftsführung im Krankenhaus.
MIT Risiko Manager	Ein Mitarbeiter oder Beauftragter einer verantwortlichen Organisation, der für die Umsetzung des Risikomanagements verantwortlich ist.
Medizinprodukte-Hersteller	Der Hersteller eines Medizinproduktes. Er ist verantwortlich dafür, der verantwortlichen Organisation Informationen und Dokumente zur Verfügung zu stellen, die für den Betrieb eines Geräts – auch in einem Netzwerk – notwendig sind.
IT-Dienstleister	Der Dienstleister stellt die Infrastruktur für die Informationstechnologie (Rechner, Netze, etc.) zur Verfügung, aber KEINE Medizingeräte.

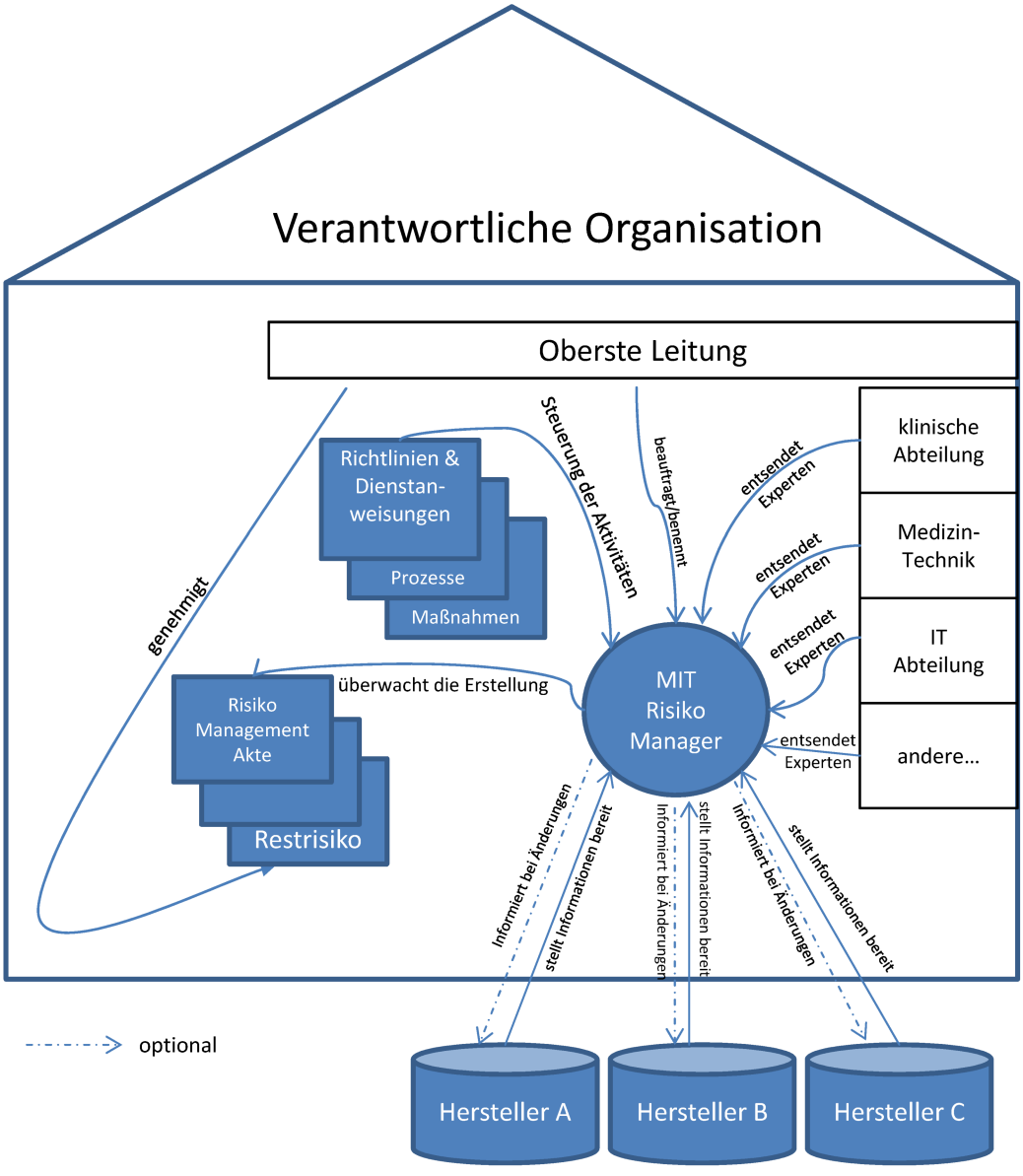

Abbildung 3: Organisationsstruktur gemäß IEC 80001-1, abgeglichen mit DIN EN 80001-1

eines Medizingerätes durchgeführt werden kann und unter welchen Bedingungen dies passiert.

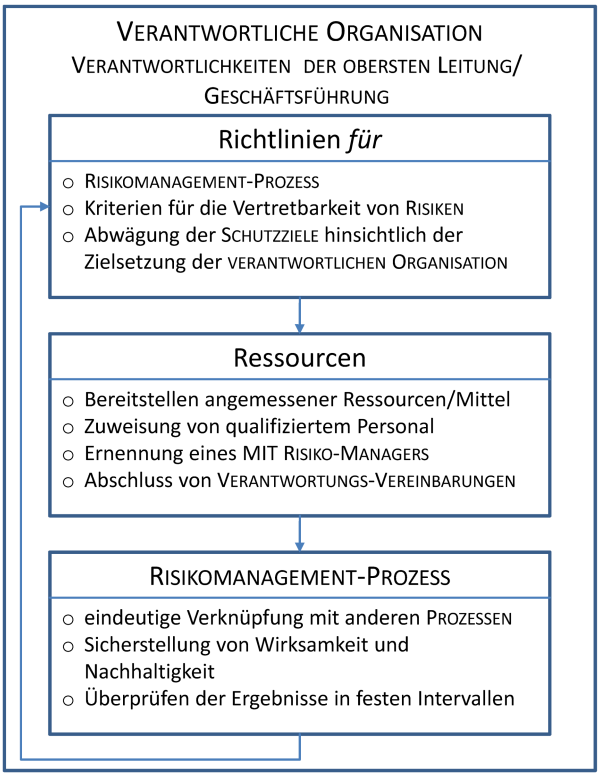

Abbildung 4: Verantwortlichkeiten der obersten Leitung/Geschäftsführung (basierend auf IEC 80001-1 und DIN EN 80001-1)

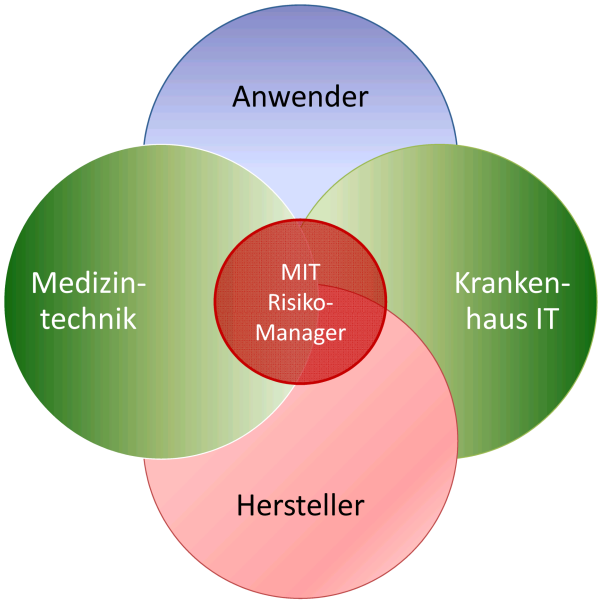

Abbildung 5: Aufgabe des MIT-Risikomanagements ist die Koordination der verschiedenen Interessensvertreter

Weiterhin sollte der MIT-Manager die Kommunikation mit dem von der verantwortlichen Organisation benannten Datenschutzbeauftragten suchen. Dieser ist zwar in der Norm nicht erwähnt und damit nicht direkt in den Risikomanagement-Prozess eingebunden, ist aber für das Schutzziel der Vertraulichkeit von Patientendaten im Unternehmen zuständig.

Sowohl die Vorgaben der Obersten Leitung als auch die Ergebnisse des Risikomanagements werden dokumentiert und in der Risikomanagement-Akte zusammengeführt. Der gesamte Vorgang wird ebenfalls vom Risiko-Manager überwacht, der der Obersten Leitung darüber Bericht erstattet.

3.5 Risikomanagementprozess

Der Risikomanagementprozess beginnt in der Geschäftsführung einer verantwortlichen Organisation. Ihr kommt die Aufgabe zu, Richtlinien für den Risikomanagement-Prozess, die Vertretbarkeit von Risiken und die Vereinbarkeit mit den Geschäftszielen des Unternehmens zu erarbeiten (Abbildung 4). Diese dienen dem MIT Risiko-Manager als Grundlage für die Entscheidungen im Detail. Außerdem vermittelt er, wie in Abbildung 5 dargestellt, zwischen den beteiligten Interessensvertretern und koordiniert den Prozess des Risikomanagements. Über den Fortschritt, die Einhaltung der Richtlinien und grundlegenden Anforderungen berichtet er kontinuierlich der Geschäftsführung.

Am Anfang eines neuen Projekts, dass nach den Vorgaben der IEC 80001-1 durchgeführt werden soll, wird in einer Projektbeschreibung festgehalten, wie die zu unterstützenden Prozesse aussehen, warum eine Vernetzung angestrebt wird und in welcher Form diese realisiert werden soll (siehe Abbildung 6).

Mit den beteiligten Fachleuten wird für einen definierten Prozess (eine Maßnahme, ein Eingriff, etc.) analysiert, welche Gefahrenpotenziale bestehen und für diese eine Risiko-Analyse durchgeführt. Dabei wird für jede Gefährdung festgelegt, wie wahrscheinlich ihr Eintreten und wie schwerwiegend der resultierende Schaden ist. Hierzu sind Herstellerangaben erforderlich, die die relevanten Eigenschaften und Mechanismen des Medizinproduktes beschreiben.

Nachdem diese Einschätzungen dokumentiert sind, werden Maßnahmen definiert, die das Risiko auf ein akzeptables Maß reduzieren oder ganz eliminieren. Sie können entweder präventiv durchzuführen sein oder beim Eintreten des Fehlerfalls im Sinne einer Fallback-Strategie. Der resultierende Katalog an Risiken mit Risiko-Kontroll-Maßnahmen wird in einer Risiko-Management-Akte (wie in 3.6 beschrieben) dokumentiert.

In der Risikomanagement-Akte wird dokumentiert, welche Gefahr identifiziert wurde und in welcher Situation diese auftreten kann. Dazu werden die Maßnahmen definiert, die geeignet sind, das Risiko zu senken oder zu eliminieren. Sie können entweder präventiv durchzuführen sein oder beim Eintreten des Fehlerfalls im Sinne einer Fallback-Strategie. Zuletzt muss entschieden werden, ob das nach den implementierten (Gegen-)Maßnahmen verbleibende Risiko akzeptabel ist. Diese Entscheidung ist nach den Richtlinien und dem Grad der Gefährdung für Mitarbeiter und Patienten bzw. der Wichtigkeit für das Geschäft des Betreibers zu fällen.

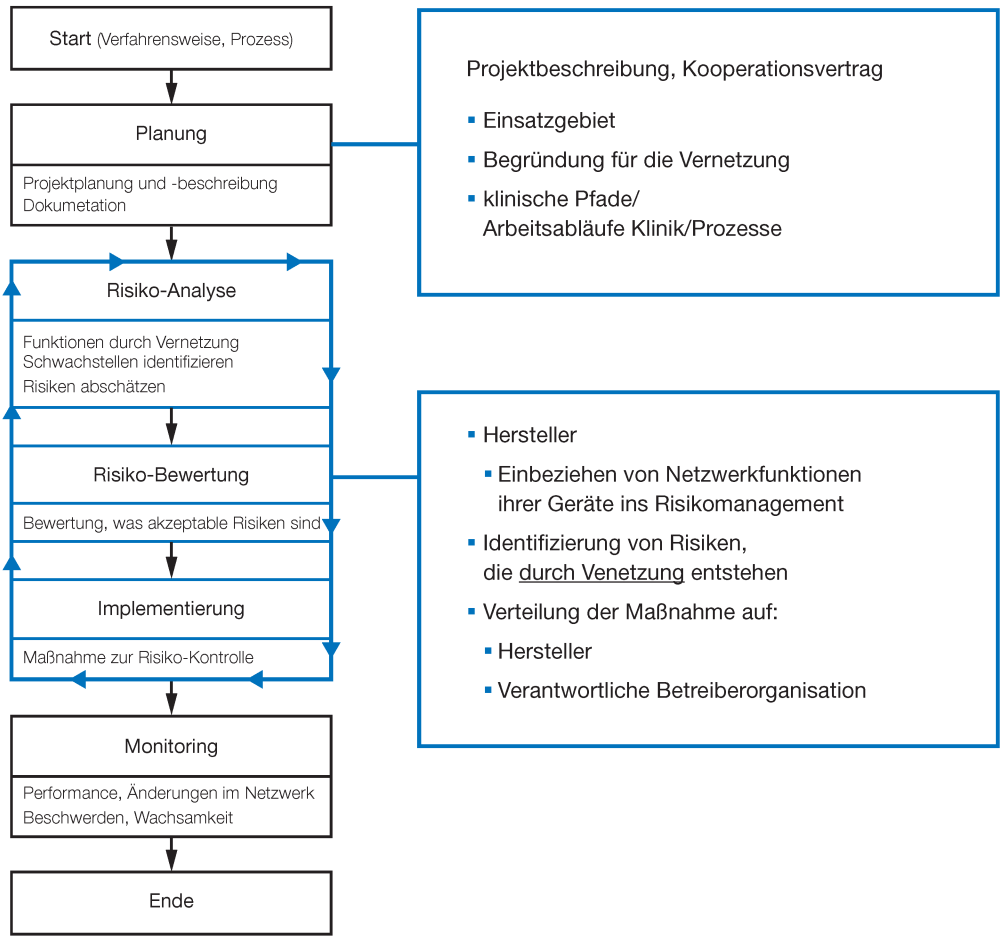

Abbildung 6: Ablauf des Risikomanagementprozesses nach IEC 80001-1

Der Prozess des Risikomanagements ist keine einmalige Sache, er muss mehrfach und vor allem bei Veränderungen der Umgebung durchgeführt werden, wie in Abbildung 6 schematisch dargestellt. Außerdem muss überwacht werden, ob die definierten Maßnahmen wirklich geeignet sind, Schaden abzuwenden oder zu begrenzen, und gegebenenfalls angepasst werden.

3.6 Risikomanagementakte

Die Risikomanagement-Akte ist der zentrale Ort der Dokumentation beim Risikomanagement. Hier werden die identifizierten Bedrohungen aufgeführt, ihre Häufigkeit und damit ihre Wahrscheinlichkeit abgeschätzt und ihre Folge bewertet. Dabei muss berücksichtigt werden, dass es Folgen sowohl für Patienten und Personal als auch für die Organisation als Ganzes, wie beispielsweise finanzielle Einbußen, geben kann. Diese beiden Schutzziele widersprechen sich mitunter und müssen gegeneinander abgewogen werden.
Im nächsten Abschnitt geht es darum, wie man Risiken reduzieren oder Gefahren abwenden kann. Für die meisten Bedrohungen gibt es offensichtliche Gegenmaßnahmen bzw. Sicherheitsvorkehrungen. Hier gibt es zum Beispiel Netzwerk-Adapter für die galvanische also elektrische Entkoppelung, die gegen einen Übertritt einer Spannung auf den Patienten absichern. Bei anderen Bedrohungen, wie Software-Fehlern in Geräten, ist es schwieriger, wirksame Gegenmaßnahmen zu finden. Das Ziel ist es, für jede Bedrohung einen Katalog an Maßnahmen definiert zu haben, die geeignet sind, Schaden zu verhindern bzw. abzuwenden, oder das Schadensausmaß zu minimieren. Zuletzt muss zu jeder Bedrohung dokumentiert werden, ob das verbleibende (Rest-)Risiko – unter den gegebenen Umständen und nach Anwendung der Gegenmaßnahmen – vertretbar ist.
Anhand der geführten Risikomanagement-Akte kann überprüft (und auch zertifiziert) werden, ob sich eine Organisation nach den Vorgaben der IEC 80001-1 richtet.

3.7 Verantwortlichkeitsvereinbarung

Um festzulegen, wer welche Verantwortung in einem Projekt übernimmt, kann eine verantwortliche Organisation mit externen Partnern, wie Herstellern und Dienstleistern, Vereinbarungen treffen. Diese können als Verträge ausformuliert und geschlossen werden und beziehen alle Beteiligten mit ein. Es wird dabei eine Person benannt, die für das Risiko-Management zuständig ist, der Rahmen des Projekts skizziert und die beteiligten Medizingeräte aufgeführt. Zusätzlich wird eine Liste (vor allem technischer) Dokumente erstellt, die der Hersteller der Geräte bereitstellen muss. Für den Fall von Zwischenfällen wird geregelt, wer diese zu bearbeiten hat.

Die vereinbarte Zusammenarbeit wird detailliert beschrieben, wozu vor allem auch gehört, wer diese initiiert, wer die Ansprechpartner sind und nach welchen Kriterien geprüft werden kann, ob die Partner ihrer Verantwortung nachgekommen sind.
Die Zuordnung der Mitarbeiter der verantwortlichen Organisation zu den hier besprochenen Rollen und Aufgaben, muss nicht zwingend aus deren genereller Rolle im Unternehmen abzuleiten sein. So kann es beispielsweise sinnvoll sein, Aufgaben an Mitarbeiter zu delegieren, die nicht ständig im Alltagsbetrieb eingebunden sind.

4 Stellungnahme der Experten zur IEC 80001-1

4.1 Ziele der IEC 80001-1

MITs sind eine zwingende Voraussetzung für eine effiziente Patientenversorgung. Die Zielsetzung der IEC 80001-1 ist die Anwendung des Risikomanagements für folgende Schutzziele:

- die Sicherheit von Patienten, Anwendern und Dritten
- die Sicherstellung der Wirksamkeit der Vernetzung von Medizinprodukten
- die System- und Datensicherheit.

Das hat zur Folge, dass bei der Anwendung der Norm auch 3 Risikoanalysen erforderlich sind, weil die Gefährdungen pro Schutzziel unterschiedliche „Güter“ schützen (Menschen, Prozesse einer Klinik, Daten). Die Akzeptanzkriterien sind für jedes Schutzziel eigenständig festzulegen.
Das Ziel der Anwendung der Norm ist die Schaffung von Transparenz bei Errichtung und Betrieb eines MIT und die Herstellung eines robusten MIT, dass sich durch die folgenden drei Eigenschaften auszeichnet (Abbildung 7):

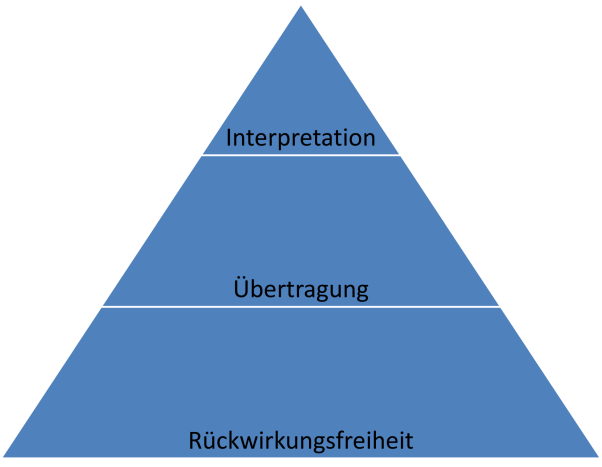

Abbildung 7: Ebenen eines robusten MIT

Rückwirkungsfreiheit: Beim Betreiben eines MIT ist darauf zu achten, dass Störungen im IT-Netzwerk keine Fehlfunktion von angeschlossenen Medizinprodukten auslösen. Dabei ist sowohl auf die elektrische, wie auch auf die logische Rückwirkungsfreiheit zu achten. Während für die elektrische Rückwirkungsfreiheit entsprechende Normen (z.B. DIN EN 60601-1) zur Verfügung stehen und in den meisten Fällen durch Standardprodukte abgedeckt wird, stellt die logische Rückwirkungsfreiheit, z.B. durch ein Dauersenden einer defekten Komponente auf ein Medizinprodukt oder dem Einbringen einer Schadsoftware (Viren, Trojaner, etc.), eine neue Herausforderung dar. Da bei aktiven Komponenten alle Zustände und deren Kombinationen zu betrachten sind entsteht schnell eine nicht oder kaum beherrschbare Komplexität, für die es in Zukunft Lösungen zu finden gilt.
Korrekte Übertragung: Es gilt der Merksatz, dass die richtigen Daten die richtige Netzwerkkomponente (Empfänger) zur richtigen Zeit erreichen müssen. Es muss also sichergestellt sein, dass die Daten unverändert den Empfänger erreichen. Das bedeutet auch, dass in einem gerouteten Netzwerk sichergestellt sein muss, dass die einzelnen Datenpakete bei der Übertragung in der richtigen Reihenfolge am Empfänger ankommen müssen, bzw. der Empfänger diese wiederherstellen können muss.
Es muss weiter sichergestellt werden, dass der richtige Empfänger erreicht wird. Dies setzt u.a. eine saubere Administration der Netzwerkadressen der Medizinprodukte und IT-Systeme voraus.
Die größte Herausforderung stellt die zeitliche Komponente dar: Je komplexer ein Netzwerk wird und je mehr aktive Komponenten zwischen Sender und Empfänger geschaltet werden (Router, Firewall, etc.) desto länger werden die Antwortzeiten. Zum anderen findet in Ethernet-Netzwerken keine Priorisierung von Nachrichten statt. Bei einer hohen Netzwerkauslastung kann es durch eine Verringerung der zur Verfügung stehenden Bandbreite nicht nur zu einer zeitlichen Verzögerung, sondern auch zu einem Abbruch der Datenübertragung durch Timeouts kommen. Hier gilt es z.B. zu betrachten, wie Systeme auf Verzögerungen oder Netzwerkabbrüche reagieren.
Interpretation: Es ist wichtig, dass die übertragenen Daten richtig interpretiert werden. Dies setzt eine syntaktische Korrektheit der Nachricht, sowie eine einheitliche Semantik zwischen Sendern und Empfängern voraus. Hierzu stehen verschiedene Standards zur Verfügung, wie z.B. die IEEE 11073 für die Datenkommunikation oder die Standards von HL7 (http://www.hl7.de/). Die größte Herausforderung liegt in der semantisch eindeutigen Kodierung. Hier sind neben den Klassifikationen, wie die ICD oder der OPS, Terminologien wie LOINC oder SNOMED CT zu nennen [7]. LOINC ist eine frei zur Verfügung stehende Terminologie, die jedoch nur die Bezeichnung (quantitativer) Parameter abbildet. Für die weiterführende Terminologie und Ontologie SNOMED CT, die aktuell die Basis nahezu aller internationalen Standards im Bereich der Interoperabilität bildet, steht in Deutschland keine nationale Lizenz zur Verfügung. Aus diesem Grund arbeiten die meisten Medizinprodukte und IT-Systeme mit proprietären Katalogen, die häufig durch die Betreiber gepflegt und an den Schnittstellen angeglichen werden müssen.

Fazit

Aus den Ausführungen geht hervor, dass ein Netzwerk respektive ein MIT nicht 100% sicher zu gestalten ist. Darüber hinaus können MIT nicht wie einzelne MP einfach ausgeschaltet oder ausgetauscht werden.
Daraus lassen sich zwei wesentliche Konsequenzen für die Erstellung eines robusten MITs ableiten:

- Ein MIT muss einem Management und damit auch einem Risikomanagement unterzogen werden
- Neben dem MIT müssen auch die MP für die Integration in ein MIT entsprechend robust gestaltet werden. Die von den Herstellern bei der Konzeption von Medizinprodukten getroffenen Maßnahmen stellen einen wesentlichen Baustein in der Risikobewertung eines MIT dar und sind im Risikomanagement eines MIT zwingend zu berücksichtigen.

4.2 Geltungsbereich

Laut Definition ist ein MIT ein IT-Netzwerk, an dem mindestens ein Medizinprodukt angeschlossen ist. Reine IT-Netzwerke oder Netzwerke ausschließlich mit Medizinprodukten eines dafür verantwortlichen Herstellers fallen nicht unter diese Definition (s. Abbildung 8).

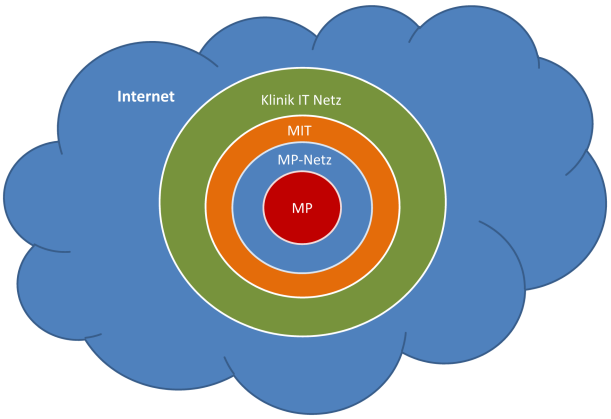

Abbildung 8: Definition eines MIT: Es bildet den Übergang zwischen einem reinen IT-Netzwerk und einem reinen Medizinprodukte Netzwerk (MP).

Mit der zunehmenden klinikübergreifenden Verbindung von IT-Netzwerken, sowie dem Anschluss von Klinik-IT-Netzwerken an das Internet ist eine Abgrenzung eines MIT entsprechend der Definition kaum möglich. Auch die Trennung von reinen MP-Netzwerken, wie die eigentlich abgeschlossenen Netzwerke für das Patientenmonitoring auf der Intensivstation wird durch Verbindungen über einen dezidierten Gatewayrechner an das Klinik-IT-Netz aufgeweicht.
Die Anwendung der IEC 80001-1 auf das gesamte Netzwerk einer Klinik ist wenig realistisch, wenn nicht gänzlich unmöglich. Deshalb ist es am Betreiber eines großen Netzwerkes, es in Subnetze zu unterteilen und Verantwortlichkeiten (und damit verantwortliche Personen) für physikalische, logische oder geschäftliche Bereiche zu bestimmen. Innerhalb dieser Teile sollte dann eine Bestandsaufnahme erfolgen und abgewogen werden, welche Teilbereiche sich für ein Risikomanagement eignen bzw. für welche es sinnvoll oder nötig erscheint. Hierbei ist abzuwägen, von welchen Teilen eine Gefährdung der Patienten- oder Anwendersicherheit ausgeht, und welche Teile missionskritisch oder unternehmenskritisch sind. Als missionskritisch wird ein Ausfall der Anwendung verstanden (z.B. ist keine Untersuchung bei Ausfall der Verbindung zwischen Steuerungs-PC und Computertomograph möglich), als unternehmenskritisch ein geschäftlicher Vorgang, ohne den eine Klinik nicht existieren kann (z.B. Übermittlung der für eine Abrechnung erforderlichen Daten).
Ein Netzwerk mit Medizinprodukten, wenn es als Ganzes wiederum ein Medizinprodukt ist, kann nicht als MIT gesehen werden. Als Beispiel kann hier ein Patientenmonitoring-System dienen, das als abgeschlossenes System Alarme am Patienten generiert und sie über ein Netzwerk an zentrale Überwachungsstationen überträgt. Das Gesamtsystem fällt nicht zuletzt wegen der Alarmierungszeiten und -garantien unter das Medizinprodukte-Gesetz [2] und die Medizinprodukte Betreiberverordnung [3]. Ein solches Netzwerk ist nicht Gegenstand der IEC 80001-1, die Anwendung ihrer Prinzipien ist aber möglich und empfehlenswert. Verbindet man dieses Netz allerdings über ein Gateway mit einem anderen Netzwerk, muss wieder nach IEC 80001-1 eine Risikoabschätzung und -bewertung stattfinden.
Ein solches MP-Netzwerk sollte ausschließlich mit Komponenten betrieben werden, die den Vorgaben des Herstellers entsprechen und von ihm abgenommen sind. In diesem Fall liegen die Verantwortung und das Haftungsrisiko beim Hersteller. Wird z.B. ein Netzwerk von bettseitigen Patientenmonitoren und einer Zentrale auf einer Intensivstation mit eigenen, nicht herstellerkonformen Netzwerkkomponenten und/oder W-LAN eingerichtet, so ist dies kein abgeschlossenes Netzwerk Klasse C gemäß Anlage H der DIN EN 60601-1. Dieser Fall gehört nicht in den Geltungsbereich der IEC 80001-1, jedoch kann deren Anwendung bei dem erforderlichen Risikomanagement weiterhelfen.
In solchen, wie auch mit der IEC 80001-1 zu behandelnden Fällen ist es wichtig, dass die IT-Netze die herstellerseitigen Risiko-Strategien nicht unterlaufen. Das bedeutet, dass Hersteller ihre Risikoeinschätzung bezüglich Risiken, die sie nicht allein beherrschen können oder die vermutlich bei einer Vernetzung auftreten können, den Betreibern der Produkte mitteilen müssen, damit die identifizierten Risiken mit in das Risikomanagement einfließen können [8].
In der Definition des Geltungsbereiches ist die Definition des Medizinproduktes enthalten. Ein Medizinprodukt wird in der 4. Novelle des MPG in §3 (1) wie folgt definiert:

> *„Medizinprodukte sind alle einzeln oder miteinander verbunden verwendeten Instrumente, Apparate, Vorrichtungen, Software, Stoffe und Zubereitungen aus Stoffen oder andere Gegenstände einschließlich der vom Hersteller speziell zur Anwendung für diagnosti-*

sche oder therapeutische Zwecke bestimmten und für ein einwandfreies Funktionieren des Medizinproduktes eingesetzten Software, die vom Hersteller zur Anwendung für Menschen mittels ihrer Funktionen zum Zwecke

a) der Erkennung, Verhütung, Überwachung, Behandlung oder Linderung von Krankheiten,

b) der Erkennung, Überwachung, Behandlung, Linderung oder Kompensierung von Verletzungen oder Behinderungen,

c) der Untersuchung, der Ersetzung oder der Veränderung des anatomischen Aufbaus oder eines physiologischen Vorgangs [...]

zu dienen bestimmt sind und deren bestimmungsgemäße Hauptwirkung im oder am menschlichen Körper weder durch pharmakologisch oder immunologisch wirkende Mittel noch durch Metabolismus erreicht wird, deren Wirkungsweise aber durch solche Mittel unterstützt werden kann."

Ein Produkt wird durch den Hersteller über die subjektive medizinische Zweckbestimmung und der vorgesehenen medizinischen Verwendung zum Medizinprodukt. Eine zweckfremde Verwendung eines Nichtmedizinprodukts allein macht dies noch nicht zu einem Medizinprodukt. Verändert eine Person oder stellt etwas Neues her, um es in der Medizin zu verwenden, fällt dies in den Bereich der Eigenherstellung und das Resultat wird zum Medizinprodukt. Ein wesentliches Problem stellen zunehmend Produkte dar, deren Funktionsumfang oder Produkteigenschaft weit über die beschriebene Zweckbestimmung hinausgeht. Dies betrifft meist Geräte, die auf „normalen" PCs basieren und die über offene Schnittstellen verfügen. Die teilweise kontrovers geführte Diskussion, in wie weit Software, wie Krankenhausinformationssysteme (KIS) oder Intensivinformationsmanagementsysteme (IMS), ein Medizinprodukt ist [9], [10], [11], wurde nun durch die Europäische Kommission mit einer Guidance zur „Qualifikation und Klassifikation von Standalone-Software" (MEDDEV 2.1/6 Jan 2012) weitestgehend geklärt. KIS und IMS/PDMS sind per se nicht als Medizinprodukt einzustufen (Module, die zusätzliche Information zur Diagnostik, Therapie oder Fortschreibungen/Nachfolgeuntersuchungen anbieten, sind als Medizinprodukt einzustufen.) [12].

IMS fallen unabhängig von der Einstufung als MP in den Geltungsbereich der IEC 80001-1, da IMS mit MP wie Patientenmonitoren, Beatmungsgeräten oder Blutgasanalysegeräten verbunden sind.

Reine IT-Netzwerke fallen nicht unter die Bestimmung der IEC 80001-1. Die Erfahrungen und Prinzipien der Norm können jedoch auch auf unternehmenskritische IT-Netzwerke angewendet und so Schaden von den Betreiberorganisationen abgewendet werden.

Bei Projekten empfiehlt es sich, gezielt nach dem vorgesehenen klinischen Prozess mit den dazu gehörenden Anwendungsfällen zu schauen, und die dabei auftretenden Risiken zu betrachten. Dieser Ansatz verspricht eine begrenzte Zahl an Szenarien, für die Risiken abgeschätzt werden müssen, während bei einer generellen Betrachtung praktisch kaum ein Ende absehbar ist. Hierbei gilt es zu beachten, dass gerade teure und komplexe Geräte oder -kombinationen in verschiedenen Prozessen genutzt werden oder die Form der Nutzung kontinuierlich erweitert wird. Reduziert man die Anwendungsfälle auf die im Prozess wichtigen Anwendungsfälle, kann man die Risiken eventuell viel niedriger ansehen, als sie wirklich sind. Mit steigender Anzahl an Projekten mit Risikomanagement, werden auch mehr Anwendungsfälle betrachtet und die Einschätzung des Risikos wird realistischer.

Fazit

- In einer Klinik (Betreiberorganisation) sollte das IT-Netzwerk in die Subnetze anhand von logischen, organisatorischen und geschäftlichen Bereichen getrennt werden.
- Es sollten für die Subnetzbereiche verantwortliche Personen benannt werden.
- Durch die Verantwortlichen ist eine Prüfung durchzuführen, ob die IEC 80001-1 auf das Subnetz anzuwenden ist.

4.3 Durchführung von Risikoidentifikation, Risikobewertung, Risikomanagement

> *„Entscheidend für die Sicherheit ist nicht allein die Funktionalität im Regelfall, sondern auch die Rückwirkung im Störfall auf das Medizinprodukt und die resultierenden Risiken für Patient, Anwender und Betreiber!"* (Peter Roß)

Das Ziel der Risikoidentifikation ist, mögliche Störfälle und Schäden zu identifizieren. Das Ziel der Risikobewertung ist, die Schadenshäufigkeit und das Schadensausmaß abzuschätzen, um im Risikomanagement die Ursachen identifizieren und geeignete Gegenmaßnahmen ergreifen zu können.

Die Risikoidentifikation und -bewertung erfolgt in Verantwortung des MIT-Risiko-Managers. Dieser sollte eine Arbeitsgruppe aus Anwendern, Medizintechnik, Medizininformatik (Applikationen), IT-Netzwerkadministration als betroffene Beteiligte zusammenstellen und, wo notwendig, auch die Hersteller einbeziehen.

Die Anwender nehmen bei der Risikoidentifikation und -bewertung eine zentrale Stellung ein. Sie beschreiben die klinischen Prozesse und damit die Verwendung der eingesetzten MP und IT-Systeme des MIT. Danach gilt es systematisch für alle Funktionalitäten und Kommunikationsszenarien Störfälle anzunehmen und deren hypothetische Auswirkungen durchzugehen.

Dazu sind detaillierte Kenntnisse über die Funktionsweise und Implementierung der MP und IT-Systeme erforderlich, die nur der Hersteller besitzt. Daher sind die Hersteller von MP verpflichtetet, die folgenden Informationen an die Betreiber herauszugeben:

- Zweckbestimmung, Leistungsmerkmale des MP
- Anforderungen an das MIT
- Technische (elektrische und logische) Spezifikation der Netzwerk-Schnittstellen
- Funktionsweise der Kommunikation mit anderen MP, MIT und IT-Systemen
- Informationen über die Bewertung von Restrisiken (Risikoanalyse des Herstellers)
- Liste der Gefährdungssituationen, wenn das MIT die Anforderungen nicht erfüllt.

Die Herausgabe dieser Informationen ist durch die IEC 60601-1:2005 geregelt und auch in der IEC 80001-1 Kapitel 3.5 beschrieben. Sollten für die Risikobewertung der Betreiberorganisation Informationen erforderlich sein, die der Hersteller als Firmengeheimnis einstuft, so können diese vertraulichen Informationen durch eine Vertraulichkeitsvereinbarung zwischen Betreiberorganisation und Hersteller geschützt werden.
Schwieriger stellt sich die Situation bei den Informationen über die in das MIT integrierten IT-Systeme dar. Zum einen fehlt hier eine Verpflichtung für die Hersteller zur Offenlegung der Risikoanalyse, zum anderen werden Restrisiken häufig von den Herstellern nicht regelhaft identifiziert, bewertet und dokumentiert. Aufgrund deutlich kürzerer Releasezyklen und einer Vielzahl von Abhängigkeiten (Betriebssystem, Virenscanner, Schnittstellen zu Subsystemen) und Freiheitsgraden (Parametrierungen des Betreibers bis zur Programmierung) stellt sich hier für die Hersteller auch die Frage der Machbarkeit. Hersteller von IT-Systemen sollten aber folgende Informationen zur Verfügung stellen:

- Technische Beschreibungen und technische Handbücher/Betriebsanleitungen
- Beschreibung der Parametrierungsoptionen und deren Auswirkungen
- System- und Betriebsanforderungen, inkl. Anforderungen an das IT-Netzwerk/MIT
- bekannte Inkompatibilitäten mit anderen Produkten
- Informationen über erforderliche Updates und Patches
- Sicherheitshinweise

Insbesondere die Auflistung der Kompatibilitäten/Inkompatibilitäten stellt eine Schwierigkeit dar, da diese für jeden Firmware Version und jeden Patch von jedem Gerät in unterschiedlichen Kombinationen getestet und veröffentlicht werden müsste.
Die Herausforderung für Betreiber besteht vor allem darin, mit mehreren Herstellern oder Lieferanten mit unterschiedlicher Risikomanagementkultur zu sprechen und die gesammelten Informationen abzugleichen. Dies kann nur durch einen kooperativen Dialog zwischen allen Beteiligten geschehen.
Der Austausch der Informationen sollte nach Meinung der Workshopteilnehmer eher eine kontinuierliche Kommunikation darstellen als eine einmalige Übermittlung. Sowohl der Hersteller sollte bei Änderungen den Kontakt zu den Betreibern suchen, als auch umgekehrt der Betreiber bei kritischen Situationen, die Produkte des Herstellers betreffen. Die Festlegung eines definierten Formats für den Datenaustausch (beispielsweise XML-Dateien nach einem Schema) und eines maximalen Zeitraums seit der letzten Aktualisierung ist hier sehr zu empfehlen.
Auch die Einschätzung der Eintrittswahrscheinlichkeit eines Schadens stellt sich schwierig dar: Während in der Medizin für Behandlungsverfahren und Arzneimittel eine Risikobewertung durch die Gegenüberstellung des Nutzens und möglicher Schäden auf einer empirischen Basis erfolgt, ist dies durch die große Anzahl verschiedenster Geräte (Heterogenität) und Dynamik in der Veränderung von MIT kaum möglich.
Bei MIT sollte die Abschätzung der Eintrittswahrscheinlichkeit eines Schadens anhand einer Gefährdung (mit der Auswirkung auf das Schutzziel) erfolgen und nicht anhand jedes einzelnen möglichen Fehlers. Dabei sind alle möglichen Stör- und Fehlerquellen zu berücksichtigen und sowohl die Auswirkungen auf das System (Ausfall, Fehlverhalten), wie auch auf den Anwender (Fehlentscheidungen, Fehlverhalten) und den Patienten zu betrachten. Führt ein Fehler zu einer Patientengefährdung, ist er missions- oder unternehmenskritisch, gilt dieser als nicht akzeptabel und es sind entsprechende Maßnahmen zu ergreifen.
Bei der Beurteilung der Eintrittswahrscheinlichkeit eines Schadens und des Schadensausmaßes ist zwingend die Betrachtung des Nutzungskontextes und damit der klinischen Prozesse und die Konformität mit den Erwartungen und dem Verhalten des Anwenders/Bedieners erforderlich. Während in dem Beispiel einer zentralen Darstellung über den Füllstand von Spritzenpumpen auf der Intensivstation ein erhebliches Risiko ausgeht (s. Beispiel 3, Kapitel 2.2) kann die gleiche Technologie im Bereich der Überwachung von Spritzenpumpen in der Patientenkontrollierten Anästhesie (PCA) in der Akutschmerztherapie einen Mehrwert ohne zusätzliches Risiko entwickeln. Hier wäre sogar der Einsatz einer unsichereren Technologie, wie WLAN, denkbar.
Zur Risikominimierung sollten vor allem technische, bzw. konstruktive und ergänzend organisatorische Maßnahmen ergriffen werden.
Besteht nach der Durchführung geeigneter technischer und organisatorischer Maßnahmen ein Restrisiko, so ist dies ebenfalls zu bewerten. Es ist die Aufgabe des obersten Managements der Betreiberorganisation die Kriterien für die Ermittlung eines akzeptablen Restrisikos festzulegen. Diese Verantwortung kann nicht delegiert werden.

Fazit

- Basis für die Risikoanalyse ist der klinische Prozess (Nutzungskontext).
- Für die Risikoidentifizierung sind Informationen der MP und IT-Systemhersteller erforderlich.
- Die Bereitstellung der notwendigen Informationen sollte in einem strukturierten Dialog erfolgen und auch strukturiert abgelegt (z.B. in einem XML-Dokument) werden.

- Die Risikobewertung sollte anhand des Schadens im 1. Fehlerfall erfolgen.
- Zur Risikominimierung sollten vor allem technische, bzw. konstruktive und ergänzend organisatorische Maßnahmen ergriffen werden.
- Vorgaben für die Akzeptanz des Restrisikos müssen vom obersten Management erfolgen.

4.4 Empfehlung zur Einführung und Aufrechterhaltung des Risikomanagementprozesses

4.4.1 Allgemeine Empfehlungen

Die IEC 80001-1 ist keine harmonisierte Norm und dient nicht zur Ausfüllung der grundlegenden Anforderungen der MDD-Richtlinie einschließlich der ergänzenden Verordnungen. Sie stellt den Stand der Technik dar und dient zu belegen, dass bestimmte Prozesse in der verantwortlichen Betreiberorganisation erfüllt wurden. Sie kann als solche ggf. in Gutachten oder Gerichtsverfahren zitiert werden. Somit dient die Einhaltung der Prozesse entsprechend der Norm der Reduktion von Haftungsrisiken.
In den seltensten Fällen gibt es in verantwortlichen Organisationen einen definierten Prozess für die Errichtung oder Erweiterung eines MIT. Auch fehlt meist eine zentrale benannte Stelle, die für diese Aufgabe zuständig ist. Eher wird man den Zustand einer historisch gewachsenen IT- und MP-Infrastruktur mit wenig beschriebenen MITs vorfinden. Die IEC 80001-1 bezieht sich auf den gesamten Lebenszyklus eines MIT: Das Risikomanagement ist von der Planung über die Inbetriebnahme und den Betrieb bis zum Abschalten durchzuführen. Daher müssen früher oder später alle Systeme einem Risikomanagement unterzogen werden. Um die Einführung handhabbar zu gestalten, empfiehlt sich folgendes Vorgehen:

- Benennung eines Verantwortlichen für das Risikomanagement des gesamten IT-Netzwerks
- Aufteilung des Netzwerkes in Subnetze anhand von logischen, organisatorischen und geschäftlichen Bereichen (wie auch in Kapitel 4.2 beschrieben)
- Bewertung der Subnetze bzgl. der Geltungsbereiche der IEC 80001-1
- Bewertung der Risiken in den einzelnen Subnetzen und Priorisierung eines Netzes, mit dem die Umsetzung begonnen und Erfahrungen mit der IEC 80001-1 gewonnen werden kann
- Ebenfalls bietet es sich an, alle neuen Projekte einem Risikomanagement gemäß IEC 80001-1 zu unterziehen.

Fazit

Die Einführung sollte zunächst an einem neuen Projekt pilotiert und danach ausgeweitet werden. Da sich der Nutzen der Aktivitäten nicht einfach und automatisch erschließt, ist ein internes Marketing für die IEC 80001-1 empfehlenswert. Nur so kann mit der Umsetzung der Norm der Dialog zwischen den verschiedenen Fachdisziplinen gefördert werden. Aus Erfahrung der Workshopteilnehmer ist davon auszugehen, dass die Umsetzung der IEC 80001-1 in den meisten verantwortlichen Organisationen mehrere Jahre dauert. Daher ist es wichtig, bereits frühzeitig damit zu beginnen. Beim ersten Projekt kann man sich meist auf besonders auf kritische Komponenten des bestehenden Netzwerkes und solche mit denen man direkt interagiert beschränken.

4.4.2 MIT-Risiko-Manager

Die Oberste Leitung der verantwortlichen Organisation hat nach Vorgaben der Norm IEC 80001-1 einen MIT-Risiko-Manager zu benennen. Aufgrund der Komplexität von MIT sollten Risikoidentifizierung und Risikobewertung jedoch nicht von einer einzelnen Person, sondern durch eine Gruppe durchgeführt werden, in der folgende Kompetenzen vertreten sind:

- Risiko-/Qualitätsmanagement
- Medizintechnik
- Medizinische Informatik
- Netzwerk- und Systemtechnik
- Klinische Anwender (Ärzte, Pflege, etc.)

In einem Klinikverbund oder einem größeren Gesundheitsdienstleister mit mehreren Kliniken kann es sich anbieten, eine solche Arbeitsgruppe klinikübergreifend in der Konzernzentrale anzusiedeln. So können Erfahrungen aus den verschiedenen Projekten synergetisch anderen Kliniken zur Verfügung gestellt werden.
Können in einer Betreiberorganisation nicht alle Kompetenzbereiche abgedeckt werden, ist ein Outsourcing an einen Hersteller oder eine unabhängige Beratungsfirma möglich. Es ist jedoch zu überlegen, in wie weit das Betreiben eines MIT aufgrund unternehmenskritischer Eigenschaften zu den Kernprozessen einer Klinik gehört und ein eigener Kompetenzaufbau angestrebt werden sollte.

4.4.3 Einrichtung einer Anlaufstelle für neue Projekte

Für die Anwender und andere Stakeholder sollte eine Anlaufstelle und ein Prozess geschaffen werden, an der alle Projekte und Beschaffungen anzumelden sind, bei denen Geräte an ein Netzwerk angeschlossen werden. Dies sollte eine Prüfung nach sich ziehen, ob das Projekt oder die Beschaffung in den Geltungsbereich der IEC 80001-1 fallen. Da potentiell alle Geräte mit einem Netzwerkanschluss an ein MIT angeschlossen werden und für die Anwender die Einteilung in die Subnetze (s. Kapitel 4.2 und 4.4.1) nicht immer transparent und nachvollziehbar sind, sollte dies über den Verantwortlichen für das Gesamtnetzwerk oder den MIT-Risiko-Manager erfolgen.

4.4.4 Durchführung des Risikomanagementprozesses

Hinweise zu Risikoidentifikation, Risikobewertung und Risikomanagement wurden in Kapitel 4.3 beschrieben.
Bei der Etablierung des Prozesses ist an verschiedenen Stellen mit Widerständen zu rechnen:
Ein wesentlicher Punkt ist eine „Bastelbudenmentalität“: So findet die Integration von IT-Systemen im Gegensatz zur Strategie bei MP häufig mit einer „Trial-and-Error“ Strategie statt. In manchen Fällen werden (Software-)Produkte auch in Gebieten eingesetzt, für die sie nicht explizit entwickelt wurden, Funktionalitäten also „zweckentfremdet“ oder nicht dokumentierte Systemeigenschaften als „Feature“ genutzt werden. Da in diesen „Projekten“ zudem häufig zu wenig Zeit für Dokumentation und Tests aufgewendet wird, können schnell Funktionalitäten und damit nach außen sichtbare Erfolge hergestellt werden. Mit der Umsetzung einer schnellen Lösung entspricht man kurz- bis mittelfristig den Wünschen und Vorstellungen der Anwender bzgl. einer Leistungs- und Dienstleistungsorientierten IT-Abteilung, bzw. Herstellers.
Bei diesem Vorgehen fehlen jedoch die Schritte einer sauberen Prozess- und Umfeldanalyse, eine Festschreibung von Verantwortlichkeiten und Entscheidungsbefugnissen, sowie die erforderliche Dokumentation/Kommunikation und damit letztendlich die notwendige Transparenz. Somit ist keine verlässliche Risikoanalyse möglich. Umgekehrt ist mit einem Risikomanagement eine Integration neuer Geräte oder Systeme „nur mal eben schnell“ nicht mehr möglich.
Dies unterstreicht sowohl die Notwendigkeit eines professionell verwalteten Netzwerkes, als auch den erforderlichen politischen Willen und den Rückhalt durch das Management (inklusive der Obersten Leitung) des Krankenhauses für die Umsetzung.
Ein weiterer wichtiger Punkt ist die Rolle des MIT-Risiko-Managers: Er begleitet die für den Betrieb und das Projekt verantwortlichen Mitarbeiter durch das Risikomanagement. Dabei ist zu definieren, in wie weit er eine rein begutachtende oder beratende und unterstützende Rolle einnimmt. Um die Vorteile der IEC 80001-1 nutzen zu können, empfehlen die Autoren, unbedingt Beratung und Unterstützung des MIT-Risikomanagers in Anspruch zu nehmen. Außerdem obliegt ihm die Entscheidung, Änderungen am MIT freizugeben. Eine aktive Einbindung in frühe Projektphasen ist also empfehlenswert.

4.4.5 Die Achillesferse: Risikomonitoring und Change Management

Während bei der Einführung eines neuen Systems oder eines Medizinprodukts klare, transparente Projektschritte (Projektantrag, Projektfreigabe, Abnahme) vorhanden sind, ist der fließende Prozess des Routinebetriebes mit der Risikoüberwachung schwieriger zu handhaben.
Betrachtet man ein IT-Netzwerk in einer Klinik, so vergeht kaum ein Tag an dem nicht an einem IT-System, einem Datenbanksystem, einer Firewall, einem Virenscanner oder einer anderen Applikation ein Update oder Patch installiert wird. Es ist nahezu unmöglich, all diese Veränderungen an einem MIT, die zu einem Großteil aufgrund einer hohen Sicherheitsrelevanz zeitnah auszuführen sind (z.B. Betriebssystem Patch, Update Virenscanner, aber auch Fehlerbehebung in IT-Systemen) einer umfangreichen Risikoanalyse oder gar einem vollständigen Test auf Seiteneffekte in einem MIT zu unterziehen. Dies drückt sich auch darin aus, dass mehr Softwarefehler durch Seiteneffekte und Inkompatibilitäten bei Updates als durch Konstruktionsfehler bei Entwurf und Implementierung auftreten.
Umso wichtiger ist es, klare Regeln für die Risikoüberwachung und das Changemanagement in MIT zu erarbeiten und zu etablieren. Um Funktionalitäten und IT-Systeme/MP hinsichtlich von Seiteneffekten/unerlaubten Rückwirkungen bei der Risikoanalyse im Changemanagement priorisieren zu können, ist die bereits angesprochene Aufteilung des Gesamtnetzwerkes in Subnetze mit organisatorisch abhängigen IT-Verfahren zwingend erforderlich. Der MIT-Risikomanager des betroffenen Subsystems benötigt insbesondere folgende Informationen:

- Informationen des MP Herstellers zu dem Update
- Informationen des IT-Herstellers zu dem Update
- Information über notwendige oder durchgeführte Konfigurationsänderungen an IT-Systemen, MP oder Netzwerk.

Neben robusten MP und IT-Systemen, die auf logische Fehler in der Kommunikation erwartungskonform reagieren, stellt die Protokollierung von Kommunikationsfehlern eine wesentliche Voraussetzung für eine Fehlerüberwachung dar, die eine schnelle Reaktion der Verantwortlichen des MIT auf entsprechende Fehler erlaubt.
Während im Bereich der Medizintechnik durch das Medizinproduktegesetz und die Medizinprodukte-Betreiberverordnung klare gesetzliche Regelungen für das Fehlermanagement existieren, ist dies im Bereich der IT-Administration weniger geregelt. So ist der defacto Standard für das IT-Servicemanagement ITIL® (IT Infrastructure Library®, http://www.itil-officialsite.com/), in der Medizin kaum verbreitet [13]. ITIL bietet verschiedene Prozesse zur Strukturierung von internen und externen IT-Dienstleistern an. Die Prozesse zum Incident-, Problem-, Change- und Releasemanagement können einen wertvollen Baustein darstellen, ein MIT sicher zu überwachen und zu managen. Auf diese Weise kann die Kluft zwischen der Kultur der Medizintechnik und der IT-Administration geschlossen werden.

4.4.6 Dokumentation in der Risikomanagementakte

Die Dokumentation in der Risikomanagementakte dient vor allem der Transparenz der Risiken und der Rechtssicherheit im Schadensfall.
In der Akte soll das bestehende MIT inklusive der eingesetzten Medizinprodukte und Software und dem Verantwortlichen dokumentiert werden. Fehlen Informationen

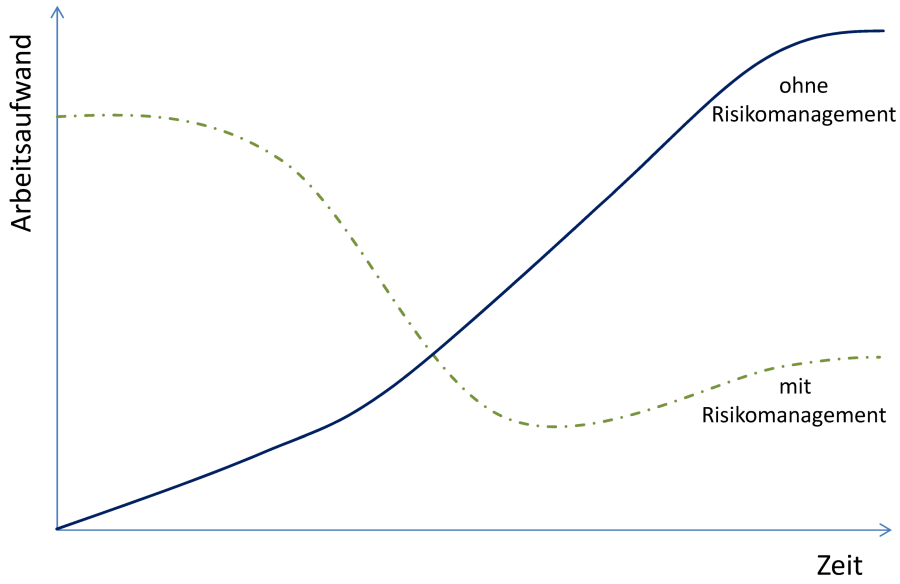

Abbildung 9: Schematisch skizzierter Aufwandsvergleich

zu Geräten, die vernetzt werden sollen, so sollte sowohl die Anfrage beim Hersteller als auch dessen Antwort in der Akte festgehalten werden, jeweils mit einem Verweis auf den verantwortlichen (betriebseigenen) Mitarbeiter. Des Weiteren wird hier der Risikobewertungs- und Risikokontroll-Prozess dokumentiert (siehe Kapitel 3.6).
Darüber hinaus sollte festgeschrieben werden, wie die Überwachung des Risikos stattfindet und wer dafür verantwortlich ist. Außerdem sind Abläufe für Änderungen an der Risikomanagementakte sowie Veränderungen am MIT hier dokumentiert.
Es gibt kein vorgegebenes Format, in dem die Daten erfasst und gespeichert werden sollten. Allerdings ist strikt auf Versionierung, Zugriffsrechte und Signierung der Dokumente zu achten, um die Verwendbarkeit in einem Rechtsstreit oder Zertifizierungsverfahren zu erhalten. Eine Vorgehensweise analog einem audit trail [14] kann hier eingesetzt werden.

4.5 Pro und Contra IEC 80001-1

Eines zeigt die Diskussion über die IEC 80001-1: Sie hat den verantwortlichen Organisationen aufgezeigt, welche Betreiberrisiken existieren. Dabei ist entscheidend, dass die Haftungsrisiken nicht durch die IEC 80001-1 auftreten, sondern durch sie aufgezeigt und damit beherrschbar werden.
Ein weiterer Vorteil ist eine klare Definition der Verantwortlichkeiten, einschließlich des Zusammenspiels und der Kommunikation mit den Herstellern.
Dem Zugewinn an Sicherheit für Patienten und Anwender steht ein erhöhter administrativer Aufwand gegenüber: Die Position des MIT-Risiko-Managers muss ausgefüllt und Verantwortlichkeiten müssen geklärt werden. Die Risikoanalyse vor dem eigentlichen Projektbeginn erhöht den administrativen Aufwand für den Projektverantwortlichen und verlangsamt die Einführung neuer Technologien. So kann die IT-Abteilung nicht mehr so flexibel auf Anwenderwünsche eingehen.
Die Vorteile zeigen sich nach Meinung der Autoren bereits im Projektverlauf. Durch die Dokumentation und Transparenz, die im Projektvorlauf geschaffen wurde, können vor allem folgende Projekte schneller und zuverlässiger mit einem hohen Maß an Sicherheit durchgeführt werden. Dies ergibt sich hauptsächlich durch die Vermeidung von Problemen in späteren Projektphasen, wie in Abbildung 9 schematisch dargestellt.

Fazit

In Abwägung aller Argumente für und gegen eine Anwendung der IEC 80001-1 (Abbildung 10) überwiegen deutlich die Vorteile. Aufgrund der zunehmenden Komplexität der Netzwerke und der Schnittstellen, letztendlich basierend auf der Komplexität der abzubildenden klinischen Prozesse, werden die Kliniken in den nächsten Jahren keine Alternative zur Einführung eines strukturierten Managements von MIT haben. Die Herausforderung liegt nicht (allein) in der Technik, die eingesetzt wird, sondern vielmehr in der Organisation und Struktur der Betreiberfirmen. Sie erfordert Veränderungen und vor allem Kooperation im Unternehmen, um interne Analysen durchführen zu können. Auch wenn externe Beratung und Unterstützung sehr empfehlenswert ist, kann sie hierbei nur einen zusätzlichen Baustein zum betriebseigenen Know-How darstellen.
Für die Zukunft wäre es wünschenswert, die Synergien zwischen Medizinproduktegesetz und IEC80001-1 zu verbessern, in dem die erforderlichen Geräte und Systembeschreibungen vereinheitlicht werden.

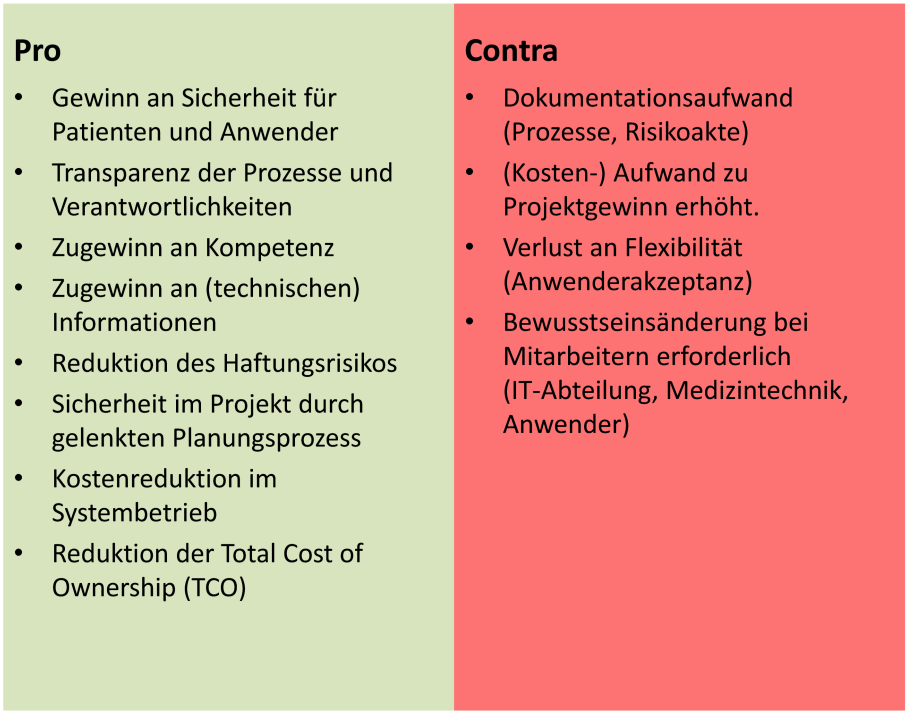

Abbildung 10: Pro und Contra-Argumente zur IEC 80001-1

5 Abkürzungsverzeichnis

DGBMT – Deutsche Gesellschaft für Biomedizinische Technik
DIVI – Deutsche Interdisziplinäre Vereinigung für Intensiv- und Notfallmedizin e.V. (Interdisziplinäre und interprofessionelle Fachgesellschaft und Dachverband von Fachgesellschaften und Berufsverbänden)
HL7 – Health Level Seven: Gruppe von Standards/Organisation, die diese Standards herausgibt
IEC – International Electrotechnical Commission
IHE – Integrating the Healthcare Enterprise
IMS – Intensivinformationsmanagementsystem Synonym PDMS
IT – Informationstechnologie
LOINC – Logical Observation Identifiers Names and Codes: Nomenklatur für die Bezeichnung von (Labor-) Parametern (Observation Identifier)
MIT – Medizinisches-IT-Netzwerk: IT-Netzwerk mit mindestens einem Medizinprodukt
MP – Medizinprodukt
PACS – Picture Archiving and Communication System
PDMS – Patientendatenmanagementsystem, Synonym für ein Intensivinformationsmanagementsystem
SNOMED CT – Systematized Nomenclature of Human and Veterinary Medicine – Clinical Terms; umfassende medizinische Nomenklatur
TOC – Total Cost of Ownership (Gesamtkosten für den Betreiber über die Gesamtnutzungsdauer eines Systems)
VDE – Verband der Elektrotechnik, Elektronik und Informationstechnik

Anmerkung

Positionspaper Risikomanagement für medizinische Netzwerke (MIT) DIVI – Sektion IT und Medizintechnik unter Beteiligung

- des Verbandes der Elektrotechnik Elektronik Informationstechnik e.V. (VDE),
- der Deutschen Gesellschaft für Biomedizinische Technik im VDE (DGBMT),
- der Deutschen Interdisziplinären Vereinigung für Intensiv- und Notfallmedizin (DIVI),
- des Bundesverbandes Gesundheits-IT (BVITG)
- und der Deutschen Gesellschaft für Fachkrankenpflege (DGF).

Ergebnisse eines Workshops am 13. Dezember 2010 in Gießen.

Unter Mitarbeit von:

- Rawan Al-Alawi, Rhön-Klinikum AG
- Prof. Dr. Björn Bergh, Uniklinikum Heidelberg/IHE Deutschland
- Dipl.-Ing. Oliver Christ, Prosystem AG
- Christoph Isele, Siemens AG Healthcare
- Andreas Kassner, BVITG
- Matthias Meierhofer, Meierhofer AG/BVITG
- Dr. Klaus Neuder, VDE/DKE
- Dr. Norbert Pauli, Dräger Medical GmbH
- Peter Roß, Rhön-Klinikum AG
- Andreas Schäfer, DGF
- Christian Schübel, TÜV Süd
- Dr.-Ing. Dipl.-Wirt. Ing. Olaf Such, Philips/DGBMT

Interessenkonflikte

Die Autoren erklären, dass sie keine Interessenkonflikte in Zusammenhang mit diesem Artikel haben.

Literatur

1. Fähling J, Köbler F, Leimeister J, Krcmar H. Wahrgenommener Wert von IT in Krankenhäusern – eine empirische Studie. In: Hansen HR, Karagiannis D, Fill HG, eds. Business Services: Konzepte, Technologien, Anwendungen. Wien: ocg; 2009. p. 709-18.
2. Medizinproduktegesetz in der Fassung der Bekanntmachung vom 7. August 2002 (BGBl. I S. 3146), das zuletzt durch Artikel 11 des Gesetzes vom 19. Oktober 2012 (BGBl. I S. 2192) geändert worden ist.
3. Medizinprodukte-Betreiberverordnung in der Fassung der Bekanntmachung vom 21. August 2002 (BGBl. I S. 3396), die zuletzt durch Artikel 4 des Gesetzes vom 29. Juli 2009 (BGBl. I S. 2326) geändert worden ist.
4. Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM). Design-/Konstruktionsfehler. [last accessed May 4th 2011]. Available from: http://www.bfarm.de/DE/Medizinprodukte/riskinfo/wissauf/statist/statist-Auswert_Fehlerursache_Design-Konstrukfehler.html
5. Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM). Aktuelle statistische Auswertungen der Abteilung Medizinprodukte. [last accessed May 4th 2011]. Available from: http://www.bfarm.de/DE/Medizinprodukte/riskinfo/wissauf/statist-auswertung.html?nn=1012476
6. Deutsches Institut für Normung. Anwendung des Risikomanagements für IT-Netzwerke, die Medizinprodukte beinhalten: Teil 1: Aufgaben, Verantwortlichkeiten und Aktivitäten (IEC 80001-1:2010); Deutsche Fassung EN 80001-1:2011. 2011.
7. Röhrig R, Rüth R. Intelligente Telemedizin in der Intensivmedizin – Patientennaher Einsatz von Medizintechnik und IT in der Intensivmedizin. Bundesgesundheitsblatt Gesundheitsforschung Gesundheitsschutz. 2009 Mar;52(3):279-86. DOI: 10.1007/s00103-009-0792-x
8. Deutsche Industrie Norm (DIN). DIN EN 60601-1: Medizinische elektrische Geräte – Teil 1: Allgemeine Festlegungen für die Sicherheit einschließlich der wesentlichen Leistungsmerkmale.
9. Gärtner A. MDD 2007/47/EG: Software als Medizinprodukt. E-Health-Com. 2012. Available from: http://www.e-health-com.eu/fileadmin/user_upload/dateien/Downloads/Gaertner-Medizinprodukte-Gesetz.pdf
10. Johner C, Geis T. Medizinproduktegesetz MPG und Klassifikation von Software. In: Johner C, Haas P, eds. Praxishandbuch IT im Gesundheitswesen. München: Carl Hanser Verlag München; 2009. p. 13-15.
11. Johner C, Hölzel-Klüpfel S, Wittorf S, eds. Basiswissen medizinische Software. Heidelberg: dpunkt-Verlag; 2011.
12. European Commission DG Health and Consumer, Directorate B, Unit B2 "Health Technology and Cosmetics". Guidelines on the qualification and classification of stand alone software used in healthcare within the regulatory framework of medical devices. 2012. MEDDEV 2.1/6. Available from. http://ec.europa.eu/health/medical-devices/files/meddev/2_1_6_ol_en.pdf
13. Hoerbst A, Hackl WO, Blomer R, Ammenwerth E. The status of IT service management in health care – ITIL® in selected European countries. BMC Medial Informatics and Decision Making. 2011;11:76. DOI: 10.1186/1472-6947-11-76
14. General Services Administration Information Technology Service. Federal Standard 1037C: Glossary of Telecommunications Terms. 1996.

Korrespondenzadresse:
Deutsche Gesellschaft für Biomedizinische Technik (DGBMT) im VDE e.V., Fachausschuss Methodik der Patientenüberwachung
c/o Prof. Dr. med. Michael Imhoff, Abteilung für Medizinische Informatik, Biometrie und Epidemiologie, Ruhr-Universität Bochum, Universitätsstraße 150, 44801 Bochum, Deutschland, Tel.: +49 231 9730220
mike@imhoff.de

Bitte zitieren als
Ahlbrandt J, Röhrig R, Dehm J, Wrede C., Imhoff M, Sektion IT & Medizintechnik der Deutschen Interdisziplinären Vereinigung für Intensiv- und Notfallmedizin e.V., Deutsche Gesellschaft für Biomedizinische Technik (DGBMT) im VDE e.V., Fachausschuss Methodik der Patientenüberwachung. Risikomanagement für medizinische Netzwerke in der Intensiv- und Notfallmedizin. Gemeinsames Positionspapier zur Norm IEC 80001-1. GMS Med Inform Biom Epidemiol. 2013;9(3):Doc09.
DOI: 10.3205/mibe000137, URN: urn:nbn:de:0183-mibe0001378

Artikel online frei zugänglich unter
http://www.egms.de/en/journals/mibe/2013-9/mibe000137.shtml

Veröffentlicht: *19.02.2013*