Einführung der IEC 80001-1 im Deutschen Herzzentrum Berlin anhand eines Pilotprojektes

Bachelorarbeit

im Studiengang Medizintechnik

vorgelegt von

Paul Stappert

Hamburg, Januar 2012

Gutachter: Prof. Dr. Jürgen Stettin

Dr. Christine Bertram

Danksagung

Die Bachelorarbeit entstand im Auftrag der Firma mediplan Krankenhausplanungsgesellschaft mbH und der Hochschule für angewandte Wissenschaften Hamburg. Bedanken möchte ich mich bei Dr. Christine Bertram, die meine Arbeit seitens mediplan betreut hat und mir mit Rat und Tat zur Seite stand. Außerdem gilt mein Dank Herrn Prof. Stettin, welcher mir die Möglichkeit gegeben hat, über dieses spannende Thema meine Bachelorarbeit zu schreiben. Besonders möchte ich dem Deutschen Herzzentrum Berlin und speziell Herrn Saudhof danken. Nur durch diese nette und konstruktive Zusammenarbeit ist die Bachelorarbeit erst möglich geworden. Im Deutschen Herzzentrum Berlin möchte ich außerdem Herrn Vogel und Herrn Prof. Wellnhofer, sowie Herrn Vogler von der Firma Mediarch GmbH für die Hilfe und Zusammenarbeit danken.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

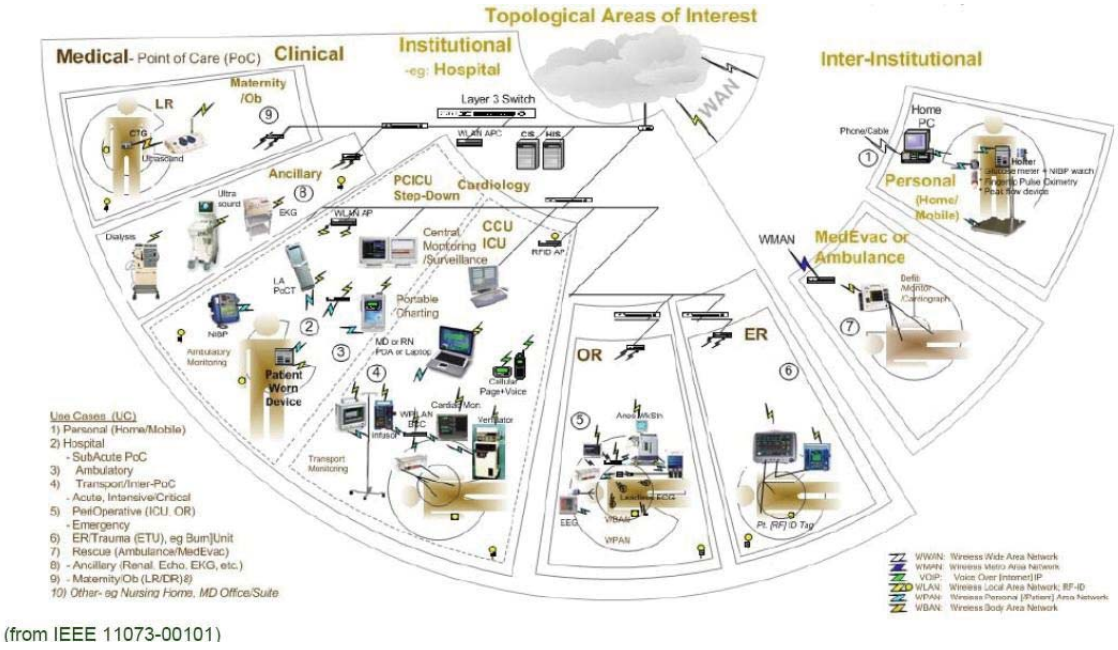
Abkürzungsverzeichnis

DHZB	Deutsches Herzzentrum Berlin
IT	Informationstechnologie
PEMS	Programmierbares Elektrisches Medizinisches System
PACS	Picture Archiving and Communication System
KIS	Krankenhausinformationssystem
DICOM	Digital Imaging and Communications in Medicine
MS	Microsoft
TCP/IP	Transmission Control Protocol / Internet Protocol
LWL	Lichtwellenleiter
IP	Internet Protocol
GE	General Electric
USV	Unterbrechungsfreie Stromversorgung
CIS	Cardiovaskuläres Imaging System
RIS	Radiologisches Informationssystem
PDMS	Patientendatenmanagementsysteme

1 Einleitung

1.1 Hintergrund

IT-Netzwerke erlangen eine immer größere Bedeutung im Arbeitsalltag eines Krankenhauses. Ursprünglich wurden diese eingesetzt um Verwaltung und Abrechnungen zu vereinfachen. Durch die zunehmende Vernetzbarkeit von Medizinprodukten, wird das Krankenhausnetzwerk verstärkt zur Dokumentation von Diagnosen und Behandlungen von Patienten eingesetzt. Speziell bei den bildgebenden Verfahren wird ein IT-Netzwerk zur Übertragung und Speicherung von medizinischen Daten verwendet, welche im Ernstfall lebensnotwendig sein können. Da ein IT-Netzwerk in einem Krankenhaus heutzutage aus einer Vielzahl von Komponenten und Systemen medizinischer und nicht-medizinischer Natur besteht, ist es nötig neue Standards für den Betrieb von solchen Medizinischen IT-Netzwerks einzuführen (Abbildung 1).



(from IEEE 11073-00101)

Abbildung 1: Mit einem Netzwerk verbundene Medizinprodukte

Die Norm IEC 60601-1:2005 regelte dies zunächst in geringem Maße, indem sie die Hersteller von Medizinprodukten verpflichtet, Informationen zur Verfügung zu stellen, um ihre Produkte sicher und funktionsfähig in ein Netzwerk einbinden zu können. Da in einem Krankenhausnetzwerk aber vermehrt Medizinprodukte unterschiedlicher Hersteller eingebunden werden, kann ein Hersteller eines einzelnen Medizinprodukts nicht mehr bei Problemen, welche durch andere Medizinprodukte oder durch Netzwerkkomponenten verursacht wurden, zur Verantwortung gezogen werden. Durch diese Stö-

rungen oder Überlastungen im Netzwerk können Gesundheitsmaßnahmen in einem Krankenhaus beeinträchtigt werden oder komplett ausfallen. Aus diesem Grund wurde die Norm IEC 80001-1 erarbeitet.

Die IEC 80001-1 richtet sich an Betreiber von IT-Netzwerken mit integrierten Medizinprodukten, wie es in Krankenhäusern üblich ist. Sie klärt die Verantwortlichkeiten zwischen den Parteien, welche in ein medizinisches IT-Netzwerk involviert sind. Bei den Verantwortlichkeiten wird auch auf Pflichten eingegangen, welche Medizinprodukt-Hersteller und IT-Infrastruktur-Hersteller im Zuge dieser Norm erfüllen müssen. Außerdem werden Aufgaben beschrieben, welche der Betreiber eines Medizinischen IT-Netzwerks zu erfüllen hat. Hierzu zählt z.B. die Durchführung eines Risikomanagements für das gesamte IT-Netzwerk. Durch die IEC 80001-1 soll die Kommunikation zwischen den verschiedenen Parteien eines Medizinischen IT-Netzwerks verbessert werden. Es werden Anforderungen definiert, die erfüllt werden müssen, um ein Medizinisches IT-Netzwerk sicher zu betreiben.

1.2 Ziele

Ziel dieser Arbeit ist es in Kooperation mit dem Deutschen Herzzentrum Berlin (DHZB), als Betreiber eines Medizinischen IT-Netzwerks, ein Verständnis für die Norm zu entwickeln. Zu diesem Zweck werden die ersten Schritte zur Einführung der Norm anhand eines Pilotprojektes durchgeführt. Fragestellungen während der Durchführung sind:

- Sind die Anforderungen der Norm verständlich und konkret beschrieben?
- Kann eine Motivation zur Umsetzung der Norm geschaffen werden?
- Werden während der Einführung Fragestellungen/Probleme deutlich, welche in der Norm konkreter aufgearbeitet werden sollten?
- Welche Strukturen der IEC 80001-1 sind im DHZB bereits vorhanden oder in Planung?

1.3 Vorgehensweise

Um die oben genannten Ziele zu erreichen, wird in Kapitel 2 eine Einführung in die IEC 80001-1 gegeben. Es werden die Verantwortlichkeiten der einzelnen Parteien erläutert, sowie die Aufgaben der Betreiber eines Medizinischen IT-Netzwerks, welche sich aus der Norm ergeben, beschrieben. Mit den erworbenen Kenntnissen werden in Kapitel 3 die Methoden zur Einführung der Norm in einem Krankenhaus dargelegt. Es wird beschrieben welche Dokumentationsstrukturen geschaffen werden und welche Prozesse zur Erfüllung der Norm eingeführt werden müssen. In Kapitel 4 geht es darum, die IEC 80001-1 anhand eines Pilotprojektes umzusetzen. Während der Durchführung der einzelnen Schritte in Zusammenarbeit mit dem Deutschen Herzzentrum Berlin, wird auf die auftretenden Probleme eingegangen, die sich bei der Bearbeitung ergeben haben. Die Arbeit wird im Kapitel 5 abgeschlossen durch eine Zusammenfassung der Ergebnisse und einen Ausblick wie im DHZB die Einführung und Erfüllung der IEC 80001-1 vorangetrieben wird.

2 Grundlagen der IEC 80001-1

2.1 Verantwortlichkeiten der IEC 80001-1

2.1.1 Verantwortung der Verantwortlichen Organisation

Nach IEC 80001-1 steht die Verantwortliche Organisation als Betreiber des medizinischen IT-Netzwerks in der Pflicht den sicheren Betrieb zu gewährleisten. Somit muss auch die Gesamtverantwortung des Risikomanagements für das Medizinische IT-Netzwerk bei der Verantwortlichen Organisation liegen. Der Prozess des Risikomanagements, welcher „[…] Planung, Entwicklung, Installation, Geräteverbindung, Konfiguration, Anwendung, Wartung und das Außerbetriebnehmen von Geräten“ beinhaltet, muss Eigentum der Verantwortlichen Organisation sein ([1], S. 13). Die Oberste Leitung ist, als Leiter der Verantwortlichen Organisation, dazu verpflichtet Richtlinien für das Risikomanagement bezüglich der Einbindung von Medizinprodukten zu definieren. Hierfür muss festgelegt werden, wie vertretbare Risiken, mit Berücksichtigung von Normen und Vorschriften, bestimmt werden. Außerdem muss die Oberste Leitung die notwendigen personellen und finanziellen Ressourcen zur Umsetzung bereitstellen. Sie muss gewährleisten, dass „[…] alle Beteiligten des Netzwerkes sich ihrer Verantwortung und Aufgaben bewusst sind“ ([3], S. 6). Hierzu wird eine Verantwortlichkeitsvereinbarung (Responsibility Agreement) unter den Beteiligten geschlossen (Abbildung 2).

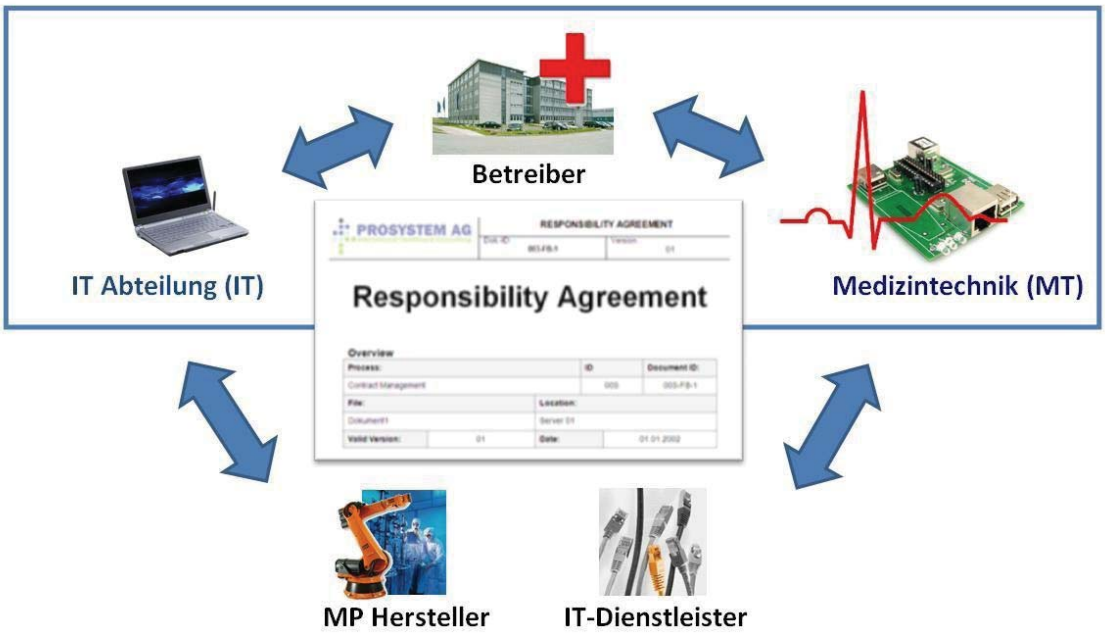


Abbildung 2: Parteien eines Medizinischen IT-Netzwerkes[1]

Durch diesen Vertag wird die Zusammenarbeit zwischen den einzelnen Parteien (Betreiber, IT-Abteilung, Medizintechnik, Medizinprodukthersteller und IT-Dienstleister) über den gesamten Lebenszyklus des Medizinischen IT-Netzwerks geregelt (Abbildung 2). „Dieser wird benötigt, wenn mehr als ein Hersteller Medizinprodukte in ein beim Betreiber bestehendes Netzwerk einbinden soll“ ([3], S.19). Den Inhalt dieser Verantwortlichkeitsvereinbarung legen die beteiligten Vertragsparteien fest. Sie beschreibt das betroffene Medizinische IT-Netzwerk und definiert die Ziele des Projekts.

Tabelle 1: Aufgaben der Vertragsparteien

Interne Partner (Medizintechnik, Informationstechnik, Haustechnik)	**Externe Partner (Medizinprodukthersteller, IT-Infrastruktur)**
Organisatorische/Technische Schutzmaßnahmen	Bereitstellung von Informationen (siehe auch 2.1.2)
Dokumentation und Überwachung	Mitteilung über Ereignisse aus anderen Netzwerken
Planung/Durchführung von Änderungen	Implementierung von technischen Schutzmaßnahmen, Festlegung von Regeln und Prüfvorschriften

Die Verantwortlichkeitsvereinbarung verpflichtet die Hersteller von Medizinprodukten und IT-Infrastruktur Informationen über Produkte oder Ereignisse aus anderen Netz-

[1] Quelle: [3], S. 18

werken zur Verfügung zu stellen (näheres in Abschnitt 2.1.2). Falls dies vertrauliche Informationen der Hersteller betrifft, kann zusätzlich eine Vertraulichkeitsvereinbarung getroffen werden. Außerdem unterstützen die externen Parteien die Implementierung von technischen Schutzmaßnahmen. Die internen Parteien Medizintechnik und Informationstechnik stehen in der Pflicht eine Liste der Medizinprodukte und anderer Geräte einschließlich Namen der Hersteller zu erstellen, welche in das IT-Netzwerk eingebunden sind. Diese Liste muss auch Inhalt der Verantwortlichkeitsvereinbarung sein. Die internen Parteien verpflichten sich außerdem organisatorische und technische Schutzmaßnahmen zu implementieren. Die Überwachung des IT-Netzwerks liegt ebenso in der Verantwortung der internen Parteien, wie die Planung und Überwachung von Änderungsmaßnahmen (Tabelle 1). Alle Parteien sind folglich Mitglieder des Risikomanagement-Teams, in unterstützender oder ausführender Form.

Rollen, Aufgaben und Verantwortlichkeiten werden somit vertraglich festgesetzt, um Pflichten und Verantwortungen bei der Bearbeitung von Projekten und Vorfällen festzulegen.

Die Oberste Leitung kann für jedes Medizinische IT-Netzwerk einen Risikomanager ernennen. Dieser Risikomanager stellt alle für das Risikomanagement relevanten Informationen zu den vernetzten Medizinprodukten zusammen und ist verantwortlich für die Einbindung dieser Medizinprodukte gemäß den jeweiligen Herstellerangaben und den Richtlinien der Verantwortlichen Organisation. Er ist verantwortlich für den gesamten Risikomanagement-Prozess. Außerdem dient er als Moderator zwischen den beteiligten internen und externen Parteien, sowie bei der Durchführung von Änderungen im Medizinischen IT-Netzwerk. Weitere Aufgaben des Risikomanagers sind die Freigabe von Dokumenten über zum Beispiel Änderungsplanungen und das Informieren der Obersten Leitung über unvertretbare Risiken und Gefährdungen durch Konfigurationsänderungen.

2.1.2 Verantwortung der Hersteller

Hersteller von Medizinprodukten sind nach IEC 80001-1 Lieferanten der Betreiber. Medizinprodukte, welche unter die IEC 60601-1:2005 fallen, werden als PEMS bezeichnet (Programmierbares Elektrisches Medizinisches System). Die Hauptverantwortung der Hersteller bezieht sich auf das Kapitel 14.13 der IEC 60601-1:2005, durch welches sie verpflichtet sind zusätzliche Informationen für die sichere Integration der Medizinprodukte in ein IT-Netzwerk bereitzustellen. In den Begleitpapieren (den sog. accompanying documents) wird unter anderem die Zweckbestimmung für das PEMS definiert, welches in ein IT-Netzwerk eingebunden wird. Hierfür sind Informationen beizufügen welche Folgen die Fehler im Netzwerk auf die Zweckbestimmung des Gerätes haben, um die Risiken abschätzen zu können. Außerdem werden die erforderlichen Charakteristiken und Konfigurationen des IT-Netzwerks zur Verwendung des Medizinproduktes erläutert. Technische- und Sicherheitsspezifikationen der erforderlichen Netzwerkverbindung müssen ebenso beschrieben werden wie der vorgesehene Informationsfluss zwischen den PEMS, dem IT-Netzwerk und anderen Einheiten des Netzwerks.

Als Folge der IEC 80001-1 stellen Betreiber weitergehende Anforderungen an die Hersteller von Medizinprodukten und IT-Komponenten. Die wichtigste Anforderung der Sicherheit für die Vernetzung, welche auch schon durch die 60601-1:2005 abgedeckt wird, bleibt natürlich bestehen und dient als Basis der weiteren Aufgaben. Hierfür müssen zum einen die Anweisungen zur Einbindung der Medizinprodukte in ein IT-Netzwerk spezifiziert werden.

Folgende Anweisungen müssen von den Medizinprodukt-Herstellern nach IEC 80001-1 spezifiziert werden:

- Zweck der Einbindung des Medizinprodukts in ein IT-Netzwerk
- Geforderte Eigenschaften/Leistungsmerkmale des IT-Netzwerks
- Geforderte Konfiguration des IT-Netzwerk
- Das beabsichtigte Routing durch das IT-Netzwerk, wenn relevant
- Benutzung der Schnittstellen der Medizinprodukte zur Einbindung in ein IT-Netzwerk
- Liste der Gefährdungssituationen, die resultieren, wenn ein IT-Netzwerk nicht die Eigenschaften bereit hält, die den Zweck der Anbindung erfüllen

(Vgl. [1], S. 16)

Hersteller für IT-Technologien (Geräte oder Software), welche keine Medizinprodukte sind, wie zum Beispiel für Infrastrukturkomponenten, sind ebenfalls dazu verpflichtet Informationen, welche in der Verantwortlichkeitsvereinbarung geklärt wurden, bereitzustellen.

Hierzu zählen unter anderem:

- Technische Beschreibungen und technische Handbücher
- Erforderliche Eigenschaften des IT-Netzwerks
- Empfohlene Produkt-Konfigurationen
- Bekannte Inkompatibilitäten und Einschränkungen
- Betriebsanforderungen
- Korrekturmaßnahmen am Produkt und Rückrufaktionen
- Hinweise zur Internetsicherheit

([1], S.17)

Um das Risikomanagement zu unterstützen, können bei Herstellern auch ergänzende Informationen eingeholt werden. Hierzu zählen zum Beispiel Prüfstrategien, Offenlegung von Ausfallmodi oder Statistiken über Systemzuverlässigkeit.

Zum Anderen müssen alle Hersteller Strategien für Virenfreiheit entwickeln. Außerdem werden die Hersteller in Projekte und Prozesse des Medizinischen IT-Netzwerks ein-

gebunden. Sie werden zum Beispiel bei Änderungen der IT- bzw. Produkt-Infrastruktur mit in die Projektplanung einbezogen. In das Risikomanagement werden die Hersteller insofern integriert, in dem sie verpflichtet werden Gefährdungskategorien und Fehlerzustände der Produkte zur Verfügung zu stellen. Hierzu zählen auch technische Informationen für eine Risikoanalyse des IT-Netzwerks.

Insgesamt soll eine kontinuierliche Gesprächsbereitschaft zwischen den Betreibern und den Herstellern aufgebaut werden, um die Weitergabe von Information oder die Unterstützung bei Updates/Patches zu gewährleisten. Wenn die bereitgestellten Informationen der Hersteller für die Durchführung des Risikomanagements nicht ausreichen, können zusätzliche Informationen unter Berufung auf die Verantwortlichkeitsvereinbarung eingeholt werden.

2.2 Pflichten der IEC 80001-1 an die Betreiber

2.2.1 Grundlage

Die IEC 80001-1 stellt verschiedene neue Anforderungen und Aufgaben an die Betreiber eines medizinischen IT-Netzwerks. Die Anforderungen beziehen sich auf die Bereiche Dokumentation und Planung, Risikomanagement, Implementierung und Überwachung.

2.2.2 Dokumentation und Planung

Die IEC 80001-1 fordert ein umfassendes Dokumentationssystem anhand einer Risikomanagement-Akte. Diese könnte, die in Abbildung 3 aufgelisteten Erläuterungen, Dokumente und Prozessbeschreibungen enthalten.

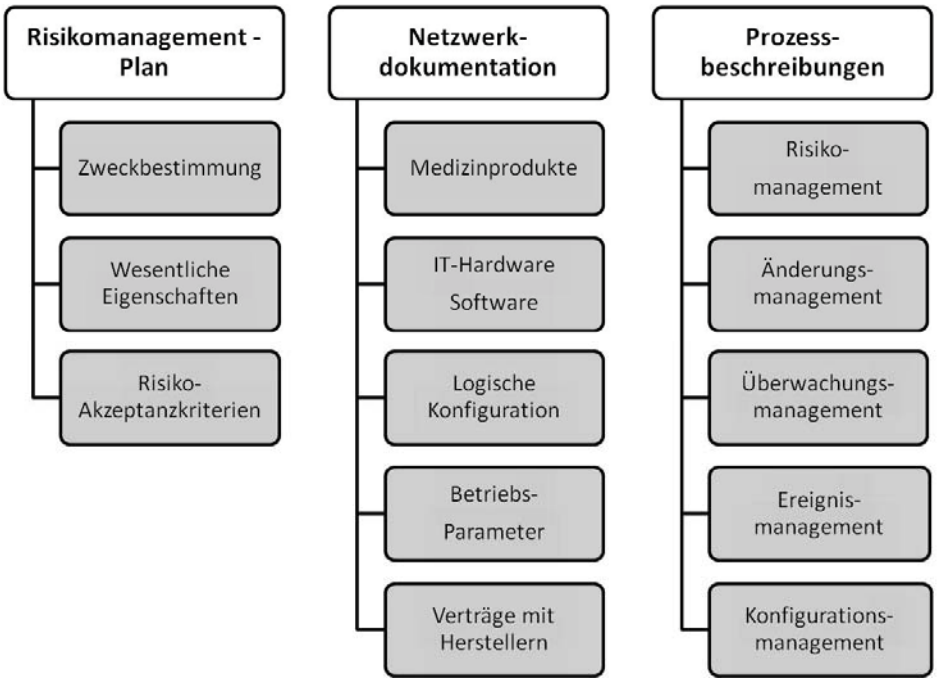


Abbildung 3: Auszug aus der Risikomanagement-Akte[2]

Der Risikomanagement-Plan beinhaltet eine detaillierte Zweckbestimmung des medizinischen IT-Netzwerks, in welcher der Gebrauch und der erwartete Nutzen des Netzwerks definiert werden. Im Risikomanagement-Plan werden alle Elemente (u.a. Hardware, Software und Daten) aufgeführt die für „[…] die Zweckbestimmung des Medizinprodukts und die vorgesehene Verwendung des Medizinischen IT-Netzwerks wichtig sind“ ([1], S.21). Diese speziellen Elemente können zu Gefährdungen und Risiken beitragen und müssen deshalb in den Risikomanagement-Prozess einbezogen werden. Elemente, welche hier aufgelistet und beschrieben werden müssen, sind die integrierten Medizinprodukte inklusive medizinischer Anwendungssoftware, sowie die Komponenten des Netzwerks, welche den Betrieb des Medizinischen IT-Netzwerks gewährleisten. Die Aufgabe der Geräte und Software muss hier auf Basis der Zweckbestimmung beschrieben werden. Betriebsmerkmale wie Bandbreiten oder Latenzen der IT-Infrastruktur sind hier ebenfalls zu dokumentieren, wie Daten über die Konfiguration von Hardware und Software. Weitere Elemente, welche für das Risikomanagement relevant sind, sind die Patientendaten, welche im Netzwerk verwendet werden. Mit den Patientendaten geht einher Informationen zu den medizinischen Behandlungsverfahren, inklusive der Anwender, aufzuführen, da dies auch Teil der Zweckbestimmung der Medizinprodukte und des Medizinischen IT-Netzwerks ist. Aufgaben und Verantwortlichkeiten von allen beteiligten Parteien des Medizinischen IT-Netzwerks werden außerdem im Risikomanagement-Plan aufgelistet. Eine grafische Darstellung der Zweckbestimmung ist in Abbildung 4 anhand eines Teilnetzes zu sehen.

[2] Quelle: [2], S. 6

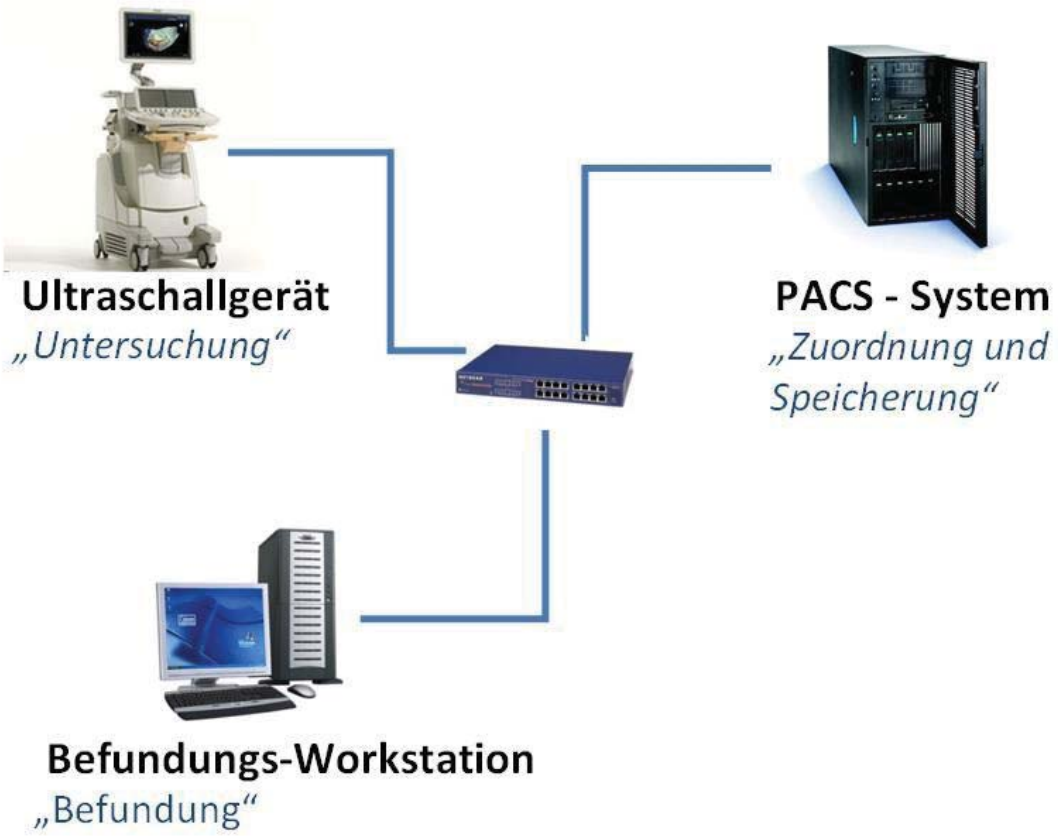


Abbildung 4: beispielhafte Zweckbestimmung eines Teils des Med. IT-Netzwerkes[3]

Ein weiterer Inhalt des Risikomanagement-Plans ist es Kriterien für die Vertretbarkeit von Risiken festzulegen. Hierzu werden Schutzziele (sog. key properties) für jedes medizinische IT-Netzwerk definiert. In der IEC 80001-1 werden drei unterschiedliche Arten von Schutzzielen festgelegt:

- Sicherheit
    - Für Patienten, Anwender und Dritte
- Effektivität/Wirksamkeit
    - Einer Gesundheitsmaßnahme, eines Workflows
- Daten- und Systemsicherheit
    - Schutz vor dem Verlust der Vertraulichkeit, der Vollständigkeit und der Verfügbarkeit der Daten und Systeme

([2], S. 10)

Die Schutzziele müssen nach Prioritäten gegliedert werden, wobei auch darauf geachtet werden muss, dass sich Schutzziele gegenseitig beeinflussen können.

[3] Quelle: [2], S. 9

Auf Basis dieser Schutzziele werden Akzeptanzkriterien des Betreibers entsprechend der Risikopolitik der Obersten Leitung festgelegt. Hier ist zu beachten, dass Akzeptanzkriterien von der Zweckbestimmung eines Medizinprodukts abhängig sind. Außerdem können auch Risiken mit unklarer Auftretenswahrscheinlichkeit existieren.

Weiterhin wird in der Risikomanagement-Akte eine Netzwerk-Dokumentation erstellt. Diese beinhaltet die physikalische und logische Netzwerkstruktur einschließlich einer Definition der Netzwerk-Grenzen. Zur Netzwerkstruktur müssen auch elektrische Eigenschaften gehören, welche das Netzwerk und die eingebundenen Geräte beeinflussen können, wie Erdung, galvanische Trennung oder Fehlerströme. Angewandte Normen und Konformitätserklärungen werden hier dokumentiert, sowie die physikalische und logische Client/Server-Struktur. Beschreibungen zur Netzwerksicherheit müssen ebenso verfasst werden wie der Informations- und Datenfluss des Netzwerks (Abbildung 5).

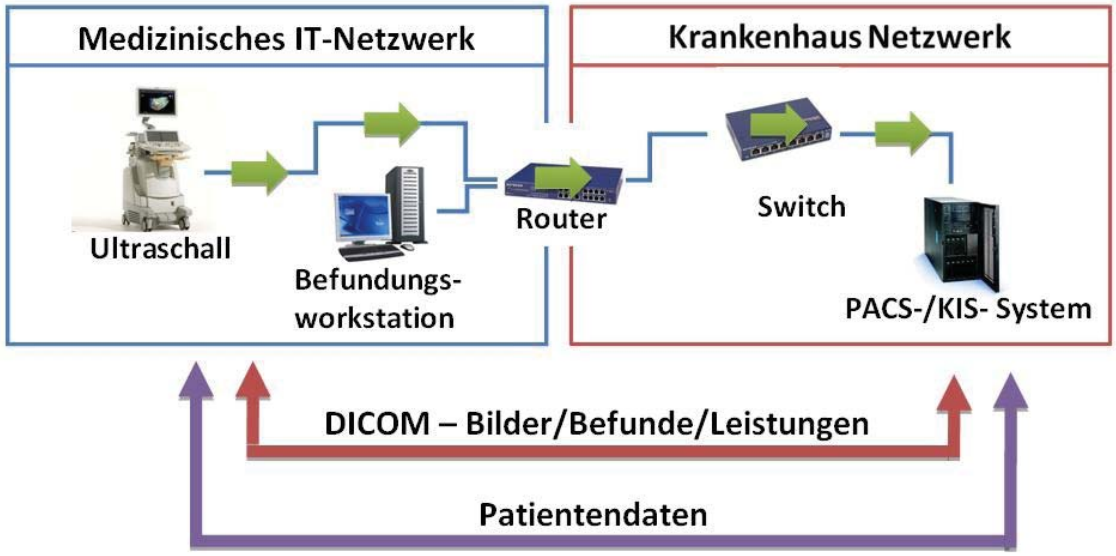


Abbildung 5: Informations- und Datenfluss[4]

Außerdem werden in der Akte die Anforderungen der Medizinprodukte an das Netzwerk erfasst, um Konfigurationen der Medizinprodukte, die benötigten Bandbreiten oder andere Voraussetzungen in die Planung mit einbeziehen zu können. Verträge für zum Beispiel Wartung und Serviceintervalle werden ebenso dokumentiert wie Softwarelizenzen und Ansprechpartner der Medizinprodukte.

Ebenfalls werden in der Risikomanagement-Akte alle, durch die IEC 80001-1, erforderlichen Prozesse dokumentiert, welche in den Kapiteln 2.2.3 ff. und ergänzend in Kapitel 3.5.4 beschrieben sind.

[4] Vgl. Quelle: [2], S. 13

2.2.3 Risikomanagement

Die Durchführung eines Risikomanagements und die damit verbundene Risikoanalyse ist der zentrale Punkt der IEC 80001-1. Eine Risikoanalyse muss bei Inbetriebnahme eines Medizinischen IT-Netzwerks und bei Änderungen am Netzwerk und/oder Komponenten durchgeführt werden. Ziel dieses Prozesses ist es, Gefährdungen zu identifizieren, deren Risiken zu bewerten und folglich zu beherrschen. Dieser Prozess findet immer unter Berücksichtigung der Zweckbestimmung des Netzwerkes und statt.

Zu erst müssen Gefährdungen erkannt werden. Gefährdungen sind Kategorien, welche einen oder mehrere der drei Schutzziele schädigen können. Wurde die Gefährdung identifiziert, analysiert man die Ursachen dieser Gefährdung und klärt ob Gefährdungssituationen aus dieser Gefährdung entstehen können. Gefährdungssituationen sind Umstände, in welchen Personen oder Infrastrukturen den Gefährdungen ausgesetzt sind. Ein vereister Bürgersteig wäre zum Beispiel eine Gefährdung. Eine Gefährdungssituation würde daraus entstehen, wenn eine Person diesen Bürgersteig benutzt. Nachdem die Gefährdungssituationen bekannt sind, können die möglichen Schäden im Bezug auf die Schutzziele beschrieben werden. Dies wären Schäden die den Patienten betreffen, den klinischen Workflow beeinträchtigen oder Schäden welche sich auf die Daten- und Systemsicherheit auswirken können. Nachdem die Risikoanalyse abgeschlossen ist, schließt sich die Risikobewertung an. Abhängig von der Risikoanalyse werden vorhandene Maßnahmen, welche das Risiko einer Gefährdung bzw. Gefährdungssituation abschwächen in die Bewertung aufgenommen. Anschließend wird die Auftretenswahrscheinlichkeit der Gefährdungssituation ermittelt.

Tabelle 2: Auftretenswahrscheinlichkeit einer Gefährdungssituation[5]

QUALITATIVER ANSATZ	QUANTITATIVER ANSATZ (1 Auftreten : n Anwendungen)	Klasse
unwahrscheinlich	< 1:1.000.000	W-1
fernliegend	< 1:100.000	W-2
gelegentlich	< 1:10.000	W-3
wahrscheinlich	< 1:1.000	W-4
häufig	< 1:100	W-5

Zur Bestimmung der Auftretenswahrscheinlichkeit werden die Wahrscheinlichkeiten in Klassen von W-1 bis W-5 eingeteilt. Diese Abstufung ist exemplarisch und kann je nach Risikopolitik der Verantwortlichen Organisation angepasst werden. Als unwahrscheinlich ist eine Gefährdung anzunehmen, wenn sie einmal alle 1.000.000 Anwen-

[5] Quelle: [2], S. 16

dungen auftritt (Klasse W-1). Häufige Gefährdungen treten einmal alle 100 Anwendungen auf und werden als W-5 klassifiziert (Tabelle 2)

Nach Bestimmung der Auftretenswahrscheinlichkeit geht es darum den Schweregrad eines Schadens zu ermitteln. Der Schweregrad wird für jedes in der IEC 80001-1 definierte Schutzziel (Sicherheit, Wirksamkeit/Effektivität und Daten-/Systemsicherheit) erfasst.

Tabelle 3: Schweregrad für das Schutzziel Sicherheit[6]

Klasse		**Grad des Einflusses auf Funktion und/oder Erscheinung**
		Einfluss auf den Patient, Anwender oder Dritte:
S_s -1	unerheblich	keine Verletzung, Unannehmlichkeit
S_s -2	geringfügig	leichte Verletzung, keine Behandlung nötig
S_s -3	ernst	Verletzung, medizinische Behandlung nötig
S_s -4	kritisch	lebensbedrohliche Verletzung, bleibende Schäden
S_s -5	katastrophal	schwerste Verletzung oder Tod

Die Klassifizierung des „Schweregrads“ Sicherheit reicht von S_s -1 unerheblicher Schaden bis S_s -5 katastrophaler Schaden. Bei einem unerheblichen Schaden treten keine Verletzungen oder nur Unannehmlichkeiten auf. Treten schwerste Verletzungen oder Tod auf ist dieses ein Schaden des Schweregrades katastrophal bzw. S_s -5 (Tabelle 3).

Der Schweregrad für das Schutzziel „Wirksamkeit/Effektivität“ wird gegliedert in $S_{W/E}$ -1 bis $S_{W/E}$ -5. Wobei $S_{W/E}$ -1 keinen Einfluss oder nur Unannehmlichkeiten auf den medizinischen Workflow bedeutet. Bei einem Schaden des Schweregrades $S_{W/E}$ -5 sind Gesundheitsmaßnahmen bzw. die Durchführung medizinischen Workflows nicht mehr möglich (Tabelle 4).

Tabelle 4: Schweregrad für das Schutzziel Wirksamkeit/Effektivität[7]

Klasse		**Grad des Einflusses auf die Wirksamkeit / Effektivität**
		Einfluss auf Gesundheitsmaßnahmen / med. Workflow:
$S_{W/E}$ -1	unerheblich	keine Verletzung, Unannehmlichkeit
$S_{W/E}$ -2	geringfügig	leichte Störung oder Belastung
$S_{W/E}$ -3	ernst	Störung, kurze Unterbrechung
$S_{W/E}$ -4	kritisch	Unterbrechung, Verzögerung
$S_{W/E}$ -5	katastrophal	Abbruch, nicht länger möglich

[6] Quelle: [2], S. 17
[7] Quelle: [2]. S. 18

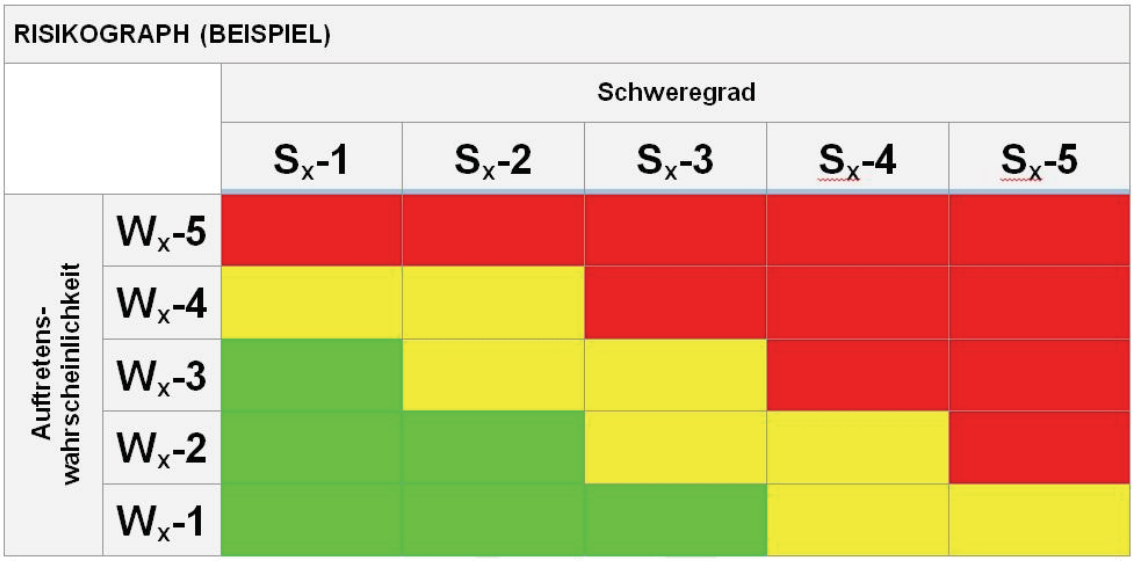
Schäden, die dem Bereich Daten- und Systemsicherheit zuzuordnen sind, werden nach den Einflüssen auf die Verfügbarkeit/Vertraulichkeit und Integrität gegliedert. Ein Schaden nach $S_{D/S}$ -1 hat keinen Einfluss auf Daten oder Systeme, wohingegen ein $S_{D/S}$ -5- Schaden zu längeren Ausfällen von System/Anwendungen führt und einen schweren Verlust an Vertraulichkeit von Daten zur Folge hat (Tabelle 5)

Tabelle 5: Schweregrad für das Schutzziel Daten- und Systemsicherheit[8]

Klasse		**Grad des Einflusses auf die Daten- und Systemsicherheit**
		Einfluss auf Verfügbarkeit/Vertraulichkeit/Integrität
$S_{D/S}$ -1	unerheblich	kein oder kaum Einfluss auf Daten und Systeme
$S_{D/S}$ -2	geringfügig	geringfügiger Einfluss auf das System; minimaler Aufwand zur Wiederherstellung
$S_{D/S}$ -3	ernst	Einfluss auf die Verfügbarkeit, Vertraulichkeit und Integrität von Daten; Erhöhter Aufwand zur Wiederherstellung
$S_{D/S}$ -4	kritisch	Führt zu Ausfällen von Systemen und Anwendungen; Verlust der Vertraulichkeit von Daten; Hoher Aufwand zur Wiederherstellung
$S_{D/S}$ -5	katastrophal	Führt zu längerem Ausfall von Systemen/Anwendungen; Schwerer Verlust an Vertraulichkeit von Daten

Nach Bestimmung der Auftretenswahrscheinlichkeit und des Schweregrades von bestimmten Fehlerzuständen, kann das Risiko durch einen Risikographen bewertet werden. Anhand dieses Risikographen kann durch Eintragung des Schweregrades und der Auftretenswahrscheinlichkeit entschieden werden, ob das Risiko einer Gefährdungssituation akzeptabel ist oder ob Maßnahmen zur Minimierung eingeleitet werden müssen (Abbildung 6).

[8] Quelle: [2], S. 19



Risiko	Beschreibung	Konsequenz
Hoch	nicht akzeptabeler Bereich	weitere Maßnahmen notwendig
Mittel	Bedingt akzeptabel Bereich	Wenn (ökonomisch und technisch) weitere Maßnahmen praktikabel sind, müssen diese umgesetzt werden.
Niedrig	Akzeptabler Bereich	keine weiteren Maßnahmen notwendig

Abbildung 6: Risikograph[9]

Wenn aus der Risikobewertung hervorgeht, dass zusätzliche Schutzmaßnahmen erforderlich sind, tritt der Prozess der Risikobeherrschung in Kraft. In der Risikobeherrschung werden Maßnahmen identifiziert, um die Risiken zu minimieren. Das Design des IT-Netzwerks wird hier einer Analyse unterzogen, um zum Beispiel zu klären, ob das Risiko durch eine physikalische Trennung des Netzwerks vermindert werden kann. Außerdem wird nach Schutzmaßnahmen, wie zum Beispiel Alarm-Funktionen, gesucht. Um Risiken zu minimieren, könnten auch zusätzliche Sicherheitsinformationen, wie zum Beispiel Warnhinweise, Arbeitsanweisungen oder Trainings Abhilfe schaffen. In der Risikobeherrschung wird auch über Änderungen an Netzwerkkomponenten oder Änderungen der Netzwerkkonfiguration nachgedacht. Änderungen an den eingebunden Medizinprodukten können auch zu einer Risikominimierung beitragen, hier ist aber zu beachten, dass man entweder vom Hersteller autorisiert ist, Änderungen an einem Medizinprodukt durchzuführen oder ob der Hersteller die Änderungen übernimmt.

Nach Verifizierung und Implementierung der Risikominimierungsmaßnahmen muss eine erneute Bewertung des Risikos durchgeführt werden, um zu überprüfen, ob das Restrisiko vertretbar geworden ist. Wenn die Verantwortliche Organisation feststellt, dass weitere Minimierungsmaßnahmen nicht praktikabel sind, muss eine Risiko/Nutzen-Analyse des Restrisikos durchgeführt und dokumentiert werden.

[9] Quelle: [2], S. 20

Die in Anhang C dargestellte Tabelle gibt einen Überblick, wie mit dem Risikomanagement-Prozess verfahren werden kann.

2.2.4 Implementierung

Wenn nach Durchführung eines Risikomanagements Risikominimierungsmaßnahmen eingeleitet werden müssen, tritt das Änderungsmanagement in Kraft. Dieses stellt sicher, „[…] dass alle Änderungen in einer kontrollierten Weise bewertet, implementiert und überprüft werden“ ([2], S. 24). Vor Durchführung einer Änderung bedarf es gründlicher Planung anhand eines Projektplans. In diesem Plan wird eine Projektbeschreibung erstellt, um beteiligte oder erforderliche Komponenten, durchzuführende Arbeitsschritte und erwartete Ergebnisse zu dokumentieren. Hier werden auch Rahmenbedingungen wie beteiligte Parteien und Zeitpunkte festgelegt. Der Projektplan soll außerdem Auskunft über die vorher/nachher Situationen von Konfigurationen und Informationsflüssen sowie eine eventuelle Erweiterbarkeit des Netzwerks geben.

Nach Erstellung des Projektplans muss die Änderung durch das Risikomanagement freigegeben bzw. genehmigt werden. Diese Änderungsgenehmigung (change permit) enthält die Voraussetzungen, Einschränkungen und Dokumentationen, welche die Änderung betreffen. Der Risikomanager steht nun in der Pflicht die Planung der Änderung und die des Risikomanagements auf ihre Vollständigkeit zu überprüfen. Ist die Planung vollständig und das Gesamt-Restrisiko der Änderung akzeptabel wird die Änderung durch den Risikomanager freigegeben und kann umgesetzt werden.

2.2.5 Überwachung

Das Medizinische IT-Netzwerk bedarf einer ständigen Überwachung, um das ursprüngliche Risikoniveau, welches durch das Risikomanagement festgelegt wurde, zu erhalten. Wenn Vorkommnisse, wie Abweichungen von Sollwerten (z.B. Netzwerkauslastung), Änderungen der Umgebung/Netzwerk, Rückmeldungen von Anwendern oder Information über mögliche Risiken von Herstellen veröffentlicht werden, auftreten, tritt das Ereignismanagement in Kraft. In diesem werden die Vorkommnisse dokumentiert und bewertet, um gegebenenfalls ein Änderungsmanagement einzuleiten.

3 Methoden zur Einführung der IEC 80001-1

3.1 Vorbereitung

Als Vorbereitung zur Einführung der IEC 80001-1 müssen Richtlinien anhand einer Risiko-Politik von der Obersten Leitung eines Krankenhauses eingeführt werden. Inhalt der Risiko-Politik ist der in Kapitel 2.2.2 eingeführte Risikomanagement-Plan, in welchem Aufgabe und Zweck des Netzwerks, die Schutzziele und Risikoakzeptanzkriterien definiert werden.

3.2 Ressourcenplanung

Erster Schritt der Ressourcenplanung ist einen Risiko-Manager durch die Oberste Leitung ernennen zu lassen, welcher als Moderator und Projektleiter des Risikomanagements fungiert. Um als nächsten Schritt die Verantwortlichkeitsvereinbarung abschließen zu können, müssen die potenziellen Partner des Medizinischen IT-Netzwerks bestimmt werden (Abbildung 7).

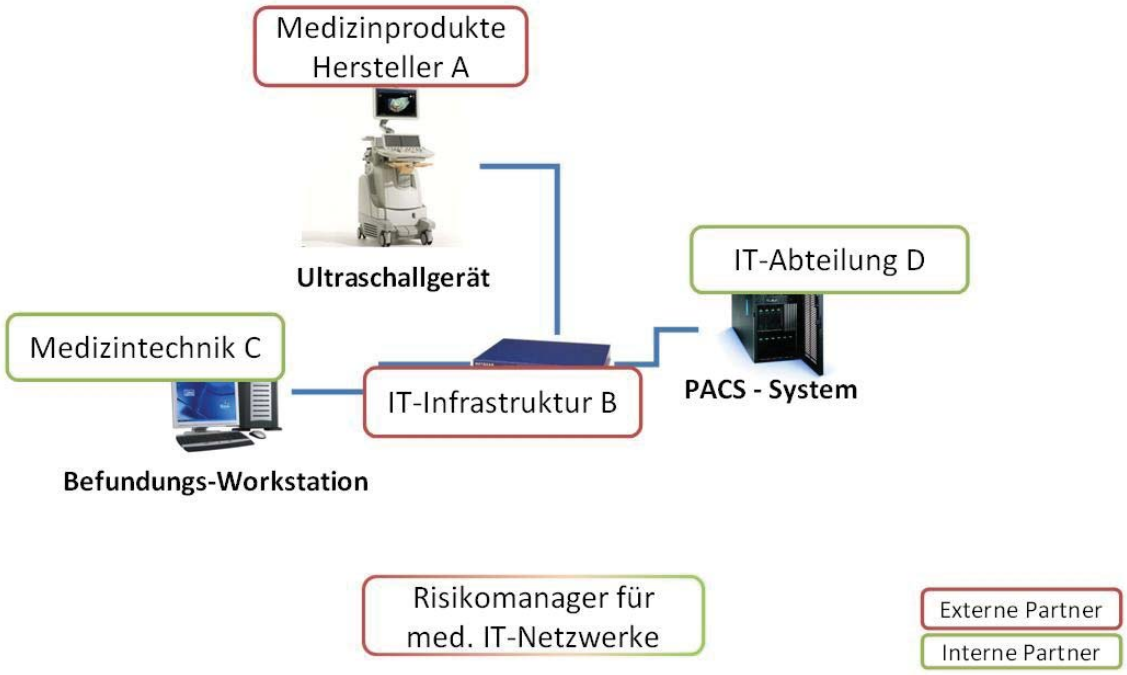


Abbildung 7: Parteien eines Medizinischen IT-Netzwerks[10]

[10] Quelle: [4], S. 11

Hiermit werden das gemeinsame Vorgehen und die Gleichberechtigung aller Parteien vertraglich abgesichert. Ferner wird durch die Verantwortlichkeitsvereinbarung ein Überblick über die zu erwartenden Aufgaben und Kosten gewährleistet. Während der Ressourcenplanung wird außerdem die Netzwerkdokumentation mit graphischen Darstellungen aller Komponenten, sowie organisatorischen und lokalen Randbedingungen entworfen.

3.3 Risikomanagement

Der Prozess des Risikomanagements wird für jedes der drei Schutzziele (Sicherheit Tabelle 3, Wirksamkeit/Effektivität Tabelle 4 und System- und Datensicherheit Tabelle 5) gesondert durchgeführt. Zu Anfang muss abhängig von den Schutzzielen eine Liste der potenziellen Gefährdungen erstellt werden.

Bei der Risikoanalyse des Schutzziels Sicherheit werden zum Beispiel Gefährdungssituationen analysiert, welche ein Medizinprodukt betreffen. Fehlerhafte Daten einer Untersuchung würden zum Beispiel im PACS (Picture Archiving and Communication System) des Krankenhauses abgespeichert und stünden für eine fehlerhafte Befundung zur Verfügung. Solche Situationen können mitunter lebensbedrohlich für den Patienten werden.

Zur Analyse der Wirksamkeit/Effektivität werden Störungen, welche den klinischen Workflow beeinträchtigen, betrachtet. Eine fehlerhafte Übertragung durch defekte Hardware oder eine Überlastung des Netzwerks können Gefährdungssituationen dieses Schutzziels sein und hätten speziell bei zeitkritischen Untersuchungen Risiken für den Patienten zur Folge.

In der Daten- und Systemsicherheit geht es speziell darum Gefährdungssituationen, welche die Verfügbarkeit, Vertraulichkeit und Vollständigkeit von Daten und Systemen beeinträchtigen, zu identifizieren. Betreffende Daten wären zum Beispiel Patientendaten im Krankenhausinformationssystem (KIS) oder DICOM-Bilder im PACS. Systeme, welche geprüft werden müssen, sind zum Beispiel Ultraschallgeräte, Server oder Datenbanken. Außerdem stehen Dienste wie Worklist-Management oder Storage/Query im PACS unter Beobachtung. Gefährdungen, welche Schäden verursachen können, sind defekte Hardware, Stromausfälle oder Hacker.

Durch die Identifikation von Gefährdungssituationen kann nun der Schaden/Schweregrad bestimmt werden. Aus einer Analyse, welche Ursachen die Gefährdungen haben, kann mit Hilfe von vorhandenen Maßnahmen die Auftretenswahrscheinlichkeit und somit das Risiko bestimmt werden. Aus dem Risiko wird in Abhängigkeit der definierten Akzeptanzkriterien deutlich, ob Minimierungsmaßnahmen/Änderungen notwendig sind.

3.4 Dokumentation und Abschluss

Formblätter, welche für das Risikomanagement benötigt werden sind der Risikomanagement-Plan, die Risikobewertung und Kontrolle, sowie der Risikomanagement-Report. Diese werden benötigt, um alle erkannten Risiken und implementierten Schutzmaßnahmen zu dokumentieren.

Eine Risikoanalyse wird mit dem Risikomanagement-Report zusammengefasst und abgeschlossen. Hier werden alle implementierten Schutzmaßnahmen erläutert und eventuell vorhandene Restrisiken begründet und legitimiert. Anhand des Risikomanagement-Reports wird die Analyse durch den Risikomanager oder der Obersten Leitung freigegeben.

3.5 Weiterführende Aufgaben

Die nachfolgenden Anforderungen an den Betreiber eines Medizinischen IT-Netzwerkes werden hier nur theoretisch behandelt und nicht anhand des Pilotprojekts umgesetzt.

3.5.1 Gliederung des IT-Netzwerks

Eine weiterführende Aufgabe besteht darin das IT-Netzwerk zu gliedern, in dem das gesamte Netzwerk in Teilnetze aufgeteilt wird. Teilnetze können nach Abteilungen, Funktionsbereichen, Technischen- oder Organisatorischen Strukturen gegliedert werden.

3.5.2 Erstellung einer Netzwerk-Dokumentation

In Kapitel 3.2 war von dem Entwurf der Netzwerk-Dokumentation die Rede. Diese wird nun in einem weiteren Schritt für das komplette Medizinische IT-Netzwerk erstellt. In der Netzwerk-Dokumentation besitzt die Zweckbestimmung des Medizinischen IT-Netzwerks oberste Priorität. Daraufhin wird die Dokumentation zum Einen in technische Dokumentationen untergliedert, in welcher die technischen Anforderungen und die Netzwerktopologie, wie in Kapitel 2.2.2, beschrieben werden. Zum Anderen werden die organisatorischen Anforderungen protokolliert. Inhalt dieser Anforderungen sind die medizinischen Workflows, sowie Wartung und Service des IT-Netzwerks inklusive der eingebundenen Komponenten (Abbildung 8). Diese Dokumentationen müssen einer regelmäßigen Prüfung unterzogen werden.

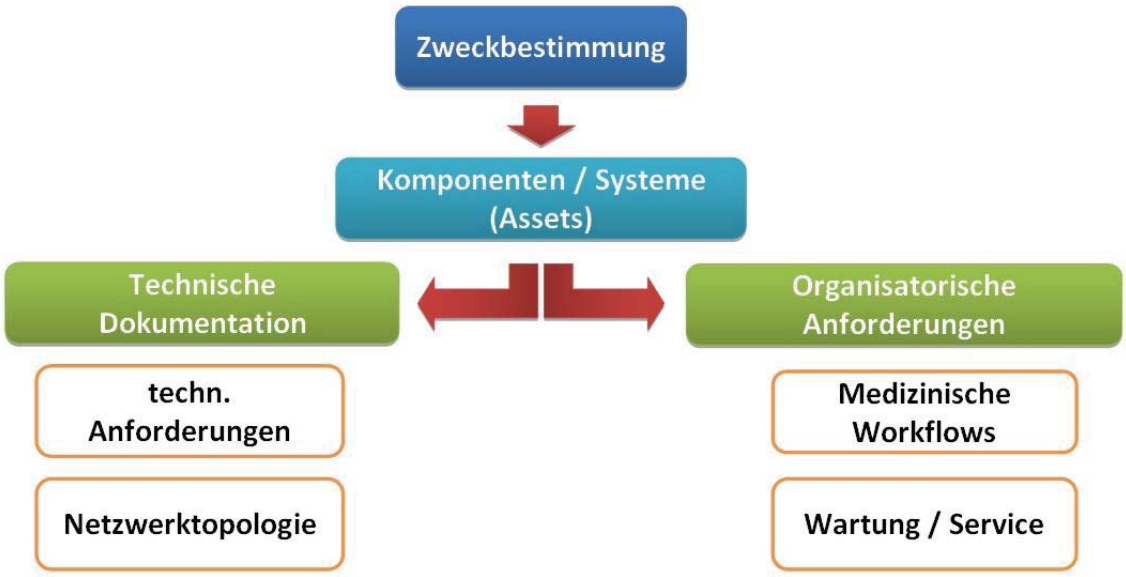


Abbildung 8: Erstellung einer Netzwerkdokumentation [11][12]

3.5.3 Erstellung eines Referenzmodells

Um den Soll-Zustand des Medizinischen IT-Netzwerks nach IEC 80001-1 zu definieren wird, nach Umsetzung an einem Pilot-Projekt, ein Referenzmodell erstellt. In diesem Referenzmodell werden zu Anfang die Kernprozesse der IEC 80001-1 als Prozessbeschreibung (PB; in Abbildung 9 VA für Verfahrensanweisung) definiert und beschrieben (näheres in Kapitel 3.5.4). Sind die Prozessbeschreibungen erstellt, werden zu den Kernprozessen Arbeitsanweisungen (AA) zum Beispiel über Projektplanungen beschrieben. Formblätter (FB) unterstützen die jeweiligen Prozesse und erleichtern die Umsetzung. Zur Dokumentation und Protokollierung der Konfigurationen kann auch eine Datenbank (DB) zur Unterstützung eingesetzt werden (Abbildung 9)

[11] Asset's = schützenswertes Gut
[12] Quelle: [4], S. 17

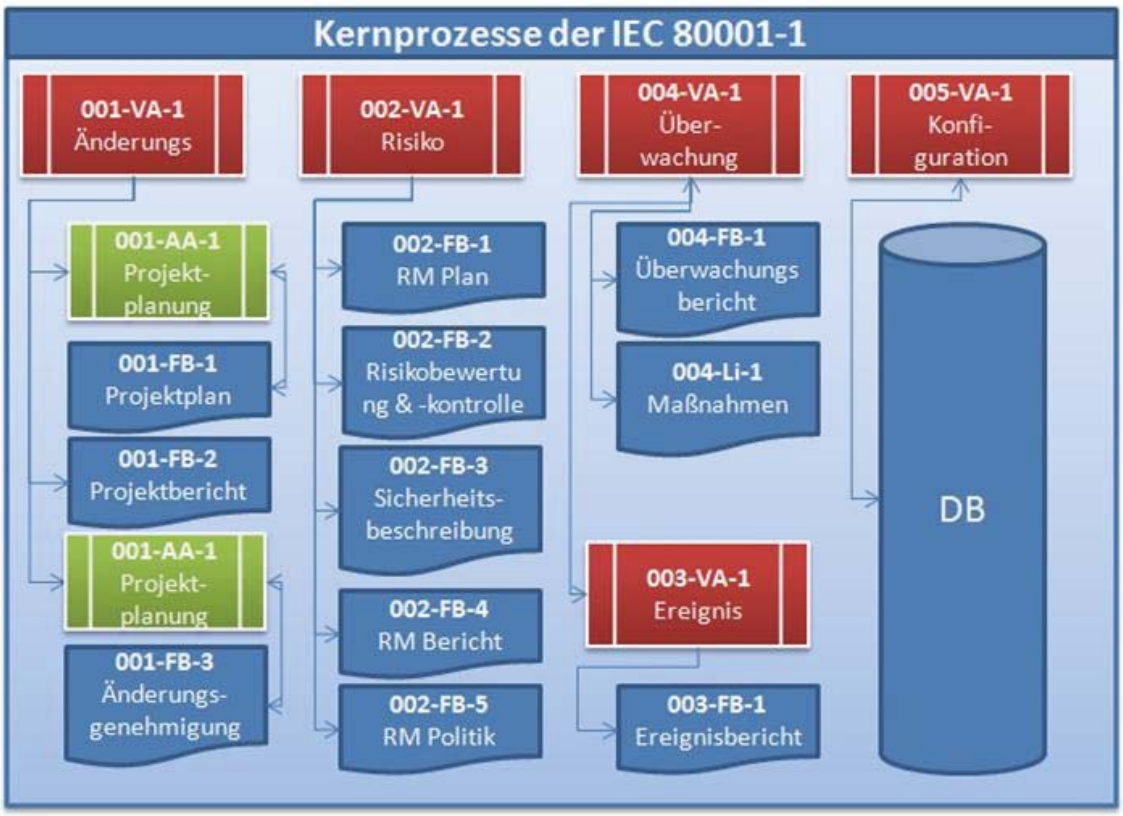


Abbildung 9: Definition des Soll-Zustands[13]

Um die Prozessbeschreibungen, Arbeitsanweisungen und Formblätter erstellen zu können, sollten folgende Kriterien berücksichtigt werden:

- Tätigkeiten
- Abläufe
- Funktionen
- Zuständigkeiten
- Befugnisse
- Dokumente
- Informationen
- Aufzeichnungen

3.5.4 Einführung von Prozessen und Prozessbeschreibungen

In den Prozessbeschreibungen werden Ziel und Zweckbestimmung der einzelnen Prozesse erläutert. Es wird auf den Geltungsbereich (Abteilungen, Netzwerke, etc.) sowie auf Zuständigkeiten und Aufgaben eingegangen. Bei Einführung der Prozesse ist auf eine sinnvolle Reihenfolge zu achten. Eine mögliche Reihenfolge wäre nach [4] S. 28 folgende:

[13] Quelle: [4], S. 26

3.5.4.1 Konfigurationsmanagement

Durch das Konfigurationsmanagement wird ein einheitliches Modell des Medizinischen IT-Netzwerkes bereitgestellt. In diesem Prozess werden die Konfigurationsinformationen der Komponenten und des IT-Netzwerks gesammelt. Hier werden alle relevanten Informationen der IT-Dokumentation abgelegt, um andere Prozesse mit den vorhandenen Informationen zu unterstützen. Bei der Umsetzung ist darauf zu achten, die Daten immer auf dem neuesten Stand zu halten. Hierbei unterstützen Programme wie MS Excel oder MS Visio bis hin zu Konfigurations-Datenbanken das Management.

3.5.4.2 Risikomanagement

In der Prozessbeschreibung des Risikomanagements geht es darum die Verfahren zur Risikoanalyse, Risikobewertung und Risikobeherrschung detailliert zu beschreiben und zu dokumentieren. Hier kann nach den folgenden Schritten vorgegangen werden ([5] S. 17f):

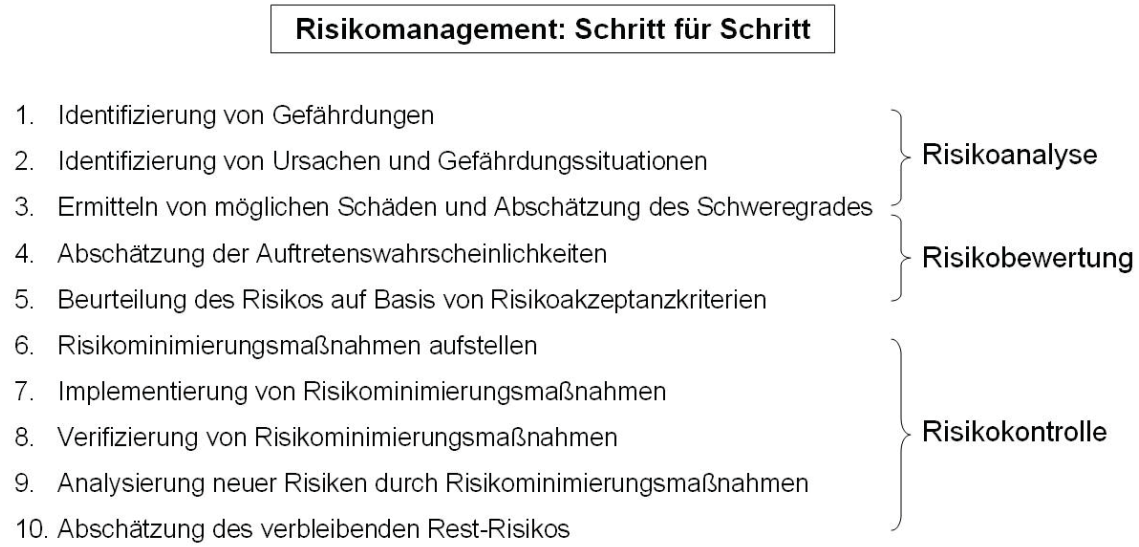


Abbildung 10: Schritte des Risikomanagements

Um das Risiko-Niveau im Netzwerk zu bestimmen sind einheitliche und vergleichbare Analysen von großer Bedeutung. Checklisten, welche vom Betreiber entworfen werden können, sorgen für eine Basissicherheit. Außerdem sollte eine Politik eingeführt werden, wie mit vorhandenen Restrisiken umzugehen sind.

3.5.4.3 Überwachungsmanagement

Im Überwachungsmanagement werden Informationen über den Zustand des Medizinischen IT-Netzwerks erfasst, um Ausfallzeiten zu verringern und die Administratoren zu entlasten. Auf Basis dieses Prozesses können spezielle Überwachungsmaßnahmen entwickelt werden, um bestimmte Risiken zu minimieren. Im Überwachungsmanagement ist darauf zu achten, dass auch Information von externen Parteien, z.B. Medizin-

produktherstellern, überwacht werden müssen. Maßnahmen zur Automatisierung dieser Überwachungen wie z.B. Tools zur Analyse von Logfiles vereinfachen diesen Prozess. Eine Auswertung dieser Logfiles führt zu verwertbaren Statistiken, um Auftretenswahrscheinlichkeiten für die Risikobewertung zu spezifizieren.

3.5.4.4 Ereignismanagement

Aufgabe dieses Prozesses ist es Ereignisse/Vorfälle zu analysieren, zu klassifizieren und zu dokumentieren. In diesem Prozess müssen die Verantwortlichkeiten klar definiert sein und es sollte einen zentralen Ansprechpartner geben. Dies ist besonders dann wichtig, wenn Ereignisse erfasst und analysiert werden, welche externe Parteien betreffen. Wird die Anzahl an Ereignissen zu groß kann auch auf „Trouble-Ticket-Tools“ zurückgegriffen werden. Sind Ereignisse oder Vorfälle erfasst, ist es auch Teil des Ereignismanagements die Maßnahmen, welche eingeleitet wurden, zu beschreiben.

3.5.4.5 Änderungsmanagement

In diesem Prozess und ihrer Beschreibung geht es darum ein „einheitliches Vorgehen bei der Planung und Durchführung von Änderungen“ zu entwickeln ([4], S. 33). Durch diese genaue Planung können Ausfallzeiten minimiert werden, welche durch Änderungsmaßnahmen entstehen. Es ist bei der Planung zu beachten, dass manche Änderungen mit Testläufen überprüft werden müssen, bevor sie in Betrieb gehen. Auch in diesem Prozess ist auf eine genau Beschreibung und Dokumentation der Projektplanung und der Änderungsmaßnahmen zu achten, um eine gewisse Nachverfolgbarkeit zu gewährleisten. Wie in Kapitel 2.2.4 erwähnt, muss vor Umsetzung einer Änderung eine Änderungsgenehmigung beim Risikomanager bzw. der Obersten Leitung eingeholt werden.

4 Praktische Umsetzung der IEC 80001-1 anhand eines Pilotprojekts

4.1 Hintergrund

Als Pilotprojekt zur Umsetzung der IEC 80001-1 dient ein Auftrag zur Ersatzbeschaffung von Sonographiegeräten für das Deutsche Herzzentrum Berlin. Dieser Auftrag wird von der Firma mediplan Krankenhausplanungsgesellschaft mbH ausgeführt. Um neue Sonographiegeräte für die Bereiche Herz-Thorax-Gefäß-Chirurgie, Anästhesiologie, Kardiologie und Kinder-Kardiologie zu beschaffen, wurde ein Leistungsverzeichnis angefertigt, in dem die Ultraschallgeräte, deren Sonden und Quantifizierungssoftware europaweit ausgeschrieben wurden. Diese Ausschreibung dient als Pilotprojekt dieser Arbeit, da die neubeschafften Ultraschallgeräte an das hauseigene PACS angeschlossen werden, um über Clients die vorgenommenen Untersuchungen zu befunden und nachzubearbeiten. Somit müssen diese Geräte in das IT-Netzwerk des Krankenhauses eingebunden werden, da es sich hierbei um neue Komponenten im Medizinischen IT-Netzwerk handelt muss ein erneutes Risikomanagement durchgeführt werden.

Auf Basis der Ultraschallgeräte können nun die ersten Schritte zur Einhaltung der Norm IEC 80001-1 durchgeführt werden.

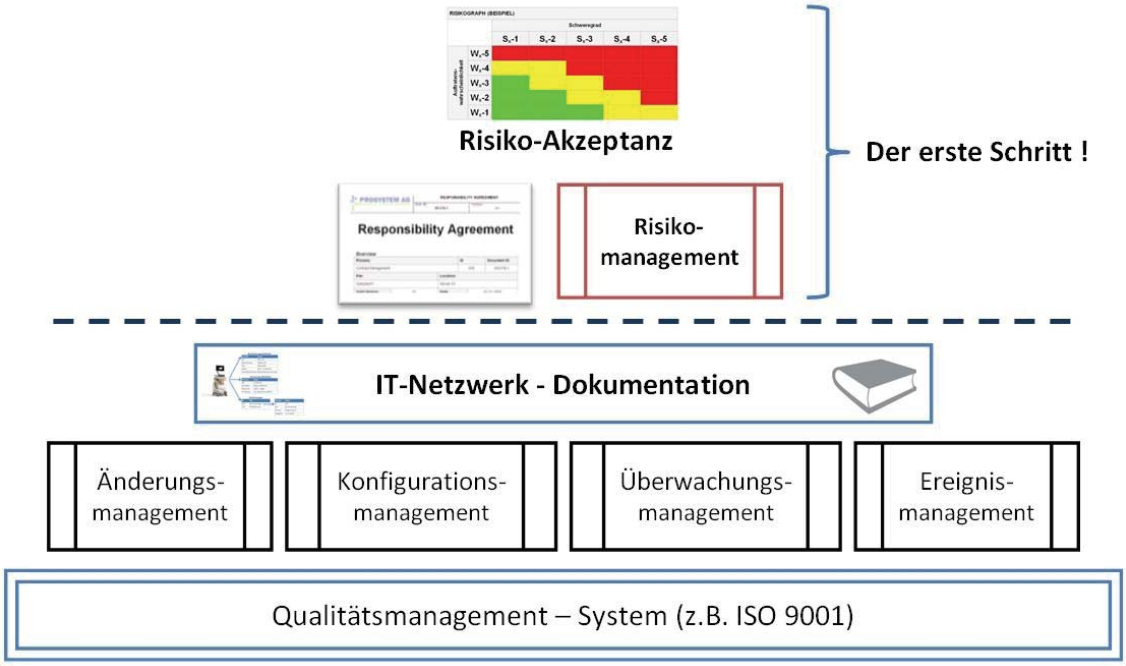


Abbildung 11: Umsetzung der IEC 80001-1[14]

In dieser Arbeit werden die ersten Schritte zur Umsetzung der IEC 80001-1 anhand des Teilnetzwerks Ultraschall „Cardiovaskuläres Imaging System“ (CIS) durchgeführt. Speziell werden die ersten Schritte auf Basis der Kardiologischen Ambulanz in der Kardiologie realisiert. Es wird primär auf die Themen Risikomanagement inklusive Risikomanagement-Plan und Verantwortlichkeitsvereinbarung eingegangen. Die Netzwerk-Dokumentation wird für das Teilnetzwerk des Pilotprojekts durchgeführt, das Änderungsmanagement, Konfigurationsmanagement, Überwachungsmanagement sowie das Ereignismanagement werden im Rahmen dieser Arbeit nicht betrachtet (Abbildung 11).

4.2 Risikomanagement-Akte

4.2.1 Netzwerk-Dokumentation

4.2.1.1 Struktur des Krankenhausnetzwerks des DHZB

Das Netzwerk des Krankenhauses ist ein multifunktionales Netzwerk um Audio, Video und sonstige Daten zu übertragen. Als Netzwerkprotokoll wird TCP/IP (Transmission Control Protocol/Internet Protocol) in der Version IPv4 verwendet. Es werden als Netzwerkadressen unter anderem die Bereiche 172.28.xxx.xxx, sowie 172.29.xxx.xxx benutzt. Aus Datenschutzgründen werden die IP-Adressen nicht weiter detailliert. Das Netzwerk ist durch Firewalls von Partnerinstitutionen und dem Internet getrennt. Die

[14] Quelle: [4], S. 4

Verbindung zum Internet wird zusätzlich über Proxy-Server abgewickelt. Zwischen den internen Abteilungen werden keine Firewalls eingesetzt.

Die physikalische Struktur des Netzwerks sieht wie folgt aus: Drei große Rechnerräume und drei kleinere Rechnerräume sorgen mit Ihren Servern und Datenbanken für den Betrieb der IT-Infrastruktur. Die drei großen Rechnerräume sind über Hochgeschwindigkeitsleitungen in Ringstruktur verbunden. Für zusätzliche Redundanz sind die Rechnerräume untereinander noch mal verbunden (siehe Abbildung 12). Die Peripherie, welche keine hohe Priorität hat, wird mit Stichleitungen und darauffolgenden Verteilern mit einer Netzwerkverbindung versorgt. Wichtige Peripherie, welche eine redundante Anbindung benötigt, wird durch kleinere Ringstrukturen verbunden (siehe Abbildung 12). In allen Netzen befinden sich Verteiler, um die notwendige Portanzahl für die angeschlossenen Geräte zur Verfügung zu stellen. Insgesamt besteht das Krankenhausnetzwerk aus ungefähr 100 Netzwerkkomponenten und 1500 netzwerknutzende Komponenten wie Server oder Clients. Aktive Netzwerkkomponenten wie Switches und Router sind unter anderem von der Firma Brocade/Foundry und besitzen eine non-blocking Routing bzw. Switching Architektur, um einen sicheren Betrieb zu gewährleisten. Die Up-Link-Module sind 10-Gigabit-Ethernet ausgelegt. Zwischen Switches werden in der Regel Lichtwellenleiter (LWL) verwendet, um längere Inhaus-Entfernungen zu überbrücken und eine galvanische Trennung herzustellen. Endgeräte sind mit den Switches durch Kupferleitungen verbunden. Alle Ports stellen 1-Gigabit-Ethernet zur Verfügung. Zu den Außenstellen des Krankenhauses, wie zum Beispiel des Paulinenkrankenhauses, existieren angemietete Netzwerk-Leitungen. Verschlüsselte Funk-Verbindungen sorgen hier für Redundanz. Mit Hilfe von Routern wird eine logische Trennung des Netzwerks in Teilbereiche vorgenommen. Im Anhang A sind die Netzwerkkomponenten mit Typen und Eigenschaften aufgelistet.

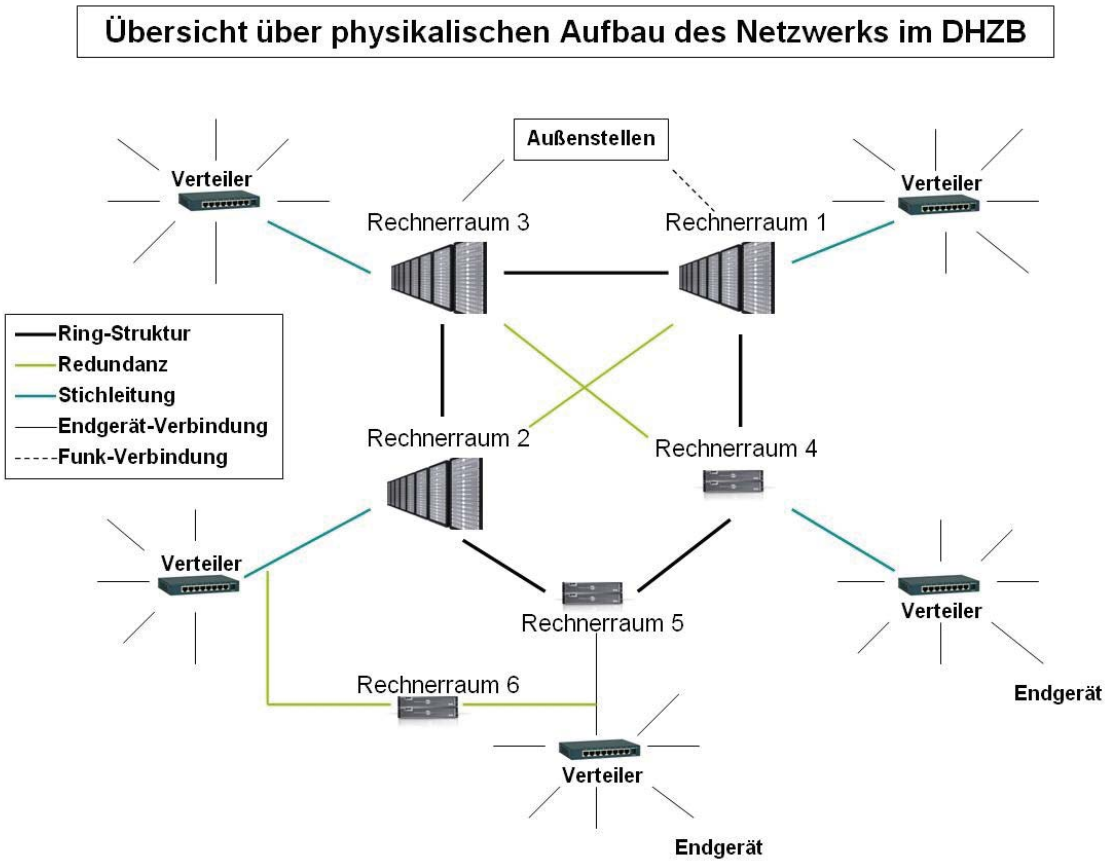


Abbildung 12: Übersicht Krankenhausnetzwerk

Der logische Aufbau des Netzwerks ist in zwei Arten aufgeteilt. Zum einen besteht ein logisch gebridgtes Netz, in welchem über alle Standorte im Netzwerk das gleiche IP-Netz herrscht. Zum Anderen bestehen in allen Verteilerpunkten eigene Subnetze, um eine Strukturierung des Netzwerkes zu ermöglichen. Dieses sind geroutete Netze mit eigenem IP-Netz, wodurch Bereiche logisch getrennt werden. Herstellerspezifische Netze sind im Krankenhaus ebenfalls eingerichtet. Hierbei handelt es sich zum Beispiel um das GE Vital-Monitoring, welches logisch sowohl physikalisch vom Krankenhausnetzwerk getrennt ist und ein in sich abgeschlossenes Netzwerk darstellt.

Damit das Netzwerk auch bei Ausfall der öffentlichen Stromversorgung funktioniert, wird das Netzwerk mit einer unterbrechungsfreien Stromversorgung (USV) betrieben. Die Netzwerkkomponenten haben 2 Netzteile, die an die beiden Stromkreise angeschlossen sind und beim Ausfall einer Stromquelle entsprechend mehr Strom aus dem verbleibenden Stromkreis ziehen. Jeder Netzwerkschrank (und damit die eingebauten Netzwerkkomponenten) ist über einen Potentialausgleich mit dem Energieversorgungsnetz verbunden. Der Potentialausgleich ist eine 56 mm Leitung aus hochfeinen Litzen, um eine ausreichende Erdung auch gegenüber hochfrequenten Strömen sicherzustellen. Eine galvanische Trennung findet innerhalb des Netzwerks durch den Einsatz von Lichtwellenleitern statt. Außerdem werden alle neuangeschafften Geräte mit einer galvanischen Trennung des Netzwerkanschlusses ausgestattet. Um die elektrischen Eigenschaften der Komponenten zu kontrollieren werden nach IEC 60601-

1:2005 Fehlerstrommessungen mit Hilfe einer Fehlerstromzange durchgeführt und dokumentiert. Normen und Konformitätserklärungen, welche im Kliniknetzwerk angewendet werden sind die DIN EN 50173, die 50174, die DIN EN 60601 und zukünftig die IEC 80001-1.

4.2.1.2 Ist-Struktur des Teilnetzwerks „Cardiovaskuläres Imaging System“

Das Teilnetzwerk „Cardiovaskuläres Imaging System“ (CIS) ist ein logisch gebridgtes Netz, welches hausweit zur Verfügung steht. Dies ermöglicht, dass die Ultraschallgeräte ortsvariabel betrieben werden können. Dafür befinden sich Netzwerkanschlüsse, welche mit dem CIS verbunden sind, in den jeweiligen Untersuchungsräumen. Eine Änderung der IP-Adresse ist demzufolge nicht notwendig. In den Räumen sind die Netzwerkanschlüsse, an welche Ultraschallgeräte angeschlossen werden können, mit der Aufschrift „Echo“ gekennzeichnet. Das Krankenhausinformationssystem (KIS) und das Radiologische Informationssystem (RIS) haben eine Verbindung zum CIS. Diese Mischung aus KIS und RIS wird als „Cardis“ bezeichnet und ist eine Eigenentwicklung des Betreibers. Cardis hält Patientendaten in einer Oracle-Cluster-Datenbank vor. Für Untersuchungen mit bildgebenden Verfahren stellt diese Informationen mittels Server-Diensten zur Verfügung. Der dahinter geschaltete „Ensemble“ Kommunikationsserver (virtuelle VMWare-Maschine) leitet die HL-7-Daten des KIS/RIS an den Worklist-Server weiter. Der Worklist-Server „Xcelera Connect R2.1L1“ von Philips übersetzt die HL-7-Daten in die DICOM-Worklist, welche von den Ultraschall-Geräten der Abteilungen abgerufen werden können (siehe Abbildung 13).

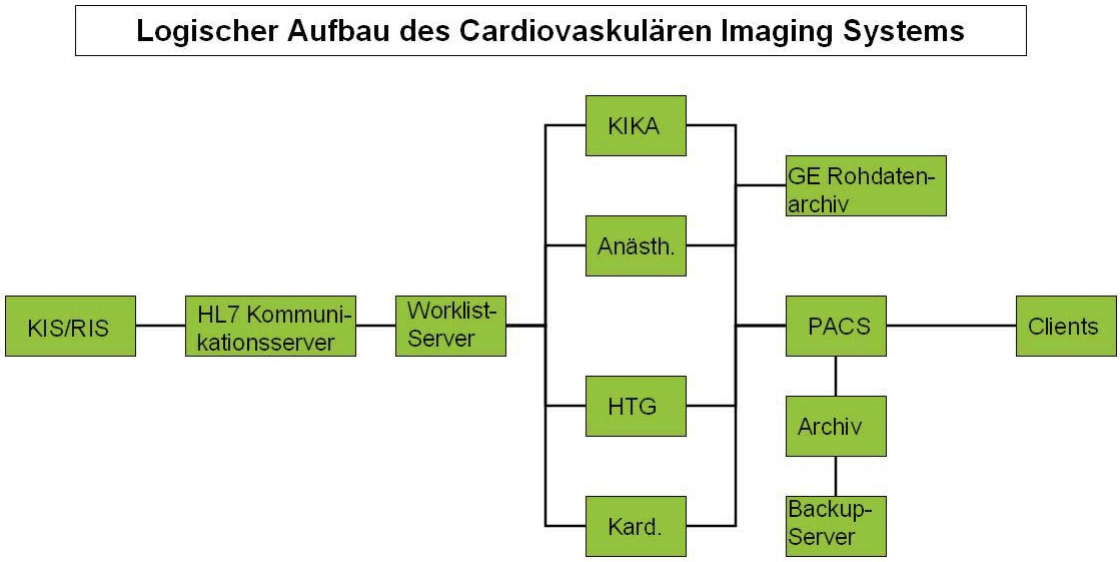


Abbildung 13: Logischer Aufbau des Teilnetzwerks

Die Worklist inklusive der Patientenstammdaten, wird von den einzelnen Ultraschallgeräten der Stationen Kinder-Kardiologie, Anästhesiologie, Herz-Thorax-Gefäß-Chirurgie und Kardiologie bei Bedarf angefordert. Nach einer Untersuchung werden die Echo-

Daten im Bildarchiv (PACS) Xcelera R3.2L1 von Philips mit 6 Terabyte Speicherplatz gespeichert. Das PACS dient nicht nur der Archivierung der Ultraschall-Untersuchungen, sondern besitzt auch Softwarepakete für die Befunderstellung, Nachbearbeitung, sowie für die Betrachtung der Daten mit einem Viewer. Diese Zusatzfunktionen können über ca. 350 Clients im Krankenhaus aufgerufen werden. Diese Clients sind Arbeitsplatz-Computer auf Windows-Betriebssystem-Basis, welche sich in Arztzimmern, Büros, Stationen oder Operationsräumen befinden. Mitarbeiter besitzen spezielle Rechte, um von den Arbeitsplatz-Computern über die Xcelera-Client-Software mit den Anwendungen des PACS arbeiten zu können. Alltägliche nicht-medizintechnische Software wie z.B. E-Mail-Clients werden an diesen Arbeitsplatz-Computern ebenso verwendet. Bei Ultraschallgeräten von GE besteht außerdem die Möglichkeit die Echo-Daten zusätzlich in einem GE Rohdatenarchiv zu speichern. Der Archivspeicher/Langzeitarchiv ist ein Xcelera-Archiv mit 70 Terabyte Speicherplatz. Als Speichertechnik wird RAID-5 verwendet. Der dahinter geschaltete Back-Up-Server erstellt zusätzlich Sicherungen der Daten des Langzeitarchivs. Lokal sind das PACS, das Langzeitarchiv und der Back-Up-Server auf alle Rechnerräume verteilt und dadurch physikalisch getrennt. Im Falle eines Brandes befinden sich diese Rechnerräume in unterschiedlichen Sicherheitszonen.

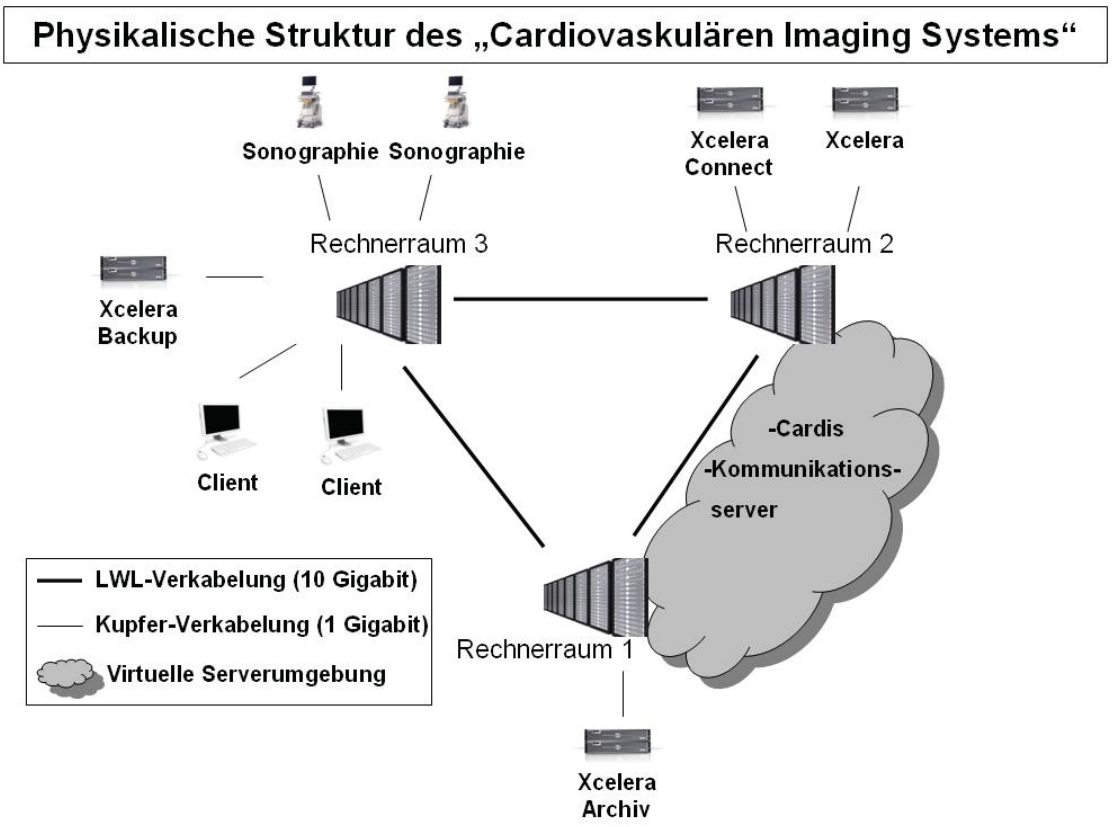


Abbildung 14: Physikalische Struktur des CIS

Das Xcelera-Backup ist in Rechnerraum 3 untergebracht. Außerdem sind hier die Ultraschallgeräte und Clients über Kupferleitungen an dem Netzwerk angeschlossen.

Endgeräte sind mit einer Bandbreite von 1 Gigabit/s angeschlossen. Im Rechnerraum 2 befinden sich die Server für das PACS selbst und Xcelera Connect. Das Xcelera Langzeitarchiv ist in Rechnerraum 1 untergebracht. Alle Rechnerräume sind über Lichtwellenleitungen mit 10 Gigabit-Ethernet redundant verbunden. Die virtuellen Server-Dienste des Cardis und des Kommunikationsservers laufen je nach Auslastung und Kapazität auf einem der 6 verschiedenen VMWare-Server in Rechnerraum 1 oder 2 (Abbildung 14). Die Bestandslisten der Komponenten befinden sich in Anhang A.

Somit sieht der Informations- und Datenfluss im Cardiovaskulären Imaging System wie folgt aus:

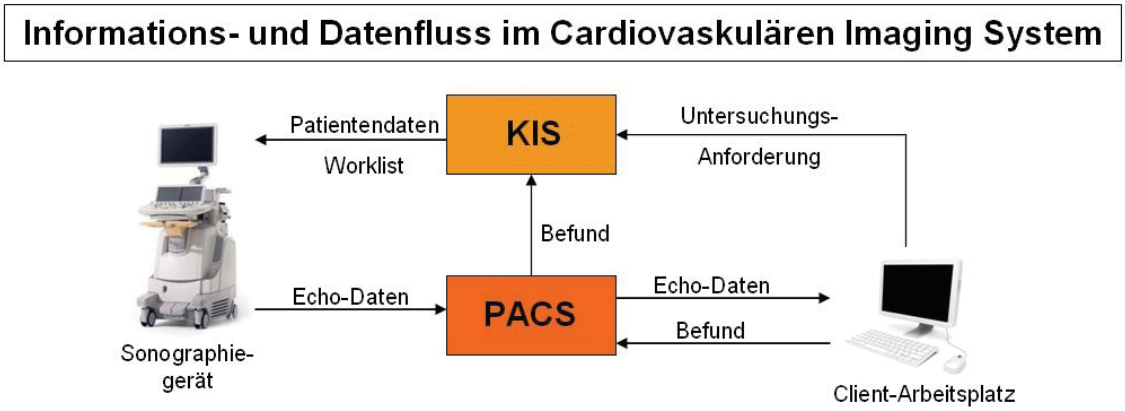


Abbildung 15: Informations- und Datenfluss im DHZB

Der Informations- und Datenfluss beginnt damit, dass vom Client-Arbeitsplatz über die Software von Cardis eine Untersuchungsanforderung gestellt wird. Diese Untersuchungsanforderung wird im KIS in eine Worklist mit entsprechenden Patientenstammdaten umgewandelt und steht nun den Ultraschallgeräten zur Verfügung. Nach der Untersuchung werden die Daten im PACS abgespeichert. An den Client-Arbeitsplätzen werden aus den Daten Befunde erstellt oder Nachbearbeitungen durchgeführt. Die Befunde werden im PACS abgespeichert und abschließend ins KIS übernommen (Abbildung 15).

4.2.1.3 Fazit

Die geforderte Risikomanagement-Akte als zentrales Dokumentationselement, welche die theoretischen Inhalte aus Kapitel 2.2.2 und die konkreten Inhalte aus Kapitel 4.2 enthalten soll, ist im Klinikum schon teilweise umgesetzt. Als Bestandslisten sind alle erforderlichen Informationen digital in Form von Excel-Tabellen und PDF-Dokumenten vorhanden. Eine zentralisierte Form der Dokumentation, zum Beispiel anhand einer Datenbank, ist aber nicht umgesetzt. Inhalte zu medizintechnischen Geräte werden von der Medizintechnik-Abteilung und deren Verantwortlichen verwaltet. Netzwerkkomponenten und die Beschreibungen von Netzwerkstrukturen werden in der IT-Abteilung aufgelistet und bearbeitet. In der IT wurde die Dokumentation auf die Berei-

che Serversysteme/Rechenzentrum, aktive und passive Netzwerkkomponenten aufgeteilt, weshalb hier die Dokumentation nochmals aufgeteilt ist. Für die Einhaltung der IEC 80001-1 müssten die unterschiedlichen Dokumentationen der verschiedenen Bereiche vereinheitlicht und zentral, zum Beispiel in einer „Risikomanagement-Akten-Datenbank“, abgespeichert werden. Falls eine zentralisierte Lösung nicht praktikabel ist, muss eine Vereinheitlichung mit Verweisen und Referenzen zu den Quellen gegeben sein.

Auf Grundlage dieser Arbeit wurden in der IT-Abteilung bereits Gespräche geführt, um mit allen beteiligten der Abteilung das weitere Vorgehen bezüglich der IEC 80001-1 zu besprechen. Ein Ergebnis dieser Gespräche ist die Dokumentationsstruktur nach IEC 80001-1 aufzubauen. Hierfür sollen Orientierungshilfen in Form von Checklisten erstellt werden. Ergebnis dieser Checklisten soll eine Übersicht über Inhalte und Standorte von Dokumenten sein. Außerdem sollen Checklisten zur Integration von Komponenten in Medizinische IT-Netzwerke erstellt werden. Um eine lückenlose Dokumentation zu gewährleisten sind Planungen in Arbeit, in welchen Dokumentationen während der Integration von Medizinprodukten detaillierter durchgeführt werden sollen. Die Protokollierung und Dokumentierung soll begleitend zu den Schritten Qualitätsprüfung, Risikobewertung, Beherrschung des Restrisikos, Übergabe an die Unternehmensleitung bis zur Betriebsbereitschaft konsequent durchgeführt werden.

Um eine stringente Dokumentationsstruktur nach IEC 80001-1 einzuführen sind aber noch Fragestellungen seitens des Betreibers zu klären. Einerseits ist zu klären, wer verantwortlich für die Umsetzung der Risikomanagement-Akte im Klinikum ist und wie diese allen beteiligten Mitarbeitern zur Verfügung gestellt werden kann. Andererseits ist unklar, mit welchem Kostenaufwand in Bezug auf Personal und neuer Infrastruktur zu rechnen ist. Da ein Großteil der relevanten Dokumentation in Papierform vorhanden ist, ist Skepsis vorhanden viel Geld für eine Digitalisierung oder zentrale Lagerung auszugeben. Außerdem ist zu klären, ob Dokumentationen der Medizinprodukt-Hersteller auch im Klinikum zentral gespeichert werden können oder ob es Möglichkeiten gibt bei Bedarf auf Dokumentation der Hersteller über, zum Beispiel das Internet, zuzugreifen. Speziell bei Dokumenten von Medizinprodukt-Hersteller wird nun erwartet, dass zum Beispiel Lieferscheine oder Bedienungsanleitung auch digital zur Verfügung gestellt werden, um diese in der Dokumentation schnell wiederfinden zu können.

4.2.2 Risikomanagement-Plan

4.2.2.1 Zweckbestimmung

4.2.2.1.1 Gebrauch und Nutzen

Das betrachtete Teilnetzwerk Cardiovaskuläres Imaging System (CIS) wird zur Speicherung von Ultraschall-Behandlungen in Abhängigkeit des untersuchten Patienten in einem Bildarchiv verwendet. Das Bildarchiv stellt die Daten für Folgeuntersuchungen zur Verfügung. Zur Nachbearbeitung können Client-Arbeitsplätze auf die Daten zugrei-

fen. Um die Untersuchungen zu bearbeiten oder Befunde zu erstellen, sind verschiedene Softwarepakete auf den Client-Arbeitsplätzen verfügbar. Somit können Befunde elektronisch über das Netzwerk erstellt werden, welche im Krankenhausinformationssystem in die Patientendaten integriert werden. Das Netzwerk wird außerdem zur Langzeitarchivierung und Back-Up-Erstellung der sensiblen Ultraschall-Daten verwendet. Erwartet wird, dass unabhängig vom Hersteller des Ultraschallgeräts die Daten an Arbeitsplätzen/Clients nachbearbeitet und Befunde erstellt werden können. Diese Zweckbestimmung gilt natürlich auch für die Kardiologische Ambulanz in der Kardiologie. Somit dient das CIS als Hilfsmittel zur Durchführung des Untersuchungsprozesses. Diese Untersuchungen werden durch eine schnellere Durchführung der Untersuchung und eine elektronische Befunderstellung unterstützt. Damit stehen Befunde und Nachbearbeitungen der Untersuchung für Folgeuntersuchungen oder Behandlungen im Netzwerk zur Verfügung. Außerdem wird durch das Netzwerk die Verfügbarkeit der Daten und Sicherung der Daten gewährleistet.

4.2.2.1.2 Behandlungsverfahren

In der Kardiologischen Ambulanz werden Ultraschall-Untersuchungen routinemäßig durchgeführt. In dieser Abteilung sind 8 Ärzte für die Ultraschall-Untersuchungen zuständig. Untersucht wird überwiegend transthorakal, aber auch die transösophageale Echokardiographie wird angewendet. Standard-Untersuchungen sind zweidimensionale Untersuchungen des Herzens mit Dopplern aller Art. Hierfür werden Linear-Sonden und Sektor-Sonden verwendet. Spezielle Untersuchungen sind Diagnosen in den Bereichen Abdomen, Koronargefäße oder der Schilddrüse. Bei Bedarf können Bereiche des Herzens in Echtzeit dreidimensional mit Hilfe der transösophagealen und transthorakalen Echokardiographie dargestellt werden. Die untersuchten Patienten finden sich in allen Altersgruppen, Geschlechtern und Gewichten wieder. Speziell in der Kinder-Kardiologie werden Neugeborene und Kinder untersucht und behandelt.

In den anderen Abteilungen der Herz-Thorax-Gefäß-Chirurgie und der Anästhesiologie wird das komplette Spektrum der Ultraschall-Bildgebung angewendet. Dies bedeutet, dass auch intraoperative Eingriffe durch Ultraschall-Geräte begleitet werden, weshalb hier andere Zweckbestimmungen und Workflows beschrieben werden müssen und somit ein anderes Anforderungsprofil besteht.

Die zweite Untersuchung, welche im CIS der Kardiologischen Ambulanz durchgeführt wird, ist die Anwendung von Software an Client-Arbeitsplätzen. Hier werden die Befunde erstellt, welche auf den Daten der Untersuchungen basieren. Außerdem werden hier die Ultraschall-Daten nachbearbeitet. Jede Untersuchung wird hier vermessen und mit anderen Darstellungsmodi analysiert. Softwareanwendungen, welche hier verwendet werden, sind zum Beispiel auf die Untersuchung des linken oder rechten Ventrikels des Herzens ausgelegt oder können dreidimensionale Ultraschalldaten auswerten.

4.2.2.1.3 Klinischer Workflow

Um Untersuchungen mit Unterstützung des CIS durchzuführen, wird als erster Schritt des klinischen Workflows der Kardiologischen Ambulanz eine Untersuchungsanforderung von einem Client-Arbeitsplatz erstellt. Über den Client des Cardis wird diese Anforderung erstellt und an das KIS übermittelt. Die Untersuchungsanforderung steht nun zum Abruf für die Ultraschallgeräte als Worklist inklusive der Patientendaten im KIS zur Verfügung. Die Untersuchung kann nun mit Hilfe der relevanten Patientendaten an den Ultraschallgeräten durchgeführt werden. In der Regel besitzen die Ultraschallgeräte in der Kardiologischen Ambulanz einen festen Standort. Es ist aber auch möglich die Ultraschallgeräte variabel innerhalb der Abteilungen einzusetzen. Hierbei werden die Geräte, nach Abruf der Worklist, vom Netzwerk getrennt und zum Bestimmungsort gebracht. Dies ist durch die in Kapitel 4.2.1.2 erwähnte Netzwerkstruktur möglich. Während den Untersuchungen werden die Daten auf der internen Festplatte des Ultraschallgeräts gespeichert. Je nachdem ob eine Netzwerkverbindung während der Untersuchung vorherrscht, werden die Daten parallel im PACS hinterlegt oder bei der nächsten Verbindung mit dem Netzwerk im PACS gespeichert. Die nachträgliche Speicherung der Daten im PACS muss manuell eingeleitet werden. Im PACS stehen die Daten nun für weitere Untersuchungen bereit. Von den Client-Arbeitsplätzen wird auf die Daten zugegriffen, um Nachbearbeitungen und Befunde zu erstellen. Erstellte Befunde werden in die Patientendaten eingepflegt und wieder im KIS abgespeichert.

Dieser Workflow kann durch medizinische Notfälle oder Netzwerkprobleme unterbrochen werden. Dann stünden bei der Untersuchung keine Patientendaten zur Verfügung. Der Name des Patienten würde somit per Hand eingetragen werden. Die Speicherung der Daten nach einer Untersuchung würde zeitlich verzögert durchgeführt werden. Falls die Client-Arbeitsplätze keine Netzwerkverbindung haben, kann zum Beispiel der Befund mit Hilfe einer Freitext-Eingabe auch offline erfolgen.

4.2.2.2 Risikobehaftete Elemente des CIS

Alle Komponenten des CIS können zu Risiken beitragen, welche sich auf die in Kapitel 2.2.2 und 4.2.2.3 definierten Schutzziele auswirken können. Die integrierten Medizinprodukte werden im Anhang B aufgelistet, wobei die Bestandslisten der Kardiologischen Ambulanz aufgrund der exemplarischen Betrachtung, detaillierter beschrieben sind. Die vorhandenen Ultraschallgeräte sind in den Bestandslisten farbig markiert. Grün hinterlegte Geräte bleiben auch nach Beschaffung von neuen Geräten vorhanden. Die Abstufungen gelb, orange und rot weisen auf das Alter der Geräte hin. Generell gilt bei der Neubeschaffung, dass alle Geräte, die älter als 5 Jahre sind, ersetzt werden sollen. Zusätzlich werden in den Abteilungen Anästhesiologie und Herz-Thorax-Gefäß-Chirurgie jeweils ein neues Gerät angeschafft, sowie in der Kinder-Kardiologie zwei neue Geräte. Speziell die Geräte der Kardiologischen Ambulanz sollen hier in den Vordergrund gerückt werden, da an diesem Bereich beispielhaft die Risikoanalyse durchgeführt wird. Außerdem unterliegen die Geräte der Kardiologischen Ambulanz exakt den in Abbildung 14 beschriebenen Strukturen. Auch die in Kapitel

4.2.1.2 beschriebenen Netzwerkkomponenten, welche im CIS zum Einsatz kommen, sind Elemente, welche für die Risikoanalyse relevant sind. Die Auflistung der Netzwerkkomponenten und deren Eigenschaften befinden sich in Anhang A. Um eine genügende Bandbreite ohne Latenzen zu gewährleisten, wird das Gigabit-Ethernet als Netzwerk-Technologie verwendet. Zwischen größeren Rechnerverbünden existiert zur Datenübertragung ein 10 Gigabit-Ethernet, Endgeräte werden mit 1 Gigabit-Ethernet versorgt. Insbesondere die Software, welche an den Arbeitsplätzen/Clients verwendet wird ist risikorelevant, da hier medizinische und nicht-medizinische Software zusammentreffen.

Tabelle 6: Software auf Arbeitsplätzen/Clients

Anwendungssoftware	
nicht-medizinische Software	**medizinische Software**
Office-Paket inkl. E-Mail-Konto	Cardis (Worklist-Anforderung, Befundung)
Acrobat Reader	Medfolio (KIS)
Virenscanner (McAfee)	EMTEK (PDMS)
Dienstplan-Software	Xcelera-Client (PACS)
Oracle Client-Software	Lauris Client (Laborinformationssystem)
Intranet-Client	QLAB (Auswertesoftware für Echo-Daten)

Die in Tabelle 6 aufgelisteten Softwarepakete sind die Anwendungen, welche standardmäßig auf jedem Arbeitsplatz installiert werden. Hinzu kommt besondere Anwendungssoftware zur Auswertung, Nachbearbeitung oder Befunderstellung, welche über die Xcelera-Client-Anwendung freigeschaltet und lizenziert werden. Auch die Patientendaten sind im Bezug auf das Schutzziel „Daten- und Systemsicherheit“ ein risikorelevantes Element. Im CIS werden alle Patientendaten, welche im Krankenhausinformationssystem gespeichert sind, verwendet. Je nachdem welche Untersuchungen durchgeführt werden, kann jede Information eines Patienten relevant sein. Hierzu zählen Arztbriefe, Patientenstammdaten, Bilder aus dem PACS, Befunde oder OP-Dokumentationen. Diese hochsensiblen Daten unterliegen den hauseigenen und gesetzlichen Datenschutzbestimmungen.

Um die genannten Elemente zu überprüfen sind Sicherheitsmechanismen implementiert worden. Virenscanner von McAfee, welche über eine zentrale Updateverwaltung (McAfee EPO 3.5) auf dem neuesten Stand gehalten werden, sind ebenso vorhanden wie dauerhaft erreichbare Rufbereitschaftsdienste für die Bereiche Software, Systemtechnik und Netzwerk. Präventiv finden systematisch Überprüfungen der Netzwerke und deren Komponenten statt, um Probleme schon vor deren Auftreten zu erkennen. Außerdem sammeln die Systeme auch eigenständig Daten (Log-Files), welche im Fehlerfall über SMS und E-Mails die zuständigen Bereiche informieren.

4.2.2.3 Definition der Schutzziele und Risikoakzeptanz

Patientensicherheit:

Im Schutzziel der Patientensicherheit geht es darum zu analysieren, an welchen Stellen des klinischen Workflows in der Kardiologischen Ambulanz Gefährdungen für den Patienten eintreten können. Hierbei sind alle Komponenten, welche in den Workflow integriert sind, zu berücksichtigen. Dazu zählen die Ultraschallgeräte, Komponenten des Netzwerks, allgemeine Infrastruktur (z.B.: Stromversorgung), Anwender oder auch die Patienten selbst.

Wirksamkeit/Effektivität:

In diesem Schutzziel wird analysiert ob Gefährdungen auftreten können, die den klinischen Workflow der Kardiologischen Ambulanz beeinträchtigen oder komplett lahmlegen können.

Daten/-Systemsicherheit:

Die Daten- und Systemsicherheit bewertet Gefährdungen, welche die Vertraulichkeit, Vollständigkeit und Verfügbarkeit von Daten betreffen können. In der Kardiologischen Ambulanz betrifft dies die Patientendaten aus dem Krankenhausinformationssystem, sowie die Ultraschall-Untersuchungen, welche im PACS abgespeichert werden.

4.3 Verantwortlichkeitsvereinbarung

4.3.1 Allgemein

Um eine Verantwortlichkeitsvereinbarung zu erstellen, müssen zu Beginn die internen und externen Parteien identifiziert werden, welche in einem Medizinischen IT-Netzwerk eines Krankenhauses involviert sind. Interne Parteien sind dann involviert, wenn sie in Bezug auf Wartung, Inbetriebnahme oder Verwaltung für bestimmte Gerätegruppen zuständig sind oder mit den Geräten arbeiten. Hierzu zählen in einem Krankenhaus die Medizintechnik, Informationstechnik, Betriebstechnik (zuständig für z.B. Energie und Klima) sowie Ärzte, andere Anwender und die Verwaltung. Jede Partei muss über potentielle Gefährdungen informiert werden und wird deshalb in einer internen Verantwortlichkeitsvereinbarung berücksichtigt.

Externe Parteien, welche in einem Krankenhaus mit Hard- und Software vertreten sind, können ebenfalls eine Verantwortlichkeitsvereinbarung unterzeichnen.

Inhalte der Verantwortlichkeitsvereinbarung sind die Aufgaben und Pflichten, welche in Kapitel 2.1 erläutert sind. Um eine Verantwortlichkeitsvereinbarung zu verfassen, muss innerhalb der Verantwortlichen Organisation der Zweck der Vereinbarung zwischen den einzelnen Parteien definiert werden, um die Inhalte vertraglich festzulegen.

4.3.2 Inhalte einer Verantwortlichkeitsvereinbarung

Um eine Verantwortlichkeitsvereinbarung exemplarisch mit einem Medizinprodukt-Hersteller zu schließen, wurde der Kontakt zu einem Hersteller aufgenommen. Der Zweck der Verantwortlichkeitsvereinbarung ist es das Risikomanagement mit Informationen zu den Produkten zu unterstützen. Hierbei wurden Informationen angefordert über Fehlerzustände der Geräte bei Netzwerkausfall, Informationen über offene Ports und Status der Virenscanner.

Aus den Gesprächen mit den Verantwortlichen des Betreibers wurde deutlich, dass der Betreiber eines Netzwerks noch weitere Anforderungen an einen Medizinprodukt-Hersteller stellt. Somit könnten in der Verantwortlichkeitsvereinbarung auch Befugnisse und Kompetenzen von speziellen Mitarbeitern eines Betreibers geregelt werden. Dies hätte für den Betreiber den Nutzen, dass bei bestimmten Problemen oder Neukonfigurierungen kein Service-Mitarbeiter des Herstellers gerufen werden müsste, sondern ein Mitarbeiter im Klinikum die Befugnisse hätte, dieses durchzuführen. Zum Beispiel wäre das Klinikum, unabhängig von einem Service-Mitarbeiter des Herstellers, dann dazu befugt Ultraschallgeräte in das Netzwerk einzubinden. Außerdem müssen für den Betreiber Informationen zur Verfügung stehen, welche Mitarbeiter eines Herstellers bei Fragen zu erreichen sind und in das Thema eingearbeitet sind. Es sollte auch eine Informationspflicht vereinbart werden, in dem der Hersteller die Betreiber über z.B. Firmwareupdates in Kenntnis zu setzen hat.

Generell sollte die Verantwortlichkeitsvereinbarung vor Anschaffung von Neugeräten bei Verhandlungen mit dem Hersteller vereinbart werden. Die Forderungen der Betreiber an die Hersteller könnten auch Inhalt von Leistungsverzeichnissen für Ausschreibungen sein. Ein Planungsbüro für Medizin-/Informationstechnik kann hier als Berater fungieren oder die Verhandlungen zwischen Betreiber und Hersteller führen, um eine Einigung anhand der Verantwortlichkeitsvereinbarung zu erzielen.

4.3.3 Fazit

Die Erstellung eines Vertrags für eine Verantwortlichkeitsvereinbarung zwischen einem Betreiber eines Medizinischen IT-Netzwerks und einem Medizinprodukt-Hersteller wurde aus zeitlichen Gründen im Rahmen dieser Bachelorarbeit nicht durchgeführt. Während der Gespräche mit den Herstellern fielen Nachfragen auf, was eine Verantwortlichkeitsvereinbarung ist. Dies lässt den Schluss zu, dass manche Medizinprodukt-Hersteller sich noch nicht ausreichend mit der IEC 80001-1 beschäftigt haben. Um die Norm in einem Krankenhaus umsetzen zu können, ist aber ein Grundwissen seitens der Mitarbeiter des Herstellers erforderlich, damit auf Forderungen der Betreiber reagieren werden kann.

4.4 Risikomanagement

4.4.1 Hintergrund

Bei der Umsetzung eines Risikomanagements wurden anfänglich Gespräche mit Verantwortlichen der Informationstechnik geführt. In diesen Gesprächen ging es grundsätzlich darum, ein Verständnis für das Risikomanagement der IEC 80001-1 zu entwickeln. Auf Basis der Tabelle „Risikomanagement des Cardiovaskulären Imaging Systems in der Kardiologischen Ambulanz“ aus Anhang C wurde in den Gesprächen über Gefährdungen, deren Ursachen, Gefährdungssituationen, mögliche Schäden, vorhandene Maßnahmen und zukünftige Maßnahmen diskutiert. Aus diesen Diskussionen über tatsächlich existierende risiko-relevante Themen resultierten die Ergebnisse des Anhangs C. Um nun das Risikomanagement exemplarisch durchzuführen, wurden aus den Ergebnissen für jedes der drei Schutzziele Beispiele ausgewählt, an denen die Risikoanalyse und die Risikobewertung durchgeführt werden. In der Risikobeherrschung wurde auf theoretisch durchführbare Risikominimierungsmaßnahmen eingegangen. Die tatsächliche Implementierung und Verifizierung von Risikominimierungsmaßnahmen ist nicht Teil des Risikomanagements dieser Arbeit. In diesem Risikomanagement geht es primär darum ein grundsätzliches Verständnis für die Durchführung des Risikomanagements auf Grundlage der IEC 80001-1 mit dem Betreiber eines Medizinischen IT-Netzwerks zu erarbeiten. Auf Basis von [5] S. 63 wurde das Risikomanagement durchgeführt.

Verwendete Abkürzungen (Vgl. [5], S. 31):

- Gefährdung (Gef)
- Ursache (U)
- Gefährdungssituation (GS)
- Schaden (S)
- Risikominimierungsmaßnahme (R)

4.4.2 Risikomanagement an Beispielen

4.4.2.1 Lizenzmanagement

Die Anwendungssoftwarepakete an den Client-/Server-Arbeitsplätzen zur Befunderstellung und Nachbearbeitung der Ultraschalldaten wurden mit einer sogenannten „floating licence“ angeschafft. Dies bedeutet, dass die Software auf beliebig vielen Arbeitsplätzen installiert werden kann. Sie kann aber nur von einer, in der Lizenz vereinbarten, Anzahl gestartet werden.

Schritt 1: Identifizierung von Gefährdungen

Gef01: Durch dieses Lizenzmodell kann es zu Situationen kommen, in welchen behandelnde Ärzte auf bestimmte Softwarepakete nicht zu greifen können, da

die vorgegebene Anzahl der gestarteten Software bereits vergeben sind. Hierdurch kann der klinische Workflow beeinträchtigt werden.

Schritt 2: Identifizierung der Ursachen und Gefährdungssituationen

U01: Die Anzahl der erworbenen Lizenzen ist nicht ausreichend, um den alltäglichen Workflow zu decken.

U02: Ärzte lassen die Software nach Benutzung gestartet, ohne diese weiter zu verwenden.

GS01: Schutzziel Effektivität/Wirksamkeit: Software zur Befunderstellung oder Nachbearbeitung steht nicht zur Verfügung, um eine Ultraschalluntersuchung abzuschließen.

Schritt 3: Ermittlung von möglichen Schäden und Abschätzung des Schweregrades

S01: Die computerunterstützte Nachbearbeitung und Befunderstellung kann erst durchgeführt werden, wenn die Software gestartet werden kann. Bei zeitkritischen Untersuchungen muss auf eine manuelle Nachbearbeitung und eine handschriftliche Befundung zurückgegriffen werden. Da in der Regel die Software zeitnah wieder zur Verfügung steht ist der Schweregrad auf „ernst = $S_{W/E}$-3“ (Tabelle 4) einzuschätzen.

Schritt 4: Abschätzung der Auftretenswahrscheinlichkeit

GS01: Da für eine genügend große Anzahl an Lizenzen gesorgt ist, ist die Wahrscheinlichkeit, dass auf Software nicht zugegriffen werden kann auf „fernliegend = W-2“ (Tabelle 2) einzustufen.

Schritt 5: Beurteilung des Risikos

GS01: Mit Hilfe des Risikographen (Abbildung 6) kann das Risiko dieser Gefährdung auf „Mittel“ eingestuft werden. Dies bedeutet, dass Risikominimierungsmaßnahmen implementiert werden müssen, wenn diese ökonomisch und technisch praktikabel sind.

Schritt 6: Risikominimierungsmaßnahmen aufstellen

R01: Anschaffung einer „Site Licence“ für Software, die am häufigsten benutzt wird.

R02: Integration von Timern, welche gestartete Software nach Benutzung automatisch schließen.

Anhand dieser Risikominimierungsmaßnahmen kann nun eine erneute Risikobewertung durchgeführt werden. Darauffolgend können die Schritte 7 bis 10 des Risikomanagements, nach Abbildung 10, bearbeitet werden.

4.4.2.2 Mechanische Zerstörung

Da die Ultraschallgeräte des Krankenhauses, speziell der Kardiologischen Ambulanz, nicht per WLAN mit dem Netzwerk verbunden sind, ist bei Bewegung darauf zu achten

das Netzwerkkabel vom Gerät zu trennen. Im Arbeitsalltag aber auch in Notfällen kann es passieren, dass vergessen wird die Geräte bei Bewegung vom Netzwerkkabel zu trennen. Dadurch kann es zur Beschädigung des Netzwerkkabels, der Netzwerkdose oder des Ultraschallgeräts kommen. Auch unsachgemäßes Überfahren der Netzwerkkabel kann diese schädigen.

Schritt 1: Identifizierung von Gefährdungen

Gef01: Keine Verbindung zum Netzwerk vorhanden.

Schritt 2: Identifizierung der Ursachen und Gefährdungssituationen

U01: Kabelbruch durch nicht ordnungsgemäßes Abstecken des Netzwerkkabels vor Bewegung des Ultraschallgeräts

U02: Netzwerkbuchse wird durch Bewegung des Geräts beschädigt

GS01: Schutzziel Effektivität/Wirksamkeit: Es ist keine Verbindung zum KIS, vorhanden, um Patientendaten abzurufen. Außerdem gibt es keine Möglichkeit die Patientendaten im PACS abzuspeichern, wodurch keine zeitnahe Nachbearbeitung und Befunderstellung möglich ist.

GS02: Schutzziel Datensicherheit: Dadurch, dass die Ultraschalluntersuchung nicht direkt nach der Untersuchung abgespeichert werden kann, muss dafür gesorgt werden, die Daten nachträglich im PACS zu speichern. Dadurch kann es zu unvollständigen Datenbeständen kommen, wenn diese nicht nachträglich eingepflegt werden.

Schritt 3: Ermittlung von möglichen Schäden und Abschätzung des Schweregrades

S01: Die Ultraschalluntersuchung ist nur ohne Patientendaten aus dem KIS möglich. Die Untersuchung kann aber durchgeführt werden, wenn am Gerät selbst der Name des Patienten eingetragen wird. Durch den internen Speicher des Ultraschallgeräts gehen die Daten nicht verloren. Wenn die Netzwerkverbindung wieder steht, können die Daten vom internen Speicher ins PACS gespeichert werden. Der Schweregrad ist auf „ernst“ (Tabelle 4) einzuschätzen, da die Untersuchung auch ohne Netzwerkverbindung durchgeführt werden kann. Die Daten stehen aber kurzfristig nicht zur Nachbearbeitung und Befunderstellung zur Verfügung.

S02: Der Schweregrad für die Datensicherheit ist bei „unerheblich“ (Tabelle 5) anzusiedeln, da die Daten in der Regel bei erneuter Netzwerkverbindung ins PACS übertragen werden. Diese Speicherung muss aber durch einen Anwender eingeleitet werden.

Schritt 4: Abschätzung der Auftretenswahrscheinlichkeit

GS01: Die Wahrscheinlichkeit, dass die Netzwerkverbindung durch Netzwerkkabelbrüche ausfällt, ist auf „gelegentlich“ (Tabelle 2) einzustufen, da speziell bei Notfällen oft nicht darauf geachtet werden kann das Gerät vom Netzwerk zu trennen.

Schritt 5: Beurteilung des Risikos

GS01: Das Risiko, welches den klinischen Workflow betrifft, ist somit „mittel“ (Abbildung 6).

GS02: Das Risiko, welches die Datensicherheit betrifft, liegt im niedrigen/akzeptablen Bereich (Abbildung 6). Risikominimierungsmaßnahmen sind nicht notwendig.

Schritt 6: Risikominimierungsmaßnahmen aufstellen

R01: Um das Risiko des Netzwerkausfalls, durch mechanische Zerstörung, zu minimieren, können Ersatz-Netzwerkkabel in den Bereichen bevorratet werden, in welchen Ultraschallgeräte zum Einsatz kommen. Außerdem könnten Arbeitsanweisungen und Warnhinweise an den Geräten platziert werden, um darauf hinzuweisen die Geräte vor Bewegung vom Netzwerkkabel zu trennen.

Anhand dieser Risikominimierungsmaßnahmen kann nun eine erneute Risikobewertung durchgeführt werden. Darauffolgend können die Schritte 7 bis 10 des Risikomanagements, nach Abbildung 10, bearbeitet werden.

4.4.2.3 Untersuchungsdaten

Für eine Ultraschalluntersuchung wird die Worklist mit den relevanten Patientendaten benötigt. Falls aus Gründen fehlender Konnektivität keine Verbindung zum KIS besteht, müssen die Patientendaten am Ultraschallgerät per Hand eingetragen werden. Hier wird meistens nur der Name eingetragen, da dieser ausreichend ist, um die Untersuchung zu starten. Nun kann es aus Zeitmangel oder mangelnder Konzentration passieren, dass der Name falsch geschrieben wird. Dies hat zur Folge, dass die Daten der Untersuchung nicht in den Patientendaten des richtigen Patienten abgespeichert werden, sondern im PACS eine neue Patientendatei erstellt wird. Weiterhin kann es dadurch, dass nur der Nachname am Ultraschallgerät eingetragen wird zu Doppelnennungen kommen. Im späteren Verlauf kann nur noch schwer entschieden werden, ob die doppelten Namen Untersuchungen von einem Patienten oder mehreren Patienten sind.

Schritt 1: Identifizierung von Gefährdungen

Gef01: Beeinträchtigung des klinischen Workflows.

Gef02: Verlust der Vollständigkeit von Patientendaten bzw. Gefahr von doppelten Daten und/oder fehlerhafte Zuordnung.

Gef03: Durchführung von Untersuchungen mit unvollständigen Patientendaten.

Schritt 2: Identifizierung der Ursachen und Gefährdungssituationen

U01: Anwender speichert Untersuchung unter falsch geschriebenem Namen.

U02: Patientenname kommt doppelt im PACS vor. Dadurch, dass bei keiner Verbindung zum KIS nur der Name eingetragen wird, fehlen wichtige Zuordnungsparameter, wie Patientennummer, Vorname und Geburtsdatum.

GS01: Schutzziel Effektivität/Wirksamkeit: Untersuchungsdaten werden im PACS unter falschem Namen abgespeichert. Dadurch fehlen den Ärzten bei Folgeuntersuchungen Informationen.

GS02: Schutzziel Datensicherheit: Bei Speicherung von falschen oder unvollständigen Patientendaten kommt es zu lückenhaften Patientendaten. Eine falsche Zuordnung von Untersuchungsdaten kann speziell bei mehrfach auftretenden Namen vorkommen.

GS03: Schutzziel Patientensicherheit: Durch unvollständige Patientendaten oder falscher Zuordnung von Patientendaten, kann es zu einer Gefährdung des Patienten kommen.

Schritt 3: Ermittlung von möglichen Schäden und Abschätzung des Schweregrades

S01: Wichtige Patientendaten stehen für Untersuchungen nicht zur Verfügung. Der klinische Workflow ist dadurch beeinträchtigt, da die Untersuchung verzögert oder gar nicht durchgeführt werden kann. Vorausgesetzt der anwendende Arzt erkennt das Fehlen von Untersuchungsdaten. Aus diesen Gründen ist der Schweregrad mit „kritisch“ (Tabelle 1) einzustufen.

S02: Der Schweregrad für die Daten- und Systemsicherheit ist mit „geringfügig“ (Tabelle 5) zu bewerten, da die Patientendaten in jedem Fall gespeichert sind. Es bedarf nur einer korrekten Zuordnung oder Vervollständigung der Daten.

S03: Durch Unvollständigkeit und Zuordnungsfehlern der Untersuchungsdaten, können wichtige Informationen bei Folgeuntersuchungen vorenthalten werden. Außerdem können Patienten, bei falscher Zuordnung von Patientendaten, einer irrtümlichen Behandlung unterzogen werden. Der Schweregrad ist hier auf „katastrophal“ (Tabelle 3) einzustufen, da lebensbedrohliche Folgen nicht auszuschließen sind.

Schritt 4: Abschätzung der Auftretenswahrscheinlichkeit

GS01: Die Wahrscheinlichkeit für diese Gefährdungen kann mit „fernliegend“ (Tabelle 2) bewertet werden. Zum Einen liegt dies darin begründet, dass die Verbindung zum KIS in der Regel hergestellt ist. Zum Anderen werden regelmäßige Kontrollen der Untersuchungsdaten im PACS durchgeführt, um zu kontrollieren, ob Untersuchungen keine vollständige Patientenzuordnung besitzen.

Schritt 5: Beurteilung des Risikos

GS01: Das Risiko, welches den klinischen Workflow betrifft, ist somit bei „mittel“ (Abbildung 6).

GS02: Das Risiko der Datensicherheit liegt bei „niedrig“ (Abbildung 6).

GS03: Das Risiko der Patientengefährdung ist somit auf „hoch“ (Abbildung 6) einzustufen.

Schritt 6: Risikominimierungsmaßnahmen aufstellen

R01: Maßnahmen zur Risikominimierung wären in dem Fall: Das Schreiben von Arbeitsanweisungen, welche, speziell bei keiner Verbindung zum KIS, darauf hinweisen, die manuell eingetippten Patientendaten zu kontrollieren. Außerdem könnte eine Abfrage im PACS programmiert werden, welche die Untersuchungsdaten durchsucht und Alarm schlägt, wenn eine Untersuchung keine eindeutige Zuordnung besitzt. Eine eindeutige Zuordnung wäre in dem Fall, wenn Patientennummer, Vorname, Nachname und Geburtsdatum der vorhandenen Patientendatei im PACS und der zu speichernden Untersuchung, gleich sind.

Anhand dieser Risikominimierungsmaßnahmen kann nun eine erneute Risikobewertung durchgeführt werden. Darauffolgend können die Schritte 7 bis 10 des Risikomanagements, nach Abbildung 10, bearbeitet werden.

4.4.2.4 E-Mail-Verkehr

Das Verschicken von Patientendaten per E-Mail ist durch die Datenschutzbestimmungen verboten. Ausgenommen sind Fälle, in denen relevante Daten von Patienten an zum Beispiel Hausärzte weitergeleitet werden müssen oder für externe Studien weiterverwendet werden können. Außerdem ist es in Ausnahmen möglich intern im Krankenhaus relevante Patientendaten an Ärzte zu schicken, welche an weiteren Untersuchungen beteiligt sind.

Schritt 1: Identifizierung von Gefährdungen

Gef01: Verlust der Vertraulichkeit von Daten.

Schritt 2: Identifizierung der Ursachen und Gefährdungssituationen

U01: Durch unbefugte Weiterleitung der Patientendaten an Empfänger, die keinen Bezug zu den Patientendaten haben.

U02: Virusbefall der Computer mit welchen E-Mails verschickt oder empfangen werden.

GS01: Schutzziel Datensicherheit: Unbefugte Personen können Zugriff auf sensible Patientendaten erhalten, welches die Vertraulichkeit der Patientendaten beeinflusst.

Schritt 3: Ermittlung von möglichen Schäden und Abschätzung des Schweregrades

S01: Durch die fehlerhafte Verteilung von Patientendaten über den E-Mail-Verkehr können Patientendaten für unbefugte Zwecke missbraucht werden. Um dies zu verhindern, sind bereits Maßnahmen vorhanden. Die automatische E-Mail-Weiterleitung wurde deaktiviert, um zu vermeiden, dass Patien-

tendaten an Dritte weitergeleitet werden. Eine weitere Maßnahme ist, dass die Größe der anhängbaren Daten auf 15 MB beschränkt ist, was zur Folge hat, dass nur Teile der Patienteninformation hochgeladen werden können, aber keine kompletten Patientendaten. Außerdem schützen Virenscanner die Computer vor Virenbefall. Dadurch ist der Schweregrad auf „unerheblich“ (Tabelle 5) einzustufen.

Schritt 4: Abschätzung der Auftretenswahrscheinlichkeit

GS01: Die Wahrscheinlichkeit, dass E-Mails mit Patienteninformationen verschickt werden ist mit „gelegentlich“ (Tabelle 2) zu bewerten, da Informationen für Studien oder Hausärzte verschickt werden. Informationen für Studien werden nur in anonymisierter Form verschickt.

Schritt 5: Beurteilung des Risikos

GS01: Das Risiko für diese Gefährdung ist somit „niedrig“ (Abbildung 6).

Schritt 6: Risikominimierungsmaßnahmen aufstellen

R01: Es sind keine Risikominimierungsmaßnahmen erforderlich.

4.4.3 Fazit

Anhand der Gespräche mit den Verantwortlichen des Medizinischen IT-Netzwerks konnte ein grundlegendes Verständnis für den Ablauf des Risikomanagementprozesses erzielt werden. Eine gute Hilfe zur Durchführung der Risikoanalyse war der „technical report“ IEC/TR 80001-2-1, in welchem der Prozess des Risikomanagement Schritt für Schritt erklärt ist. Grundlegend entstand am Anfang des Risikomanagementprozesses das Problem, dass uns zur Umsetzung der Analyse ein Modell für den Risikomanagementprozess des CIS fehlte. Nach einigen Gesprächen erschien uns der klinische Workflow der Kardiologischen Ambulanz, als Modell der Wirkungsketten des Risikomanagements, als geeignet. Anhand dieser Wirkungskette wurde über konkrete Gefährdungen gesprochen und der Risikomanagementprozess durchgeführt. Unklarheiten während der Risikoanalyse entstanden noch dadurch, dass die Definitionen von Gefährdung, Ursache, Gefährdungssituation und möglicher Schaden sich zum Teil überschnitten. Dadurch entstand das Problem der konkreten Zuordnung von Inhalten aus den Gesprächen zu einem der genannten Teilbereiche. Schweregrade und Auftretenswahrscheinlichkeiten von auftretenden Gefährdungssituationen wurden ebenfalls in den Gesprächen diskutiert. Hier stellte sich die Frage nach der Reproduzierbarkeit der Ergebnisse, da Schweregrad und Auftretenswahrscheinlichkeit nur diskutiert wurden, aber nicht mit Statistiken untermauert sind. Somit können diese nur als Orientierungshilfe dienen, um einen Anfang im Bereich Risikomanagement zu machen. Im späteren Verlauf der Umsetzung werden sich, durch einen größeren Erfahrungsschatz konkretere Ergebnisse einstellen.

Um die Risikoanalysen in Zukunft durchführen zu können, wurde dieser Bereich in technische Planung und medizinische Planung des Risikomanagements gegliedert.

Der Risikomanagementprozess sollte schrittweise bei Neuanschaffungen der Informationstechnik und Medizintechnik durchgeführt und eingeführt werden, um der Norm Schritt für Schritt gerecht zu werden. Unterstützung bei der Einführung und Durchführung dieser Prozesse kann auch bei Planungsbüros der Medizintechnik/Informationstechnik eingeholt werden.

5 Diskussion und Ausblick

Ziel dieser Arbeit war es, die ersten Schritte zur Einführung der IEC 80001-1 im Deutschen Herzzentrum Berlin durchzuführen, um mit einem Betreiber eines Medizinischen IT-Netzwerks ein Verständnis für die Norm zu entwickeln. Zu diesem Zweck wurden mehrere Treffen mit der Verantwortlichen IT-Abteilung einberaumt, um in erster Linie Inhalte der Norm zu diskutieren und Fragestellungen zur Umsetzung zu klären. Infolgedessen wurden eine Dokumentationsstruktur inklusive Bestandslisten, ein Risikomanagement anhand exemplarischer Risiken sowie Anfänge einer Verantwortlichkeitsvereinbarung erstellt.

Dabei ergaben sich, in Bezug auf die gesteckten Ziele, folgende Ergebnisse:

Die IEC 80001-1 gibt verständlich Aufschluss über die neuentstehenden Verantwortlichkeiten und Aufgaben, welche sich für den Betreiber eines Medizinischen IT-Netzwerks ergeben. Die zu erstellende Dokumentationsstruktur (Risikomanagement-Akte inklusive Risikomanagement-Plan und Netzwerkdokumentation) wird mit ihren Anforderungen konkret beschrieben. Probleme bei der Erstellung einer Netzwerk-Dokumentation im Krankenhaus ergaben sich dadurch, dass die Dokumente von verschiedenen Verantwortlichen in der Medizintechnik und Informationstechnik gepflegt werden und somit die Wege der Beschaffung der Bestandslisten lang waren. Außerdem ergaben sich Kommunikationsschwierigkeiten zwischen der Medizin- und Informationstechnik, welche Inhalte, in Bezug auf die Norm, wichtig sind und welcher Aufwand in die Detaillierung gesteckt werden muss. Somit motiviert die IEC 80001-1 zu einer stärkeren Zusammenarbeit zwischen Medizin- und Informationstechnik, um gemeinsam eine Dokumentationsstruktur zu erstellen. Durch eine engere Zusammenarbeit der Abteilungen können Kosten gesenkt werden und Zeit beim Suchen von Dokumenten eingespart werden.

Während der Durchführung des Risikomanagements wurde deutlich, dass nur anhand der IEC 80001-1 der Prozess schwerlich durchgeführt werden kann, da konkrete Definitionen und Beispiele fehlen. Diese konkreten Anweisungen werden im „technical report“ IEC/TR 80001-2-1 gemacht, weshalb damit der Risikomanagement-Prozess durchgeführt konnte. Probleme, auf welche in Kapitel 4.4.3 eingegangen wurde, betrafen die Einteilung der einzelnen Risiken in Gefährdungen, Ursachen, Gefährdungssituationen und mögliche Schäden. Außerdem traten Probleme bei der Erstellung eines Modells zur Durchführung des Risikomanagements auf. Die Motivation zur Durchführung eines Risikomanagements für Medizinische IT-Netzwerke besteht darin, bei Klagen gegen den Betreiber des Netzwerks, Dokumente und Begründungen liefern zu können, welche Maßnahmen zur Risikominimierung implementiert sind und weshalb Restrisiken vorhanden sind. Dadurch kann sich der Betreiber vor Haftungsansprüchen schützen. Außerdem dient das Risikomanagement, speziell vor der Anschaffung von Neugeräten, einer detaillierteren Planung und Integration von Geräten in ein Medizini-

sches IT-Netzwerk. Ein Ziel des Risikomanagements soll es sein die Ausfallzeiten des Medizinischen IT-Netzwerks zu verringern, um somit auch Kosten einsparen zu können.

Inhalt und Zweck einer Verantwortlichkeitsvereinbarung wurde in der IEC 80001-1 klar definiert und aufgelistet. In den Gesprächen wurden ergänzende Inhalte einer Vereinbarung diskutiert. Speziell für die Betreiber eines Medizinischen IT-Netzwerks ergeben sich dadurch neue Wege an relevante Informationen der Hersteller zu kommen. Mit Hilfe einer Verantwortlichkeitsvereinbarung, welche vor Anschaffung von Neugeräten geschlossen werden sollte, können diese Informationen nun eingefordert werden.

Allgemein kristallisierte sich während der Gespräche die Frage nach der Ressourcenplanung heraus. Betreiber eines Medizinischen IT-Netzwerks können schwer abschätzen, welche Kosten für die Umsetzung der IEC 80001-1 entstehen. In erster Linie muss für eine adäquate Umsetzung Know-How für die konkrete Durchführung angeschafft werden. Außerdem würden neben neuen Personalkosten, Lagerkosten für die Dokumentation, auch Kosten für Neuanschaffungen von Geräten aus dem Risikomanagement resultieren. Abhilfe könnten hier zum Beispiel Planungsbüros der Medizin-/Informationstechnik schaffen. Diese könnten während der Planung von zum Beispiel Neugeräten oder Netzwerken, auch die Anfänge des Risikomanagements übernehmen. Außerdem könnten diese Dienstleiter als Berater die Verhandlungen zwischen Betreibern und Medizinprodukt-Hersteller für die Unterzeichnung einer Verantwortlichkeitsvereinbarung koordinieren und leiten. Planungsbüros können auch die Aufgaben des Risikomanagers übernehmen und somit den Betreiber eines Medizinischen IT-Netzwerks entlasten.

Abschließend kann festgestellt werden, dass sich im Zuge dieser Arbeit ein grundlegendes Verständnis zur Umsetzung der IEC 80001-1 beim Betreiber des Medizinischen IT-Netzwerks gebildet hat. Dies ist auf eine professionelle Zusammenarbeit mit vielen aufschlussreichen Gesprächen und Diskussionen mit den Verantwortlichen des Betreibers zurückzuführen. Infolgedessen hat sich bereits ein Aktionsteam in der IT-Abteilung des Krankenhauses gebildet, um an einer Dokumentationsstruktur zu arbeiten. Außerdem ist zu empfehlen die Abteilung Einkauf darauf hinzuweisen, dass vor der Anschaffung von Neugeräten auf die Aspekte der IEC 80001-1 Rücksicht genommen werden muss. Die ersten Schritte zur Einführung der Norm sind somit ausgeführt. Es wird eine Herausforderung für die Zukunft sein, diese Schritte in allgemeingültige Unternehmensprozesse umzusetzen. Bei der generellen Umsetzung sollten Neuanschaffungen von Medizinprodukten und Netzwerkkomponenten bevorzugt zum Anlass genommen werden, die Anforderungen der IEC 80001-1 zu erfüllen.

Literaturverzeichnis:

[1] DIN EN 80001-1 (VDE 0756-1):2011-11: „Anwendung des Risikomanagements für IT-Netzwerke, die Medizinprodukte beinhalten“

[2] Prof. Dr. J. Stettin. : Präsentation „Einführung in die IEC 80001-1“ im Rahmen eines Seminars gehalten am 19.05.2011 in Hamburg

[3] Dipl. Ing. P. Christ: Präsentation „Welche Vorteile bietet die IEC 8000-1? Kontext – Entstehung – Nutzen“ im Rahmen eines Seminars gehalten am 19.05.2011 in Hamburg

[4] Lukas Vogler: Präsentation „Strategien zur Einführung der IEC 80001-1 für Krankenhäuser und Medizinprodukte-Hersteller“ im Rahmen eines Seminars gehalten am 19.05.2011 in Hamburg

[5] IEC/TR 80001-2-1 Ed.1: „Application of risk management for IT-networks incorporating medical devices – Part2-1: Step by step risk management of medical IT-networks; Practical applications and examples” (noch nicht veröffentlicht)

Anhang A:

Involvierte Netzwerkkomponenten der Kardiologischen Ambulanz							
Hersteller	**Typ**	**Lieferdatum**	**Standort**	**Betriebssystem**	**Software**	**Aufgaben**	**Besonderheiten**
Clients							
DELL	Optiplex 760	01.2009	0.3381	Windows XP	siehe Kapitel 5.2.2.2 Tabelle 6	Nachbearbeitung, Befunderstellung	Doppelmonitor
DELL	Optiplex GX620	04.2006	0.3363	Windows XP	siehe Kapitel 5.2.2.2 Tabelle 6	Nachbearbeitung, Befunderstellung	Doppelmonitor
DELL	Optiplex 780	06.2010	0.3364	Windows XP	siehe Kapitel 5.2.2.2 Tabelle 6	Nachbearbeitung, Befunderstellung	
DELL	Optiplex 780	08.2010	0.3364.1	Windows XP	siehe Kapitel 5.2.2.2 Tabelle 6	Nachbearbeitung, Befunderstellung	
DELL	Optiplex 780	08.2010	0.3364.2	Windows XP	siehe Kapitel 5.2.2.2 Tabelle 6	Nachbearbeitung, Befunderstellung	
Server							
DELL	PowerEdge 2950	03.2008	01.2535	Windows 2003 Server	Xcelera R3.2L1	digitales Bildarchiv	
DELL	PowerVault MD3000	03.2008	01.2535			digitales Bildarchiv Speicher	6 Terabyte
DELL	PowerVault MD1000	03.2008	01.2535			digitales Bildarchiv Speicher	
DELL	PowerEdge 2950	06.2007	01.2316	Windows 2003 Server	Windows Dateifreigabe	digitales Bildarchiv Archivserver	
DELL	PowerVault MD1000	06.2007	01.2316		keine sonstige Software	digitales Bildarchiv Archivserver Speicher	
DELL	PowerVault MD1000	06.2007	01.2316			digitales Bildarchiv Archivserver Speicher	30 Terabyte
DELL	PowerVault MD1000	06.2007	01.2316			digitales Bildarchiv Archivserver Speicher	
DELL	PowerEdge 2950	08.2009	01.2316	Windows 2008 Server	Windows Dateifreigabe	digitales Bildarchiv Archivserver	
DELL	PowerVault MD3000	08.2009	01.2316		keine sonstige Software	digitales Bildarchiv Archivserver Speicher	
DELL	PowerVault MD1000	08.2009	01.2316			digitales Bildarchiv Archivserver Speicher	40 Terabyte
DELL	PowerVault MD1000	09.2010	01.2316			digitales Bildarchiv Archivserver Speicher	
DELL	PowerEdge 2950	06.2007	01.3373.08	Windows 2003 Server	Backup Exec 11	digitales Bildarchiv Backupserver	
DELL	MD6020	06.2007	01.3373.08			digitales Bildarchiv Backupserver Library	50 TB
SUN	SPARC M4000	09.2007	01.2535	SunOS 5.10 64 bit Cluster	Oracle 10	KIS Datenbankserver	
SUN	SPARC M4000	09.2007	01.2316	SunOS 5.10 64 bit Cluster	Oracle 10	KIS Datenbankserver	
NetApp	FAS 3140	12.2006	01.2316/01.2535	Ontap 7.3.4	NFS-Freigabe,keine Software	KIS Datenbankspeicher	
DELL	PowerEdge 2950	08.2007	01.2535	Windows 2003 Server	Xcelera Connect R2.1L1	Worklistserver	
DELL	PowerEdge 2950	07.2007	01.2316	vSphere 4 Enterprise	keine Software	Plattform für virtuelle Server	VMWare Server
DELL	PowerEdge 2950	07.2007	01.2535	vSphere 4 Enterprise	keine Software	Plattform für virtuelle Server	VMWare Server
DELL	PowerEdge 2950	11.2008	01.2316	vSphere 4 Enterprise	keine Software	Plattform für virtuelle Server	VMWare Server
DELL	PowerEdge 2950	11.2008	01.2535	vSphere 4 Enterprise	keine Software	Plattform für virtuelle Server	VMWare Server
DELL	PowerEdge 2950	02.2009	01.2316	vSphere 4 Enterprise	keine Software	Plattform für virtuelle Server	VMWare Server
DELL	PowerEdge 2950	02.2009	01.2535	vSphere 4 Enterprise	keine Software	Plattform für virtuelle Server	VMWare Server
virt. Maschine				Windows 2003 Server	Cache for Windows 2010.2.3 (E	HL7 Kommunikationsserver	Kommunikationsserver (Ensemble)
virt. Maschine				Windows 2003 Server	ifc_ris (Eigenentwicklung)	Schicken von Anforderungen im HL7 Forma	Kommunikationsserver (Cardis)
virt. Maschine				Windows 2003 Server	ifc_ris (Eigenentwicklung)	Schicken von Anforderungen im HL7 Forma	Kommunikationsserver (Cardis)
virt. Maschine				Windows 2003 Server	ifc_ris (Eigenentwicklung)	Schicken von Anforderungen im HL7 Forma	Kommunikationsserver (Cardis)
Switches							
Foundry	SuperX	2008	01.3373			Verteiler	Anbindung Clients/Server 1 GB, Switche untereinander 10 GB
Foundry	SuperX	2008	01.2535			Verteiler	Anbindung Clients/Server 1 GB, Switche untereinander 10 GB

Anhang B:

Ultraschallgeräte DHZB

Standort	Kommentar	Typ / Modell	Anschaffung	Hersteller	InventarNr.	Bereich	Abt	Besch.	Alter
OP-Säle (DHZB)	OP	VIVID I (portabel)	29-Jun-06	GE Ultraschall, Deutschland GmbH	0000018317	OP	Anae	2006	4
		3S-RS Probe			0000018317/1	OP	Anae	2006	4
		6Tc-RS TEE Probe Adult			0000018317/2	OP	Anae	2006	4
OP-Säle (DHZB)	OP	VIVID I (portabel)	20-Dec-07	GE Ultraschall, Deutschland GmbH	0000023230	OP	Anae	2007	3
		6Tc-RS TEE Probe Adult			0000023230/2	OP	Anae	2007	3
OP-Säle (DHZB)	OP	VIVID I (portabel)	22-Dec-07	GE Ultraschall, Deutschland GmbH	0000023229	OP	Anae	2007	3
		6Tc-RS TEE Probe Adult			0000023229/2	OP	Anae	2007	3
OP-Säle (DHZB)	OP	VIVID I (portabel)	22-Dec-07	GE Ultraschall, Deutschland GmbH	0000023231	OP	Anae	2007	3
		6Tc-RS TEE Probe Adult			0000023231/2	OP	Anae	2007	3
OP-Säle (DHZB)	***OP***	***VIVID 7***	***01-Oct-04***	***GE Ultraschall, Deutschland Gm***	***0000019701***	***OP***	***Anae***	2004	6
		M3S AMA Sector Probe			*0000019701/1*	*OP*	*Anae*	2004	6
		6T TEE Probe			*0000019701/2*	*OP*	*Anae*	2004	6
		3V Probe			*0000019701/3*	*OP*	*Anae*	2004	6
OP-Säle (DHZB)	OP	VIVID I (portabel)	13-Aug-08	GE Ultraschall, Deutschland GmbH	0000023232	OP	Anae	2008	2
		6Tc-RS TEE Probe Adult			0000023232/2	OP	Anae	2008	2
OP-Säle (DHZB)	OP	VIVID I (portabel)	13-Aug-08	GE Ultraschall, Deutschland GmbH	0000023233	OP	Anae	2008	2
		6Tc-RS TEE Probe Adult			0000023233/2	OP	Anae	2008	2
Anästhesie (DHZB)	***PKH OP***	***SSD 5000 ProSound***	***12-Oct-00***	***ALOKA GmbH, Geschäftsstelle B***	***0000016488***	***OP***	***Anae***	***2000***	10
		UST-5284-2,5			0000016488/3	OP	Anae	***2000***	10
		UST-5293-5 (5,0 MHz)			0000016488/4	OP	Anae	***2000***	10
Chirurgie Allgemein	IPS 2	SSD 5500 Cololor Pro SO	19-Dec-06	ALOKA GmbH	0000018231	IPS	Chir	2006	4
		UST-52101N			0000018231/1	IPS	Chir	2006	4
Chirurgie Allgemein	Dr. Dandel	VIVID 7	28-Oct-05	GE Ultraschall, Deutschland Gm	0000019484	HTX	Chir	2005	5
		3V Probe			0000019484/1	HTX	Chir	2005	5
		M4S Probe			0000019484/2	HTX	Chir	2005	5
		6T-OR TEE Probe			0000019484/3	HTX	Chir	2005	5
PS[illegible]G	H 3	SSD 5000 ProSound Color P	06-May-02	ALOKA GmbH, Geschäftsstelle Be	0000017328	HTX	Chir	2002	8
		UST-9119 60"			0000017328/3	HTX	Chir	2002	8
		UST-5293-5 (5,0 MHz)			0000017328/4	HTX	Chir	2002	8
		UST-5545			0000017328/5	HTX	Chir	2002	8
		UST-5297			0000017328/6	HTX	Chir	2002	8
H8-HTG-Chirurgie		T 3000 (Terason Portable Ult	10-Jan-07	ALOKA GmbH	0000018139	H8	Chir	2007	3
		4C2A curved array transducer			0000018139/1	H8	Chir	2007	3
		12L5 linear array transducer			0000018139/2	H8	Chir	2007	3
		AV2 phased array transducer			0000018139/3	H8	Chir	2007	3
PS1-HTG		SSD-ALPHA 10	18-Nov-09	ALOKA GmbH	0000023442	IPS	Chir	2009	1
		UST-52105			0000023442/1	IPS	Chir	2009	1
		UST-5412			0000023442/2	IPS	Chir	2009	1
		UST-9130			0000023442/3	IPS	Chir	2009	1
PS1-HTG	tragbares Ge	SA600-GER-CHGP	09-Dec-97	SonoAce GmbH, Ultrasound	0000011964	IPS	Chir	1997	13
Kard. Ambulanz	IE33 AMB3	IE 33	20-Dec-05	Philips Medizin Systeme GmbH	0000018590	MVZ	Kard	2005	5
		D5 CWC			0000018590/1	MVZ	Kard	2005	5
		S5-1			0000018591/1	MVZ	Kard	2005	5
		L11-3			0000018592/2	MVZ	Kard	2005	5
		C5-1			0000024059	MVZ	Kard	2005	5
Kard. Ambulanz	IE33 AMB2	IE 33	21-Dec-05	Philips Medizin Systeme GmbH	0000018592	MVZ	Kard	2005	5
		S5-1			0000018592/1	MVZ	Kard	2005	5
Kard. Ambulanz	IE33 AMB1	IE 33	20-Dec-05	Philips Medizin Systeme GmbH	0000018591	MVZ	Kard	2005	5
		L11-3			0000018590/2	MVZ	Kard	2005	5
		S5-1			0000018590/3	MVZ	Kard	2005	5
		S7-2 TEE Transducer			0000018591/2	MVZ	Kard	2005	5
		X3-1			0000018591/3	MVZ	Kard	2005	5
		X7-2 T TEE Transducer			**0000018591/4**	MVZ	Kard	2005	5
Kard. Ambulanz		***Envisor C***	***21-Dec-05***	***Philips Ultraschall***	***0000018593***	MVZ	***Kard***	2005	5
		S4-2			***0000018593/1***	MVZ	***Kard***	2005	5
Forschung Kardiolo		Volumetrics-Modell 1.0	22-Jul-02	Volumetrics Medical Imaging LLC	[illegible]	Forsch	Kard	2002	8
HK 2 (Kinder)	HK	VIVID 7	31-Dec-04	GE Ultraschall, Deutschland Gm	0000018852	HK	Kika	2004	6
	HK	3S Sector Probe			0000018852/1	HK	Kika	2004	6
	HK	7S- 02 Probe			0000018852/2	HK	Kika	2004	6
.2122	Kinder Ambu	VIVID 7	31-Dec-04	GE Ultraschall, Deutschland Gm	0000018849	MVZ	Kika	2004	6
		7S- 02 Probe			0000018849/2	MVZ	Kika	2004	6
		10S Probe without Yoke			0000018849/3	MVZ	Kika	2004	6
.2122	Kinder Ambu	VIVID 7	31-Dec-04	GE Ultraschall, Deutschland Gm	0000018851	MVZ	Kika	2004	6
		6T TEE Probe			0000018851/2	MVZ	Kika	2004	6
H4-AHF		VIVID 7	03-Jan-05	GE Ultraschall, Deutschland Gm	0000018850	Kika	Kika	2005	5
		3S Sector Probe			0000018850/1	Kika	Kika	2005	5
.2207	Kinder IPS	VIVID 7	03-Jan-05	GE Ultraschall, Deutschland Gm	0000018853	KIPS	Kika	2005	5
		3S Sector Probe			0000018853/1	KIPS	Kika	2005	5
		7S- 02 Probe			0000018853/2	KIPS	Kika	2005	5
Kinderkard. Allgem	**tragbares Ge**	**ACUSON**	**19-Dec-05**	**Siemens AG, Medizinische Techr**	**0000018607**	**Kika**	**Kika**	**2005**	5
		3V2c			**0000018607/1**	**Kika**	**Kika**	**2005**	5
Forschung AHF Allg.		VIVID q BT10	20-Aug-10	GE Ultraschall, Deutschland GmbH	0000024215	Forsch	Kika	2010	0
		4C-RS Probe			0000024215/1	Forsch	Kika	2010	0
		8L-RS Probe			0000024215/2	Forsch	Kika	2010	0
		M4S-RS Probe			0000024215/3	Forsch	Kika	2010	0
		6S-RS Phase Array Ped. Probe			0000024215/4	Forsch	Kika	2010	0

Anhang C:

Deutsches Herzzentrum Berlin
Risikomanagement nach IEC 80001-1
Teilnetzwerk: Ultraschall

Risikomanagement des Cardiovaskulären Imaging Systems in der Kardiologischen Ambulanz															
Risikoanalyse						Risikobewertung				Risikobeherrschung					
Nr.	Schutzziel	Gefährdung	Ursache	Gefährdungssituation	Möglicher Schaden	Vorhandene Maßnahmen	S_x	W_x	Risiko	Risikominimierende Maßnahmen	Umsetzung/ Implementierung	Verifizierung	S_x	W_x	Risiko
	Effektivität/ Wirksamkeit														
1		**Einschränkung des klin. Workflows**	Festplattenausfall	Speichern von Daten auf PACS/KIS nicht möglich	Untersuchungen können nur ohne speichern der Daten durchgeführt werden; Befunde können nicht auf KIS gespeichert werden	RAID-5; Cardis-Freitext-Befundung									
2			Virus auf Ultraschallgerät	Verlust an Hardware-Performance; Falsche Bildgebung	Abbruch der Untersuchung	Firewalls; Zentraler Virenscanner									
4			Speicher des Bildarchivs voll	Speichern von Daten auf PACS/KIS nicht möglich	Untersuchungen können nur ohne speichern der Daten durchgeführt werden; Befunde können nicht auf KIS gespeichert werden	Archivspeicher mit 70 TB									
5			zu wenig Lizenzen vorhanden; Anwender lassen Anwendungen gestartet	Software für Untersuchung oder Nachbearbeitung nicht verfügbar	Keine adäquate Untersuchung/Nachbearbeitung möglich		3	2	mittel	Überblick über vorhandene und benötigte Lizenzen verschaffen; Site-License einführen					
6			mangelnde Einweisung/Schulung	Fehlerhafte Bedienung	fehlerhafte Speicherung von Ultraschalldaten im PACS					Schulungen					
7			Anwender	Patientendaten falsch eingetragen	Daten für Untersuchung/Nachbearbeitung nicht vorhanden oder schwer zu finden	Patientendaten inkl. Untersuchungen werden kontrolliert	4	2	mittel	PACS-Abfrage:"Wie viele Untersuchungen konntne nicht eindeutig zugeordnet werden"					
8			Datenpaketverlust			TCP/IP									

]

Risikomanagement des Cardiovaskulären Imaging Systems in der Kardiologischen Ambulanz																
Risikoanalyse						Risikobewertung				Risikobeherrschung						
Nr.	Schutzziel	Gefährdung	Ursache	Gefährdungssituation	Möglicher Schaden	Vorhandene Maßnahmen	S_x	W_x	Risiko	Risikominimierende Maßnahmen	Umsetzung/ Implementierung	Verifizierung	S_x	W_x	Risiko
9		**speziell: Verbindungsabbruch**	PACS Ausfall	Keine Verbindung zum PACS	Keine Speicherung der Untersuchung möglich; Keine Befunderstellung/ Nachbearbeitung möglich	SNMP; Untersuchung/Befund kann per Hand geschrieben werden				Redundanz					
10			KIS-Server Ausfall	Keine Verbindung zum KIS	Patientendaten/Worklists nicht abrufbar; Nur eingeschränkte Untersuchung möglich	SNMP				Redundanz					
11			Switchausfall	Keine Netzwerkverbindung	Untersuchung/Befunderstellung/ Nachbearbeitung nur ohne Daten aus PACS/KIS möglich	Cold-Standby-Geräte									
12			Kabelbruch durch nicht ordnungsgemäße Bewegung der Geräte in Stationen/Ops	Keine Netzwerkverbindung	Untersuchung nur ohne Patientendaten möglich; keine Speicherung der Daten möglich	Patientendaten etc. können per Hand nachgetragen werden	3	2	mittel	Arbeitsanweisungen; Ersatzkabel vor Ort; W LAN					
13			Absturz/Aufhängen von Komponenten	Keine Verbindung zum PACS oder KIS	Untersuchung/Befunderstellung/ Nachbearbeitung nur ohne Daten aus PACS/KIS möglich	SNMP									
14			Defekte Netzbuchse durch nicht ordnungsgemäßes Abstecken des Kabels vor Transport	Keine Verbindung zum PACS oder KIS	Untersuchung/Befunderstellung/ Nachbearbeitung nur ohne Daten aus PACS/KIS möglich	durch gebridgtes Netz, andere Buchse verwendbar									
15			Feuer durch Kurzschluss, Gasleck,Mitarbeiter etc.	Keine Netzwerkverbindung	Untersuchung/Befunderstellung/ Nachbearbeitung nur ohne Daten aus PACS/KIS möglich	Rechnerräume haben Sauerstoffreduktion und sind in anderen Brandschutzbereichen									
16			Wassereinbruch	Keine Netzwerkverbindung	Untersuchung/Befunderstellung/ Nachbearbeitung nur ohne Daten aus PACS/KIS möglich	Auffangschalen unter der Decke									
17			Hohe Luftfeuchtigkeit; Temperatur	Keine Netzwerkverbindung	Untersuchung/Befunderstellung/ Nachbearbeitung nur ohne Daten aus PACS/KIS möglich	Temperaturregulation; Wasserversorgung der Klimanlage redundant									
18			Stromausfall	Keine Netzwerkverbindung	Untersuchung/Befunderstellung/ Nachbearbeitung nur ohne Daten aus PACS/KIS möglich	2 unabhängige Stromversorger; USV; Notstromdiesel									
19			unerwartet hoher Datenaustausch/ zu geringe Bandbreite	Keine/langsame Netzwerkverbindung	Verzögerung von Speichervorgängen oder laden von Daten					?					

]

Risikomanagement des Cardiovaskulären Imaging Systems in der Kardiologischen Ambulanz															
Risikoanalyse						Risikobewertung				Risikobeherrschung					
Nr.	Schutzziel	Gefährdung	Ursache	Gefährdungssituation	Möglicher Schaden	Vorhandene Maßnahmen	S_x	W_x	Risiko	Risikominimierende Maßnahmen	Umsetzung/ Implementierung	Verifizierung	S_x	W_x	Risiko
	Daten -/ Systemsicherheit														
1		**Verlust der Vertraulichkeit von Daten/Systemen**	Hacker	Datenmanipulation	Veränderte Patientendaten könnten bei Befundung verwendet werden	Benutzerkontensteuerung: Nur bestimmte Personen dürfen Daten ändern (ist an Win gekoppelt); Firewalls;				Verschlüsselung der Echo-Daten direkt am Ultraschallgerät					
2			Verschicken von Patientendaten per Mail	Verletzung der Datenschutzbestimmungen	Verlust der Integrität; Strafrechtliche Konsequenzen	automatische Mail-Weiterleitung deaktiviert; Größe des Anhangs beschränkt	1	3	niedrig	Anonymisierung der Patientendaten					
3			Eindringen in Rechnerräume	Diebstahl	Verlust der Integrität; Unautorisierte Verwendung von Daten	Firewalls; Zentraler Virenscanner; RFID-Schlösser für Rechnerreäume inkl. Log-Files				Firewalls zwischen Abteilungen; zwischen logisch getrennten Netzwerken					
4			Viren	Diebstahl	Verlust der Integrität; Unautorisierte Verwendung von Daten	Firewalls nach außen; Zentraler Virenscanner; Virenscan von Patienten-CD's; Internet-Restriktion									
5		**Verlust der Vollständigkeit von Daten**	Anwender	Patientendaten falsch eingetragen	Daten für Untersuchung/Nachbearbeitung nicht vorhanden/schwer zu finden/unvollständig	Patientendaten inkl. Untersuchungen werden kontrolliert	1	3	niedrig	PACS-Abfrage:"Wie viele Untersuchungen konntne nicht eindeutig zugeordnet					
6			Feuer durch Kurzschluss, Gasleck, Mitarbeiter	Datenverlust	Patientendaten/Befunde für Untersuchung/Nachbearbeitung nicht verfügbar	Rechnerräume haben Sauerstoffreduktion und sind in anderen Brandschutzbereichen									
7			Wassereinbruch	Datenverlust	Patientendaten/Befunde für Untersuchung/Nachbearbeitung nicht verfügbar	Auffangschalen unter der Decke									

]

Risikomanagement des Cardiovaskulären Imaging Systems in der Kardiologischen Ambulanz															
Risikoanalyse						Risikobewertung				Risikobeherrschung					
Nr.	Schutzziel	Gefährdung	Ursache	Gefährdungssituation	Möglicher Schaden	Vorhandene Maßnahmen	S_x	W_x	Risiko	Risikominimierende Maßnahmen	Umsetzung/ Implementierung	Verifizierung	S_x	W_x	Risiko
8	**Daten -/ Systemsicherheit**	**Verlust der Vollständigkeit von Daten**	Speicher voll	Datenverlust	zu speichernde Daten können nicht gespeichert werden	Archivspeicher mit 70 TB									
9			Hohe Luftfeuchtigkeit; Temperatur	Datenverlust	Patientendaten/Befunde für Untersuchung/Nachbearbeitung nicht verfügbar	Temperaturregulation; Wasserversorgung der Klimanlage redundant									
10			Stromausfall	Datenverlust	Patientendaten/Befunde für Untersuchung/Nachbearbeitung nicht verfügbar	2 unabhängige Stromversorger; USV; Notstromdiesel									
11				Datenpaketverlust		TCP/IP									
12		**Verlust der Verfügbarkeit von Daten/Systemen**	Verbindungsabbruch (siehe oben)												
	Patienten-sicherheit														
1		Gefährdung des Patienten	Hacker	Datenmanipulation	Veränderte Patientendaten könnten bei Befundung verwendet werden	Benutzerkontensteuerung: Nur bestimmte Personen dürfen Daten ändern (ist an Win gekoppelt); Firewalls;				Verschlüsselung der Echo-Daten direkt am Ultraschallgerät					
2			Viren	Datenmanipulation	Veränderte Patientendaten könnten bei Befundung verwendet werden	Benutzerkontensteuerung: Nur bestimmte Personen dürfen Daten ändern (ist an Win gekoppelt); Firewalls;				Verschlüsselung der Echo-Daten direkt am Ultraschallgerät					
3			Anwender	Patientendaten falsch eingetragen	Daten für Untersuchung/Nachbearbeitung nicht vorhanden/schwer zu finden/unvollständig	Patientendaten inkl. Untersuchungen werden kontrolliert	5	2	hoch	PACS-Abfrage:"Wie viele Untersuchungen konntne nicht eindeutig zugeordnet					
4			Virus auf Ultraschallgerät	Verlust an Hardware-Performance; Falsche Bildgebung	Untersuchungen können durch die Virenbelastung verfälscht werden	Firewalls; Zentraler Virenscanner									

]