Anthea Nadine Haas, BSc

Einbindung elektromedizinischer Geräte in die IT-Infrastruktur von Gesundheitseinrichtungen

Masterarbeit

zur Erlangung des akademischen Titels
Diplom-Ingenieur

Biomedical Engineering
Technische Universität Graz

Betreuer: Assoc.Prof. Dipl.-Ing. Dr.techn. Jörg Schröttner
Institut für Health Care Engineering
Institutsleitung: Univ.-Prof. Dipl.-Ing. Dr.techn. Christian Baumgartner

Bad Goisern, Dezember 2020

EIDESSTATTLICHE ERKLÄRUNG

AFFIDAVIT

Ich erkläre an Eides statt, dass ich die vorliegende Arbeit selbstständig verfasst, andere als die angegebenen Quellen/Hilfsmittel nicht benutzt, und die den benutzten Quellen wörtlich und inhaltlich entnommenen Stellen als solche kenntlich gemacht habe. Das in TUGRAZonline hochgeladene Textdokument ist mit der vorliegenden Masterarbeit/Diplomarbeit/Dissertation identisch.

I declare that I have authored this thesis independently, that I have not used other than the declared sources/resources, and that I have explicitly indicated all material which has been quoted either literally or by content from the sources used.
The text document uploaded to TUGRAZonline is identical to the present master's thesis/diploma thesis/doctoral dissertation.

Datum / Date

Unterschrift / Signature

Die Technische Universität Graz übernimmt mit der Betreuung und Bewertung einer Masterarbeit keine Haftung für die erarbeiteten Ergebnisse: Eine positive Bewertung und Anerkennung (Approbation) einer Arbeit bescheinigt nicht notwendigerweise die vollständige Richtigkeit der Ergebnisse.

Danksagung

Danke an meine Schwester Selina, welche bei Höhen mit mir gefeiert und mich bei Tiefen getröstet hat. Danke für die schönen und lustigen Jahre in der gemeinsamen WG, danke dass du mich stets motiviert hast und mir immer zur Seite stehst.

Ich möchte auch meinem Mann Marko danken, mit dem ich gemeinsam durch das Studium gegangen bin. Danke, dass du das gesamte Studium für mich da warst, dir immer meine Probleme angehört und meine Launen ertragen hast und mich auch manchmal, wenn es nötig war, gepusht hast.

Vor allem danke ich meinen Eltern, die mich von Anfang bis zum Schluss immer unterstützt haben, mir Mut gemacht und an mich geglaubt haben. Ohne eure Unterstützung wäre mein gesamtes Studium nicht möglich gewesen.

Kurzfassung

Ziel dieser Arbeit ist es, eine Art „best-practice“-Verfahren aufzuzeigen, dass alle relevanten Normen berücksichtigt, um die Einbindung von Medizingeräten in ein IT-Netzwerk in Gesundheitseinrichtungen durchzuführen.
Hierzu wurde zu Beginn dieser Arbeit zum einen eine Normenrecherche und zum anderen eine Literaturrecherche zu dieser Thematik durchgeführt. Daraus wurde in den Ergebnissen ein Flussdiagramm für den Einbindungsprozess erstellt.
Von großer Bedeutung für einen geregelten Einbindungsprozess ist ein strukturierter Ablauf von einzelnen Prozessschritten. Die wichtigsten Punkte hierbei sind eine normengerechte Durchführung eines Risikomanagementprozesses und eine genaue Festlegung der Verantwortlichkeiten und Aufgabenbereiche. Durch einen standardisierten Einbindungsprozess und die Mitarbeit aller beteiligten Berufsgruppen kann man ein bestmögliches Ergebnis erzielen, bei dem möglichst alle Risiken erkannt und minimiert werden.
Die MDR verpflichtet den Betreiber zwar dazu, geeignete Überwachungsmaßnahmen, bei der Zusammenstellung von Medizinprodukten zu einer Behandlungseinheit, anzuwenden, jedoch gibt es keine genauen Vorgaben welche und wie diese zu handhaben sind, dadurch hat jeder Betreiber selbst für die Einführung und Umsetzung eines geregelten Einbindungsprozess zu sorgen.

Keywords: EN 80001, Med-IT-Risikomanager, Risikomanagementprozess, wiederkehrende sicherheitstechnische Prüfung

Abstract

The aim of this work is to show a kind of "best-practice" procedure that complies with all relevant standards to integrate medical devices into an IT network in healthcare facilities.
At the beginning of this work, standards research and literature research on this topic were carried out. With this basis, a flowchart for the integration process was created.
A structured sequence of individual process steps is of great importance for a regulated integration process. The most important points here are a standard-compliant implementation of a risk management process and a precise definition of the area of responsibility. Through a standardized integration process and the cooperation of all professional groups involved, the best possible result can be achieved in which all risks are identified and minimized as far as possible.
Although the MDR obliges the operator to use suitable monitoring measures when combining medical devices into a medical system, there are no precise specifications as to which and how these are to be handled, so each operator is responsible for the introduction and implementation of a regulated integration process to care.

Keywords: EN 80001, Med-IT-Risk-Manager, risk management process, periodic technical safety test

Inhaltsverzeichnis

Abkürzungen

BASG	Bundesamt für Sicherheit im Gesundheitswesen
CT	Computertomografie
DICOM	Digital Imaging and Communications in Medicine
DSGVO	Datenschutz-Grundverordnung
FMEA	Fehlermöglichkeits- und -einflussanalyse (Failure Mode and Effect Analysis)
FTA	Fehlerbaumanalyse (Fault Tree Analysis)
HACCP	Hazard Analysis on Critical Control Points
HAZOP	Hazard and Operability
HL7	Health Level 7
IVD	In-vitro-Diagnostik
KIS	Krankenhausinformationssystem
LAN	Local Area Network
ME-System	medizinisches elektrisches System
MDR	Medizinprodukteverordnung (medical device regulation)
MPBV	Medizinprodukte-Betreiberverordnung
MPG	Medizinproduktegesetz
MTK	messtechnische Kontrolle
PACS	Picture Archiving and Communication System
PHA	Vorläufige Gefährdungsanalyse (Preliminary Hazard Analysis)
PSA	Persönliche Schutzausrüstung
RPZ	Risikoprioritätszahl
SDC	Service-oriented Device Connectivity
TSB	Technischer Sicherheitsbeauftragter
WLAN	Wireless Local Area Network
wSTP	wiederkehrende sicherheitstechnische Prüfung

1 Einleitung

Die zunehmende Digitalisierung unserer Gesellschaft macht auch vor der Medizintechnik-Branche keinen Halt. Es ist nicht von der Hand zu weisen, dass die Anzahl der Medizingeräte in den letzten Jahrzehnten stark angestiegen ist.
Laut Bundesamt für Sicherheit im Gesundheitswesen (BASG) wird die Anzahl der unterschiedlichen sich am Markt befindlichen Medizinproduktetypen in Europa zwischen 500.000 und einer Million geschätzt. Dazu zählen zwar neben den elektromedizinischen Geräten auch Gebrauchsartikel, wie Verbandsmaterialien und Pflaster, diagnostische Tests, Laborgeräte, usw., trotzdem kann man bei der enormen Anzahl der Medizinprodukte am Markt, den Anteil der elektromedizinischen Geräte erahnen. [1]

Eine Prognose von Statista zeigt die Umsatzentwicklung der Medizintechnikindustrie von 2005 – 2024. Laut dieser Vorhersage steigt der Gesamtumsatz in dieser Branche von 219 Milliarden US Dollar im Jahr 2005 auf 594,5 Milliarden US Dollar im Jahr 2024 weltweit. [2] Das entspricht einer Steigerung um 171,5% innerhalb von 20 Jahren. Diese Zahlen verdeutlichen den imposanten Anstieg an Medizingeräten am Markt. Dazu kommt, dass die Anzahl der einzelnen Medizingeräte, die miteinander verbunden und somit zu einem Netzwerk werden, zunimmt. Diese sogenannten medizinischen IT-Netzwerke werden auch in Zukunft immer komplexer und die Risikobeherrschung wird kaum noch zu bewältigen sein.
Es ergeben sich zahlreiche Probleme bei der Einbindung von Medizingeräten in ein bestehendes IT-Netzwerk. Angefangen bei der Interoperabilität der einzelnen Komponenten, über einen möglichen Ausfall und die Gefahr eines daraus resultierenden Datenverlustes oder Verzögerungen bei der Datenweiterleitung bis hin zur Angreifbarkeit eines medizinischen Netzwerks und der Gewährleistung des Datenschutzes.
Die Herausforderung der Gesundheitseinrichtungen besteht hierbei, eine sichere Einbindung von Medizingeräten in die IT-Infrastruktur gewährleisten zu können. Dies ist ohne die Einführung eines geeigneten Risikomanagements nicht möglich.

1.1 Begriffsdefinitionen

Im Folgenden werden einige für diese Masterarbeit relevante Begriffe definiert. Diese Definitionen stammen in erster Linie von facheinschlägigen Normen.

Medizinprodukt: Zu einem Medizinprodukte zählen alle Geräte, welche vom Hersteller für eine der folgenden Anwendungen bestimmt sind:

- Zur Erkennung, Prävention, Überwachung oder Linderung von Krankheiten, Verletzungen oder Behinderungen
- Zur Untersuchung oder Unterstützung des anatomischen Aufbaus oder physiologischer Vorgänge
- Zur Empfängnisverhütung
- Zur Desinfektion jeglicher Medizinprodukte
- Zur In-vitro-Untersuchung von menschlichen Proben

Außerdem darf die Hauptwirkung eines Medizinproduktes nicht pharmakologisch, immunologisch oder metabolisch sein. [3]

IT-Netzwerk: Ein IT-Netzwerk ist ein System, welches über Kommunikationsknoten und Leitungen oder drahtlosen Verbindungen Übertragungen ermöglicht. [4]

Medizinisches IT-Netzwerk: Wenn ein IT-Netzwerk mindestens ein Medizinprodukt enthält, wird daraus ein medizinisches IT-Netzwerk. [4]

Medizinisches elektrisches Gerät: Ein medizinisches elektrisches Gerät (ME-Gerät) hat eine medizinische Zweckbestimmung und besitzt entweder einen Anwendungsteil oder überträgt Energie von bzw. zu einem Patienten. [5]

Medizinisches elektrisches System: Sind mehrere Geräte über eine Funktionsverbindung oder über eine Mehrfachsteckdose zusammengeschlossen, wobei mindestens ein Gerät davon ein medizinisches elektrisches Gerät sein muss, spricht man von einem medizinischen elektrischen System (ME-System). [5]

Risiko: Das Risiko ergibt sich aus der Wahrscheinlichkeit des Auftretens eines Schadens und dessen Schweregrad. [6]

Rest-Risiko: Als Rest-Risiko bezeichnet man das Risiko, welches nach Durchführung aller Maßnahmen zur Risikobeherrschung noch verbleibt. [6]

Schaden: Als Schaden kann man die Schädigung von menschlicher Gesundheit, von materiellen Gütern oder der Umwelt bezeichnen. [6]

Gefährdung: Eine mögliche Schadensquelle nennt man Gefährdung. [6]

Gefährdungssituation: Eine Gefährdungssituation ergibt sich daraus, wenn Personen, Güter oder die Umwelt Gefährdungen ausgesetzt sind. [6]

Lebenszyklus: Im Zusammenhang dieser Masterarbeit, umfasst der Begriff Lebenszyklus alle Phasen eines Medizinproduktes, welche im Laufe seines Lebens durchlaufen werden, von der Planung und Herstellung bis hin zur Außerbetriebnahme und Entsorgung. [6]

Hersteller: Als Hersteller zählt jene natürliche oder juristische Person, welche für die Herstellung eines Medizinproduktes die Verantwortung übernimmt und unter deren Namen das Medizinprodukt bereitgestellt wird. [3]

Risikomanagement: Um ein Risikomanagement durchzuführen werden Managementstrategien und -verfahren systematisch angewendet, um Risiken zu analysieren, zu bewerten, zu beherrschen und zu überwachen. [6]

1.2 Schutzziele

Ein medizinisches IT-Netzwerk muss Personensicherheit und Funktionalität gewährleisten, doch was bedeutet das konkret? Um ein sicheres IT-Netzwerk zu definieren, kann man folgende Schutzziele festlegen:

- Sicherheit
- Effektivität
- Daten- und Systemschutz [4]

Beim Betrieb eines medizinischen IT-Netzwerks muss als erstes sichergestellt werden, dass es zu keinen unvertretbaren Risiken kommt. Dazu zählen sowohl Interaktionen mit anderen Geräten oder Software, als auch vorhersehbarer Missbrauch oder Irrtum. Zu den zu schützenden Personen zählen Patienten, Anwender und Dritte, wobei hiermit auch die Sicherheit von materiellen Gütern und der Umwelt miteinbezogen werden soll.
Zum anderen spielt die Effektivität eine große Rolle. D.h. die Funktion und Leistungsfähigkeit des Medizingeräts darf nicht durch das IT-Netzwerk oder durch andere Geräte oder Software beeinträchtigt werden. Hierzu können medizinische Netzwerke, je nach Kritikalität, in verschiedene Klassen eingeteilt werden, um eine Hierarchie aufstellen zu können, wo die Daten am dringendsten benötigt werden.
Auch nicht zu vernachlässigen ist der letzte Punkt, der Daten- und Systemschutz. Vor allem für gesundheits- und personenbezogene Daten gilt das höchste Maß an Vertraulichkeit. Bei der Einbindung von Geräten in ein IT-System muss darauf geachtet werden, dass es keine ungesicherten Schnittstellen gibt. Außerdem müssen die Daten auch jederzeit innerhalb des Netzwerks zur Verfügung stehen und abrufbar sein. Bei diesem Schutzziel müssen selbstverständlich auch alle Anforderungen, welche die Datenschutz-Grundverordnung (DSGVO) stellt, erfüllt werden. [7]

Die Verantwortlichkeiten liegen hierbei zum einen beim Hersteller, welcher unter Einhaltung des Medizinproduktegesetzes (MPG), für einen sicheren Aufbau des Medizinproduktes verantwortlich ist. Außerdem wird in diversen Normen schon bei der Herstellung die Durchführung eines Qualitäts- und eines Risikomanagementprozesses gefordert. Sicherheitsrelevante Angaben müssen in den Begleitpapieren dokumentiert sein.

Zum anderen muss der Betreiber der Gesundheitseinrichtung den fehlerfreien Betrieb sicherstellen, unter Berücksichtigung anderer Medizinprodukte, Netzwerke, Software und Schnittstellen. Dazu muss bei Einbindung eines neuen Medizingerätes in das bestehende IT-Netzwerk ein Risikomanagement durchgeführt werden.

Im Zuge der Risikoanalyse müssen alle möglich auftretenden Gefährdungen eruiert werden, die verschiedenen Methoden dazu werden in Kapitel 1.4 erläutert. In Anhang E der Norm DIN EN ISO 14971 ist eine Übersicht von Bespielen für Gefährdungen angeführt, welche helfen kann, möglichst alle Situationen abzudecken. Dazu zählen Gefährdungen durch Energie, ob mechanische, thermische, elektromagnetische oder Strahlungsenergie, biologische oder chemische Gefährdungen, Gefährdungen durch den laufenden Betrieb, also Fehler bei der Anwendung oder Funktionsfehler und Gefährdungen durch fälschliche, unzureichende oder zu komplizierte Informationen bei der Gebrauchsanweisung oder bei Hinweisen am Gerät selbst. [6]

1.3 Gesetzliche und normative Grundlagen

Um einen Überblick über die unzähligen Normen und Gesetzestexte zu schaffen, werden in diesem Kapitel jene Normen vorgestellt, auf welche in der vorliegenden Masterarbeit Bezug genommen wird.

DIN EN 80001

Die bedeutendste Norm für diese Thematik ist die DIN EN 80001, welche die Anwendung eines Risikomanagements für IT-Netzwerke, welche Medizingeräte beinhalten, beschreibt. In Teil 1 dieser Norm werden vor allem die Verantwortlichkeiten der einzelnen Parteien und deren Aufgaben definiert. [4]

Die Gesundheitseinrichtung trägt die Gesamtverantwortung für den Risikomanagementprozess, von der Planung über die Umsetzung bis hin zur Außerbetriebnahme, über den gesamten Lebenszyklus eines medizinischen IT-Netzwerkes hinweg. Zu den Aufgaben der obersten Leitung zählen die Erstellung von Richtlinien für das Risikomanagement und für die Bewertung der Vertretbarkeit von Risiken, die Bereitstellung aller notwenigen Ressourcen und qualifiziertem Personal und die Dokumentation aller Ergebnisse in der Risikomanagement-Akte. [4]

Außerdem muss die oberste Leitung laut DIN EN 80001 einen Med-IT-Risikomanager benennen, welcher für die Durchführung des Risikomanagementprozesses die Verantwortung trägt, auch wenn verschieden Aufgaben an andere übertragen werden können. Der Med-IT-Risikomanager dient als Schnittstelle zwischen allen Teilnehmern am Prozess und koordiniert die Zusammenarbeit zwischen allen Parteien, von hausinternen Personen bis hin zu externen Teilnehmern. Zum internen Teilnehmerkreis am Risikomanagementprozess zählen Medizintechniker, Mitarbeiter der IT-Abteilung in der Gesundheitseinrichtung und die Anwender der elektromedizinischen Geräte, die in die IT-Infrastruktur eingebunden werden sollen. Zu den externen Mitgliedern zählen vor allem die Hersteller der Medizinprodukte und die Lieferanten dieser, anderer IT-Geräte oder Software. [4]

Die Aufgaben eines Med-IT-Risikomanagers beginnen bei der Planung der Einbindung von Medizingeräten in die bestehende IT-Infrastruktur. Hierbei müssen alle erforderlichen Unterlagen gesammelt und die Herstellerangaben mit den Richtlinien der Gesundheitseinrichtung vereint werden. Anschließend muss ein Risikomanagementprozess durchgeführt werden. Diese Schritte gelten auch für

jegliche Änderungen von medizinischen Netzwerken oder darin beinhaltete Medizingeräte. Dabei entdeckte unvertretbare Risiken müssen der verantwortlichen Organisation gemeldet werden. [4]

Für Medizingeräte, welche in ein medizinisches IT-Netzwerk eingebunden werden können, müssen laut DIN EN 80001 vom Hersteller Begleitpapiere bereitgestellt werden. Diese müssen unter anderem den Einbindungszweck, die Leistungskriterien des Netzwerkes in das eingebunden wird, die Daten, welche dafür vorgesehen sind zwischen dem Medizingerät und dem IT-Netzwerk zu fließen und eine Liste von möglich auftretenden Risiken, wenn erforderlichen Maßnahmen nicht erfüllt werden können, beinhalten. Dies wird auch in der DIN EN 60601-1 [5] so gefordert. Anbieter von anderen IT-Technologien, welche keine Medizinprodukte darstellen, können sämtliche erforderlichen Unterlagen, zu technischen Eigenschaften, Inkompatibilitäten und ähnliches zur Verfügung stellen, jedoch wird dies von dieser Norm nicht gefordert. Auf Anfrage der verantwortlichen Organisation hin, muss der Anbieter hingegen die ergänzenden Informationen bereitstellen. [4]

Das Risikomanagement beinhaltet folgende drei Hauptprozesse:

- Risikoanalyse, bei der das Ziel lautet, alle möglichen Risiken zu identifizieren
- Risikobewertung, bei der entschieden wird, ob das Risiko vertretbar ist
- Risikobeherrschung, bei der festgestellt wird, ob Maßnahmen zur Risikominderung existieren und ob das Restrisiko vertretbar ist

Um diese Prozesse abarbeiten zu können, werden von der verantwortlichen Organisation Unterlagen, wie eine Auflistung der risikorelevanten Elemente, also die Daten aller relevanten Komponenten und Software des medizinischen IT-Netzwerks, die Dokumente des medizinischen IT-Netzwerks, wie die Netzwerkkonfiguration, die Zuverlässigkeit des Netzwerks, die Datenintegrität usw. und ein Risikomanagementplan, der Tätigkeiten, Verantwortlichkeiten, die vorgesehene Verwendung, den Personenkreis, welcher über Risiken informiert werden muss und Kriterien für die Risikovertretbarkeit, definiert, bereitgestellt. [4]

Die DIN EN 80001 besagt, dass sowohl jede Neueinbindung eines Medizingerätes in ein medizinisches IT-Netzwerk, als auch jede Änderung an einem Medizingerät innerhalb eines medizinischen IT-Netzwerks bzw. am medizinischen IT-Netzwerk selbst, ein Projekt darstellt, einen Risikomanagementprozess durchlaufen muss. Eine Ausnahme bilden sogenannte Routine-Änderungen, welche unter vertretbarem Risiko

die Bedingungen nur minimal ändern. Für diese Art von Änderungen kann die verantwortliche Organisation eine Änderungserlaubnis aussprechen. [4]
Nachdem der Risikomanagementprozess erfolgreich durchlaufen ist, muss der Med-IT-Risikomanager vor dem Start in den Echtbetrieb, nach einer abschließenden zusammenfassenden Untersuchung, nur noch das medizinische IT-Netzwerk freigeben. Teil des Risikomanagements ist auch die Überwachung über den gesamten Lebenszyklus und die Dokumentation der identifizierten Risiken, deren Bewertung und Beherrschung in der Risikomanagement-Akte. [4]

Medizinprodukte-Betreiberverordnung

Diese Verordnung, welche seit 1. April 2007 gilt, richtet sich an die Betreiber von Gesundheitseinrichtungen und thematisiert die Errichtung, Anwendung, Instandhaltung und das Betreiben von Medizinprodukten. Grundsätzlich trägt der Betreiber die Verantwortung für den sicheren Betrieb innerhalb der Gesundheitseinrichtung. [8]
Die Aufgaben starten bereits bei der Lieferung eines neuen Medizingerätes. Bei allen Geräten, welche in Anhang 1 der MPBV bestimmt sind und welche der Technische Sicherheitsbeauftragte (TSB) bestimmt, ist der Betreiber dafür verantwortlich, dass eine Eingangsprüfung im Umfang einer wiederkehrenden sicherheitstechnischen Prüfung (wSTP) durchgeführt wird. Mit Ausnahme von Geräten, welche bei der Lieferung ein Prüfprotokoll des Herstellers oder des Lieferanten beinhalten, hierbei reicht eine Kontrolle auf mögliche Schäden beim Transport. [8]
Außerdem muss der Betreiber sicherstellen, dass alle Mitarbeiter, welche ein Medizinprodukt verwenden, in die sachgerechte Anwendung eingeschult werden, sofern nicht davon ausgegangen werden kann, dass sie aufgrund ihrer Ausbildung oder Erfahrung die Handhabung des Medizingerätes beherrschen. Diese Einweisung muss für Geräte, welche vom TSB bestimmt werden und für Geräte nach Anhang 1 typenbezogen dokumentiert werden. Bei der Dokumentation müssen die eingewiesene Person und das Medizingerät, auf das eingewiesen wurde, klar identifizierbar sein. Bei Sicherheitsvorfällen oder bei Grund zur Annahme, dass eine Einweisung wiederholt werden sollte, hat der Betreiber für eine wiederkehrende Schulung zu sorgen.

Der Betreiber hat auch dafür Sorge zu tragen, dass regelmäßig eine ordnungsgemäße Instandsetzung laut Herstellerangaben erfolgt, ohne dabei die Sicherheit aller Beteiligten zu gefährden. [8]

Bei allen nicht implantierbaren Medizinprodukten muss regelmäßig eine wSTP durchgeführt werden, wobei immer die Herstellerangaben erfüllt werden müssen. Wenn keine Angaben des Herstellers existieren, muss die Überprüfung nach dem Stand der Technik erfolgen. Diese wSTP darf nur von qualifizierten Personen durchgeführt werden, die Anforderungen sind in der MPBV in Anhang 3 definiert. Ergebnisse der Überprüfung müssen in einem Protokoll festgehalten werden, welches auch Informationen wie Name des Prüfers, Datum und eine Beurteilung der Prüfung beinhalten muss. Der Betreiber hat dafür zu sorgen, dass dieses Prüfprotokoll in der Gerätedatei jederzeit zugänglich aufbewahrt wird. Intervalle sind laut den Herstellerangaben einzuhalten, legt dieser kein Intervall fest, kann eine fachlich geeignete Person dieses bestimmen. Für messtechnische Kontrollen (MTK) gelten ähnliche Bestimmungen. Medizinprodukte, welche einer MTK unterzogen werden müssen, sind in der MPBV in Anhang 2 beschrieben, inklusive deren Intervalle, wenn die Herstellerangaben entfallen. [8]

Die schon erwähnte Gerätedatei muss alle Geräte, welche einer wSTP oder einer MTK unterzogen werden müssen, beinhalten. Angaben wie gerätebezogene Daten zur Identifizierung des Medizingerätes, Datum und Umfang von Eingangsprüfung, wSTP, MTK, Instandsetzung und Informationen zu Zwischenfällen stellen den Inhalt der Gerätedatei dar. Die Art der Aufbewahrung ist dem Betreiber freigestellt, unter der Bedingung, dass die Daten jederzeit zugänglich und abrufbar sind, bis 5 Jahre nach der Außerbetriebnahme. [8]

Das Bestandsverzeichnis kann gemeinsam mit der Gerätedatei geführt werden und beinhaltet Daten aller aktiven Medizinprodukte, welche in der Gesundheitseinrichtung verwendet werden. Aufgezeichnet werden Informationen wie Type, Seriennummer, Jahr der Herstellung und Name und Adresse des Herstellers und des Vertreibers. Auch der Standort des Medizinproduktes bzw. die zugeordnete Abteilung werden dokumentiert. Wie die Gerätedatei muss die Verfügbarkeit und Zugänglichkeit des Bestandsverzeichnisses sichergestellt werden, ob in Papierform oder digital wird dem Betreiber wiederum freigestellt. [8]

Medizinproduktegesetz

Das Medizinproduktegesetz trat 1998 in Kraft und regelt sämtliche Aktivitäten, welche in Zusammenhang mit einem Medizinprodukt stehen. Diese starten bei der Herstellung, gehen über den Vertrieb bis hin zur Überwachung und Instandhaltung über den gesamten Lebenszyklus, immer mit dem Ziel die Sicherheit und Qualität zu gewährleisten. [9]

Medizinprodukte müssen so herstellt werden, dass bei ihrer Anwendung die Sicherheit von Patienten, Anwendern und von Dritten nicht gefährdet wird. Mögliche Risiken, welche bei bestimmungsgemäßem Gebrauch auftreten können, müssen in Abstimmung mit dem Nutzen des Medizinproduktes vertretbar sein und die Gesundheit muss dabei immer im Vordergrund stehen und geschützt werden. Die Risiken müssen durch den Aufbau des Medizinproduktes weitestgehend reduziert werden. Für die restlichen Risiken, welche durch die Konstruktion nicht abgewendet werden können, sind bei der Produktion Alarm- bzw. Schutzvorrichtungen vorzusehen. Über alle Restrisiken müssen die Anwender informiert werden. [9]

Medizinprodukte müssen mit einem CE-Kennzeichen versehen werden, dies ist aber nur nach positiv erfolgter Konformitätsbewertung möglich und wenn alle geltenden Anforderungen und Vorschriften bei der Herstellung erfüllt wurden. [9]

Das MPG regelt auch die Registrierung von Herstellern, Prüfeinrichtungen und Betreibern von bestimmten Medizinprodukten, wie aktiv implantierbare Medizinprodukte und Medizinprodukte der Risikoklasse 2a oder höher. Form und Inhalt der Meldungen werden vom Gesundheitsminister bestimmt. Jegliche Einrichtungen, welche aufgrund ihres Gewerbes mit Medizinprodukten hantieren, sei es zur Herstellung, Prüfung, Lagerung, Reinigung oder zum Transport, können von beauftragten Sachverständigen kontrolliert und überwacht werden. Bei Identifizierung von Zwischenfällen im Zuge der beruflichen Tätigkeit, wie Mängel an einem Medizinprodukt, Fehlfunktionen oder bisher unbekannte Wechselwirkungen, haben Angehörige von Gesundheitsberufen diese Informationen unverzüglich dem BASG weiterzuleiten, welches bei begründetem Verdacht die jeweiligen Fälle bewertet und erforderlichenfalls Maßnahmen einleitet. [9]

Medizinprodukteverordnung (MDR, medical device regulation)

Am 25.02.2017 publizierten das europäische Parlament und der Rat die neue MDR, welche am 04.04.2017 vom EU-Parlament verabschiedet wurde. Ursprünglich sollte die MDR am zwanzigsten Tag nach ihrer Veröffentlichung in Kraft treten und ab dem 26.05.2020 gelten. Aufgrund der im Jahr 2020 auftretenden COVID-19-Pandemie wurde der Geltungsbeginn um genau ein Jahr auf den 26.05.2021 verschoben. [10]

Diese neue Medizinprodukteverordnung löst die 93/42/EWG [11] Richtlinie des Jahres 1993 ab, welche zuletzt 2007 geändert wurde und kombiniert diese mit der Richtlinie 90/385/EWG [12] für aktive implantierbare Medizinprodukte.

Ziele der neuen Medizinprodukteverordnung sind ein hohes Maß an Sicherheit und Gesundheitsschutz zu garantieren und Transparenz, Nachhaltigkeit und Innovationen zu fördern. Außerdem wird ein international hoher Standard für Qualität und Sicherheit von Medizinprodukten und eine vorbildliche internationale Zusammenarbeit angestrebt. [10]

Um eine Standardisierung zu erreichen, wurde das UDI-System (Unique Device Identification System) eingeführt, welches verpflichtend für alle neu produzierten bzw. für alle neu in Verkehr gebrachten Medizinprodukte, mit Ausnahme von Sonderanfertigungen, zu verwenden ist. Je nach Produktklasse startet diese Verpflichtung zwischen einem und fünf Jahren nach Geltungsbeginn dieser neuen Medizinprodukteverordnung. Durch dieses System sollen die Rückverfolgbarkeit von Produkten, die Effektivität, die Meldung von besonderen Vorkommnissen und die behördliche Überwachung verbessert werden. Außerdem soll dadurch das Inverkehrbringen von Fälschungen reduziert werden. [10]

Dieses neu eingeführte UDI-System beinhaltet eine eigene UDI-Produktkennung, die UDI-DI (Unique Device Identification - Device Identifier) und eine UDI-Herstellungskennung, die UDI-PI (Unique Device Identification – Production Identifier). Auf jedem Medizinprodukt und dessen Verpackung muss eine UDI-Nummer platziert werden, welche unter anderem Informationen wie die Menge pro Packung, Name und Adresse des Herstellers, die Seriennummer und die Risikoklasse beinhaltet. Vertrauliche geschäftliche Informationen werden nicht in der UDI-Datenbank gespeichert. Die gesammelten Daten müssen validiert werden und öffentlich unentgeltlich zugänglich sein. Um die internationale Zusammenarbeit, die Transparenz und die Zugänglichkeit der Produktinformationen für die Öffentlichkeit zu verbessern wird die Eudamed (Europäische Datenbank für Medizinprodukte) erweitert. [10]

Die Nomenklatur wird den Herstellern und juristischen Personen kostenfrei bereitgestellt, um die Handhabung der Datenbank zu erleichtern und eine Vereinheitlichung der Daten zu erreichen. Die Eudamed beinhaltet die UDI-Datenbank, das elektronische System für die Registrierung von Produkten und Wirtschaftsakteuren, für Benannte Stellen und Bescheinigungen, für klinische Prüfungen, für Vigilanz, für die Überwachung nach dem Inverkehrbringen und für die Marktüberwachung. [10]

In der Eudamed-Datenbank gibt es zwei Bereiche: einen Bereich, in dem alle erfassten Daten von der Kommission und den Mitgliedstaaten abgefragt werden können und einen für die Öffentlichkeit zugänglichen Bereich, in dem nur ausgewählte Daten ersichtlich sind. Die Kommission hat dafür zu sorgen, dass dieser Bereich benutzerfreundlich und übersichtlich gestaltet wird. Die Datenbank enthält personenbezogene Daten, nur in dem Ausmaß, in dem sie für die Bearbeitung benötigt werden. Die Patienten haben jederzeit das Recht, in die Daten einzusehen, diese zu ändern oder zu löschen. [10]

Ein weiterer wichtiger Punkt, welcher in der MDR geregelt ist, ist die Gewährleistung einer sicheren Interaktion von Medizinprodukten mit ihrer Umgebung.

Es muss sichergestellt werden, dass mögliche Kombinationen von Produkten keine Sicherheitsrisiken bürgen. Auch negative Wechselwirkungen von Medizinprodukten mit der IT-Umgebung müssen laut Anhang 1 Absatz 14 vermieden bzw. so weit wie möglich minimiert werden. Außerdem müssen laut Artikel 22 bei der Zusammenstellung von medizinischen Systemen geeignete Methoden zur Überwachung und Überprüfung dieser angewendet werden. [10]

DIN EN 60601-1

In dieser Norm werden unter anderem elektrische und mechanische Sicherheitsmerkmale von Medizingeräten, deren Kennzeichnungen und Warnhinweise, sowie die elektromagnetische Verträglichkeit geregelt. Sie bezieht sich vor allem auf die Herstellung von Medizinprodukten und deren Erstprüfung. [5]

Es wird die Anforderung gestellt, dass der Hersteller ein Risikomanagement einzuführen hat. Im Zuge des Risikomanagementprozesses muss die Eintrittswahrscheinlichkeit und das Ausmaß der Folgen der Gefährdungen abgeschätzt und Maßnahmen zur Minimierung des Risikos unternommen werden. Nach der Durchführung der Risikobeherrschung muss die Vertretbarkeit der

Restrisiken bewertet werden. Vorbild ist hierbei die Norm ISO 14971, welche untenstehend kurz beschrieben wird, wobei der Risikomanagementprozess in der DIN EN 60601-1 nicht so umfangreich gefordert wird. [5]
Außerdem wird gefordert, dass der Hersteller bei Medizinprodukten, welche in ein IT-Netzwerk eingebunden werden können, die dadurch entstehenden Risiken mitberücksichtigt und in den Risikomanagementprozess miteinbezieht. Außerdem muss er Informationen und Anweisungen zur Einbindung in ein IT-Netzwerk bereitstellen, diese wurden obenstehend unter der DIN EN 80001 schon erläutert.
Die verantwortliche Organisation muss vom Hersteller dazu angewiesen werden ein Risikomanagement, mit Identifikation, Analyse, Bewertung und Beherrschung der Risiken, durchzuführen. [5]

ÖVE/ÖNORM EN 62353

Diese Norm bezieht sich auf wiederkehrende Prüfungen von medizinisch elektrischen Geräten. Dabei wird auf die genaue Prüffolge und auf die verschiedenen Messungen eingegangen, welche bei einer Wiederholungsprüfung, bei einer Prüfung vor Inbetriebnahme und nach Instandsetzung, durchzuführen sind. [13]
Für die Thematik der Einbindung elektromedizinischer Medizingeräte in ein IT-Netzwerk ist die Messung von medizinischen elektrischen Systemen (ME-Systemen) relevant. Die Definition von einem ME-System ist in Kapitel 1.1 angeführt. Die EN 62353 besagt, dass innerhalb eines ME-Systems sowohl jedes Gerät, welches über einen Netzanschluss verfügt, extra geprüft bzw. gemessen werden muss, als auch die Gesamteinheit des Systems. Auch bei medizinisch elektrischen Geräten eines ME-Systems, welche über eine Funktionsverbindung miteinander verbunden sind, muss der Schutzleiterwiderstand einzeln gemessen werden. [13]
Ein weiterer wesentlicher Punkt dieser Norm ist die Tatsache, dass diejenige Person, welche ein ME-System zusammenstellt oder wesentliche Veränderungen an einem ME-System vornimmt, zum Hersteller wird und somit die Verantwortung übernimmt und Messvorgaben festlegen muss. [13]

DIN EN ISO 14971

Die DIN EN ISO 14971 beschreibt die Anwendung eines Risikomanagements auf Medizinprodukte. Ziel ist es schon bei der Herstellung alle Risiken, welche mit einem Medizinprodukt einhergehen, zu identifizieren, zu bewerten, zu minimieren und über den gesamten Lebenszyklus zu beherrschen, um ein bestmögliches Nutzen-Risiko-Verhältnis zu erreichen. [6]

Die Risikobeurteilung gliedert sich zum einen in die Risikoanalyse und zum anderen in die Risikobewertung. Bei der Risikoanalyse müssen die Zweckbestimmung eines Medizinprodukts und deren sicherheitsrelevanten Merkmale definiert, Gefährdungen identifiziert und die Risiken für die jeweiligen Gefährdungssituationen abgeschätzt werden. Für den nächsten Schritt, der Risikobeherrschung, muss zunächst analysiert werden, welche Möglichkeiten bestehen, um nachfolgend Maßnahmen zur Risikominimierung einleiten zu können. Anschließend folgt eine Analyse, der durch die Beherrschungsmaßnahmen neu entstandenen Risiken und eine Bewertung des bleibenden Restrisikos. Bevor der Risikomanagementbericht erstellt werden kann, steht noch die Entscheidung an, ob das Gesamt-Restrisiko als akzeptabel und vertretbar angesehen werden kann. All diese genannten Schritte bilden das Risikomanagement nach DIN EN ISO 14971 ab. [6]

Die Aufgaben der obersten Leitung sind alle materiellen und personellen Ressourcen zur Verfügung zu stellen, Akzeptanzkriterien für die Risikobewertung festzulegen und den Risikomanagement-Prozess regelmäßig zu überprüfen. [6]

Im Anhang bietet diese Norm noch verschiedene Informationen, wie Beispiele für Gefährdungen und Gefährdungssituationen, verschiedene Fragen, welche man zur Festlegung von sicherheitsrelevanten Eigenschaften von Medizinprodukten stellen kann und Anleitungen für Risikomanagement-Prozesse für unterschiedliche Gruppen von Medizingeräten, wie zum Beispiel In-vitro-Diagnostik (IVD). [6]

Die Norm DIN EN ISO 14971 richtet sich grundsätzlich an die Hersteller von Medizinprodukten, der Aufbau des Risikomanagements ist aber auch auf andere Bereiche übertragbar und bildet den Grundstein zur DIN EN 80001.

Weitere erwähnenswerte Normen sind die DIN EN 62304, die ÖVE/ÖNORM EN ISO 13485 und die DIN EN 61907.

Die Norm DIN EN 62304 [14] beschäftigt sich mit den Lebenszyklus-Prozessen von Medizinprodukte-Software und zeigt die Qualitäts- und Risikomanagement-Prozesse für die Entwicklung und Wartung dieser Software auf.

Die ÖVE/ÖNORM EN ISO 13485 [3] regelt die Kriterien an ein Qualitätsmanagementsystem für Medizinprodukte. In dieses Qualitätsmanagement sind alle Phasen des Lebenszyklus‘ eines Medizinproduktes eingeschlossen, von der Entwicklung bis hin zur Instandhaltung.

In der DIN EN 61907 [15] wird die Zuverlässigkeit von Kommunikationsnetzwerken thematisiert, von der Prozessplanung, über die Ausführung bis hin zur Überprüfung der Netzzuverlässigkeit.

1.4 Risikomanagement

Abbildung 1 zeigt die einzelnen Schritte der Durchführung eines Risikomanagements. Im Grunde gibt es drei Hauptpunkte: die Risikoanalyse, die Risikobewertung und die Risikobeherrschung

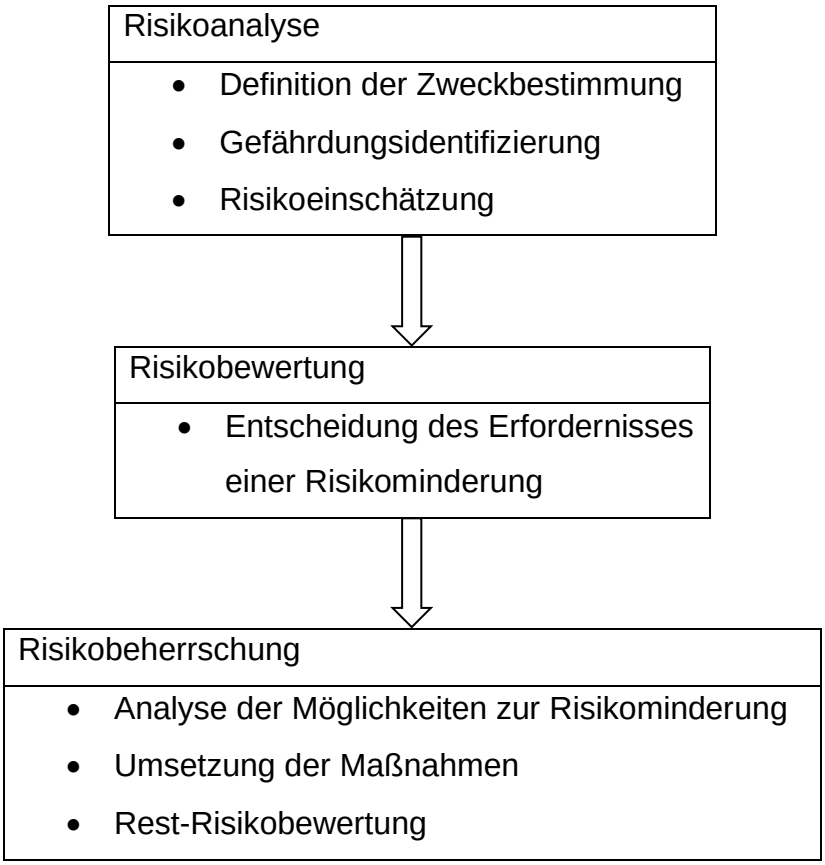

Abbildung 1: Schritte eines Risikomanagements **[6]**, **[4]**

Risikoanalyse:

Bei diesem Schritt sollten alle möglichen Risiken, die unter den unterschiedlichsten Umständen auftreten können, identifiziert werden. Dazu zählt sowohl technisches als auch menschliches Versagen. Bei der Risikoidentifikation sollen Mitglieder von allen beteiligten Berufsgruppen, wie Ärzte, Pflegepersonal, Medizintechniker und Mitarbeiter der IT, mitwirken, um möglichst jede Sichtweise abzudecken und keine Gefahr zu übersehen. Ziel der Risikoanalyse ist, alle möglich auftretenden Gefahren zusammenzufassen, um diese im nächsten Schritt bewerten zu können. [6]

Risikobewertung:
Zwei Faktoren spielen hierbei eine entscheidende Rolle: die Eintrittswahrscheinlichkeit und die Schwere der Folgen. Das Zusammenspiel der beiden Größen ergibt das Risiko. Bei diesem Schritt muss die Entscheidung getroffen werden, ob das Risiko vertretbar ist oder ob Maßnahmen zur Risikominderung eruiert und getroffen werden müssen. [6]

Risikobeherrschung:
Maßnahmen zur Risikominimierung müssen nur dann getroffen werden, wenn aus der vorangegangenen Risikobewertung ein unvertretbares Risiko resultiert.
Als ersten Schritt der Risikobeherrschung muss analysiert werden, ob bzw. welche Möglichkeiten zur Risikominderung bestehen, um dann die Maßnahme zu ermitteln, welche im nächsten Schritt umgesetzt wird. Nach Umsetzung dieser Maßnahme folgt eine Einschätzung des dadurch neu entstandenen Risikos und die Bewertung des Restrisikos. [6]

Im Folgenden werden einige Verfahren zur Risikoanalyse vorgestellt, um einen Überblick über die verschiedenen Herangehensweisen zu verschaffen.

FTA – Fehlerbaumanalyse (Fault Tree Analysis)
Bei diesem Verfahren der Risikoanalyse wird von bekannten Risiken und Gefährdungen ausgegangen und dadurch auf unbekannte Ursachen geschlossen. Die FTA zählt somit zu den Top-Down-Verfahren. Die FTA wird oft zur Analyse der Gefährdungen verwendet, welche bei anderen Verfahren identifiziert wurden.
Ausgehend von einer der identifizierten Gefährdungen wird ein Fehlerbaum mit den dazu führenden Ursachen erstellt, wobei man komplexere Systeme zur Vereinfachung in Subsysteme aufteilen kann. Hierbei besteht die Möglichkeit die Zusammenhänge mit den Bool'schen Operatoren „AND“ und „OR“ zu verknüpfen. Ziel ist es, so lange die vorangegangene Ursache zu suchen, bis man bei einem akzeptablen Risiko angelangt ist, bis man durch eine geeignete Maßnahme ergreifen kann, um diesen Ast vernachlässigen zu können oder bis man bei der Basisursache angelangt ist, wo man nicht mehr weiterkommt. Dabei ist darauf zu achten jede Gefährdung und jede Ursache zu berücksichtigen. [6], [16]

FMEA – Fehlermöglichkeits- und -einflussanalyse (Failure Mode and Effect Analysis)
Für dieses Verfahren der Risikoanalyse gilt der Bottom-Up-Ansatz, d.h. hierbei beginnt man bei den Komponenten des Medizinproduktes oder des Systems und untersucht welche Auswirkungen Fehler dieser haben können. Voraussetzung hierbei ist, dass man den Aufbau des entsprechenden Produktes, die sogenannte Systemarchitektur, kennt und diese dokumentiert ist. Nur so können die Interaktionen der Komponenten zueinander und die Auswirkungen eines Fehlers erkannt werden. Dadurch, dass bei der FMEA das System den Ansatzpunkt bildet, wird dieses Verfahren oftmals bei der Entwicklung vom Hersteller angewendet. [6], [17]

PHA – Vorläufige Gefährdungsanalyse (Preliminary Hazard Analysis)
Dieses Verfahren wird häufig in einer frühen Entwicklungsphase angewandt, da nur grobe Systembeschreibungen benötigt werden. Ähnlich wie bei der FMEA beginnt man hier wiederum bei den Komponenten und versucht dadurch entstehende Gefährdungen zu ermitteln und diese zu modellieren. [18], [19]

HAZOP – Hazard and Operability
Die deutsche Übersetzung für dieses Verfahrens lautet Prognose, Auffinden der Ursache, Abschätzen der Auswirkungen, Gegenmaßnahmen also abgekürzt PAAG.
Auch bei dieser Vorgehensweise beginnt man bei den Komponenten und analysiert, welche Fehler im System zu welchen Gefährdungen führen können. Teil des HAZOP-Verfahrens ist auch Überlegung von Gegenmaßnahmen zur Minimierung der Risiken. [6], [20]

HACCP – Hazard Analysis on Critical Control Points
Die HACCP stammt ursprünglich von der Lebensmittelindustrie, kann aber auch für die Risikoanalyse im Bereich der Medizintechnik angewandt werden.
Bei diesem Verfahren werden zunächst aller möglichen Gefahren und deren Vorbeugungsmaßnahmen identifiziert. Im nächsten Schritt werden sogenannte kritische Kontrollpunkte definiert, also jene Punkte im Prozess, wo eine Kontrolle durchgeführt werden kann, um Gefährdungen zu erkennen und zu minimieren oder zu verhindern. Dazu müssen im Vorfeld Grenzwerte festgelegt werden, also Minimal- oder Maximalwerte, bei deren Über- oder Unterschreitung eingegriffen wird. Das Verfahren soll über den gesamten Zyklus überwacht und dokumentiert werden. [6]

1.5 IT-Netzwerke

Die Bedeutung von IT-Netzwerken in Gesundheitseinrichtungen hat einen hohen Stellenwert. Zum einen nimmt die Vernetzung zwischen Medizinprodukten immer weiter zu, ein geregelter Ablauf in einer Gesundheitseinrichtung ohne ein funktionierendes IT-Netzwerk ist heutzutage undenkbar. Zum anderen können Menschenleben davon abhängen, ob ein medizinisches IT-Netzwerk einwandfrei funktioniert oder nicht.

Nur in den wenigsten Fällen kann man von einem optimalen IT-Netzwerk ausgehen, wie z.B. bei einem Neubau, wo das Netzwerk im Vorhinein durchdacht und geplant werden kann. Im Normalfall aber, wird das vorhandene IT-Netzwerk von Gesundheitseinrichtungen bei Bedarf immer weiter ausgebaut, d.h. es besteht aus „zusammengestückelten“ Teilen. Dadurch, dass an ein medizinisches IT-Netzwerk immer mehr und die unterschiedlichsten Systeme angeschlossen werden, gestaltet es sich immer schwieriger, die Zuverlässigkeit zu gewährleisten. Die Interoperabilität und Kompatibilität der einzelnen Geräte und des Netzwerks zueinander spielt hierbei eine bedeutende Rolle. Genau darin besteht die Aufgabe des Risikomanagements, alle Gefährdungen zu identifizieren, die Risiken zu bewerten und mit geeigneten Maßnahmen zu beherrschen. Je komplexer ein medizinisches IT-Netzwerk aufgebaut ist, desto problematischer und komplizierter ist die Durchführung eines Risikomanagements.

Um einen Überblick über ein Netzwerk zu verschaffen, besteht der erste wichtige Schritt darin, das IT-Netzwerk der gesamten Gesundheitseinrichtung vollständig und aktuell zu dokumentieren. Eine korrekte Dokumentation bildet die Grundlage für ein funktionierendes Risikomanagement. Außerdem spielt auch die Vollständigkeit der Dokumentation der einzelnen Geräte eine große Rolle. Ohne die Hilfe der Hersteller, welche alle für eine Einbindung in ein IT-Netzwerk relevanten Informationen zu Verfügung stellen, ist die Durchführung eines Risikomanagements nur bedingt möglich. Ohne diese wichtigen gerätespezifischen Informationen, welche nur der Hersteller liefern kann, können die möglichen Gefährdungen und daraus resultierende Folgen nur abgeschätzt werden.

Ein medizinisches IT-Netzwerk stellt eine Gesundheitseinrichtung vor verschiedene Herausforderungen. Zum einen handelt es sich bei Gesundheitsdaten immer um besondere Kategorien personenbezogene Daten, welche besonders kritisch bei der

Übertragung zu behandeln sind. [21] Zum anderen kann die Übertragung von Daten auch besonders zeitkritisch sein, z.B. Alarme auf einer Intensivstation. Vor allem bei dieser Kategorie von Daten ist es sinnvoll einen Ausfall der Datenübertragung durch eine redundante Ausführung zu verhindern und entgegenzuwirken. Es kann auch erforderlich sein, große Datenmengen zu übertragen, z.B. Bilddaten von einer Röntgeneinrichtung, CT oder MR. Zusammengefasst muss die Datenübertragung eines medizinischen Netzwerks zuverlässig, zeitnah und mit einer ausreichenden Bandbreite erfolgen. [22]

Hierzu passen auch die Sicherheitsziele für IT-Netzwerke, welche auch unter der Abkürzung CIA bekannt sind:

- Confidentiality: Die Vertraulichkeit von sensiblen, personenbezogenen Daten.
- Integrity: Die Integrität und Richtigkeit von Daten.
- Availability: Die ständige Verfügbarkeit von Daten.

Um diese Ziele zu erreichen sind Authentifizierungen erforderlich und die Zugriffe müssen protokolliert werden. Zusätzlich ist es sinnvoll, wenn die vergebenen Rechte kontrolliert und bei Bedarf und nach Prüfung geändert werden. Normalerweise werden zur Authentifizierung Passwörter verwendet, wobei biometrische Authentifizierungen, wie der Fingerprint oder die Gesichtserkennung immer weiter zunehmen. [23]

Sind die Authentifizierungen und Zugriffsrechte klar geregelt, gibt es noch weitere mögliche Angriffspunkte bei einem medizinischen IT-Netzwerk. Zum einen besteht die Gefahr von Computerviren, welche häufig über E-Mails eingeschleust werden. Um solchen Angriffen vorzubeugen, ist es wichtig alle Anwender in Bezug auf den Umgang mit E-Mails von fremden Absendern und das Öffnen von unbekannten Links zu schulen. Zum anderen stellen unbekannte Geräte, welche an das Netzwerk gekoppelt werden, eine Gefahr dar, wie beispielsweise ein Laptop oder Tablet eines externen Technikers bei der Wartung eines Gerätes. Offene Schnittstellen nach außen sind grundsätzlich zu vermeiden, da diese immer eine Gefahr für unzulässige Zugriffe darstellen. [24]

Grob kann die Datenübertragung in zwei Kategorien eingeteilt werden:

- Kabelgeführte Datenübertragung, z.B. Local Area Network (LAN)
- Kabellose Datenübertragung, z.B. Wireless Local Area Network (WLAN)

LAN-Netzwerke überzeugen mit einer höheren Sicherheit durch geringere Angreifbarkeit und einer hohen Datenübertragungsgeschwindigkeit. Für eine WLAN-Übertragung spricht der kabellose Transfer, welcher für mobile Geräte benötigt wird.

1.6 Standardisierte Schnittstellen

Das Ziel von standardisierten Schnittstellen ist, dass alle Komponenten, welche diesen Standard unterstützen, kompatibel zu einander sind und miteinander kommunizieren können. Es existieren viele verschiedene Standards, diejenigen welche im medizinischen Bereich am häufigsten verwendeten werden, werden im Folgenden kurz erläutert, um einen Überblick zu bekommen.

HL7 (Health Level 7)
Bei HL7 handelt es sich um einen Standard, welcher international verwendet wird und weit verbreitet ist. Die Versionen 2.x des Standards dienen zum Informationsaustausch zwischen verschiedenen Anwendungssystemen in Gesundheitseinrichtungen. Dieser Standard ist textbasiert und gliedert die zu übertragenden Daten in einzelne Segmente. HL7 kann für die Patientenstammdatenverwaltung, für die Befundkommunikation, für die Anforderung und Übermittlung von Leistungen, aber auch für das Ressourcenmanagement verwendet werden. Dazu werden unterschiedliche Message-Types verwendet, welche den Typ der Daten, welche übertragen werden, definieren. Um zwei Beispiele zu nennen wird zur Befundübermittlung der Nachrichtentyp ORU (Observation Result Unsolicited) verwendet, zur Übertragung von Patientendaten ADT (Admission, Discharge, Transfer). [25]

DICOM (Digital Imaging and Communications in Medicine)
DICOM ist ebenfalls ein international etablierter Standard, welcher medizinisches Bildmaterial und dazugehörige Texte übermittelt. Dies bildet gleichzeitig die Grundlage für die digitale Bildarchivierung Picture Archiving and Communication System (PACS). Die Interoperabilität zwischen verschiedenen bildgebenden Systemen und Programmen zur Bildverarbeitung ist durch die weite Verbreitung des DICOM-Standards stark gestiegen. Es gibt bei dem DICOM-Standard verschiedene Services, welche die einzelnen Dienste darstellen. Im Folgenden werden einige der wichtigsten DICOM-Dienste aufgelistet, um Einblick in die DICOM-Services zu bekommen.

- Verify: Verify überprüft, ob DICOM von einem Netzwerkknoten unterstützt wird.
- Storage: Dieser Dienst ist für die Speicherung der Daten verantwortlich.

- Storage Commitment: Mit diesem Tool kann abgefragt werden, ob die übermittelten Daten korrekt abgespeichert wurden
- Query/Retrieve: Mit diesem Service werden Objekte (Querys) eines Gerätes gesucht und auf ein anderes Gerät übertragen (retrieve).
- Structured Reporting Storage: Dieser Dienst dient der verschlüsselten Befundübermittlung.
- Procedure Step: Über Procedure Step können Daten über die Untersuchungsschritte und deren Status von einem Gerät zu einem anderen übertragen werden. [25]

OR.NET

OR.NET ist ein im Jahr 2012 gestartetes Projekt, welches einen neuen Vernetzungsstandard, als Schnittstelle zwischen allen Medizingeräten untereinander, entwickelt. Damit soll erreicht werden, dass alle Geräte in einem Operationssaal und dessen klinischen Umfeld interoperabel sind. Ziel dieses Projektes ist es, eine internationale Akzeptanz zu erarbeiten, um eine flächendeckende Standardisierung zu ermöglichen und Abstand von den jetzt herrschenden Insellösungen zu bekommen.
Dafür wurde der offene Standard Service-oriented Device Connectivity (SDC) entwickelt. Dieser ermöglicht den unkomplizierten Datenaustausch zwischen den Medizingeräten und liefert gleichzeitig das benötigte Maß an Sicherheit. Der Vorteil bei dem SDC-Standard ist, dass diese Konnektivität herstellerübergreifend funktioniert. Damit soll erreicht werden, dass nicht nur von einem Hersteller zusammengestellte System verwendet werden können, sondern dass der Betreiber einzelne Medizingeräte von unterschiedlichen Herstellern selbst zusammenstellen und bei Bedarf einzelne Geräte ohne Probleme austauschen kann. Haben alle Geräte den SDC-Standard integriert, können diese, obwohl sie von verschiedenen Herstellern stammen, miteinander kommunizieren und Daten übertragen. So können beispielsweise Vitalparameter und Bilddaten gleichzeitig auf einem Monitor angezeigt werden und auch Funktionen eines Gerätes von einem anderen ferngesteuert werden. Grundsätzlich können die Daten über eine äußere Schnittstelle nach SDC übersetzt werden oder es wird ein Chip im Medizingerät integriert. [26], [27], [28]

Es existieren natürlich noch viele andere Standards, jedoch wäre es anstrebenswert, die Anzahl zu minimieren, um eine bessere Interoperabilität zu erreichen.

2 Aufgabenstellung

Bei der Einbindung elektromedizinischer Geräte und Systeme in die IT-Infrastruktur von Gesundheitseinrichtungen entstehen immer wieder Probleme, sowohl im technischen als auch im organisatorischen Bereich.
Es stellen sich viele Fragen wie z.B.:

- Wie kann man elektromedizinische Geräte am besten technisch in das IT-System von Gesundheitseinrichtungen einbinden?
- Wer ist für die sichere Einbindung von elektromedizinischen Geräten und die sichere Datenübertragung verantwortlich?
- Wie ist bei der Einbindung elektromedizinischer Geräte in die IT-Infrastruktur gesetzeskonform vorzugehen?

Im Zuge dieser Masterarbeit sollen die Anforderungen an Medizinprodukthersteller, Medizinproduktebetreiber und Service- und Prüfeinrichtungen untersucht werden, um die jeweiligen Verantwortlichkeiten zu klären. Dafür sollen sowohl der aktuelle gesetzliche Stand, als auch relevante Literaturstellen beleuchtet werden.
In der Vorbereitungsphase erfolgt eine Einarbeitung in aktuelle Gesetze und Normen. Grundlegende Definitionen, wie IT-Netzwerk, Medizinprodukt, Risiko etc. werden im Zuge dieser ersten Phase dokumentiert. Der Vorgang der Recherche muss vor Beginn geplant und überlegt werden, was bei den methodischen Überlegungen genauer ausgeführt wird. Im Zuge der Recherche sollen alle Gesetze, Normen, Regulativen und Verordnungen, welche bei einer solchen Einbindung zum Tragen kommen, gesucht werden.
Die Ergebnisse dieser Masterarbeit sollen einen Vergleich dieser gesetzlichen und normativen Anforderungen beinhalten, ebenso wie eine Diskussion der wesentlichen auftretenden Probleme bzw. offene Fragestellungen. Die Erarbeitung einer gesetzeskonformen Vorgehensweise bei der Einbindung von elektromedizinischen Geräten in die IT-Infrastruktur von Gesundheitseinrichtungen ist ein weiteres Ziel dieser Masterarbeit.

3 Methoden

Zu Beginn dieser Masterarbeit erfolgte eine ausführliche Einarbeitung in das zu bearbeitende Thema. Dazu wurden Suchmaschinen wie Google und Google Scholar benutzt, um einen Überblick in die Materie und der sich darauf beziehenden Normen und Gesetze zu bekommen.
Einige Normen und Richtlinien sind zum Download frei zugänglich, zu den restlichen Normen verschaffte mir die Firma TÜV Austria Zugang. So konnten zunächst alle relevanten Normen und Gesetze durchgearbeitet und anschließend die Literaturrecherche gestartet werden.
Mit folgenden in Tabelle 1 dargestellten Keywords wurde nach passenden Artikeln in der Datenbank Google Scholar und Google gesucht:

Keywords	
deutsch	englisch
Einbindung elektromedizinischer Geräte	integration
	medical devices
Gesundheitseinrichtungen	health care facilities
Risikomanagement	riskmanagement
medizinisches Netzwerk	medical network

Tabelle 1: Keywords für die Literaturrecherche

Die Recherche erfolgte zuerst auf Deutsch und im zweiten Anlauf mit englischen Keywords. Die Suche fand mit verschiedenen Zusammensetzungen der Keywords statt. Zitate und Patente wurden aus der Suche ausgeschlossen. Außerdem wurden nur Artikel und Bücher, welche ab 2007 veröffentlicht wurden, eingeschlossen. Alle Ergebnisse mit einem Veröffentlichungsdatum vor 2007 wurde aufgrund von Veralterung ausgeschlossen.
Zunächst erfolgte ein Titelscreening der jeweils ersten 100 Treffer der verschiedenen Suchanfragen. Alle relevanten Titel wurden herausgefiltert und ein Abstractscreening

durchgeführt. Jene Artikel und Buchausschnitte, welche nach dem Abstractscreening noch verblieben, wurden einem Volltextscreening unterzogen.

In Abbildung 2 ist die Anzahl der relevanten Quellen ersichtlich, welche nach den jeweiligen Schritten ausgewählt wurden. Redundante Artikel wurden im letzten Schritt ausgeschlossen.

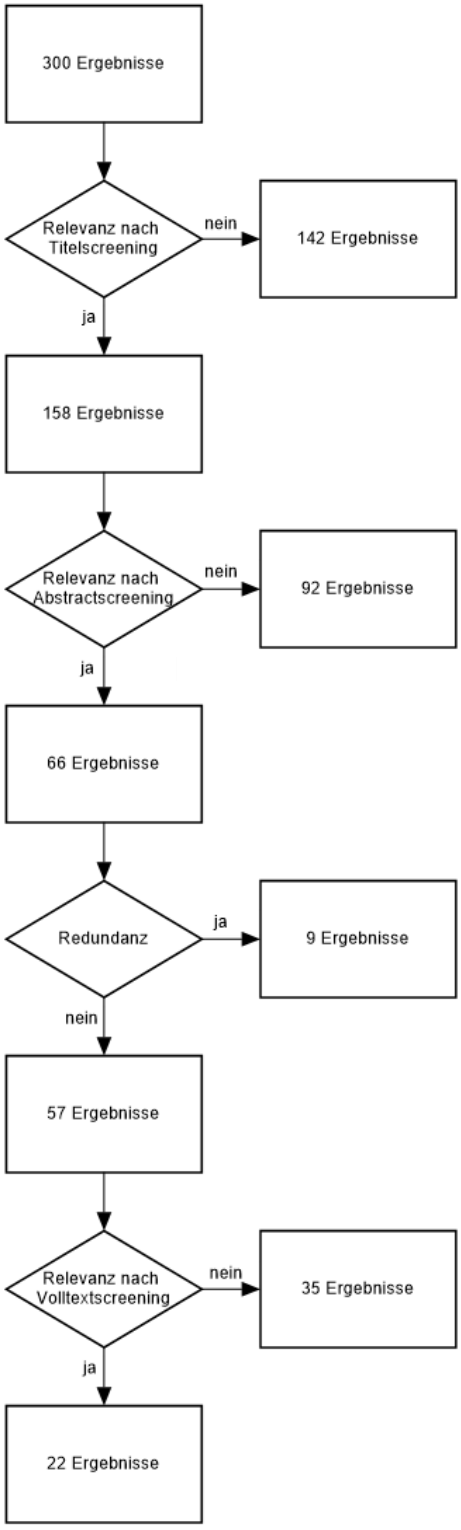

Abbildung 2: Anzahl der Suchergebnisse bei der Literaturrecherche

Nach der abgeschlossenen Literaturrecherche wurde versucht ein „best-practice“-Verfahren für die Einbindung von elektromedizinischen Geräten in die IT-Infrastruktur zu entwickeln.

Alle relevanten Normen und die recherchierte, verfügbare Literatur wurden dazu verwendet, um einen Einbindungsprozess zu erstellen. Um diesen Prozess besser zu veranschaulichen, wurden Flussdiagramme mit Teilprozessen und Entscheidungsfragen angefertigt. So wurde versucht auf jede mögliche Situation einzugehen und einen Lösungsvorschlag anzubieten.

Die Flussdiagramme oder auch ‚flow charts‘ genannt, wurden mit dem frei downloadbaren Programm ‚ClickCharts‘ erstellt. Die Verantwortlichkeiten und die In- und Outputs jeden Prozessschrittes wurden in Tabellenform zusammengefasst. Abschließend wurden noch zwei Beispiele für die Risikoanalyse bei einer Einbindung eines neuen Gerätes in eine bestehende Infrastruktur abgebildet und die Risiken analysiert und bewertet.

4 Ergebnisse

4.1 Einbindungsprozess

Betreiber sind oftmals dazu gezwungen verschiedene Geräte, oft auch aus finanziellen Gründen von unterschiedlichen Herstellern, zu einem medizinischen System zusammenzustellen und dieses dann in das IT-Netzwerk zu integrieren, um eine zeitgemäße Kommunikation sicherstellen zu können. Dadurch wird der Betreiber selbst zum Hersteller und übernimmt dabei sämtliche Haftung und Verantwortung für alle Gefährdungen, welche durch diese Zusammenstellung entstehen. Aus diesem Grund ist es sinnvoll als Betreiber bzw. als verantwortliche Organisation einen Med-IT-Risikomanager zu benennen, welcher die Verantwortung für die Durchführung der Risikomanagementprozesse übernimmt und diese koordiniert, wie in der DIN EN 80001 vorgesehen.

Das folgende Prozessdiagramm (Abbildung 3, Abbildung 4) zeigt die Prozessschritte von der Idee einer Einbindung eines Medizingerätes in ein bestehendes IT-Netzwerk bis hin zur Durchführung dieser Einbindung. Untenstehend werden die einzelnen Prozessschritte genauer erläutert.

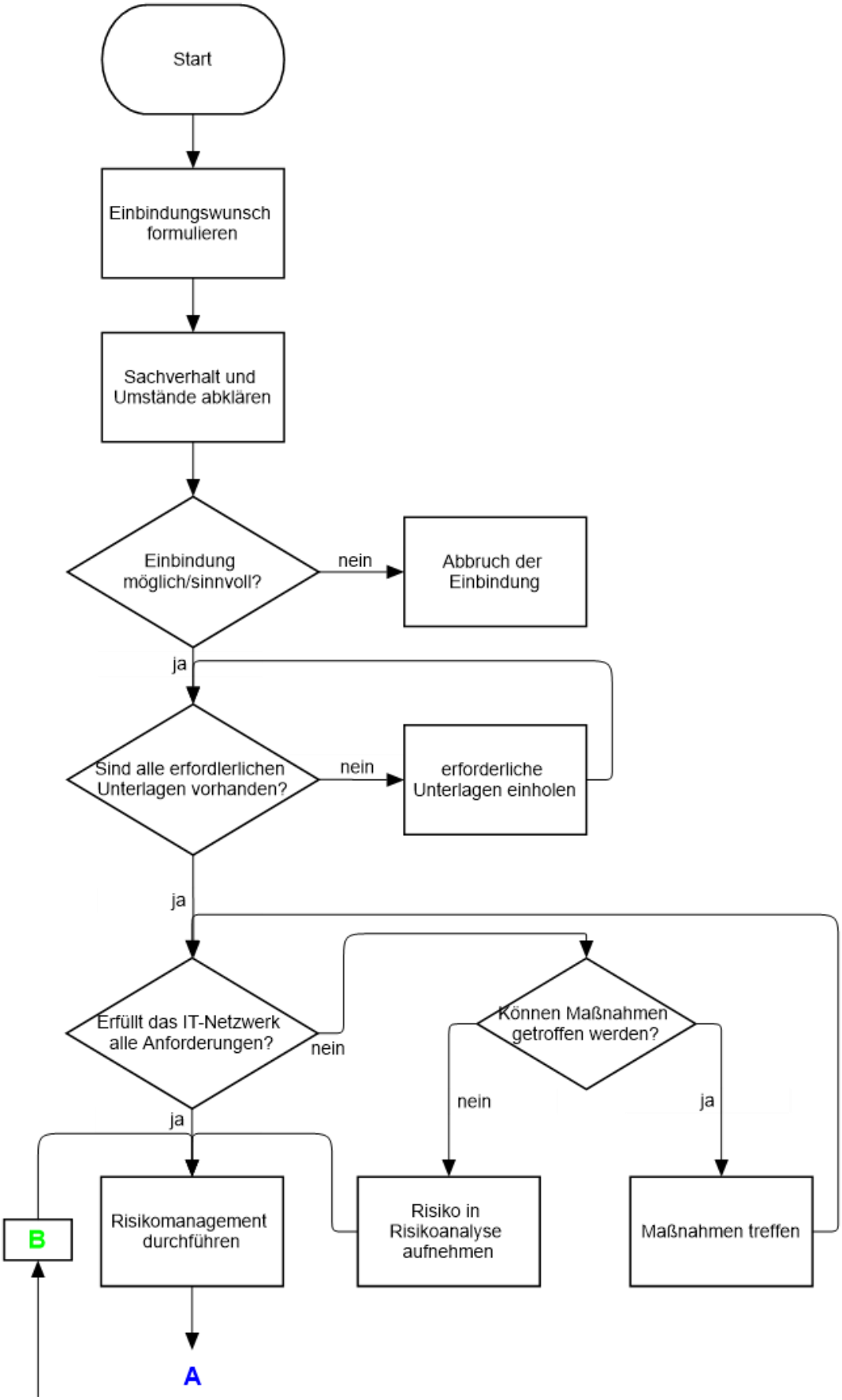

Abbildung 3: Flussdiagramm - Prozessschritte für die Einbindung eines Gerätes in ein IT-Netzwerk – Teil 1

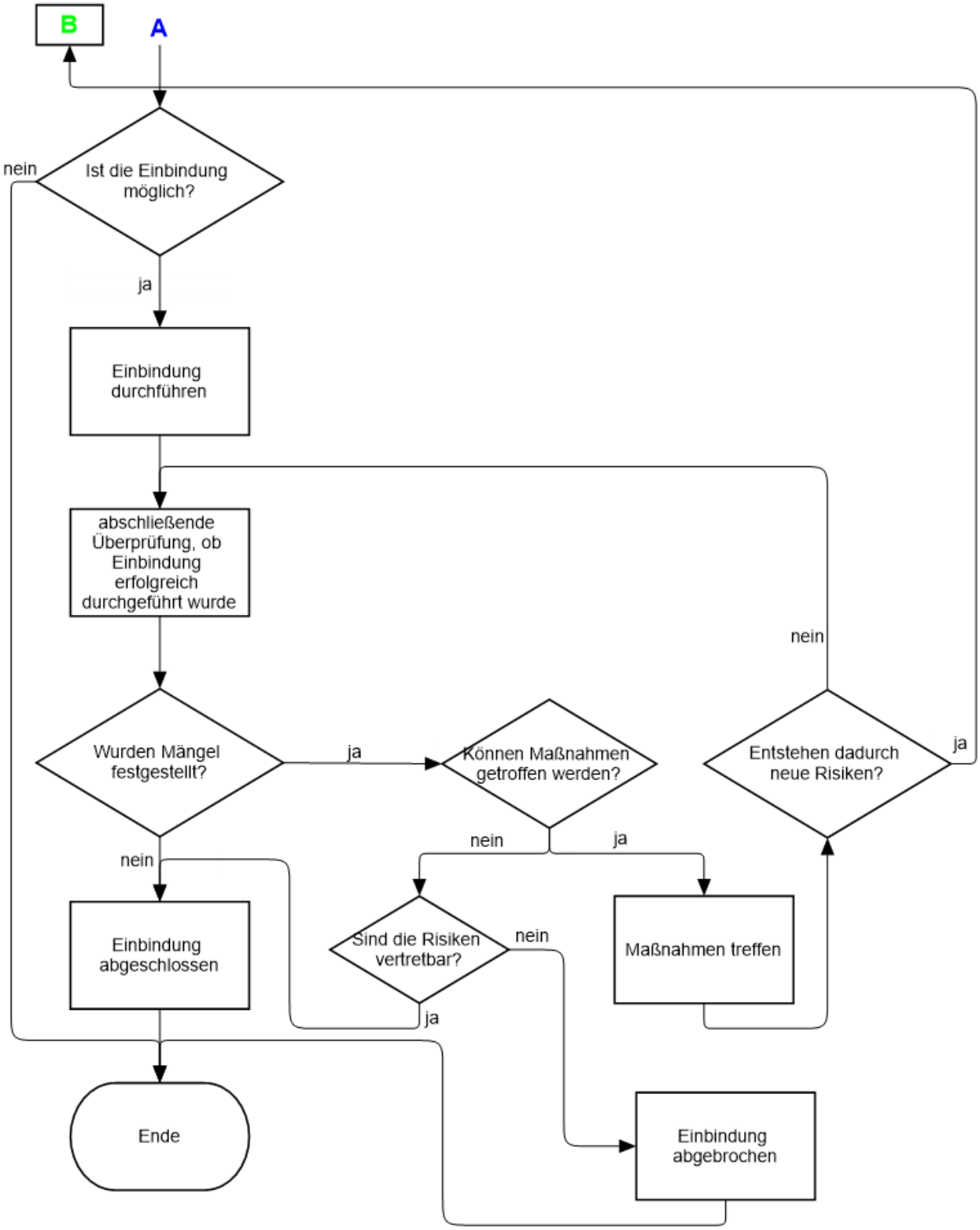

Abbildung 4: Flussdiagramm - Prozessschritte für die Einbindung eines Gerätes in ein IT-Netzwerk – Teil 2

Formulierung des Einbindungswunsches:
Am Beginn des Einbindungsprozesses eines Medizingerätes in ein bestehendes IT-Netzwerk einer Gesundheitseinrichtung steht die Formulierung des Einbindungswunsches, um den Prozess zu starten. Der Wunsch ein neues elektromedizinisches Gerät zu beschaffen und einzubinden kann von den unterschiedlichsten Seiten kommen, von Medizinern, vom Pflegepersonal, von der Verwaltung oder der Medizintechnik. Gründe dafür können sowohl eine gewünschte Aufrüstung und Verbesserung der bestehenden Diagnostik oder Therapie, als auch der Ersatz eines veralteten oder defekten Gerätes sein. Um diesen ersten Schritt abzuschließen, muss das Anliegen in die entsprechende Software eingegeben werden. Als Output entsteht der formulierte Einbindungswunsch, welcher an die zuständige Person weitergeleitet wird.

Abklärung des Sachverhalts und der näheren Umstände:
Zur Abklärung, ob die gewünschte Einbindung durchführbar ist, benötigt die verantwortliche Person, also der Med-IT-Risikomanager oder eine von ihm beauftragte Person, als Input den formulierten Einbindungswunsch und alle vorhandenen Unterlagen des Gerätes und des IT-Netzwerks. Im Zuge dieses Schrittes soll abgeklärt werden, ob die Einbindung prinzipiell machbar ist oder ob Einspruch seitens der IT- oder Medizintechnik-Abteilung erhoben wird.

Entscheidung, ob eine Einbindung möglich bzw. sinnvoll ist:
Spricht kein offensichtlicher Grund gegen eine Einbindung des Gerätes in das IT-Netzwerk, kann mit dem nächsten Schritt fortgefahren werden, ansonsten wird der Prozess abgebrochen. Die Durchführung des Risikomanagements erfolgt zu einem späteren Zeitpunkt. Output dieser Entscheidung ist eine schriftliche Genehmigung oder Absage mit den entsprechenden Begründungen.

Überprüfung der Vollständigkeit der erforderlichen Unterlagen:
Um ein Medizingerät in ein bestehendes medizinisches IT-Netzwerk einbinden zu können, muss vorher untersucht werden, ob alle dafür erforderlichen Unterlagen dem Gerät beiliegen. Dazu zählen eine gültige Konformitätserklärung vom Hersteller, eine deutschsprachige Gebrauchsanweisung, Dokumentation der Typenprüfung nach EN 60601-1 und Daten zur eindeutigen Identifikation des Herstellers, wie Name und

Adresse. Den Unterlagen muss auch entnommen werden können, welche minimalen Anforderungen das IT-Netzwerk besitzen muss, in dem das Medizingerät eingebunden wird und welche Risiken sich daraus ergeben, wenn diese Forderungen nicht eingehalten werden können. Eine vom Hersteller durchgeführte Risikoanalyse muss ebenso beiliegen, wie die Interoperabilität mit anderen medizinischen Geräten oder IT-Systemen und die Anforderungen an Netzwerkschnittstellen.
Bei neu angeschafften Medizingeräten laut Anhang 1 der MPBV muss ein Eingangsprüfungs-Protokoll vorliegen. Dazu zählen nicht implantierbare, aktive Medizinprodukte (wie z.B. Infusionspumpen, Perfusoren, Defibrillatoren, Beatmungsmaschinen, usw.), Säuglingsinkubatoren und externe, aktive Komponenten aktiver Implantate. Wurde noch keine Eingangsprüfung durchgeführt, muss dies vor der Einbindung nachgeholt werden. Der Umfang der Eingangsprüfung ist abhängig von dem mitgelieferten Messprotokoll des Herstellers bzw. des Lieferanten. Wenn ein detailliertes Prüfprotokoll beiliegt, ist eine Sichtprüfung bezüglich Transportschäden ausreichend. Fehlen jedoch wichtige Punkte im Messprotokoll, muss eine ausführlichere Eingangsprüfung erfolgen. Hierbei kann man sich am Umfang einer sicherheitstechnischen Kontrolle orientieren. Die Eingangsprüfung muss mit einem geeigneten Prüfprotokoll dokumentiert werden. [8]

Einholung der erforderlichen Unterlagen:
Sind die Unterlagen nicht vollständig vorhanden, muss sich die verantwortliche Person um die Einholung der fehlenden Unterlagen kümmern. Hierzu kann entweder direkt beim Hersteller angefragt werden oder bei dem zuständigen Lieferanten. Die erhaltenen Informationen müssen auf Korrektheit und Aktualität überprüft werden. [4]
Sind die erforderlichen Unterlagen auch nach der Nachfrage beim Hersteller bzw. Lieferanten nicht vollständig und aktuell vorhanden, können die fehlenden Daten nur abgeschätzt werden. Dementsprechend fällt auch die Risikoanalyse und -bewertung oberflächlicher aus und unterliegt einer größeren Ungenauigkeit.

Erfüllung der Anforderungen des IT-Netzwerks:
In diesem Schritt ist zu prüfen, ob das bestehende IT-Netzwerk alle vom Hersteller in den beiliegenden Unterlagen geforderten Voraussetzungen erfüllt. Sind alle Anforderungen erfüllt, kann zum nächsten Schritt übergegangen werden.

Überlegung, ob Maßnahmen zur Risikominderung existieren:
Erfüllt das IT-Netzwerk nicht die geforderten Voraussetzungen, ist die Überlegung anzustellen, ob Maßnahmen durchgeführt werden können, um die Anforderungen zu erfüllen, ohne dass daraus Gefährdungen resultieren.

Durchführung der Maßnahmen zur Risikominderung:
Ist man zu dem Entschluss gekommen, dass umsetzbare Maßnahmen existieren, sind diese durchzuführen. Wichtig hierbei ist, dass Änderungen am IT-Netzwerk immer dokumentiert werden, um zu jeder Zeit eine vollständige und aktuelle Skizzierung des Netzwerks aufweisen zu können.

Aufnahme, des Risikos in die Risikoanalyse:
Besteht keine Möglichkeit einer Einleitung von Schritten, ist das daraus resultierende zusätzliche Risiko in die Risikoanalyse miteinzubeziehen. Wie schon erwähnt, sollten die Herstellerunterlagen das Gefährdungspotential aufzeigen, welches sich durch die Nicht-Einhaltung der Anforderungen an das IT-Netzwerk ergibt.

Durchführung des Risikomanagements:
Dieser wichtige Teil, bestehend aus Risikoanalyse, Risikobewertung und Risikobeherrschung, ist in detaillierter Form in Abbildung 6 dargestellt, um eine bessere Übersicht des Prozessdiagramms zu erzielen.
Am Ende steht immer die Frage, ob die identifizierten Risiken vertretbar sind und ob diese minimiert werden können. Die entsprechenden Maßnahmen sind einzuleiten und im Bedarfsfall die Risikoanalyse und -bewertung zu wiederholen. Alle relevanten Daten werden in der Risikomanagementakte gesammelt dokumentiert.

Abklärung der Durchführbarkeit der Einbindung:
In diesem Schritt ist das Ergebnis des Risikomanagementprozesses abzufragen.
Wenn alle Restrisiken auf ein vertretbares Minimum gesenkt wurden, kann die tatsächliche Einbindung des elektromedizinischen Gerätes in das IT-Netzwerk ausgeführt werden. Können die Restrisiken nicht auf ein akzeptables Maß gesenkt werden, kann die Einbindung nicht durchgeführt werden und der gesamte Prozess wird abgebrochen. (siehe Abbildung 6)

Durchführung der Einbindung:
Bei diesem Schritt findet die tatsächliche Einbindung des Medizingerätes in das IT-Netzwerk statt, also der Anschluss an das Netzwerk, mit einem Einbindungsprotokoll als Output.

Abschließende Überprüfung:
Im Zuge dieses Prozessschrittes muss überprüft werden, ob die Anbindung erfolgreich durchgeführt wurde. Der wichtigste Faktor hierbei ist, ob das eingebundene Medizingerät mit dem IT-Netzwerk richtig interagiert. Dabei sind alle Funktionen, welche für die Zweckbestimmung des medizinischen IT-Netzwerks benötigt werden, auf ihre korrekte Funktionsfähigkeit zu testen.

Abklärung des Ergebnisses der abschließenden Prüfung:
Werden bei der Abschlussprüfung keine Mängel festgestellt und funktioniert das eingebundene Gerät einwandfrei im IT-Netzwerk, kann die Einbindung abgeschlossen werden. Ist dies nicht der Fall, sind die folgenden Schritte zu befolgen.

Überlegung, ob Maßnahmen zur Mängelbehebung existieren:
In dem Fall, dass bei dieser Abschlussprüfung Mängel festgestellt werden, muss wiederum die Frage gestellt werden, ob Maßnahmen zur Behebung der Mängel existieren und ob diese durchführbar sind.

Durchführung der Maßnahmen zur Mängelbehebung:
Realisierbare Schritte zur Mängelbehebung sind umzusetzen.

Überlegung, ob getroffene Maßnahmen das Risikomanagement beeinflussen:
Wenn durch die Umsetzung der Maßnahmen zur Mängelbehebung neue Risiken entstehen, muss der Risikomanagementprozess wiederholt werden. Besteht keine Beeinflussung des durchgeführten Risikomanagements, ist nur die abschließende Überprüfung der erfolgten Einbindung zu wiederholen.

Abklärung, der Vertretbarkeit des Risikos:
Falls keine Veränderungen zur Verbesserung getroffen werden können, muss eruiert werden, ob die entdeckten Mängel zu einem unvertretbaren Risiko führen. In diesem Fall muss die Einbindung widerrufen und das Gerät wieder abgeschlossen werden.
Kommt man nach einer ausführlichen Risikoanalyse zu dem Entschluss, es handelt sich um ein akzeptables Maß an Restrisiko, so ist der Einbindungsprozess abgeschlossen.

Abschluss der Einbindung:
Für den geregelten Abschluss einer erfolgreichen Einbindung, müssen alle erforderlichen Dokumente gesammelt und sicher, aber auch jederzeit zugänglich, aufbewahrt werden.

Werden alle Prozessschritte, wie in dem Flussdiagramm aufgezeigt, durchgeführt und wird jeder Schritt dokumentiert, kann man von einem geregelten und nachvollziehbaren Ablauf sprechen und somit von einer Vereinheitlichung des Einbindungsprozesses.
In Tabelle 2 sind noch einmal alle Prozessschritte dargestellt, inklusive der Verantwortlichkeiten und der In- und Output-Dokumente. Dabei wird deutlich, dass der Med-IT-Risikomanager durchgehend die Verantwortung trägt, dies ist in der Norm DIN EN 80001-1 so definiert. Der Med-IT-Risikomanager hat dabei die Möglichkeit jede Aufgabe an andere qualifizierte Personen oder Personengruppen zu vergeben. Schlussendlich trägt immer der Med-IT-Risikomanager die Verantwortung, auch für Aufgaben, welche er selbst nur koordiniert. In der Spalte ‚Durchführung/Mitarbeit' werden Berufs- bzw. Arbeitsgruppen angeführt, an welche der Med-IT-Risikomanager beispielsweise bestimmte Aufgaben vergeben kann.
Jene Prozessschritte, welche bis zur Einbindung auf jeden Fall durchlaufen werden müssen, sind in der Tabelle schwarz dargestellt. Nebenschritte, welche nur bei gewissen Antworten einer Abfrage erreicht werden, sind grau gekennzeichnet.

Prozessschritt	Verantwortlicher	Durchführung/Mitarbeit	Input	Output
Formulierung des Einbindungswunsches	Anwender, Medizintechniker		Formular für Einbindungswunsch	Ausgefülltes Formular für Einbindungswunsch
Abklärung des Sachverhalts und der näheren Umstände	Med-IT-Risikomanager	Mitarbeiter der IT-Abteilung, Mitarbeiter der Medizintechnik, RM-Team	Ausgefülltes Formular für Einbindungswunsch, erforderliche Dokumente	
Entscheidung, ob eine Einbindung möglich/sinnvoll ist	Med-IT-Risikomanager	Mitarbeiter der IT-Abteilung, Mitarbeiter der Medizintechnik, RM-Team		Genehmigung/Ablehnung
Überprüfung der Vollständigkeit der Unterlagen	Med-IT-Risikomanager	Mitarbeiter der Medizintechnik	Alle vorhandenen Unterlagen	Liste ev. fehlender Unterlagen
Einholung der erforderlichen Unterlagen	Med-IT-Risikomanager	Mitarbeiter der Medizintechnik	Liste der fehlenden Unterlagen Anfrage bei Hersteller	Alle erforderlichen Unterlagen
Erfüllung der Anforderungen des IT-Netzwerks	Med-IT-Risikomanager	Mitarbeiter der IT-Abteilung	Herstellerangaben des einzubindenden Gerätes, Unterlagen des IT-Netzwerkes	Liste ev. nicht erfüllter Anforderungen
Überlegung, ob Maßnahmen zur Risikominderung existieren	Med-IT-Risikomanager	Mitarbeiter der IT-Abteilung	Liste der nicht erfüllten Anforderungen	Liste ev. durchführbarer Maßnahmen
Durchführung der Maßnahmen zur Risikominderung	Med-IT-Risikomanager	Mitarbeiter der IT-Abteilung	Liste der durchführbaren Maßnahmen	Protokoll der Durchführung
Aufnahme des Risikos in die Risikoanalyse	Med-IT-Risikomanager	RM-Team	Liste der nicht erfüllten Anforderungen	Liste, der sich daraus ergebenden Risiken

Durchführung des Risikomanagements	Med-IT-Risikomanager	RM-Team	Alle erforderlichen Unterlagen des einzubindenden Gerätes und des IT-Netzwerks	Risikomanagementakte
Abklärung, der Durchführbarkeit der Einbindung	Med-IT-Risikomanager	RM-Team	Risikomanagementakte	Genehmigung/Ablehnung
Durchführung der Einbindung	Med-IT-Risikomanager	Mitarbeiter der Medizintechnik	Genehmigung	Einbindungsprotokoll
Abschließende Überprüfung	Med-IT-Risikomanager	Mitarbeiter der Medizintechnik	Einbindungsprotokoll	Prüfungsprotokoll
Abklärung des Ergebnisses der abschließenden Prüfung	Med-IT-Risikomanager	Mitarbeiter der Medizintechnik	Prüfungsprotokoll	Ev. Mängelliste
Überlegung, ob Maßnahmen zur Risikominderung existieren	Med-IT-Risikomanager	Mitarbeiter der Medizintechnik, RM-Team	Mängelliste	Liste ev. durchführbarer Maßnahmen
Durchführung der Maßnahmen zur Risikominderung	Med-IT-Risikomanager	Mitarbeiter der Medizintechnik	Liste der durchführbaren Maßnahmen	Protokoll der Durchführung
Abklärung, der Vertretbarkeit des Risikos	Med-IT-Risikomanager	RM-Team, Mitarbeiter der Medizintechnik	Mängelliste	Genehmigung/Ablehnung
Abbruch der Einbindung	Med-IT-Risikomanager		Ablehnung	Abbruch-Bestätigung
Abschluss der Einbindung	Med-IT-Risikomanager			Bestätigung für erfolgreiche Einbindung

Tabelle 2: Verantwortlichkeiten, In- und Outputs der einzelnen Prozessschritte

4.2 Risikomanagement

Das Risikomanagement teilt sich, wie oben schon erwähnt, in drei Hauptschritte auf, der Risikoanalyse, der Risikobewertung und der Risikobeherrschung, welche in Abbildung 5 dargestellt sind. Die Risikoüberwachung bildet den vierten Schritt des Risikomanagements und startet den Kreislauf, welcher über den gesamten Lebenszyklus eines Medizingerätes regelmäßig durchlaufen wird.

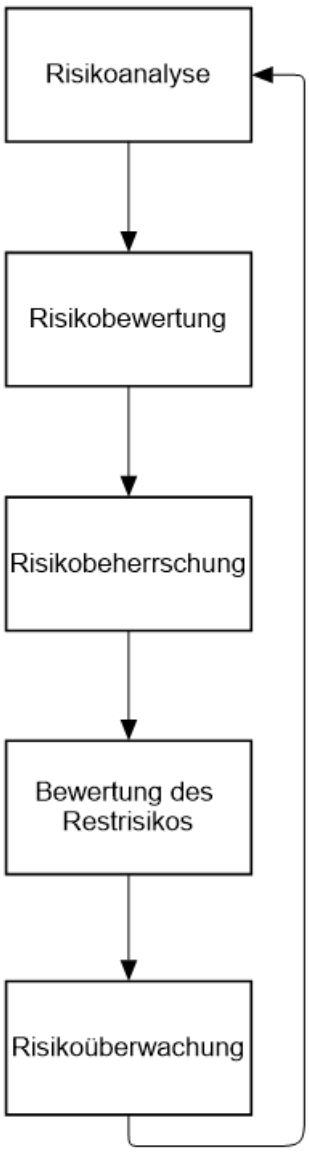

Abbildung 5: Kreislauf des Risikomanagements

Der Prozessschritt „Risikomanagement durchführen“ aus dem Flussdiagramm in Abbildung 3 und Abbildung 4 wird im Folgenden genauer betrachtet. Dazu werden die einzelnen Schritte wiederum in einem Flussdiagramm dargestellt (Abbildung 6). Nachstehend wird auf die skizzierten Prozessschritte einzeln genauer eingegangen.

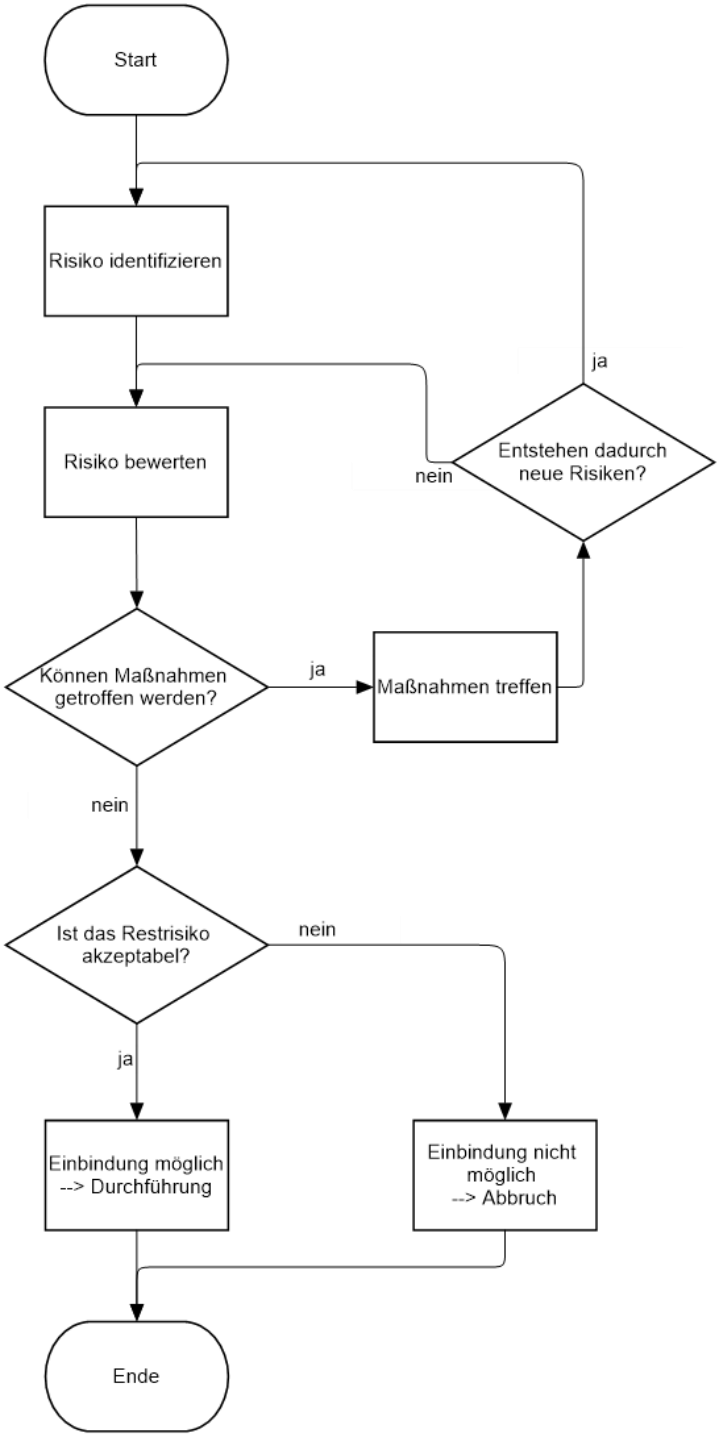

Abbildung 6: Flussdiagramm - Prozessschritte Risikomanagement

Risikoanalyse:

Bei der Risikoanalyse eines medizinischen IT-Netzwerks ist es von großer Bedeutung, dass alle einzelnen Netzwerkkomponenten getrennt voneinander betrachtet werden und eruiert wird, welche Konsequenzen der Ausfall der einzelnen Komponenten mit sich bringen kann. Dazu zählt, dass die Kommunikation zwischen den Geräten genau betrachtet und das Risiko von Signalausfällen abgeschätzt wird. Auch mutwillige sowie unbeabsichtigte Fehlanwendungen müssen berücksichtigt werden. Im Zuge der Risikoanalyse müssen alle möglichen auftretenden Risiken durchgespielt und die daraus resultierenden Folgen abgeschätzt werden.
Für den ersten Schritt, der Identifizierung aller möglich auftretenden Risiken, müssen alle Beteiligten befragt werden, da diese den besten Überblick über mögliche Probleme in den jeweiligen Bereichen haben. Zum einen weiß der Hersteller am besten, welche Probleme mit seinem Produkt auftreten können und welche Spezifikationen das IT-Netzwerk aufweisen muss, um eine reibungslose Datenübertragung gewährleisten zu können. Der IT-Sicherheitsexperte der Gesundheitseinrichtung kennt die Schwachstellen und Angriffspunkte des hausinternen IT-Netzwerkes und kann in dieser Hinsicht am besten die Risiken abschätzen. Bezüglich der Handhabung können die Nutzer der Medizingeräte am besten die Risiken, welche bei der tatsächlichen Anwendung entstehen, einschätzen.
Die Medizintechniker der Gesundheitseinrichtung bilden ein Bindeglied zwischen allen genannten Parteien und können wiederum mit einem neuen Blickwinkel andere Risiken identifizieren. Generell gilt, je mehr Personen aus den unterschiedlichsten Bereichen miteinbezogen werden, desto mehr verschiedene Blickwinkel auf eine Thematik werden abgedeckt. Nur durch das Zusammenarbeiten aller beteiligten Parteien, kann eine umfassende Risikoidentifikation erfolgen.
Wie in der Einleitung schon erwähnt gibt es unterschiedliche Ansätze eine Risikoanalyse anzugehen. Grob unterscheidet man zwischen dem Top-Down- und Bottom-Up-Ansatz. Hierbei muss überlegt werden, ob es sinnvoller ist von den einzelnen Ursachen auszugehen und zu analysieren, welche Risiken daraus resultieren können (Bottom-Up) oder ist man erfolgreicher, wenn man bei den möglichen Risiken und Gefährdungen startet und daraus auf die potentiellen Ursachen schließt (Top-Down).

Im Fall einer Einbindung von Medizingeräten in ein bestehendes IT-Netzwerk ist es sinnvoll nach dem Bottom-Up-Ansatz vorzugehen. Ein Grund dafür ist, dass man den Aufbau des gesamten Systems genau kennt und so die Risiken, welche von den einzelnen Komponenten ausgehen können, gut einschätzen kann. So kann jede Komponente und dessen Risiken einzeln betrachtet werden. Um sicherzustellen, dass man alle Risiken miteinbezieht, kann nach Beendigung dieses Verfahrens, eine weitere Risikoanalyse nach dem Top-Down-Verfahren erfolgen. Somit wird die Analyse noch einmal von einer anderen Seite betrachtet. Durch eine neue Sichtweise können möglicherweise auch andere Risiken erkannt werden. Durch eine doppelte Durchführung der Risikoanalyse, jeweils von unterschiedlichen Ansätzen ausgehend, wird die Chance alle Risiken zu identifizieren deutlich erhöht. Man kann z.B. die FMEA mit einer anschließenden FTA kombinieren.
Falls die Möglichkeit zur Definition von Kontrollpunkten besteht, bietet sich eine Risikoanalyse nach dem HACCP-Prinzip an. Der Vorteil hierbei besteht darin, Risiken über die Kontrollpunkte frühzeitig zu erkennen und dadurch möglicherweise verhindern zu können.

Um die Identifizierung von Risiken zu erleichtern, ist in Tabelle 3 ein Fragenkatalog dargestellt. Die Fragenstellungen sind nach Personengruppen gegliedert, welche für die Beantwortung vorgesehen sind. Die Tabelle soll helfen, verschiedene Aspekte, welche Gefährdungen verursachen können, zu betrachten und eventuelle Fehlerquellen aufzufinden, aber auch Risiken ausschließen zu können.
Fragestellungen, welche das Medizinprodukt selbst betreffen, wie z.B. ob dem Patienten Energie zugeführt wird oder ob es sich um ein implantierbares Medizinprodukt handelt, sind in dieser Tabelle 3 nicht angeführt. Hier wurden lediglich beispielhafte Fragen zusammengefasst, welche für die Analyse der Risiken, welche bei der Einbindung eines Medizingerätes in ein IT-Netzwerk entstehen, relevant sind. Für Fragen, welche sich auf die Sicherheit eines Medizinproduktes beziehen, kann auf die Norm DIN EN ISO 14971 verwiesen werden. In Anhang C dieser Risikomanagement-Norm für Medizinprodukte sind Fragen zur Identifizierung von Risiken von Medizinprodukten aufgelistet. [6]

IT-Experten	Wie werden die Patientendaten gesichert?
	Werden die Signale verschlüsselt übertragen?
	Werden alle Anforderungen des Herstellers an das IT-Netzwerk eingehalten?
	Welches Virenprogramm wird verwendet? Welchen Schutz vor Hackerangriffen besteht?
	Wie werden Zugangsbeschränkungen realisiert? Werden die Passwörter regelmäßig geändert? Welche Personen haben Zugang zu den Daten?
	Wie werden die Daten übertragen (WLAN, LAN, Funk)?
	Wie ist das IT-Netzwerk der Gesundheitseinrichtung aufgebaut?
	Ist das medizinische IT-Netzwerk getrennt ausgeführt?
	Wo werden die Patientendaten archiviert?
	Wird eine Firewall verwendet?
	Werden regelmäßig Updates durchgeführt?
	Ist es möglich USB-Sticks an den firmeneigenen Computern zu verwenden?
	Wie wird mit nicht oder nicht mehr benötigte Patientendaten umgegangen? Wie lange werden Patientendaten gespeichert?
	Existiert eine USV-Versorgung, an der alle IT-Geräte angeschlossen sind?
	Sind eigene EDV-Steckdosen ausgeführt? Sind alle Anwender über die Verwendung der unterschiedlich versorgten Steckdosen geschult?
	Existieren seitens der IT-Abteilung Bedenken bezüglich der Einbindung des Medizingerätes in das IT-Netzwerk?
Hersteller	Was passiert, wenn die Signalweiterleitung ausfällt? Kann das Gerät auch offline verwendet werden?
	Gibt es beim Gerät einen Schutz vor unbeabsichtigtem Einschalten/Verändern?
	Speichert das Medizingerät Daten?
	Gibt es ein Backup, falls Daten verloren gehen?

	Existieren seitens des Herstellers Bedenken bezüglich der Einbindung des Medizingerätes in das IT-Netzwerk?
Anwender	Wie bekommen Patienten und deren Angehörige Zugriff auf ihre Daten? (Passwort-Regelung)
	Können Patienten durch eine falsche Anwendung oder durch einen Netzausfall einen Schaden davontragen?
	Existieren seitens des Anwenders Bedenken bezüglich der Einbindung des Medizingerätes in das IT-Netzwerk?
Medizin-techniker	Wurden alle Nutzer eingeschult?
	Wo wurden die Einschulungen dokumentiert?
	Sind alle berechtigten Anwender dokumentiert?
	Warum wird das Medizingerät in das IT-Netzwerk eingebunden? Was ist der Vernetzungszweck?
	Existieren seitens der Medizintechnik-Abteilung Bedenken bezüglich der Einbindung des Medizingerätes in das IT-Netzwerk?

Tabelle 3: Fragenkatalog für die Risikoanalyse

Risikobewertung:

Um ein Risiko bewerten zu können, müssen zwei Faktoren und deren Verhältnis zueinander berücksichtigt werden:

1. Eintrittswahrscheinlichkeit
2. erwartetes Schwereausmaß der Folgen

Eine mögliche Kombination aus diesen zwei Faktoren ist in Abbildung 7 ersichtlich.

		erwartetes Schadensausmaß			
		unwesentlich	gering	kritisch	katastrophal
Eintritts-wahrscheinlichkeit	unvorstellbar				
	unwahrscheinlich				
	vorstellbar				
	gelegentlich				
	wahrscheinlich				
	häufig				

Abbildung 7: Risikomatrix

Jedes einzelne Risiko, welches im ersten Schritt, der Risikoanalyse, identifiziert wurde, muss einer Risikobewertung unterzogen werden. Mithilfe der Risikomatrix kann man das Risiko in drei verschiedene Bereiche einteilen:

- grüner Bereich: akzeptables Risiko
- gelber Bereich: Risiko, welches durch den Einsatz von Maßnahmen reduziert werden soll
- roter Bereich: inakzeptables Risiko, welches vermieden werden muss

Es müssen dynamische Risikoakzeptanzkriterien definiert werden. Einen besseren Überblick behält man, wenn diese Kriterien für die drei Schutzziele (Sicherheit, Effizienz und Daten- und Systemschutz) getrennt ausgeführt werden. Zum Beispiel stellen im Bereich der Sicherheit der Tod eines Patienten oder schwerewiegende gesundheitliche, nicht reversible Folgen ein katastrophales Schadensausmaß dar. Bei der Effizienz ist der schlimmste mögliche eintretende Fall das Gerät nicht verwenden zu können. Für den Daten- und Systemschutz ist darauf zu achten, dass keine nicht befugte Person Zugang zu den sensiblen Gesundheitsdaten bekommt und im schlimmsten Fall das ganze System lahmlegen würde.

Die Eintrittswahrscheinlichkeit kann mithilfe von Prozentangaben auch genauer definiert werden. Diese müssen je nach zu bewertendem Bereich angepasst werden. So entsteht für jeden der drei Schutzziele eine eigene Risikomatrix mit angepassten Bewertungskriterien.

Überlegung, ob Maßnahmen zur Risikobeherrschung existieren:
Um ein identifiziertes Risiko zu reduzieren, soll zuerst eruiert werden, welche Maßnahmen getroffen werden können. Wenn durchführbare Maßnahmen existieren, sind diese im nächsten Schritt auszuführen, ansonsten muss die Akzeptanz des Gesamtrisikos bewertet werden.

Durchführung der Maßnahmen zur Risikobeherrschung:
Zur Auswahl von Maßnahmen zur Risikominderung kann man sich nach dem TOP-Prinzip richten.
Technische Maßnahmen: Im besten Fall kann ein Risiko mit der Durchführung von technischen Maßnahmen reduziert werden. Dazu zählen alle Änderungen am Gerät direkt oder an dessen unmittelbaren Umgebung, wie z.B. die Aufstellung eines Trenntransformators, die Verlegung eines zusätzlichen Schutzleiters und die Einbindung aller Geräte und leitfähigen Oberflächen in den Potentialausgleich.
Organisatorische Maßnahmen: Dieser Gruppe gehören z.B. das Anbringen von Warnhinweisen oder die Einführung von Zugangsbeschränkungen und Authentifizierungen an.
Personenbezogene Maßnahmen: Zu personenbezogenen Maßnahmen zählt jegliche persönliche Schutzausrüstung (PSA), zu welcher die Anwender bei der Benutzung angehalten werden, diese zu verwenden, aber auch die Einweisung bzw. Einschulung der Anwender.
Diese Herangehensweisen sollen, wenn möglich, in der oben genannten Hierarchie durchgeführt werden. D.h. wenn ein Risiko technisch reduziert werden kann, soll diese Lösung zuerst gewählt werden. Danach folgen organisatorische und zuletzt personenbezogene Maßnahmen.

Überlegung, ob getroffene Maßnahmen neue Risiken herbeiführen:
Werden durch die Umsetzung der Maßnahmen zur Risikobeherrschung neue Risiken hervorgerufen, muss die Risikoanalyse zur Identifizierung der neuen Risiken

wiederholt werden. Entstehen keine neuen Risiken, kann mit der Risikobewertung fortgesetzt werden.

Entscheidung, ob das Restrisiko vertretbar ist:
Im Zuge der Risikobewertung, wurde neben den einzelnen Risiken auch das gesamte Restrisiko bewertet. Nun stellt sich die Frage, ob das Restrisiko akzeptabel ist. Kommt man zu dem Entschluss, dass es sich um ein vertretbares Restrisiko handelt, kann die Einbindung genehmigt werden und mit dem nächsten Prozessschritt, der tatsächlichen Einbindung, fortfahren. Bei diesem Punkt kann man wieder zum Flussdiagramm in Abbildung 4 springen. Wird das Restrisiko als nicht akzeptabel bewertet, muss der Einbindungsprozess abgebrochen werden.

4.3 Beispiele

Um den Risikomanagementprozess zu veranschaulichen, werden im Folgenden zwei Beispiele aufgezeigt, zum einen ein Patientenüberwachungsmonitor und zum anderen ein Computertomograph (CT). Es werden nur Risiken betrachtet, welche durch die Einbindung des Medizingerätes in das IT-Netzwerk entstehen, keine Risiken, welche nur von Medizingerät selbst ausgehen.
Da es sich nur um veranschaulichende Beispiele handelt, werden natürlich nicht alle möglich auftretenden Risiken betrachtet, sondern nur eine kleine Auswahl an möglich auftretenden Gefahren.

4.3.1 Beispiel 1: Patientenüberwachungsmonitor

Als erstes Beispiel dient ein Patientenüberwachungsmonitor auf einer Intensivstation.

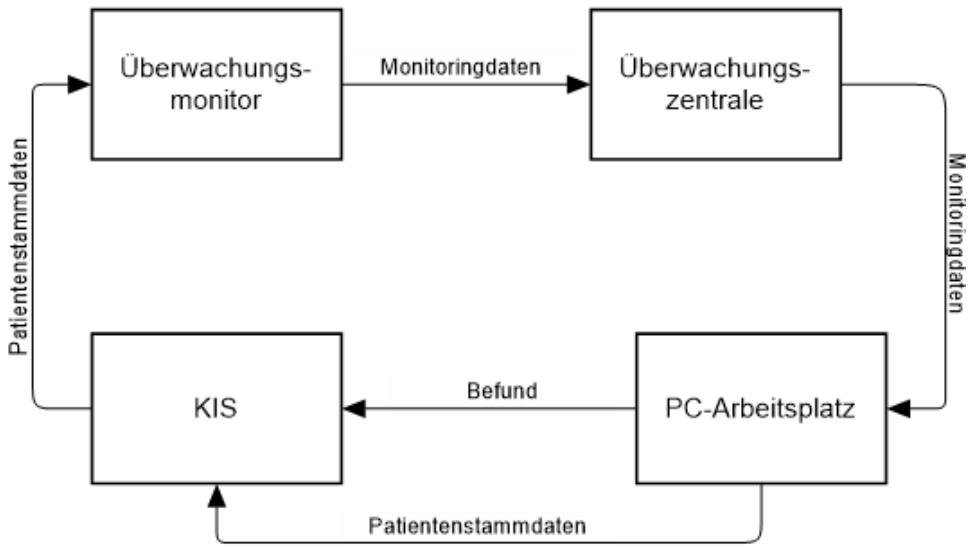

Abbildung 8: Beispiel 1 Überwachungsmonitor - Skizzierung des Datenverlaufs

Im ersten Schritt werden bei der Aufnahme die Stammdaten des Patienten an einem PC-Arbeitsplatz in den Computer eingegeben und an das Krankenhausinformations-system (KIS) weitergeleitet. Das KIS überträgt die notwendigen Daten an den Überwachungsmonitor, welcher an den Patienten angeschlossen wird und dessen Vitalparameter überwacht. Diese Monitoringdaten, inklusive eventuellen Alarmen bei Grenzwertüber- oder -unterschreitung der Vitalparameter, werden an eine Überwachungszentrale im Pflegestützpunkt weitergeleitet. Die Monitoringdaten

werden wiederum von der Überwachungszentrale an den PC-Arbeitsplatz übertragen, wo ein Befund verfasst wird, welcher wiederum im KIS archiviert wird. Dieser Ablauf ist in Abbildung 8 skizziert.

Risikoanalyse:
Der erste Schritt des Risikomanagementprozesses ist die Identifizierung von möglichen Risiken. Bestreitet man dies nach dem Bottom-Up-Ansatz, betrachtet man zuerst die einzelnen Komponenten und analysiert welche Gefährdungen von Fehlern dieser Komponenten ausgehen können. Um einen besseren Überblick zu verschaffen, wird die Risikoanalyse in drei Bereiche aufgeteilt. Es wird jeweils eins der drei Schutzziele betrachtet, die Sicherheit, die Effektivität und der Daten- und Systemschutz.

Erstes Schutzziel – Sicherheit:
Betrachtet man die Übertragung der Monitoringdaten vom Patientenmonitor zur Überwachungszentrale, erkennt man das es sich hierbei um die kritischste Verbindung handelt. Das kann im schlimmsten Fall dazu führen, dass Alarme nicht weitergeleitet und somit nicht erkannt werden.
Zweites Schutzziel – Effektivität:
Es ist abzuklären, ob die Funktion des Medizingerätes beeinträchtigt werden kann, wenn die Patientenstammdaten nicht oder nur unvollständig auf den Überwachungsmonitor übertragen werden.
Drittes Schutzziel – Daten- und Systemschutz:
Jede Datenübertragung stellt ein mögliches Risiko für den Daten- und Systemschutz dar. In diesem Bespiel sind alle Geräte über eine HL7-Schnittstelle miteinander verbunden, die Daten werden verschlüsselt übertragen. Einen weiteren Angriffspunkt stellt die Überwachungszentrale dar, wo die Patientendaten zugänglich sind.

Risikobewertung:
Bei der Bewertung der identifizierten Risiken werden Eintrittswahrscheinlichkeit und Schweregrad der Folgen gegenübergestellt. Mithilfe der Risikomatrix (Abbildung 7) ist das Risiko abzuschätzen.

Erstes Schutzziel – Sicherheit:

Werden die Vitalparameter und Alarme eines Intensivpatienten nicht weitergeleitet, kann dies mitunter zu schwerwiegenden gesundheitlichen Folgen bis hin zum Tod des Patienten führen. Der Schweregrad der Folgen kann in der Risikomatrix unter ‚katastrophal' eingegliedert werden. Die Eintrittswahrscheinlichkeit ist abhängig von der Ausfallhäufigkeit des Netzwerks bzw. dessen Verbindungen. In unserem Beispiel wird die Eintrittswahrscheinlichkeit als ‚gelegentlich' eingestuft. Somit fällt dieses Risiko in der Risikomatrix in den roten, inakzeptablen Bereich. Es müssen auf jeden Fall im nächsten Schritt Maßnahmen zur Minderung des Risikos getroffen werden.

Zweites Schutzziel – Effektivität:

Die Überwachung der Vitalparameter funktioniert auch ohne die Übertragung der Stammdaten des Patienten uneingeschränkt. Es ergeben sich, bei Ausfall dieses Übertragungsweges somit keine wesentlichen Folgen.

Drittes Schutzziel – Daten- und Systemschutz:

Geraten sensible Gesundheitsdaten in die falschen Hände handelt es sich um ‚kritische' Folgen. Die Eintrittswahrscheinlichkeit schwankt in unserem Bespiel zwischen ‚unwahrscheinlich' und ‚vorstellbar'. Somit landet dieses Risiko in der Matrix im gelben Bereich, das heißt es sind, wenn möglich, Maßnahmen zur Risikominderung umzusetzen.

Risikobeherrschung:

Je nach bewertetem Risiko ist es sinnvoll Maßnahmen zur Risikominderung zu finden und diese umzusetzen. Wenn technische Maßnahmen umgesetzt werden können, sollen diese zuerst erfolgen, gefolgt von organisatorischen Maßnahmen und zuletzt werden personenbezogene Maßnahmen umgesetzt. Anschließend kann eine neue Risikoanalyse bzw. -bewertung durchgeführt werden.

Erstes Schutzziel – Sicherheit:

Zur Vermeidung des Nicht-Erkennens eines Alarms muss zuerst überlegt werden, welche technische Maßnahmen umgesetzt werden können. Eine technische Maßnahme, welche Abhilfe schaffen kann ist, dass die Lautstärke des Alarms, welche am Patientenüberwachungsmonitor eingestellt werden kann, so weit erhöht wird, dass dieser jederzeit vom Pflegepersonal bemerkt wird, wenn sie sich am Stützpunkt oder auch an einem anderen Ort auf der Intensivstation aufhalten. Gleichzeitig soll die

Alarmlautstärke aber auch nicht störend auf die Patienten wirken. Weiters wäre es von Nöten, als organisatorische bzw. personenbezogene Maßnahme, das Personal über den erlaubten Aufenthaltsbereich zu schulen. Das Pflegepersonal darf sich nur in diesem Bereich aufhalten, in dem der Alarm, auch bei Ausfall der Weiterleitung zur Überwachungszentrale, zu hören ist. Außerdem soll eingerichtet werden, dass die Überwachungszentrale eine Fehlermeldung anzeigt, sobald keine Daten vom Überwachungsmonitor übermittelt werden. Durch Umsetzung dieser Maßnahmen kann bei erneuter Risikobewertung der Schweregrad der Folgen auf ‚gering' reduziert werden. Das bedeutet, dass bei ‚gelegentlichem' Ausfall das Risiko vom roten Bereich der Risikomatrix in den gelben Bereich gemindert wurde.

Um die Eintrittswahrscheinlichkeit ebenfalls zu mindern gilt es die Ursache der fehlgeschlagenen Alarmweiterleitung zu bekämpfen. Hierfür können zum einen die Bandbreite erhöht und zum anderen per Quality of Service wichtige Datenübertragungen, wie Alarme, gegenüber weniger wichtigen Daten priorisiert werden, wenn es zu einer Netzüberlastung kommt. Somit kann auch die Eintrittswahrscheinlichkeit von ‚gelegentlich' auf ‚unwahrscheinlich' reduziert werden, somit wandert das Risiko in der Risikomatrix in den grünen Bereich.

Zweites Schutzziel – Effektivität:

Trotz des unwesentlichen Schweregrades der Folgen kann durch eine erhöhte Bandbreite und einer priorisierten Datenübertragung, die Eintrittswahrscheinlichkeit dieses Risikos gemindert und somit das Risiko im grünen Bereich eingestuft werden.

Drittes Schutzziel – Daten- und Systemschutz:

Mit den standardisierten Schnittstellen und der Verschlüsselung der Daten sind schon wichtige Kriterien für den Daten- und Systemschutz erfüllt. Eine weitere wichtige Maßnahme stellt die Zugriffsbeschränkung mittels Authentifizierung dar. Befindet sich kein Pflegepersonal im Stützpunkt, dürfen die PC-Arbeitsplätze nicht frei zugänglich sein. Dies kann so realisiert werden, dass der Computer schon nach kurzer Zeit der Nichtbenutzung, erneut eine Authentifizierung erfordert. So kann verhindert werden, dass nicht befugte Personen Zugriff auf die sensiblen Patientendaten erhalten. Außerdem kann neben diesen organisatorischen Maßnahmen, auch die personenbezogene Maßnahme der Schulung der Mitarbeiter umgesetzt werden. Ziel hierbei ist es, das Personal darauf zu schulen, bei Emails auf den Absender zu achten und keine unbekannten Dateianhänge oder Links zu öffnen. Außerdem sind alle Mitarbeiter darauf hinzuweisen, keine Informationen an Außenstehende und nicht

autorisierte Personen weiterzugeben. Das Schwereausmaß der Folgen liegt nach Umsetzung dieser Maßnahmen noch immer im ‚kritischen' Bereich, die Eintrittswahrscheinlichkeit konnte auf ‚unwahrscheinlich' gesenkt werden. Nach Durchführung aller möglichen Maßnahmen liegt das Risiko immer noch im gelben Bereich der Risikomatrix.

In Tabelle 4 ist der beschriebene Prozess zur Veranschaulichung als vereinfachte FMEA tabellarisch dargestellt.

	Risikoanalyse			Risikobewertung				Risikobeherrschung			
	Mögliche Fehler			Derzeitige Situation				Empfohlene Maßnahmen			
	Art	Folgen	Ursachen	Maß-nahmen	Eintritts-wahrsch.	Schwere-grad	Gesamt-bewertung	Empfohlene Maßnahmen	Eintritts-wahrsch.	Schwere-grad	Gesamt-bewertung
Schutzziel Sicherheit	Alarme werden nicht weiter-geleitet	Alarme werden nicht sofort erkannt	Netzwerkausfall/-überlastung	keine	gele-gentlich	katastrophal	roter Bereich	Lautstärke des Alarmtons beim Pat.-monitor erhöhen	unwahr-scheinlich	gering	grüner Bereich
			Hardwarefehler					Schulung des Pflegepersonals über Aufenthaltsbereich			
								Fehlermeldung bei Überwachungszentrale			
								Bandbreite nachrüsten			
								wichtige Datenübertragungen priorisieren			
Schutzziel Effektivität	Patientendaten werden nicht vollständig übertragen	Keine	Netzwerkausfall/-überlastung	keine	gele-gentlich	un-wesentlich	gelber Bereich	Bandbreite nachrüsten	unwahr-scheinlich	unwesent lich	grüner Bereich
			Hardwarefehler					wichtige Datenübertragungen priorisieren			
Schutzziel Daten- und Systemschutz	Sicherheitslücken bei der Daten-übertragung	Sensible Daten gelangen in falsche Hände	Keine/ unzureichende Verschlüsselung	HL7-Schnitt-stellen	unwahr-scheinlich	kritisch	gelber Bereich	keine	-	-	-
	Zugängliche Patientendaten in Zentrale		unzureichende Zugriffs-beschränkungen	keine	vorstellbar	kritisch	gelber Bereich	Zugriffsbeschränkung mittels Authentifizierung	unwahr-scheinlich	kritisch	gelber Bereich
								Schulung der Mitarbeiter			

Tabelle 4: FMEA Beispiel 1 - Überwachungsmonitor

Bewertung des Restrisikos:

In Tabelle 5 ist die Risikomatrix für dieses Beispiel nach der Umsetzung der Maßnahmen zur Risikobeherrschung dargestellt.

Das gesamte Restrisiko konnte auf ein mittleres Maß gesenkt werden. Durch die Einhaltung aller gesetzten Maßnahmen und einer regelmäßigen Risikoüberwachung, kann das Restrisiko als vertretbar eingeschätzt werden.

		erwartetes Schadensausmaß			
		unwesentlich	gering	kritisch	katastrophal
Eintrittswahrscheinlichkeit	unvorstellbar				
	unwahrscheinlich	Patientendaten werden nicht vollständig übertragen	Alarme werden nicht weitergeleitet	Sicherheitslücken bei der Daten-übertragung zugängliche Patientendaten	
	vorstellbar				
	gelegentlich				
	wahrscheinlich				
	häufig				

Tabelle 5: Risikomatrix nach der Durchführung der Risikobeherrschung - Beispiel 1 - Überwachungsmonitor

4.3.2 Beispiel 2: Bildgebende Diagnostik mittels CT

In Abbildung 9 ist der Datenverlauf einer bildgebenden CT-Untersuchung dargestellt.

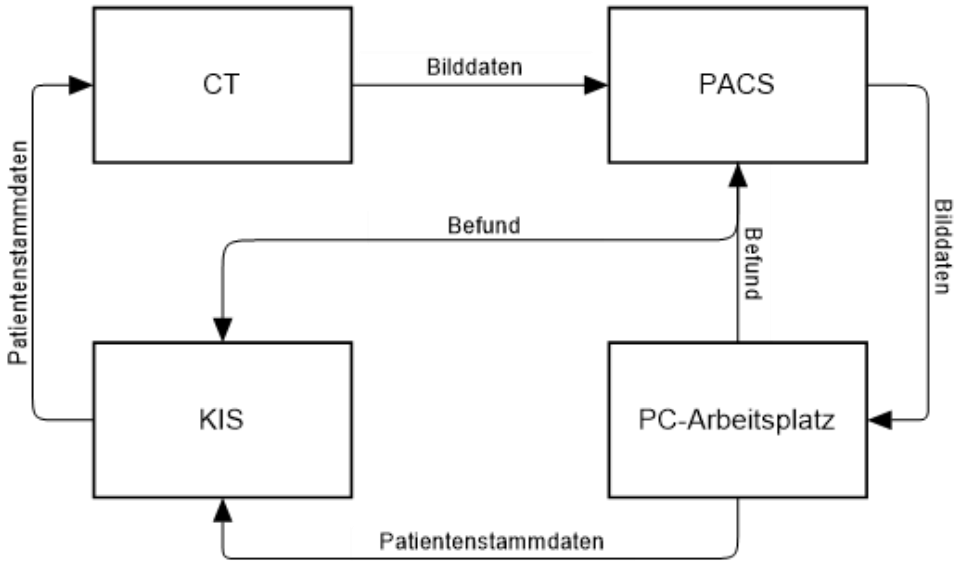

Abbildung 9: Beispiel 2 Bildgebende Diagnostik mittels CT - Skizzierung des Datenverlaufs

Zu Beginn werden die Patientenstammdaten an einem PC aufgenommen und an das KIS übertragen. Das KIS wiederum leitet die für die Untersuchung benötigten Daten an das CT-Gerät weiter. Nach der Untersuchung werden die Bilddaten an das PACS übergeben, welche jederzeit über einen PC-Arbeitsplatz abgerufen werden können, um z.B. den Befund fertigzustellen. Dieser Befund wird sowohl im PACS gespeichert als auch im KIS hinterlegt.

Risikoanalyse:
Zu Beginn werden wiederum die Risiken, welche durch die Einbindung entstehen, identifiziert.
Erstes Schutzziel – Sicherheit:
Das größte Risiko für die Sicherheit der Patienten besteht darin, dass die Bilddaten nicht weitergeleitet werden können und somit keine Diagnose gestellt werden kann.
Zweites Schutzziel – Effektivität:
Nach der Eingabe der, bei der Anamnese ermittelten, Patientendaten, werden diese und die Anforderungsbestimmungen an die Untersuchung über das KIS an das CT-

Gerät weitergeleitet. Ohne Informationen über den zu untersuchenden Bereich kann keine Bildgebung stattfinden.
Drittes Schutzziel – Daten- und Systemschutz:
Jede Schnittstelle stellt in diesem Szenario ein Risiko dar. Bei jeder Übertragung besteht die Gefahr, dass Patienten-, Bild- oder Befunddaten an nicht befugte Personen gelangen.

Risikobewertung:
Anschließend werden die identifizierten Risiken mithilfe der Risikomatrix bewertet.
Erstes Schutzziel – Sicherheit:
Würde die CT-Untersuchung keine Bilddaten hervorbringen, kann dies bei akuten Fällen zu ‚katastrophalen' Risiken führen. Da aber die Ergebnisse der Untersuchung im Fall der Nichtweiterleitung der Daten auch direkt vom CT-Gerät abgelesen werden können, kann das Schadensausmaß auf ‚gering' gesenkt werden. Bei einer ‚gelegentlichen' Eintrittswahrscheinlichkeit, befinden wir uns im gelben Bereich der Risikomatrix.
Zweites Schutzziel – Effektivität:
In unserem Beispiel ist die Funktion des CT-Gerätes auch bei Ausfall der Datenweiterleitung gewährleistet, da die benötigten Untersuchungsdaten auch manuell direkt am CT eingegeben werden können.
Drittes Schutzziel – Daten- und Systemschutz:
Ähnlich wie beim ersten Beispiel landen wir wiederum im gelben Bereich der Risikomatrix, wenn die Folgen für den Daten- und Systemschutz als ‚kritisch' und die Eintrittswahrscheinlichkeit als ‚unwahrscheinlich' bis ‚vorstellbar' eingestuft werden.

Risikobeherrschung:
In diesem Schritt werden Maßnahmen zusammengefasst, welche für die Risikominderung umgesetzt werden können.
Erstes Schutzziel – Sicherheit:
Um das Risiko einer Netzwerküberlastung mindern zu können, kann man auf eine höhere Bandbreite und eine priorisierte Datenübertragung von wichtigen Daten per Quality of Service setzen. Somit kann die Eintrittswahrscheinlichkeit von ‚gelegentlich' auf ‚unwahrscheinlich' gemindert und das Risiko somit im grünen Bereich eingestuft werden.

Zweites Schutzziel – Effektivität:
Um für dieses Schutzziel das Risiko im grünen Bereich einstufen zu können, kann auch hier mit einer größeren Bandbreite und einer Priorisierung von wichtigen Datenübertragungen die Eintrittswahrscheinlichkeit von ‚gelegentlich' auf ‚unwahrscheinlich' gesenkt werden.
Drittes Schutzziel – Daten- und Systemschutz:
Um die Gesundheitsdaten bestmöglich zu schützen, sollen wie in Beispiel 1, organisatorische Maßnahmen der Authentifizierung und Zugriffsbeschränkungen und personenbezogene Maßnahmen, wie Schulungen, umgesetzt werden. Technische Voraussetzungen zum Schutz der übertragenen Daten, wie eine Schnittstellenstandardisierung und eine Verschlüsselung der Daten sind schon gegeben.

Die Darstellung dieser Schritte ist wiederum in exemplarischer Form einer verkürzten FMEA zur Veranschaulichung in Tabelle 6 abgebildet.

	Risikoanalyse			Risikobewertung				Risikobeherrschung			
	Mögliche Fehler			Derzeitige Situation				Empfohlene Maßnahmen			
	Art	Folgen	Ursachen	Maß-nahmen	Eintritts-wahrsch.	Schwere-grad	Gesamt-bewertung	Empfohlene Maßnahmen	Eintritts-wahrsch.	Schwere-grad	Gesamt-bewertung
Schutzziel Sicherheit	Bilddaten werden nicht weiter-geleitet	Diagnose kann nicht erfolgen	Netzwerkausfall/-überlastung Hardwarefehler	Bilddaten können vom CT direkt abgelesen werden	gele-gentlich	gering	gelber Bereich	Bandbreite nachrüsten wichtige Datenübertragungen priorisieren	unwahr-scheinlich	gering	grüner Bereich
Schutzziel Effektivität	Patientendaten werden nicht vollständig übertragen	Unter-suchung nicht möglich	Netzwerkausfall/-überlastung Hardwarefehler	Patienten-daten können direkt am CT eingegeben werden	gele-gentlich	un-wesen-tlich	gelber Bereich	Bandbreite nachrüsten wichtige Datenübertragungen priorisieren	unwahr-scheinlich	un-wesen-tlich	grüner Bereich
Schutzziel Daten- und Systemschutz	Sicherheitslücken bei der Daten-übertragung	Sensible Daten gelangen in falsche Hände	Keine/ unzureichende Verschlüsselung	HL7-Schnitt-stellen	unwahr-scheinlich	kritisch	gelber Bereich	keine	-	-	-
	zugängliche Patientendaten		unzureichende Zugriffs-beschränkungen	keine	vorstellbar	kritisch	gelber Bereich	Zugriffs-beschränkung mittels Authentifizierung Schulung der Mitarbeiter	unwahr-scheinlich	kritisch	gelber Bereich

Tabelle 6: FMEA Beispiel 2 - Bildgebende Diagnostik mittels CT

Bewertung des Restrisikos:

In Tabelle 7 ist die Risikomatrix nach Durchführung der Risikobeherrschung dargestellt. Es konnte nur eine minimale Verbesserung erreicht werden. Das Restrisiko kann auch in diesem Beispiel als vertretbar eingestuft werden.

		erwartetes Schadensausmaß			
		unwesentlich	gering	kritisch	katastrophal
Eintrittswahrscheinlichkeit	unvorstellbar				
	unwahrscheinlich	Patientendaten werden nicht vollständig übertragen	Bilddaten werden nicht weitergeleitet	Sicherheitslücken bei der Daten-übertragung zugängliche Patientendaten	
	vorstellbar				
	gelegentlich				
	wahrscheinlich				
	häufig				

Tabelle 7: Risikomatrix nach der Durchführung der Risikobeherrschung - Beispiel 2 - Bildgebende Diagnostik mittels CT

5 Diskussion

Wie zu Beginn in der Einleitung schon erwähnt, wächst der Markt für Medizinprodukte kontinuierlich. Hierfür gibt es verschiedene Gründe. Zum einen führt die demografische Entwicklung dazu, dass der Anteil der älteren Personen in unserer Bevölkerung stark ansteigt und somit immer mehr medizinische Behandlungen erforderlich werden. Zum anderen geht der Trend auch für die jüngere Bevölkerungsschicht in Richtung Gesundheit. Das Gesundheitsbewusstsein wurde in den letzten Jahren zu einem Statussymbol. Aus diesem Grund sind die Menschen bereit, mehr Geld für ihre Gesundheit auszugeben.
Außerdem ist noch zu erwähnen, dass die Forschung im Bereich der Medizintechnik große Fortschritte macht und dadurch viele neue Medizingeräte auf den Markt kommen. [29]
Außerdem zeichnete sich in den letzten Jahren eine enorme Digitalisierung ab, welche noch nicht an ihrem Höhepunkt angekommen ist. Die Schwierigkeit besteht nun darin diesen erhöhten Bedarf an Medizingeräten in die immer komplexer vernetzte IT-Infrastruktur einzubinden.
In einigen Jahren werden voraussichtlich alle Geräte in einer Gesundheitseinrichtung miteinander vernetzt sein. Verliert man jetzt den Anschluss, wird es schwer dies wieder aufzuholen. Deshalb ist es von großer Bedeutung den Einbindungsprozess zu standardisieren und ein umfangreiches Risikomanagement durchzuführen. Dies bedeutet einen großen Arbeitsaufwand zur Vorbereitung und Planung am Beginn, ist dieser Prozess aber einmal genau geregelt, fallen die zukünftigen Schritte deutlich leichter. Eine weitere Problematik, welcher sich Gesundheitseinrichtungen stellen müssen, ist die Budgetierung. Oftmals bleibt für den IT-Bereich nur ein kleiner Anteil des Budgets übrig, da der Großteil für medizinische Bereiche verwendet wird. Mit diesem Bruchteil muss der IT-Bereich auskommen, wobei bei der Einführung eines vereinheitlichten Einbindungsprozesses vor allem personelle Ressourcen gefragt sind, welche in den meisten Fällen kaum im Überfluss vorhanden sind. Dem benannten Med-IT-Risikomanager soll genügend Zeit zur Verfügung stehen, um sich mit dieser Thematik intensiv auseinandersetzen zu können.

Dokumentation:

Ein erster essentieller Schritt, um diese Herausforderung meistern zu können, ist eine vollständige und aktuelle Dokumentation aller relevanten Bereiche. Dies beginnt bei der Dokumentation des bestehenden IT-Netzwerks. Sind die Unterlagen des IT-Netzwerk nicht auf dem aktuellen Stand, kann keine genau Risikoanalyse und -bewertung durchgeführt werden. Deshalb ist es von großer Bedeutung, bevor ein Risikomanagement für die Einbindung von Medizingeräten startet, die Dokumentation des IT-Netzwerks auf Vollständigkeit und Aktualität zu überprüfen und gegebenenfalls zu ergänzen. Dieser Schritt kann unter Umständen umfangreicher ausfallen als erwartet, da die Netzwerke in Gesundheitseinrichtungen erfahrungsgemäß immer weiter ausgebaut wurden, um den in den letzten Jahren steigenden Anforderungen und der wachsenden Digitalisierung im Gesundheitsbereich gerecht werden zu können. Dabei ist fraglich, ob die am Anfang bestandene Dokumentation übersichtlich erweitert wurde. Dies scheint unter Umständen fast unmöglich zu sein, da sich die IT-Netzwerke in den letzten Jahren so stark verändert haben und um ein Vielfaches gewachsen sind. Daher kann es sinnvoll sein, einen Netzwerkplan komplett neu zu skizzieren und auch Raum für Erweiterungen vorzusehen. Die Dokumentation des IT-Netzwerks bildet eine wichtige Grundlage, erst wenn dies vollständig erledigt ist, kann zu dem nächsten Schritt übergegangen werden.

Die Bedeutung einer umfassenden Dokumentation startet beim IT-Netzwerk und zieht sich durch den gesamten Einbindungsprozess. Jeder Prozessschritt soll dokumentiert werden, vom Einbindungswunsch angefangen, über den gesamten Risikomanagementprozess, bis hin zur tatsächlichen Einbindung. Dies gilt nicht nur für den Einbindungsprozess an sich, sondern eine umfassende Dokumentation soll über den gesamten Lebenszyklus eines Medizingerätes, bis hin zu seiner Ausscheidung, erfolgen. Im Idealfall erfolgt die Dokumentation über einheitliche, verfügbare Formulare und vorgefertigte Dokumente, um eine Vereinheitlichung und dadurch eine bessere Nachvollziehbarkeit erreichen zu können.

Zusammengefasst sind die wichtigsten Kriterien für eine effiziente Dokumentation Vollständigkeit, Aktualität, Zugänglichkeit, Einheitlichkeit und Nachvollziehbarkeit.

Eine vollständige und aktuelle Dokumentation stellt wahrscheinlich eine der größten Herausforderungen, aber auch einen der wichtigsten Grundsteine für die Durchführung eines Risikomanagements dar. Nur so kann eine Transparenz der durchgeführten Schritte erzielt werden.

Risikoanalyse:

Ein Vorteil der meisten Bottom-Up-Ansätze, wie auch der FMEA, ist die systematische Herangehensweise. Dadurch, dass alle Komponenten einzeln betrachtet werden, wird das Risiko, einen möglichen Fehler zu übersehen, gemindert. Logische Verknüpfungen sind bei einer FMEA wiederum nicht möglich, was als Nachteil einzustufen ist, weil mögliche Zusammenhänge nicht so gut dargestellt werden können. Um einen Überblick über die logischen Zusammenhänge zu bekommen, bietet sich zur grafischen Veranschaulichung eine Anwendung der FTA an. Um die Vorteile von beiden Ansätzen vereinen zu können und die Chance auf Entdeckung von so vielen Risiken wie möglich zu erhöhen, besteht die Möglichkeit beide Verfahren anzuwenden. Zuerst für eine systematische Analyse eine FMEA, anschließend zur grafischen und logischen Veranschaulichung eine FTA.

Um einen Ablauf auf seine korrekte Vorgehensweise prüfen zu können, empfiehlt sich das HACCP-Verfahren. Diese Methode geht über eine Risikoanalyse hinaus, es können Risiken identifiziert, die Einhaltung von Grenzen kontrolliert und Fehler sofort behoben werden, allerdings muss die Möglichkeit der Einrichtung von Kontrollpunkten bestehen. Außerdem müssen Grenzwerte festgelegt werden, bei deren Über- oder Unterschreitung an den Kontrollpunkten Maßnahmen gesetzt werden.

Im Allgemeinen kann davon abgeraten werden, sich auf eine Methode zu versteifen. Kombiniert man mehrere Methoden zur Risikoanalyse miteinander, erreicht man meist ein besseres und vielfältigeres Ergebnis.

Um einen besseren Überblick über die Risiken zu bekommen, ist es von Nöten die Risikoanalyse in die drei Bereiche der Schutzziele aufzuteilen, wie in den Ergebnissen schon erwähnt. So steht immer ein Schutzziel und die daraus resultierenden Risiken im Fokus. Problematisch bei jeder Risikoanalyse ist, dass man nie weiß, ob alle Risiken miteinbezogen wurden. Es besteht keine Möglichkeit einer Rückmeldung oder Kontrolle. Aus diesem Grund ist es zum einen sinnvoll verschiedene Varianten der Risikoanalyse zu kombinieren und zum anderen alle beteiligten Berufsgruppen miteinzubeziehen. Durch die Kombination der verschiedenen Blickwinkel aus Medizin, Pflege, IT und Medizintechnik, wird die Chance auf Entdeckung möglichst vieler Risiken erhöht. Nicht nur innerbetriebliche Sichtweisen sind von Bedeutung, auch die Risiken, welche von der Herstellerseite aus existieren, sind zu berücksichtigen und in die Analyse miteinzubeziehen. Nur durch die Zusammenarbeit der verschiedenen Bereiche kann eine umfassende Risikoanalyse durchgeführt werden.

Risikobewertung:

Die Risikobewertung erfolgt für jedes identifizierte Risiko individuell. Wie in den Ergebnissen schon erwähnt, ist es sinnvoll für jedes der drei Schutzziele eine eigene Risikomatrix mit angepassten Risikoakzeptanzkriterien zu entwickeln, da jedes Schutzziel andere Merkmale hat, welche als kritisch zu betrachten sind. Die Risikoakzeptanzkriterien sollen hierbei dynamisch gestaltet werden, das heißt eine Anpassung an den neuesten Stand der Technik und andere sich ändernde Begebenheiten soll möglich sein.

Im Normalfall wird für die Risikobewertung bei der FMEA die Risikoprioritätszahl (RPZ) berechnet. Diese ergibt sich aus der Multiplikation der Werte für den Schweregrad der Folgen, die Eintrittswahrscheinlichkeit und die Entdeckungswahrscheinlichkeit. Die Werte, welche multipliziert werden, liegen zwischen 1 und 10. 1 steht für eine geringe Eintrittswahrscheinlichkeit, ein geringes Ausmaß der Folgen und eine hohe Entdeckungswahrscheinlichkeit. Für einen hohen Schweregrad der Auswirkungen, eine hohe Eintritts- und eine geringe Entdeckungswahrscheinlichkeit wird der Wert 10 verwendet. Nach diesem Prinzip müssen die drei Faktoren abgeschätzt werden. Je höher nun die RPZ ist, desto höher ist das Risiko. Da aber die RPZ nicht der Risikobewertung der Norm DIN EN ISO 14971 entspricht, wurde in dieser Masterarbeit auf diese Form der Risikobewertung verzichtet. Zum einen besagt diese Norm für Risikomanagement für Medizinprodukte, dass sich das Risiko aus zwei Werten ergibt: des Ausmaßes des Schadens und der Eintrittswahrscheinlichkeit. Auf die Entdeckungswahrscheinlichkeit wird bei dieser Definition nicht eingegangen. Außerdem wird in der DIN EN ISO 14971 noch einmal explizit erwähnt, dass sich das Risiko nicht aus der Multiplikation der Faktoren ergibt. [6] Aus diesen Gründen wurde in dieser Arbeit eine zweidimensionale Risikomatrix, mit dem Schwereausmaß der Folgen an der einen und der Eintrittswahrscheinlichkeit an der anderen Achse, verwendet. Wenn also in den vorangegangenen Zeilen von der Durchführung der FMEA gesprochen wurde, ist nicht die FMEA mit Berechnung der RPZ als Risikobewertung gemeint, sondern die FMEA als Risikoanalyse. Die Bewertung des Risikos erfolgt getrennt davon.

Der Risikomanagementprozess muss über den gesamten Lebenszyklus eines Medizingerätes erfolgen. Vor allem wenn eine Veränderung vorgenommen wird, welche die Einbindung des Medizingerätes und dessen Datenübertragung betreffen,

muss eine erneute Risikoanalyse, -bewertung und -beherrschung durchgeführt werden.

Prozessdiagramm:
Das in Abbildung 3 und Abbildung 4 dargestellte Prozessdiagramm dient nur als beispielhafte Darstellung, wie der Einbindungsprozess in ein IT-Netzwerk gesetzes- und normenkonform ablaufen kann. Hierbei können einzelne Prozesse z.B. vertauscht werden. Wichtig sind der geregelte Ablauf und ein strukturierter Risikomanagementprozess. Es muss immer die Sicherheit abgefragt werden, bei eventuell auftretenden Risiken Maßnahmen zur Minimierung dieser, wenn möglich, umgesetzt werden und anschließend hinterfragt werden, ob durch diese Umsetzung eventuell neue Risiken entstanden sind. Abschließend muss immer das verbleibende Restrisiko bewertet werden.
Entscheidend ist eine genau definierte Anweisung des Einbindungsverfahrens zur Standardisierung des Prozesses.

Standardisierte Schnittstellen:
Ein weiterer wichtiger Punkt um den Einbindungs- und Risikomanagementprozess vereinheitlichen zu können, sind standardisierte Schnittstellen. Wenn bei allen Medizingeräten die gleichen Schnittstellen benutzt werden, kann auch der Einbindungsprozess standardisiert werden. Einen weiteren positiven Ansatz erkennt man beim OR.NET-Projekt, welches in der Einleitung kurz vorgestellt wurde. Ursprünglich wurde dieses System entwickelt, um Geräte in Operationssälen miteinander verbinden zu können und eine Kommunikation zwischen den verwendeten Medizingeräten zu ermöglichen, weil in diesem Bereich besonders viele Medizingeräte gleichzeitig verwendet werden. Es ist aber denkbar, dass dieses Kommunikationssystem auch in anderen Bereichen Verwendung findet, wie im Intensivbereich, im Rettungswesen, aber auch im ambulanten Bereich. Je mehr Bereiche mit den gleichen Systemen miteinander vernetzt sind, desto besser ist die Interoperabilität zueinander. Eine weitreichende Interoperabilität ist eines der wichtigsten Ziele in der Medizintechnik, standardisierte Schnittstellen bilden hierbei eine wichtige Grundlage.

Gesetzeskonformität:

Ein großer Teil dieser Masterarbeit bestand darin, die Gesetze und Normen, welche mit der Einbindung von Medizinprodukten in ein IT-Netzwerk in Zusammenhang stehen, zusammenzufassen und einen gesetzeskonformen Einbindungsprozess zu erarbeiten. Eine Kurzfassung über alle relevanten Normen zu dieser Thematik ist in der Einleitung ersichtlich. Zusammengefasst gibt es drei wichtige Gesetzte in Österreich, welche in Bezug auf Medizingeräte gelten. Das MPG, die MPBV und die MDR. Diese Gesetze müssen selbstverständlich eingehalten werden. Die MDR bezieht sich großteils auf den Herstellungsprozess und eine neue vereinheitlichte Form der Dokumentation und Registrierung von Medizinprodukten. Aber es wird auch auf eine Verpflichtung zur sicheren Zusammenstellung von Medizinprodukten und zur Anwendung von geeigneten Methoden zur Überprüfung und Überwachung dieser hingewiesen.

Neben den Gesetzen gibt es einige Normen, welche berücksichtigt werden sollten. Am bedeutendsten für diese Thematik sind die DIN EN 80001 und die DIN EN ISO 14971. Diese beziehen sich direkt auf das Risikomanagement für medizinische IT-Netzwerke bzw. auf das Risikomanagement von Medizinprodukten. Diese Normen bilden eine gute Grundlage für die Erarbeitung eines Einbindungs- und Risikomanagementprozesses. Aber die Einhaltung dieser Normen ist nicht gesetzlich gefordert und beruht somit auf freiwilliger Basis. Führt man eine Einbindung ohne Konzept und ohne einen Risikomanagementplan durch, kann dies schnell zu Problemen führen. Deshalb ist es von Vorteil sich nach den existierenden Normen zu halten und ein Risikomanagement nach DIN EN 80001 bzw. nach DIN EN ISO 14971 durchzuführen.

6 Schlussfolgerung

Das rasante Wachstum im digitalisierten, medizinischen Bereich erfordert von Gesundheitseinrichtungen gewisse Maßnahmen. Die Kommunikation und Vernetzung der Medizingeräte miteinander und mit dem IT-Netzwerk verlangt die Einführung eines standardisierten Einbindungsprozesses.

Ohne die Durchführung eines Risikomanagements kann die Einbindung eines Medizingerätes in ein IT-Netzwerk nicht verantwortet werden. Dabei geht es nicht darum, welche Werkzeuge zur Risikoanalyse verwendet werden, sondern darum, dass ein Prozess festgelegt wird, welcher ohne Ausnahme eingehalten werden muss. Wichtig hierbei ist, dass im Vorfeld alle Verantwortlichkeiten und Aufgabenbereiche klar definiert werden. Das Risikomanagement begleitet den gesamten Lebenszyklus des Medizingerätes. Bei jeder Änderung der Zusammenstellung muss eine erneute Risikoanalyse, -bewertung und -beherrschung durchgeführt werden.

Einer der wichtigsten Punkte ist die Vereinheitlichung. Darunter fällt die Vereinheitlichung der Dokumentation, der Prozesse und der Schnittstellen. Eine vereinheitlichte Dokumentation unterstützt die Nachvollziehbarkeit der einzelnen Schritte. Auch eine Standardisierung der Prozesse ist notwendig, um für Transparenz zu sorgen. Standardisierte Schnittstellen sorgen für einen hohen Grad an Interoperabilität. Im Idealfall kommunizieren alle Geräte innerhalb einer Gesundheitseinrichtung über die gleichen Schnittstellen. HL7, für textbasierte Kommunikation, und DICOM, für die Bildgebung, stellen schon internationale Standards dar. Jedoch existieren auch noch viele andere, nicht so weit verbreitete Insellösungen, von welchen aber klar Abstand genommen werden sollte. Ziel wäre es, dass international die gleichen standardisierten Schnittstellen verwendet werden, um eine flächendeckende Interoperabilität erreichen zu können. Somit würden auch keine Unterschiede für die Einbindung bzw. für die Interoperabilität bei Geräten unterschiedlicher Hersteller mehr entstehen.

Es besteht zwar eine gesetzliche Verpflichtung eine sichere Zusammenstellung bzw. Einbindung zu gewährleisten, jedoch steht dem Betreiber die genaue Durchführung frei. Hierbei ist es sinnvoll, eine normengerechte Umsetzung der Einbindung mit der Durchführung eines Risikomanagements zu realisieren.

Abbildungsverzeichnis

Tabellenverzeichnis

Literaturverzeichnis

[1] „(BASG), Bundesamt für Sicherheit im Gesundheitswesen," 20. 10. 2016. [Online]. Available: https://www.basg.gv.at/medizinprodukte/. [Zugriff am 27. 02. 2019].

[2] „Statista - Das Statistik Portal," Statista GmbH, 2018. [Online]. Available: https://de.statista.com/statistik/daten/studie/313462/umfrage/umsatzentwicklung-der-weltweiten-medizintechnikindustrie/. [Zugriff am 17. 02. 2019].

[3] ÖVE/ÖNORM, *EN ISO 13485,* OVE Österreichischer Verband für Elektrotechnik, 2016.

[4] *EN 80001-1 Anwendung des Risikomanagements für IT-Netzwerke, die Medizinprodukte beinhalten - Teil 1: Aufgaben, Verantwortlichkeiten und Aktivitäten,* Deutsche Fassung 2011.

[5] ÖVE/ÖNORM, *EN 60601-1 Medizinische elektrische Geräte - Teil 1: Allgemeine Festlegungen für die Sicherheit einschließlich der wesentlichen Leistungsmerkmale,* DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE, 2013.

[6] *EN ISO 14971 Medizinprodukte - Anwendung des Risikomanagements auf Medizinprodukte,* 2012.

[7] M. Zauner, „Die Herausforderung, medizinische IT-Netzwerke zu betreiben," in *Dienstleistungs-Management im Krankenhaus*, Wiesbaden, Springer Gabler, 2016, pp. 311-323.

[8] RIS, „Gesamte Rechtsvorschrift für Medizinproduktebetreiberverordnung," 2007. [Online]. Available: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20005279. [Zugriff am 06 10 2019].

[9] RIS, „Gesamte Rechtsvorschrift für Medizinproduktegesetz, Fassung vom 19.10.2019," 2018. [Online]. Available:

https://www.ris.bka.gv.at/GeltendeFassung/Bundesnormen/10011003/MPG%2c%20Fassung%20vom%2019.10.2019.pdf. [Zugriff am 19 10 2019].

[10] „Medical Device Regulation," 2020. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02017R0745-20200424. [Zugriff am 05. 12. 2020].

[11] „93/42/EWG," 11 10 2007. [Online]. Available: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1993L0042:20071011:de:PDF. [Zugriff am 13 01 2020].

[12] „90/385/EWG," 11 10 2007. [Online]. Available: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1990L0385:20071011:DE:PDF%20. [Zugriff am 13 01 2020].

[13] ÖVE/ÖNORM, *EN 62353 - Medizinische elektrische Geräte - Wiederholungsprüfungen und Prüfung nach Instandsetzung von medizinischen elektrischen Geräten,* ON Österreichisches Normungsinstitut, 2009.

[14] *EN 62304 Medizingeräte-Software - Software-Lebenszyklus-Prozesse,* 2006.

[15] „EN 61907," 2019. [Online]. Available: https://www.dke.de/de/normen-standards/dokument?id=3021356&type=dke%7Cdokument. [Zugriff am 12. 01. 2020].

[16] C. Johner, „Johner Institut," 24. 06. 2015. [Online]. Available: https://www.johner-institut.de/blog/iso-14971-risikomanagement/fault-tree-analysis-fta/. [Zugriff am 30. 01. 2020].

[17] C. Johner, „Johner Institut," 06. 07. 2015. [Online]. Available: https://www.johner-institut.de/blog/iso-14971-risikomanagement/fmea-bei-medizinprodukten/. [Zugriff am 30. 01. 2020].

[18] P. Tröger, Unsicherheit und Uneindeutigkeit in Verlässlichkeitsmodellen, Potsdam, Deutschland: Springer Vieweg, 2018.

[19] P. Ott, „Medical Standard Time," 05. 11. 2018. [Online]. Available: https://medical-standard-time.de/379/mst008-regulatory-risikomanagement-verfahren-pha-fta-fmea-hazop/. [Zugriff am 01. 02. 2020].

[20] C. Johner, „Johner Institut," 05. 09. 2019. [Online]. Available: https://www.johner-institut.de/blog/iso-14971-risikomanagement/hazop-iec-61882/. [Zugriff am 01. 02. 2020].

[21] DSGVO, „EU-Datenschutz-Grundverordnung (EU-DSGVO),“ 27. 04. 2016. [Online]. Available: https://www.datenschutz-grundverordnung.eu/grundverordnung/art-9-ds-gvo/. [Zugriff am 02. 02. 2020].

[22] A. Gärtner, „Kommunizierende medizinische Systeme und Netzwerke,“ in *Medizintechnik*, Berlin Heidelberg, Springer Verlag, 2011, pp. 773-780.

[23] S. Samonas, „The CIA strikes back: Redefining Confidentiality, Integrity and Availability in Security,“ JISSec (Journal of Information System Security), Virginia, USA, 2014.

[24] C. John, „DIN 80001-1: Risikomanagement von IT-Netzwerken mit integrierten Medizinprodukten,“ *Krankenhaus-IT Journal,* pp. 28-29, 05. 2013.

[25] H. Tanck, „Fusion von Medizintechnik und Informationstechnologie,“ in *Medizitechnik: Verfahren - Systeme - Informationsverarbeitung*, Berlin, Springer Verlag, 2015, pp. 749-758.

[26] „OR.NET: multi-perspective qualitative evaluation of an integrated operating room based on IEEE 11073 SDC,“ *International Journal of Computer Assisted Radiology and Surgery,* pp. 1461-1469, 08. 05. 2017.

[27] „OR.NET e.V.,“ OR.NET e.V., 2019. [Online]. Available: https://ornet.org/. [Zugriff am 16. 02. 2020].

[28] D. F. Portheine, „medizin&technik,“ Konradin Mediengruppe, 13. 06. 2019. [Online]. Available: https://medizin-und-technik.industrie.de/digitalisierung/medizingeraete-ueber-sdc-flexibel-vernetzen/. [Zugriff am 16. 02. 2020].

[29] BVMed, *Branchenbericht Medizintechnologien 2019,* 2019.