Implementierung eines Risikobewertungsverfahrens für vernetzte Medizinprodukte gemäß DIN EN 80001-1 anhand eines Fallbeispiels.

Bachelorarbeit

Zur Erlangung des ersten akademischen Grades

Bachelor of Science (B.Sc.)

Hochschule Ruhr West

Studiengang ‚Gesundheits- und Medizintechnologien'

Fachbereich 4

eingereicht von:

Adel Amo Matrikelnummer. 11014363

eingereicht am: 13.06.2023

Ort der Durchführung: Rotenburg (Wümme)

Erstprüfer: Prof. Dr. Hennig Andreas

Zweitprüfer: Dipl.-Ing. (FH) Lohfeld, Ulrich

EIDESSTATTLICHE ERKLÄRUNG

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbständig verfasst und keine anderen als die angegebenen Hilfsmittel benutzt habe. Die Stellen der Arbeit, die dem Wortlaut oder dem Sinn nach anderen Werken entnommen wurden, wurden unter Angabe der Quelle kenntlich gemacht. Die Arbeit wurde in gleicher Weise oder ähnlicher Form bisher bei keiner anderen Institution eingereicht.

_____ _____

Rotenburg (Wümme), Datum Unterschrift

INHALTSVERZEICHNIS

1 EINLEITUNG

Der Arbeitsalltag in einem Krankenhaus ist nicht nur für Mitarbeiter eine Herausforderung, sondern auch für die erforderlichen IT-Netzwerke. Diese gewinnen aufgrund von strengen Datenschutz- und -Sicherheitsrichtlinien sowie sich ständig weiterentwickelnden Technologien immer mehr an Bedeutung. Erstmalig wurden sie bei der Verwaltung und bei Abrechnungen eingesetzt. Doch mit der zunehmenden Vernetzbarkeit von Geräten wurde das Netzwerk stetig erweitert. Hierbei spielte die Dokumentation von Patientendiagnosen eine Rolle: In kurzer Zeit konnten mehr Diagnosestellungen erfolgen und im System verwaltet werden. Bei bildgebenden Medizinprodukten wird vermehrt das IT-Netzwerk zur Übertragung und zur Speicherung von Patientendaten verwendet. Medizinprodukte sind jene Geräte, Gegenstände und Stoffe sowie Software, die zur diagnostische und therapeutische zwecks für Menschen verwendet werden.[7] In einem Krankenhaus gibt es eine Vielzahl von Medizinprodukten und dazugehörigen Komponenten, die an das IT-Netzwerk angeschlossen werden. Hierbei ist es bedeutsam, dass neue Standards eingeführt werden, um die Kommunikation zwischen den Geräten zu erleichtern sowie die damit verbundene Überlastung des IT-Netzwerks zu vermindern.

1.1 Ausgangssituation und Problemstellung

Standards sind unter der Bezeichnung ‚Normen' bekannt und existieren auch in der Medizintechnik. Eine davon ist die DIN EN 60601-1:2006, die Hersteller von Medizinprodukten verpflichtet Informationen über das Gerät zu erteilen, um dieses sicher an das Netzwerk anschließen zu können ([4], Absatz. „Zeitschiene und Anhang A1:2013"). Hierbei besteht das Problem, dass der einzelne Hersteller nur für seine Produkte Informationen erteilt und eine Verbindung möglich macht. Sobald mehrere Geräte von verschiedenen Herstellern in einem Netzwerk zusammentreffen, kann keiner von diesen für Probleme herangezogen werden, die bei einer Überlastung des Netzwerks auftreten, was somit die sichere Nutzung der Geräte verhindert. Um dem zu begegnen, wurde die DIN EN 80001-1 geschaffen.
In einem Krankenhaus ist dessen Betreiber für das IT-Netzwerk zuständig. Die DIN EN 80001-1 richtet sich auch an ihn. Sie klärt die Verantwortlichkeit zwischen den Parteien, die in einem medizinischen IT-Netzwerk verbunden werden sollen. Sowohl dessen Betreiber als auch der Hersteller von Medizinprodukten werden auf ihre Pflichten aufmerksam gemacht, die nach der Norm erfüllt werden müssen. Die Durchführung eines Risikomanagements für das gesamte IT-Netzwerk ist eine Aufgabe, die von der DIN EN 80001-1 vorgeschrieben wird. Damit soll die Kommunikation verbessert werden. Hierdurch ist die Überlastung des IT-Netzwerks geringer und somit kann ein Gerät sicher betrieben werden.

1.2 Ziele

Mit der Bachelorarbeit wird das Ziel verfolgt, mit dem AGAPLESION DIAKONIEKLINIKUM ROTENBURG als Betreiber des IT-Netzwerks und mit der Agaplesion AMTech gGmbH als Dienstleister, sowie den Herstellern, die DIN EN 80001-1 einzuführen. Dafür soll ein besseres Verständnis hinsichtlich der Kommunikation zwischen den einzelnen medizinischen Geräten entwickelt werden, um die volle Leistung bei der Nutzung von vernetzten Geräten zu ermöglichen. Dazu werden anhand eines Beispiels, nämlich eines mobilen Ultraschallgeräts (GE VScan Air), die Schritte, die in der DIN EN 80001-1 aufgeführt werden, im Krankenhaus AGAPLESION DIAKONIEKLINIKUM ROTENBURG durchgeführt. Hierbei sollen die folgenden Fragen beantwortet werden:

1) Gibt es Ansätze die die DIN EN 80001-1 in der AGAPLESION-Gruppe im Allgemeinen und im AGAPLESION DIAKONIEKLINIKUM ROTENBURG bisher umgesetzt wird?

2) Ist der vorhandene Prozess zur Umsetzung ausreichend, um die Schutzziele der DIN EN 80001-1 einzuhalten?

3) Gibt es Verbesserungspotentiale, die in der DIN EN 80001-1 nicht berücksichtigt werden, durch die aber der Prozess und somit die Norm besser etabliert werden können?

1.3 Aufbau der Arbeit

Um die Ziele der Bachelorarbeit schrittweise zu erreichen, wird im Folgenden eine Einführung in die DIN EN 80001-1 gegeben. Danach wird die Methode zur Einführung der Norm im AGAPLESION DIAKONIEKLINIKUM ROTENBURG präsentiert, wobei auf die Struktur der Dokumentation und die Einführung der Prozesse eingegangen wird. Im letzten Schritt wird die Implementierung anhand eines Beispiels durchgeführt. Hierbei wird geprüft, wie gut die Norm umsetzbar ist und welche Probleme dabei auftreten. In der Zusammenfassung werden alle Informationen verknüpft und die daraus resultierenden Probleme vorgestellt und anschließend diskutiert.

2 Grundlagen der DIN EN 80001-1

Die DIN EN 80001-1 beschreibt das Risikomanagement bei vernetzten Medizinprodukten in IT-Systemen in Krankenhäusern. Sie gilt ebenso für alle Anbieter von Gesundheitsdienstleistungen. Die Sicherheit der Patienten und der Anwender, aber auch von Dritten ist eines der Hauptschutzziele der Norm. Zu den weiteren Schutzzielen gehören die Daten- und Systemsicherheit sowie die Effektivität. In der DIN EN 80001-1 wird beschrieben, dass ein Risikomanagementprozess eingeführt werden muss. Des Weiteren ist ein Risikomanager im Bereich der Medizintechnik oder der IT-Technik zu ernennen empfehlenswert, da dieser einen direkte Verbindung zu dem Thema hat. Dieser soll die Prozesse überwachen und gegebenenfalls ändern und umsetzen. Die Dokumentation der einzelnen Schritte ist eine weitere Aufgabe des Risikomanagers ([1], S. 6).

2.1 Überblick über die Aufgabenverteilung

In der DIN EN 80001-1 wird der Betreiber des medizinischen IT-Netzwerks dazu verpflichtet, dessen sicheren Betrieb zu gewährleisten. Bei ihm liegt somit die Gesamtverantwortung des Risikomanagements. Sein Aufgabenbereich betrifft den diesbezüglichen Prozess von der Planung und der Installation bis hin zur Wartung und zur Ausmusterung der Geräte. Die Vereinbarung wird dann benötigt, wenn mehr als ein Medizinprodukthersteller das Gerät in das IT-Netzwerk einbinden will. Somit ist der höchstrangige Betreiber des IT-Netzwerks dafür zuständig, Richtlinien für das Risikomanagement bezüglich der Vernetzung von Medizinprodukten zu definieren. Dazu müssen, unter der Berücksichtigung von Normen und Vorschriften, die vertretbaren Risiken festgelegt werden. Zudem muss der höchstrangige Betreiber des IT-Netzwerks die zur Umsetzung notwendigen personellen und finanziellen Mittel zur Verfügung stellen. ([2], Absatz 3)

Nachdem alle finanziellen und Strukturelle Mittel zur Verfügung gestellt wurden, wird unter den Verantwortlichen eine Verantwortlichkeitsvereinbarung abgeschlossen (Abbildung 1). Diese regelt den gesamten Lebenszyklus des IT-Netzwerks zwischen den einzelnen Vertragspartnern, zu denen die Medizinprodukthersteller, die Medizintechnik- und die IT-Technikabteilung gehören. Im Vertrag werden die Ziele des Projekts und das betroffene IT-Netzwerk festgelegt.

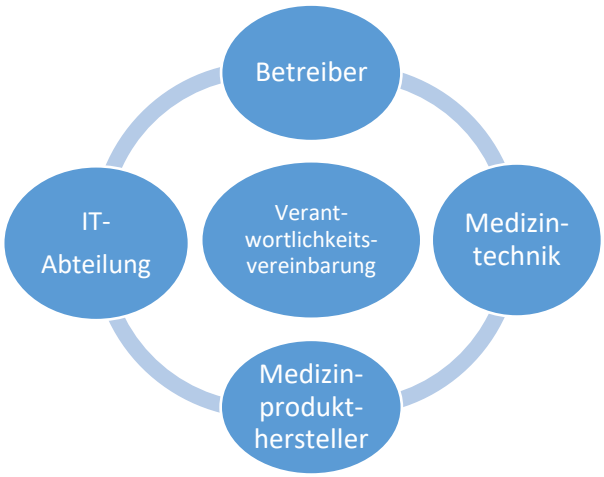

Abbildung 1: Verantwortlichkeitsvereinbarung

Durch die Vereinbarung sind sowohl die Hersteller der Medizinprodukte als auch der Betreiber des IT-Netzwerks verpflichtet Informationen über Produkte und Ereignisse aus Netzwerken zur Verfügung zu stellen. Bei streng vertraulichen Informationen des Herstellers kann eine weitere Vertraulichkeitsvereinbarung (Anhang 1) getroffen werden. Die Hersteller und Betreiber installieren Schutzmaßnahmen, um alle geheimen Informationen zu schützen. Die Medizintechnik- und die IT-Abteilung sind verpflichtet eine Liste mit allen an das IT-Netzwerk angebundenen Geräten und den dazugehörigen Herstellernamen zu erstellen. Zudem haben diese beiden Parteien organisatorische und technische Maßnahmen zu installieren. Bei Änderungsmaßnahmen haben sie zudem die Überwachung und die Planung des IT-Netzwerks zu besorgen (Tabelle 1). Daher sind alle Parteien Mitglieder des

Risikomanagementteams in Form von Unterstützung oder Ausführung. Um Verantwortlichkeiten im Umgang mit Projekten zu definieren, werden die Rollen und die Aufgaben vertraglich festgehalten.

Medizinprodukthersteller	Medizintechnik, IT-Technik, Haustechnik
➢ Bereitstellung von Informationen	➢ organisatorische und technische Schutzmaßnahmen
➢ Mitteilung der Ereignisse aus anderen Netzwerken	➢ Dokumentation und Überwachung
➢ Implementierung von technischen Schutzmaßnahmen, Festlegung von Regeln und Prüfvorschriften	➢ Planung und Durchführung von Änderungen

Tabelle 1: Vereinbarungspunkte zwischen den Vertragspartnern

Ein Risikomanager kann für jedes IT-Netzwerk durch die oberste Leitung ernannt werden. Seine Aufgabe ist es, alle für das Risikomanagement bedeutsamen Informationen zu den vernetzten Medizinprodukten zusammenzustellen. Der Risikomanager ist verantwortlich für die Etablierung der Medizinprodukte gemäß den Herstellerangaben und die Einhaltung der Richtlinien in der Organisation. Somit trägt er die Verantwortung für den gesamten Risikomanagementprozess. Bei der Kommunikation zwischen den Abteilungen Medizintechnik und IT-Technik sowie dem Hersteller tritt der Risikomanager als Kontaktperson auf. So muss er bei der Durchführung und bei der Änderung des medizinischen IT-Netzwerks stets benachrichtigt werden. Zudem stellt er der obersten Leitung Informationen zur Verfügung, auf deren Grundlage dann die möglicherweise entstehenden Risiken und die Gefährdung analysiert und vorgestellt werden ([2], Absatz 4.4.2).

2.2 Verantwortlichkeit der Hersteller

Unter den Herstellern von Medizinprodukten sind nach der DIN EN 80001-1 die Lieferanten der Betreiber zu verstehen. Sie müssen sich nach der Norm IEC 60601-1:2005 richten. Die darin benannten Medizinprodukte werden ‚programmierbares elektrisches medizinisches System' (PEMS) genannt. Die Hersteller werden dazu verpflichtet, für die sichere Anbindung der Medizinprodukte an das IT-Netzwerk Informationen zur Verfügung zu stellen. In den Accompanying Documents, den Begleitdokumenten, wird unter anderem die Zweckbestimmung der PEMS festgelegt. Um Risiken abschätzen zu können, muss der Hersteller Informationen beifügen [3]. Diese sollen die Folgen der Fehler im Netzwerk zeigen. Darüber hinaus werden die Eigenschaften und die Konfigurationen von IT-Netzwerken erläutert, die für die Verwendung medizinischer Geräte erforderlich sind. Die technischen und die sicherheitstechnischen Spezifikationen für die notwendigen Netzwerkverbindungen sowie die erwartete Kommunikation zwischen dem PEMS und dem IT-Netzwerk müssen erläutert werden. Aufgrund der DIN EN 80001-1 werden hohe Anforderungen an die Hersteller der Medizinprodukte gestellt. Der Aspekt der Sicherheit bei der Vernetzung von Medizinprodukten wird in der Norm IEC 60601-1:2005 beschrieben und dient als Grundgerüst der DIN EN 80001-1, siehe Abbildung 2 ([4]).

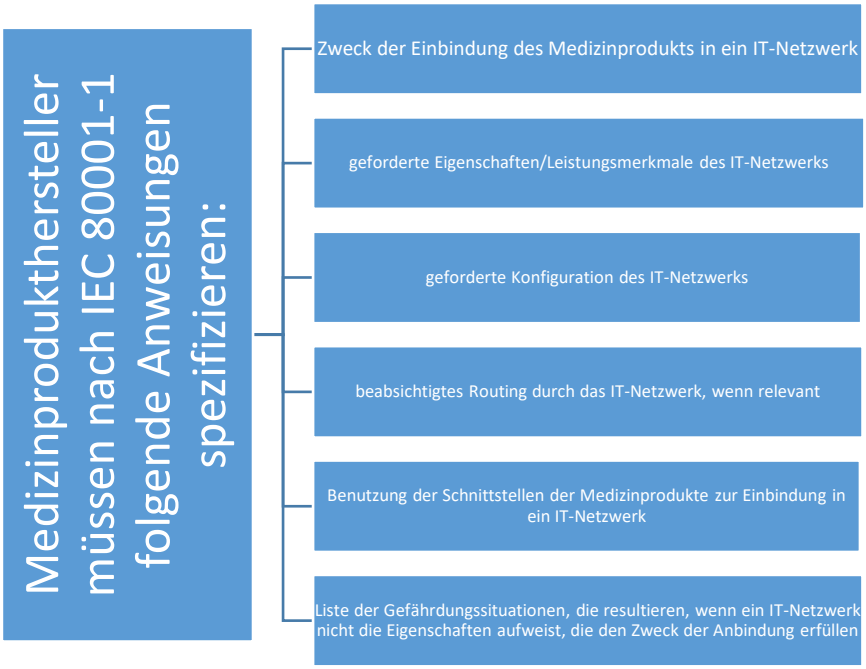

Abbildung 2: Anforderungen an die Medizinprodukthersteller

Wie die Hersteller der Medizinprodukte sind auch die Hersteller der IT verpflichtet Informationen bezüglich ihrer Gerätekomponenten und ihrer Software bereitzustellen. Dabei zählen die IT, z. B. ein Router und die damit verbundenen Komponenten, nicht als Medizinprodukte. Die Bereitstellung der Informationen wird im Voraus in der Vereinbarung erläutert (Abbildung 3).

Zur Unterstützung des Risikomanagements können vom Hersteller weitere Informationen wie Statistiken über die Systemzuverlässigkeit eingefordert werden. Dazu gehört auch die Freiheit von Viren. Für den Ausgleich der Informationsbereitstellung werden die Hersteller in Projekte und Prozesse hinsichtlich des medizinischen IT-Netzwerks eingebunden. So werden sie bei der Entwicklung und bei Änderungen der IT-Infrastruktur beteiligt. Zudem werden sie bei Änderungen der Produktinfrastruktur in die Planung eingebunden. Bei der Einbeziehung der Hersteller in das Risikomanagement werden diese dazu verpflichtet, Informationen über Gefährdungen und Fehler der Produkte bereitzustellen. Bei dieser Art des Vertrags soll eine gute Kommunikation zwischen den Herstellern und dem Betreiber aufgebaut werden. Somit ist ein ununterbrochener Informationsfluss sichergestellt und das Einbinden von Updates ist für beide Parteien leichter. [6]

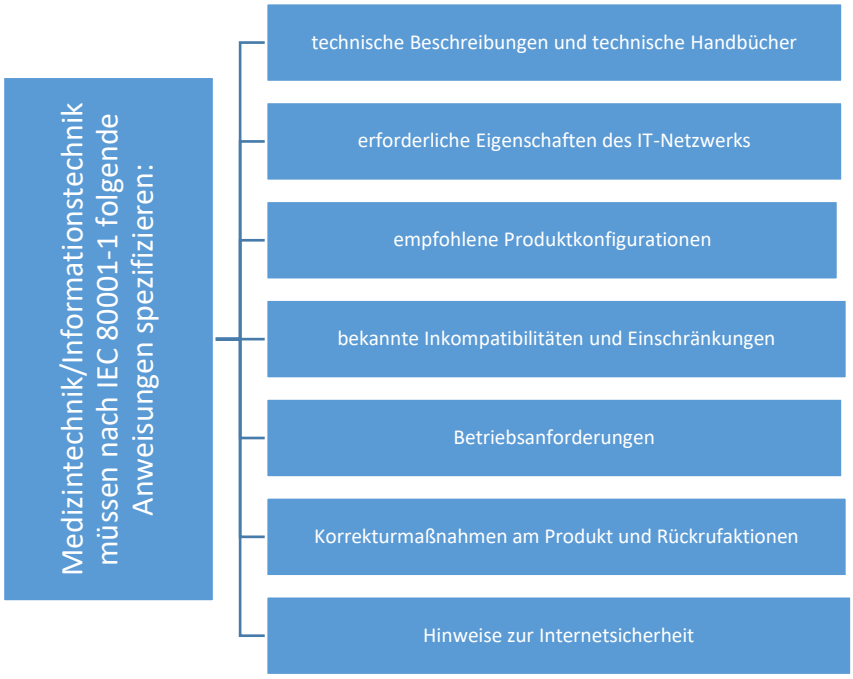

Abbildung 3: Anforderungen an die (Medizintechnik/Informationstechnik)

2.3 Verantwortlichkeit der Betreiber

Dem Betreiber des medizinischen IT-Netzwerks (Das Krankenhaus) werden durch die DIN EN 80001-1 neue Aufgaben gestellt. Dabei werden die Bereiche ‚Dokumentation und Planung', ‚Risikomanagement' sowie ‚Implementierung und Kontrolle' abgedeckt ([1], S. 6).

2.3.1 Dokumentation und Planung

Nach der DIN EN 80001-1 wird eine Risikomanagementakte angelegt, die als Dokumentationssystem dient (Abbildung 4). Dieses wird in drei weitere Unterordner eingeteilt, nämlich in die Kategorien ‚Risikomanagementplanung', ‚Netzwerkdokumentation' und ‚Prozessbeschreibung' ([1], S. 48).

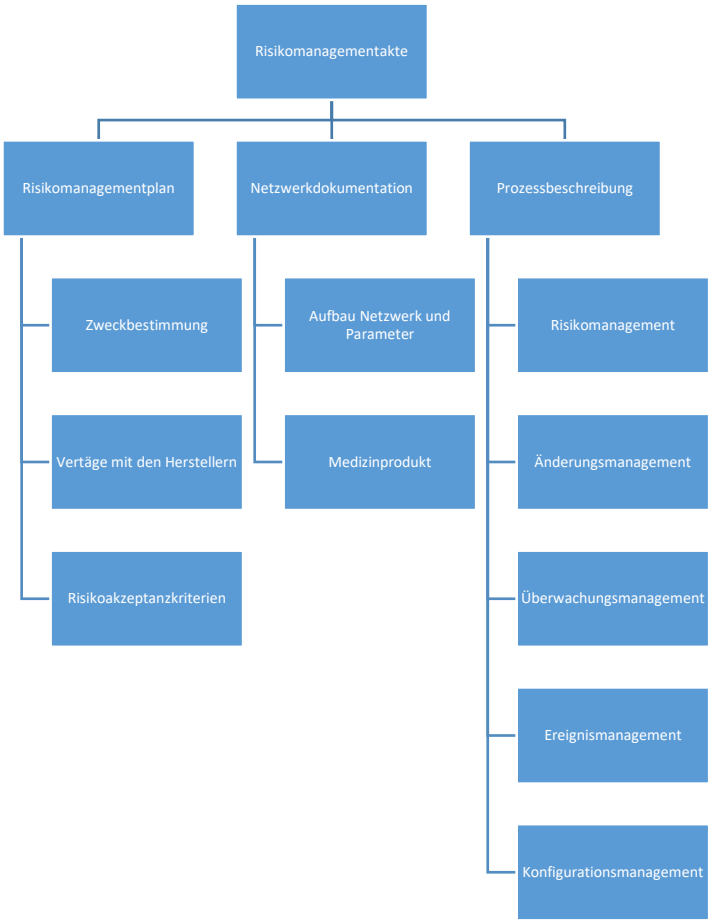

Abbildung 4: Risikomanagementakte

Der Risikomanagementplan beinhaltet eine ausführliche Beschreibung der Zweckbestimmung des IT-Netzwerks, indem dessen angestrebter Nutzen definiert wird. Die Einbindung der Elemente ist erforderlich, um eine Gefährdung und Risiken besser zu erkennen. Dabei werden alle Elemente wie die Hardware, die Software und die Daten aufgelistet (Abbildung 5). Die angeführten Daten sind für die Zweckbestimmung der medizinischen Produkte und die vorgesehene Verwendung des IT-Netzwerks von Bedeutung ([5], S.5). Neben den Elementen des Medizinprodukts sowie der dazugehörigen Software werden die Komponenten des medizinischen IT-Netzwerks aufgelistet, die dessen Nutzung sicherstellen. Dabei werden Merkmale wie die Bandbreite und die Reaktionszeit des IT-Netzwerks dokumentiert und diese Informationen werden allen Vertragsparteien zur Verfügung gestellt. Ebenfalls müssen die Aufgaben der Geräte und der Software auf Basis der Zweckbestimmung definiert werden. Die Patientendaten, die im Netz gespeichert werden, sind ebenfalls für das Risikomanagement relevant. Mit ihnen werden auch das Behandlungsverfahren sowie die Anwender aufgeführt. Zuletzt werden alle Aufgaben und Verantwortlichkeiten der Parteien des medizinischen IT-Netzwerks dargestellt.

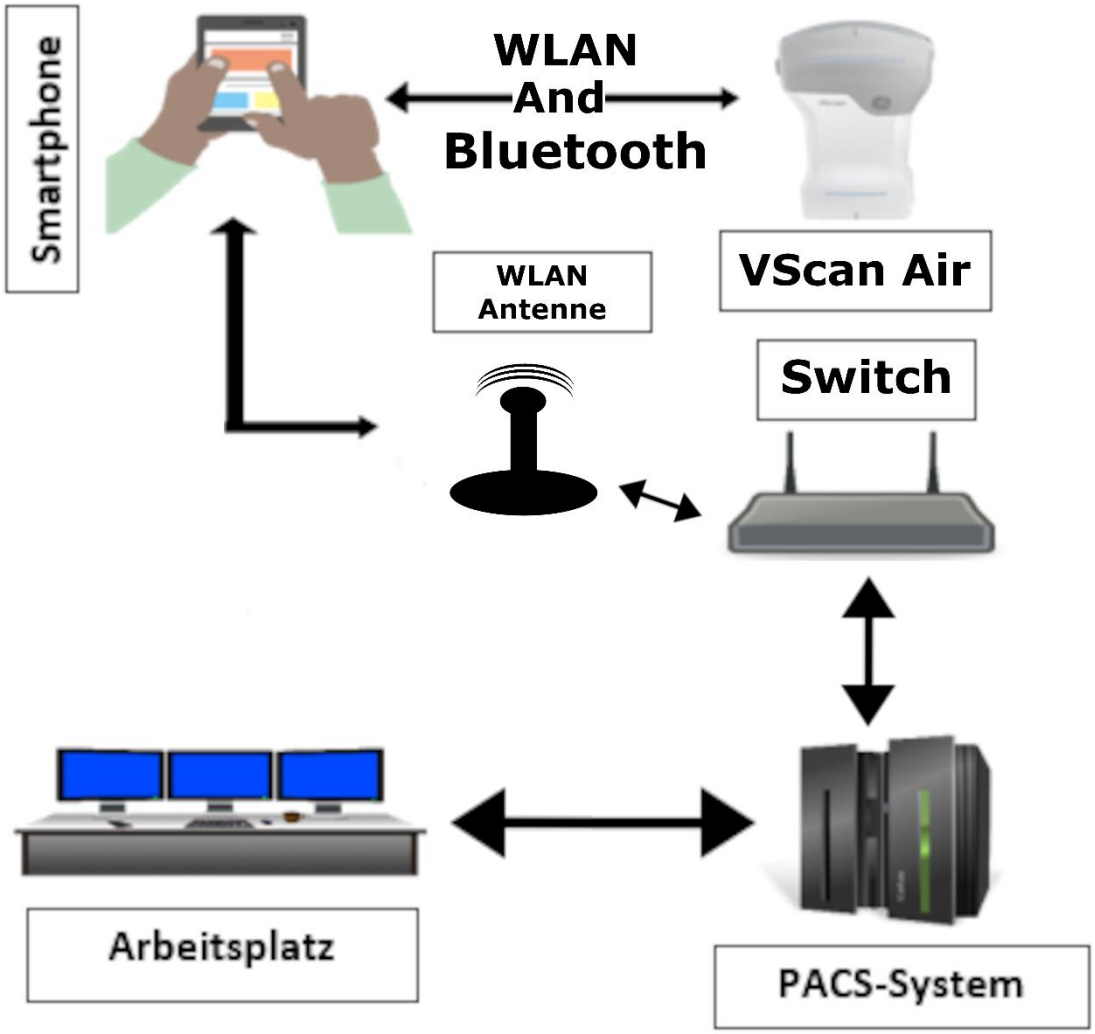

Abbildung 5: Teilnetzwerk VScan Air

Bei der Risikomanagementplanung werden auch Vertretbarkeiten und Risiken nach Kriterien aufgeteilt. Hierzu werden für jedes einzelne medizinische IT-Netzwerk so genannte Schutzziele definiert. In der DIN EN 80001-1 werden als die drei Arten der Schutzziele die Sicherheit, die Effektivität und die Daten- und Systemsicherheit festgelegt ([1], S. 47). Beim ersten Punkt, der Sicherheit, werden Schutzziele für Patienten, Anwender und Dritte bestimmt. Betreffend die Effektivität ist eine Gesundheitsmaßnahme hinsichtlich eines Workflows das Ziel. Mit der Daten- und Systemsicherheit wird auf den Schutz vor dem Verlust der Vertraulichkeit, der Vollständigkeit und der Verfügbarkeit der Daten und der Systeme abgezielt.

In der Risikomanagementakte wird auch eine Netzwerkdokumentation erstellt. (Abbildung 5) In dieser werden alle Komponenten der physikalischen und der logischen Netzwerkstruktur erfasst, wobei deren Grenzen vorgegeben werden. Umfasst werden unter anderem die elektrischen Eigenschaften, die eine Störung bei den miteinander verbundenen Geräten oder beim Netzwerk verursachen können. Zudem müssen stets Werte wie die Erdung, die galvanische Trennung oder Fehlerströme festgehalten werden.

Daher müssen Geräte sowie Netzwerkstrukturen nach Normen und Konformitätserklärungen betrieben und dokumentiert werden. Weitere relevante Punkte, die in der Risikomanagementakte definiert werden, sind die Beschreibung zur Netzwerksicherheit sowie der Informations- und Datenfluss des Netzwerks ([1], S.48).
Um alle Elemente im Einklang miteinander zu verbinden, werden in der Risikomanagementakte auch die Anforderungen der Medizinprodukte beschrieben. Dabei werden alle Voraussetzungen, wie die Bandbreite oder die Konfiguration, vordefiniert, um alle möglichen Risiken in die Planung einbeziehen zu können. Zu jedem Gerät sollten alle Verträge dokumentiert werden. Dabei werden alle relevanten Informationen festgehalten, beispielsweise Wartungen, Wartungsintervalle, Softwarelizenzen und Ansprechpartner hinsichtlich der Medizinprodukte. Ein weiterer Bestandteil der Risikomanagementakte nach der DIN EN 80001-1 ist die Prozessbeschreibung ([1], S. 49).

2.3.2 RISIKOMANAGEMENT

Der zentrale Punkt der DIN EN 80001-1 ist die Durchführung des Risikomanagements und der damit verbundenen Risikoanalyse. Letztere muss sowohl bei der Inbetriebnahme als auch bei der Änderung eines IT-Netzwerks, wozu auch der Austausch von Komponenten zählt, erfolgen. Das Ziel der Risikoanalyse ist es, Gefährdungen zu erkennen, bevor sie auftreten. Wenn solche festgestellt werden, können die Risiken nämlich im Vorhinein bewertet und kontrolliert werden.
Die Gefährdungen werden nach Schutzzielkategorien eingeteilt, wobei sie eine oder mehrere der drei Schutzziele betreffen können. Nach ihrer Erkennung wird der Grund gesucht und analysiert. Zudem sollen alle Gefährdungssituationen ermittelt und dargestellt werden, wobei alle Szenarien, bei denen Personen oder Infrastrukturen betroffen sind, aufgeführt werden. Ein Beispiel ist eine glatte Rampe im Winter. Hierbei kann eine Gefährdung entstehen, wenn Patienten oder Mitarbeiter die Rampe nutzen, um ins Gebäude zu kommen. Wird eine Gefährdungssituation erkannt, können mögliche Schäden auf Basis der Schutzziele dokumentiert werden. Die Gefährdungen werden dabei eingeteilt nach Schäden, die sich auf den Patienten beziehen, Schäden, die sich auf die Arbeitsroutine der Mitarbeiter auswirken, und Schäden, die die Daten- und Systemsicherheit betreffen.
Nach der Risikoanalyse wird die Risikobewertung durchgeführt. Bei dieser werden Maßnahmen beschrieben, die die Gefährdung abschwächen oder eliminieren.

Um die Gefährdung zu skalieren, werden die Eintrittswahrscheinlichkeiten der Gefährdungssituationen ermittelt, siehe Tabelle 2 ([1], S.54). Für eine bessere Zuordnung werden sie in Kategorien eingeteilt. Dabei ist es relevant, dass die Kategorien vordefiniert werden, damit alle Anwender sehen, was sie aussagen. Möglich ist die Einteilung in ‚sehr unwahrscheinlich', ‚unwahrscheinlich', ‚möglich', ‚wahrscheinlich' und ‚sehr wahrscheinlich'. Dabei entspricht ‚sehr unwahrscheinlich' z. B. einem vordefinierten Wert von P1 (P1= 1 Punkt, P2 = 2 Punkte, P3 = 3 Punkte usw.). Die einzelnen Kategorien kann der Anwender selbst festlegen. Der Wert wird ‚Risikoprioritätszahl' (RPZ) genannt. Diese ergibt sich aus der Eintrittswahrscheinlichkeit (*P*) multipliziert mit dem Schadensausmaß (*S*), siehe Anhang 2.

Kategorie	Bedeutung	Eintrittswahrscheinlichkeit (*P*)
P1	unvorhersehbares Problem	sehr unwahrscheinlich
P2	Problem tritt sehr selten auf	unwahrscheinlich
P3	vereinzelt treten Probleme auf	möglich
P4	Problem tritt regelmäßig auf	wahrscheinlich
P5	Fehler tritt bei jeder Anwendung des Geräts bzw. Programmes auf	sehr wahrscheinlich

Tabelle 2: Eintrittswahrscheinlichkeit

Nach der Eintrittswahrscheinlichkeit ist das Schadensausmaß zu ermitteln. Dazu werden für die drei Schutzziele ‚Sicherheit', ‚Effektivität' und ‚Daten- und Systemsicherheit' Schadensausmaßkategorien angelegt (Anhang 2).

Die Kategorie ‚Ss1' (Ss1 = 1 Punkt, Ss2 = 2 Punkte, Ss3 = 3 Punkte usw.) bedeutet in diesem Fall des Schutzziel der Sicherheit, dass es keine Verletzung der betroffenen Person gibt und das Schadensausmaß somit unbedeutend ist. Der Extremfall ‚Ss5' bedeutet hingegen eine sehr schwere Verletzung bis hin zum Tod. Er ist somit als existenzbedrohend einzustufen. Zwischen ‚Ss1' und ‚Ss5' werden weitere Kategorien vordefiniert, um das Schadensausmaß genauer zu bestimmen, siehe Tabelle 3 (Anhang 2).

Kategorie	Bedeutung	Schadensausmaß (*S*)
Ss1	keine Verletzung	unbedeutend
Ss2	leichte Verletzung	gering
Ss3	Verletzung	erheblich
Ss4	lebensbedrohliche Verletzung	wesentlich
Ss5	schwerste Verletzung oder Tod	existenzbedrohend

Tabelle 3: Schadensausmaßkategorien zum Schutzziel ‚Sicherheit'

Die Tabelle zum Schutzziel ‚Effektivität' (Tabelle 4) ist wie jene zum Schutzziel ‚Sicherheit' ausgestaltet. Die Kategorie ‚Sw1' entspricht einem unbedeutenden Schadensausmaß, wobei keine Verletzung und kein Einfluss auf die Effektivität vorliegt. Die Kategorie ‚Sw5' hingegen bedeutet das schlimmstmögliche Schadensausmaß, das als existenzbedrohend eingestuft wird. (Anhang 2)

Kategorie	Bedeutung	Schadensausmaß (*S*)
Sw1	keine Verletzung	unbedeutend
Sw2	leichte Störung oder Belastung	gering
Sw3	Störung	erheblich
Sw4	Unterbrechung	wesentlich
Sw5	Abbruch	existenzbedrohend

Tabelle 4: Schadensausmaßkategorien zum Schutzziel ‚Effektivität'

Beim Schutzziel ‚Daten- und Systemsicherheit' (Tabelle 5) sind die Einflüsse auf die Verfügbarkeit, die Vertraulichkeit und die Integrität von Bedeutung. Dabei ist das Schadensausmaß in der Kategorie ‚Sd1'

unbedeutend und hat somit keinen Einfluss auf die Daten- und Systemsicherheit. Die Kategorie ‚Sd5' entspricht einem totalen Ausfall der Sicherheit und ist somit als existenzbedrohend einzustufen. (Anhang 2)

Kategorie	Bedeutung	Schadensausmaß (*S*)
Sd1	kein Einfluss	unbedeutend
Sd2	geringfügiger Einfluss	gering
Sd3	Einfluss auf die Verfügbarkeit	erheblich
Sd4	es kommt zu Ausfällen von Systemen und Anwendungen	wesentlich
Sd5	es kommt zu einem längeren Ausfall von Systemen und Anwendungen	existenzbedrohend

Tabelle 5: Schadensausmaßkategorien zum Schutzziel ‚Daten- und Systemsicherheit'

Wurden das Schadensausmaß sowie die Eintrittswahrscheinlichkeit ermittelt, werden die gesammelten Informationen in einem Risikomatrix veranschaulicht. Mit diesem kann dann eingeschätzt werden, ob die Gefährdung vertretbar ist oder ob eine Maßnahme zur Minderung vorgenommen werden muss. Das Schadensausmaß wird mit ‚Sx' maskiert, wobei ‚Sx1' einem sehr geringen Schadensausmaß entspricht und ‚Sx5' ein sehr großes Schadensausmaß darstellt. Demgegenüber steht die Eintrittswahrscheinlichkeit mit der Beschriftung ‚Px', wobei ‚Px1' einer sehr geringen und Px5 einer sehr hohen Eintrittswahrscheinlichkeit entspricht (Anhang 2).
Liegt der Wert des RPZ (Tabelle 6) zwischen 1 und 4, so wird er in der Risikomatrix in Grün angezeigt und eine Prüfung ist jährlich erforderlich. Ist er größer als 4, so wird er in Gelb dargestellt und eine Prüfung ist mehrmals im Jahr erforderlich, je nachdem wie hoch der Wert ist. Bei Werten, die größer als 9 sind, ist eine sofortige Maßnahme erforderlich, die in weniger als sechs Monaten zu erledigen ist. Bei einem Schadensausmaß von 5 Punkten oder einem RPZ-Wert von größer als 14 muss ebenfalls sofort eine Maßnahme eingeleitet werden und das Risiko ist sofort zu beheben (Anhang 2).

	Einrichtungsintern	Verantwortlichkeit
RPZ > 14 und/oder Schadensausmaß = 5	sofortige Einleitung von Präventivmaßnahmen; Überprüfen der Wirksamkeit; Risiko muss sofort oder ohne schuldhaftes Verzögern behoben werden; Bericht an den Vorstand	Geschäftsführer berichtet dem Vorstand
RPZ > 9	sofortige Einleitung von Präventivmaßnahmen; Realisierung innerhalb von sechs Monaten; Überprüfen der Wirksamkeit	Geschäftsführer , Bereichsleiter
RPZ > 4	unterjährige Prüfung, ob sich die RPZ verändert; Überprüfen der Wirksamkeit vorhandener Präventivmaßnahmen; ggf. Einleiten von Maßnahmen durch GF	Geschäftsführer, Bereichsleiter
RPZ 1–4	jährliche Prüfung; u. U. ist eine weitere Überprüfung verzichtbar; Beobachtung in festem Rhythmus	Geschäftsführer, Bereichsleiter

Tabelle 6: Risikobewertung nach der Risikoprioritätszahl

Der grün markierte Bereich ist gefährdungsfrei und erfordert keine weiteren Maßnahmen (Tabelle 7). Beim gelben Bereich besteht ein erhöhtes Risiko und es sollten Maßnahmen zur Minderung vorgenommen werden, wenn es möglich ist. Der rot markierte Bereich ist risikogefährdend und eine Maßnahme zur Minderung ist dringend notwendig. Der lila markierte Bereich weist den größten Risikofaktor auf und eine Maßnahme ist sofort nötig. (Anhang 2). Die Risikomatrixtabelle ist eine vereinfachte Darstellung der gewonnen Daten auf dem Risikomanagement-Prozess

		Schweregrad				
		Sx1	Sx2	Sx3	Sx4	Sx5
Wahrscheinlichkeit	Px5					
	Px4					
	Px3					
	Px2					
	Px1					

Tabelle 7: Risikomatrix

Sind aufgrund der Risikobewertung zusätzliche Schutzmaßnahmen erforderlich, so kann die Risikobewältigung eingeleitet werden. Dabei ist es das Ziel, die Gefährdung so gering wie möglich zu halten. Durch die Etablierung der vorherigen Schritte können Daten und Informationen gewonnen werden, die bei der Analyse des IT-Systems dabei helfen, das Risiko zu minimieren. Zudem wird versucht, aus den gewonnenen Daten mögliche Signale zu erkennen, die auf ein Risiko deuten. Die Erkennung eines Risikoalarms ist eine der Maßnahmen, um das Risiko so gering wie möglich zu halten. Ein Risikoalarm ist das Erkennen eines Anzeichens eines Risikos. Zusätzlich können Schulungen der Mitarbeiter durch einen entsprechend geschulten Mitarbeiter der Firma das Risiko bei den verschiedenen Geräten minimieren. Auch Änderungen an IT-Netzwerkkomponenten werden in der Risikobewältigung betrachtet; beispielsweise ist das Ersetzen von alten Komponenten eine mögliche Maßnahme. Weiterhin kann das Risiko gemindert werden, wenn die Gefährdungsursache im Medizinprodukt liegt. Bei dessen Änderung ist es relevant, den Hersteller zu kontaktieren und um Erlaubnis zu fragen, denn eine solche Absprache ist vorgeschrieben. Bei diesem Schritt kann entweder der Hersteller um Erlaubnis gefragt werden oder er wird gebeten, das Produkt selbst zu verändern. Die Risikobewältigung kann in verschiedene Kategorien eingeteilt werden, siehe Tabelle 8 (Anhang 2).

Risikovermeidung	Verzicht auf besonders riskante Handlungen und Tätigkeitsfelder
Risikoreduktion	Risikoreduktion durch Informationsgewinnung, Schulung und Überwachung risikobehafteter Tätigkeiten
Selbsttragung	Bildung finanzieller Reserven (Rücklagen) durch Ansatz kalkulatorischer Wagniskosten
Risikostreuung	Diversifikation in Bezug auf Dienstleistungen, Kunden und Standorte, um nicht abwendbare Risiken zu streuen und damit so gering wie möglich zu halten
Risikoabwälzung	Reduzierung finanzieller Konsequenzen durch vertragliche Vereinbarungen (Haftungsklauseln); Abwälzung auf Dritte als Leistungserbringer
Schadenverhütung	Reduktion der Eintrittswahrscheinlichkeit und der Schadenausbreitung durch technische und/oder personelle Vorkehrungen (z. B. Alarmierungsplan)
Risikoübertragung	Übertragung nicht kalkulierbarer oder nicht tragbarer Risiken auf Versicherungsunternehmen (z. B. Berufshaftpflicht- oder Gebäudeversicherung)

Tabelle 8: Risikobewältigung

Nach der Risikobewältigung, bei der alles unternommen wird, um die Gefährdungen so gering wie möglich zu halten, wird erneut eine Risikoanalyse durchgeführt. Dabei wird überprüft, ob das Risiko vertretbar ist. Nicht alle Risikomaßnahmen sind umsetzbar, daher wird eine Risiko-Nutzen-Analyse durchgeführt. Die Arten von Risiken, die nicht behoben werden können, werden dokumentiert und dem obersten Krankenhausleitung bereitgestellt.

2.3.3 Implementierung und Kontrolle

Werden bei der Risikoanalyse Risiken erkannt und entsprechende Maßnahmen geplant, um die Gefährdung zu minimieren, wird das Änderungsmanagement eingeleitet. Mit diesem wird sichergestellt, dass alle geplanten Maßnahmen ordnungsgemäß implementiert und überprüft werden. Bevor eine Änderung vorgenommen werden kann, muss eine Planung erstellt werden. Dabei ist es relevant, alle erforderlichen Informationen anzugeben – z. B. alle betroffenen Komponenten, alle nötigen Schritte sowie das zu erwartende Ergebnis –, die für eine erfolgreiche Änderung erforderlich sind. Des Weiteren sind im Änderungsmanagement Deadlines zu dokumentieren. Dabei wird beschrieben, welche Änderungen innerhalb einer festgelegten Zeit vorgenommen werden müssen ([1], S.66).
Im Rahmen des Risikomanagements wird im Anschluss die Planung des Änderungsmanagements geprüft und das Vorhaben genehmigt und freigegeben. Sie enthält dann die Voraussetzung, die Einschränkung und die Dokumentation, die dann dem Risikomanager zur Überprüfung übergeben wird.

Nachdem Letztere abgeschlossen und das Gesamtrisiko bewertet und für akzeptabel erklärt wurde, kann die Änderung vorgenommen werden.
Die Überwachung des medizinischen IT-Netzwerks ist ein Prozess, der kontinuierlich durchgeführt werden muss. Werden im Rahmen des Systems Abweichungen von Werten erkannt, die durch Mitarbeiter oder Hersteller vorgegeben wurden, wird das Risikomanagement eingeleitet. Nach der Risikoanalyse kann dann wieder ein Änderungsmanagement in Erwägung gezogen werden.

2.4 Beispiel zur Einführung der DIN EN 8000-1

Bei der Umsetzung der DIN EN 80001-1 und der damit verbundenen Risikopolitik muss die Geschäftsleitung des Krankenhauses die Richtlinien freigeben. Bei den Richtlinien handelt es sich um ‚Sicherheitsrichtlinien' die ständig erweitert werden (Siehe Anhang 5). In dem Dokument werden alle Aufgabenbereiche festgehalten und dient der eindeutigen Erkennung von Verantwortungen und Verantwortungsbereichen.
Hierbei tritt der Risikomanagementplan in Kraft. Dessen Inhalt, die Aufgaben, der Zweck des Netzwerks sowie die Schutzziele und die damit verbundenen Risiken wurden in Kapitel 2 beschrieben.
Ein wesentlicher Schritt bei der Einführung der DIN EN 80001-1 ist die Ernennung eines verantwortlichen Risikomanagers durch die Geschäftsleitung. Dieser dient als Kommunikationsstütze für die einzelnen Vertragsgruppen und zur Kontrolle des Risikomanagementplans. Nach seiner Ernennung sind die einzelnen Vertragsgruppen zu benennen. Dabei müssen alle Vertragspartner, die einen Einfluss auf das Netzwerk haben, angegeben und involviert werden. Neben den üblichen Parteien wie den Abteilungen Medizintechnik und IT-Technik sowie dem Hersteller sollten die Haustechnikabteilung und die Anwender (Arzt, Stationsleitung) in den Vertrag aufgenommen werden.
Im Vertrag wird ein gemeinsames Vorgehen aller Parteien definiert. Dabei ist es bedeutsam, dass alle Vertragsgruppen gleich behandelt werden und es für einzelne keine Nachteile z. B. hinsichtlich der Weitergabe von Informationen gibt. Zudem werden alle zu erwartenden Kosten und Aufgaben benannt.
Damit alle Vertragspartner die Beschaffenheit des IT-Netzwerks kennen, wird eine Netzwerkdokumentation mit allen verbundenen Komponenten erstellt. Die Details werden für alle Vertragspartner freigegeben.

2.4.1 Risikomanagement

Die Prozesse des Risikomanagements müssen für alle drei Schutzziele erstellt werden. Dabei wird das Risiko hinsichtlich der Sicherheit, der Effektivität und der Daten- und Systemsicherheit separat dargestellt. Aus den ermittelten Daten hinsichtlich der Schutzziele können potentielle Gefährdungen abgeleitet werden.
Beim Schutzziel der Sicherheit werden Medizinprodukte analysiert, von denen eine potentielle Gefährdung für Anwender, Patienten oder Dritte ausgeht. Die fehlerhafte Aufnahme beispielsweise

eines medizinischen Bildes im Bildarchivierungssystem kann eine falsche Befundung zur Folge haben, was für den Patienten lebensgefährlich sein kann.
Bei der Analyse des Schutzziels der Effektivität werden der Arbeitsfluss und die damit möglicherweise verbundenen Störfaktoren betrachtet. Bei einer Operation kann beispielsweise die Überlastung eines IT-Netzwerks durch die Übertragung der Signale und der Bilder ein möglicher Störfaktor sein.
Hinsichtlich des Schutzziels der Daten- und Systemsicherheit ist die Erkennung von Risikosituationen für Daten und Systeme relevant. Dabei müssen die Verfügbarkeit, die Vertraulichkeit und die Vollständigkeit der Daten und der Systeme gewährleistet sein. Bei den Daten handelt es sich um Patienten- und Anwenderdaten im Krankenhausinformationssystem (KIS) oder um Digital-Imaging-and-Communications-in-Medicine (DICOM)-Bilder im Picture Archiving and Communication System (PACS); durch sie wird das Schutzziel der Datensicherheit überprüft. Zum System zählen das Ultraschallgerät und Datenbanken; durch sie wird das Schutzziel der Systemsicherheit überprüft. Dabei kann von Gefährdungen durch defekte Hardware, Stromausfälle oder Cyberkriminelle ausgegangen werden.
Nach der Analyse der Schutzziele folgt hinsichtlich dieser einzeln die Bestimmung des Schweregrads der Gefährdungssituation und der Wahrscheinlichkeit der Verwirklichung des Risikos. Auf Basis dessen wird dann entschieden, ob eine Maßnahme zur Minderung oder eine Änderung notwendig ist. Hinsichtlich Risiken, die im akzeptablen Bereich liegen, bedarf es keiner Maßnahme.

2.4.2 Dokumentation des Risikomanagements

Die Dokumentation des Risikomanagements sollte folgende Formblätter beinhalten: den Risikomanagementplan, die Risikobewertung sowie den Risikomanagementreport.[1] Der Risikomanagementplan sind die ersten Entwürfe, wobei theoretisch festgelegt wird, wie vorgegangen wird. Die Risikobewertung ist das Sammeln von Daten und das Ableiten von Erkenntnissen daraus. Nach der Risikoanalyse wird eine Zusammenfassung der Daten erstellt. Alle Informationen sowie die implementierten Schutzmaßnahmen werden im Report ermittelt. Die gesamte Dokumentation wird dem Risikomanager übergeben, der dann die gewonnenen Erkenntnisse und die dazugehörigen Schutzmaßnahmen freigeben kann.

2.4.3 Gliederung des IT-Netzwerks

Das IT-Netzwerk wirkt für den unbeteiligte kompliziert. Um es überschaubar und Sicher zu gestalten, wird es in kleinere Teilnetze aufgeteilt. Diese können dann nach Abteilungen (z. B. EKG-Abteilung oder Radiologie) oder Funktionsbereichen (z. B. Technik oder Pflege) untergliedert werden.
Die Einteilung des medizinischen IT-Netzwerks wird ebenfalls dokumentiert. Dabei ist die Zweckbestimmung des IT-Netzwerks wesentlich. Diese kann in die zwei Unterkategorien ‚Technische Dokumentation und Netzwerktopologie' und ‚organisatorische Anforderungen' eingeteilt werden. Bei

den organisatorischen Anforderungen ergeben sich die Unterkategorien ‚Medizinische Workflows' sowie ‚Wartung und Service des IT-Netzwerks' (Abbildung 6).

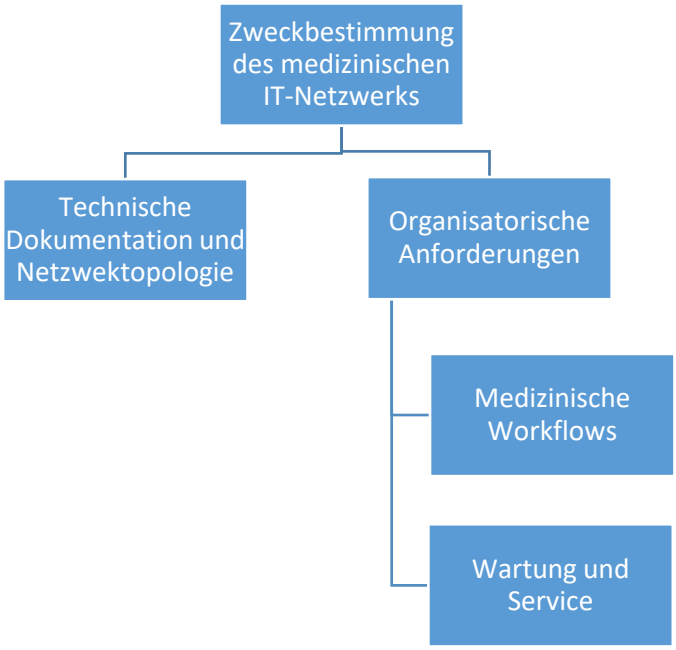

Abbildung 6: Netzwerkdokumentation

2.5 Die Prozesse

In den Prozessen werden die Ziele sowie die Zweckbestimmung festgelegt. Dabei wird auf die einzelnen Abfolgen eingegangen (Abbildung 7). Um den Überblick nicht zu verlieren, ist es relevant, vorab eine Abfolge zu bestimmen und diese dann auf alle Prozesse anzuwenden.

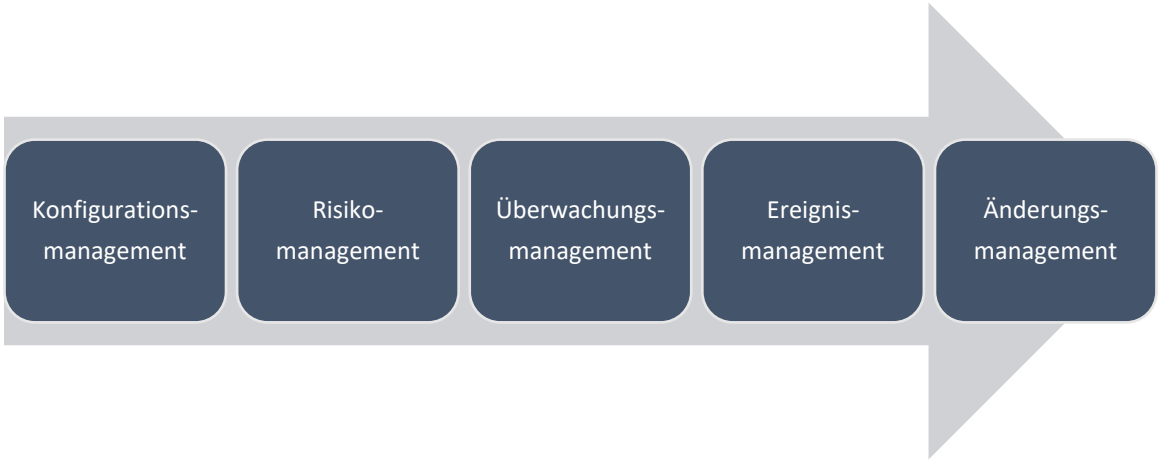

Abbildung 7: Prozessabfolge

Der erste Prozess ist das Konfigurationsmanagement. Dabei werden alle Daten zum medizinischen IT-Netzwerk sowie zu den einzelnen Komponenten gesammelt und dokumentiert. Die gewonnenen Konfigurationsdaten können dann bei den verschiedenen Prozessen zur Unterstützung genutzt werden. Da Komponenten sich immer wieder ändern und verbessert werden, ist darauf zu achten, dass die neuen Informationen ins Konfigurationsmanagement einfließen.

Im Prozess des Risikomanagements ist es das Ziel, das Risiko genau zu beschreiben, zu analysieren, zu bewerten und zu kontrollieren (Abbildung 8). Die Bestimmung des Risikoniveaus sollte einheitlich sein, da es sonst zu Verwirrung kommt und ein Vergleich nicht möglich ist. ([1], S.59).

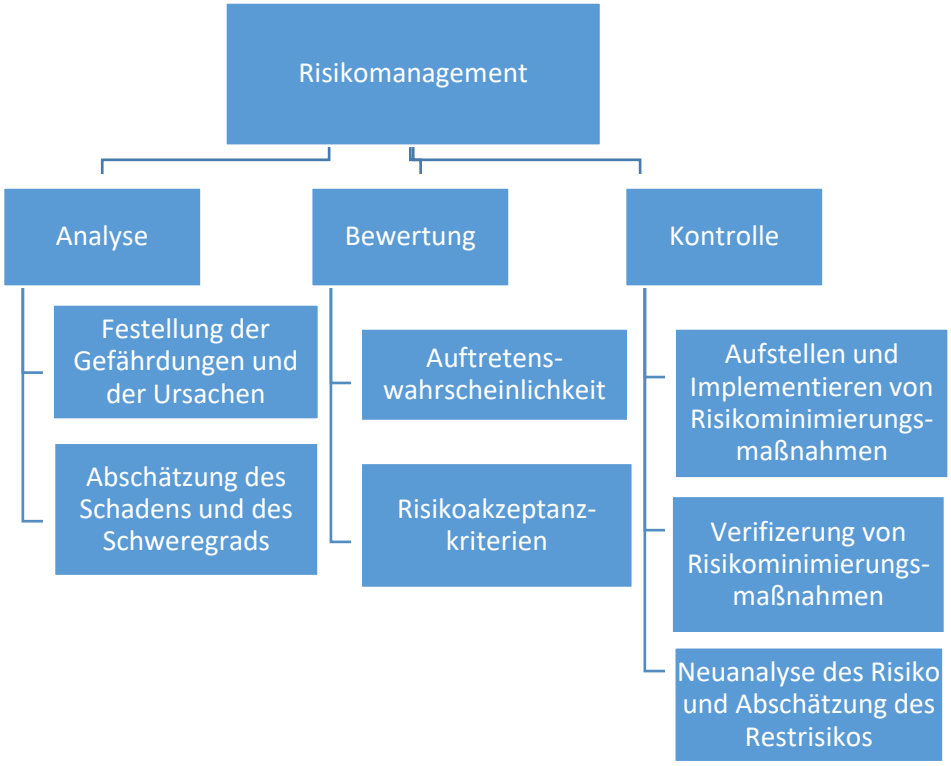

Abbildung 8: Prozess Risikomanagement

Das Überwachungsmanagement dient der Verminderung der Ausfallzeiten und gibt den Technikern die Möglichkeit, zeitnah zu handeln. So kann mit Hilfe von Überwachungssystemen ein Risiko schnell abgeschätzt oder vermieden werden. Der Medizinprodukthersteller kann mittels Tools bei der Analyse und der Risikominderung mithandeln. Er kann gewarnt werden, wenn ein Medizinprodukt in bestimmten Abständen überprüft werden muss oder es zu einer Störung gekommen ist.

Beim Ereignismanagement geht es darum, die Ereignisse sorgfältig zu analysieren. Diese werden dann in Klassen eingeteilt und der Prozess wird dokumentiert. Dabei werden die Verantwortlichkeiten definiert. Um Verwirrung zu vermeiden, wird ein Ansprechpartner ausgewählt, der dann mit dem Medizinprodukthersteller kommuniziert. Alle eingeleiteten Maßnahmen werden zudem im Ereignismanagement dokumentiert.

Im Rahmen des Änderungsmanagements ist vorgesehen, dass hinsichtlich der Planung und der Durchführung einer Änderung bei jeder Risikogruppe gleich vorgegangen wird. So kann im Ernstfall immer schnell gehandelt werden, da dieser Ernstfall im Vorfeld getestet wird, bevor es zum Einsatz des Prozesses im Betrieb kommt. Nachdem das Änderungsmanagement dokumentiert wurde, kann die Entscheidung vom Risikomanager oder der höchsten Leitung eingeholt werden und die Freigabe erfolgen.

3 UMSETZUNG DER DIN EN 80001-1 AM STANDORT ROTENBURG

Die Umsetzung eines Projektes dieser Größe bedarf meist eines Durchlaufs anhand eines Beispielgeräts. Das AGAPLESION DIAKONIEKLINIKUM ROTENBURG plant dies anhand der Anschaffung eines mobilen Ultraschallgeräts. Das Modell ‚VScan Air' der Firma ‚GE HealthCare Medical' dient in der Bachelorarbeit als Beispiel für die Umsetzung der DIN EN 80001-1 am Standort Rotenburg (Wümme). Das Ultraschallgerät wurde von der Abteilung ‚Zentrale Notaufnahme' beantragt. Für die Bearbeitung der Befunde werden die Daten vom Ultraschallgerät an das PACS gesendet, das mit dem Netzwerk verbunden ist. Somit ist die Umsetzung der DIN EN 80001-1 anhand des Ultraschallgeräts ein geeignetes Beispiel, da hierfür das Gerät in der Liste der Neuanschaffung stand. Aufgrund dessen die ersten Schritte eingeleitet werden können.

Als Grundbaustein der DIN EN 80001-1 (Abbildung 8) wurde das Risikomanagement herangezogen. Zu diesem zählt die Risikomanagementplanung und die Verantwortlichkeitsvereinbarung zwischen der Medizintechnik/IT-Technik und dem Hersteller. (Abbildung 9)

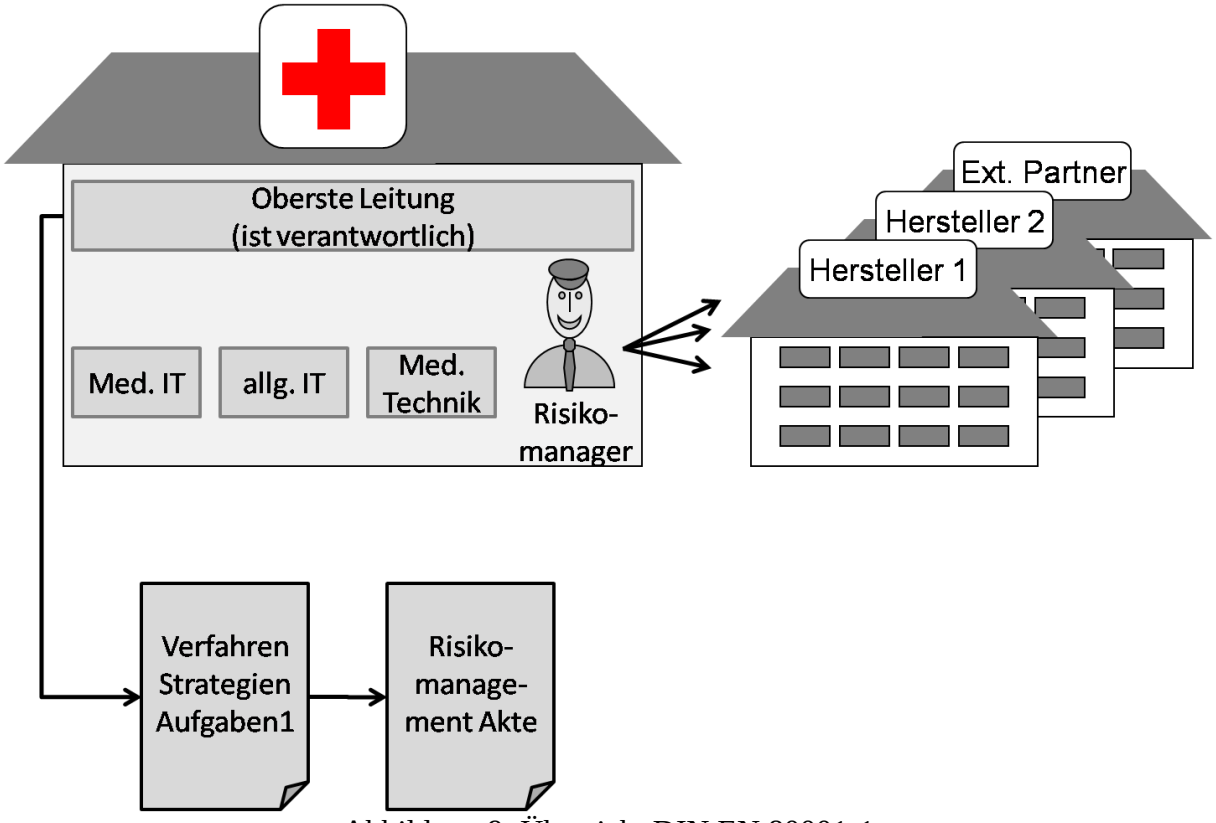

Abbildung 9: Übersicht DIN EN 80001-1

3.1 RISIKOMANAGEMENTAKTE

Bei der Dokumentation laut der DIN EN 80001-1 ist die Risikomanagementakte der große ‚Behälter', in dem alle Informationen gesammelt werden. Dabei werden alle gewonnenen Daten bezüglich des Netzwerks und der Geräte und die davon ausgehenden Gefahren sowie die Wahrscheinlichkeiten deren Eintritts beschrieben. In der Risikomanagementakte sind die Risiken für die Patienten, das Personal und die Organisation aufzuführen.

Die Vereinbarung zwischen den Vertragspartnern (Medizintechnik/IT-Technik, Hersteller) ist ebenfalls in der Risikomanagementakte zu finden. Dabei wird im Voraus festgelegt, wer welche Verantwortung bei der Umsetzung der DIN EN 80001-1 trägt. Die Vereinbarung wird vertraglich zwischen dem Verantwortlichen der Organisation und einem ernannten Risikomanager festgelegt und ist somit rechtskräftig. Die Risikomanagementakte ist schnell angelegt, es handelt sich dabei um ein Ordner auf dem Server, auf dem nur bestimmte Personen Zugriff haben.

Die Umsetzung der Strukturen der Risikomanagementakte in der Form, wie sie in der DIN EN 80001-1 gewünscht ist, steht am Standort Rotenburg (Wümme) derzeit am Anfang. Es wurden zwar Listen und PDF-Dateien angefertigt, die in die richtige Richtung weisen. Dennoch sind aktuell Fragen wie Ressourcen, Mittel und Umfang zu klären, wie eine Umsetzung der DIN EN 80001-1 auszusehen hat.

Nach Gesprächen über Teams wurde eine noch engere Zusammenarbeit dieser Abteilungen beschlossen, was die Umsetzung der DIN EN 80001-1 erleichtern soll. Es wurde dabei eine Aufgabenteilung besprochen. Die dabei erstellten Dokumente wie z.B die Verantwortlichkeitsvereinbarung und die Risikoübersicht wurden im Nachhinein erstellt und immer weiter erweitert, um die Dokumente der DIN Norm anzugleichen.

3.1.1 NETZWERKDOKUMENTATION

In den Krankenhäusern ist in den letzten Jahren eine schnelle Entwicklung der IT-Infrastruktur erfolgt. Der Grund hierfür ist die Digitalisierung der Ergebnisse vieler Medizinprodukte, z. B. der Röntgenanlage. Dabei werden die erzeugten Bilder direkt digitalisiert auf dem Rechner angezeigt und nicht wie früher üblich auf Schablonen ausgedruckt. Das hat dazu geführt, dass die IT-Infrastruktur immer weiterentwickelt werden musste, um die Anforderungen der medizinischen Geräte zu erfüllen.

Das Netzwerk des Krankenhauses ist vielseitig und dient der Übertragung von Audio- und Videodateien sowie herstellerspezifischen Daten. Als Netzwerkprotokoll wird das ‚Transmission Control Protocol/Internet Protocol' (TCP/IP) verwendet. Die genutzte Version ist IPv4. Die Netzwerkadressen werden aus Sicherheitsgründen nur erwähnt und nicht benannt, da es sich hierbei um ein KRITIS Einrichtung (Kritische Infrastrukturen) handelt. Das gesamte Netzwerk des Krankenhauses ist durch eine Firewall der Firma McAfee geschützt. Damit kann die IT-Abteilung die Anwendungen, die im Krankenhaus genutzt werden, vom VLAN Netzwerk (Virtual Local Area Network) trennen und einen separaten Zugang zum Internet ermöglichen. Dazu wird ein VLAN eingerichtet. Ein VLAN ist ein logisches Teilnetzwerk eines LANs (physischen Local Area Networks). Es teilt das LAN Netzwerk in

logische Segmente auf. Der VLAN wird eingesetzt, um beispielsweise Datenverkehr zu priorisieren oder Datenströme zu trennen.

Die Netzwerkstruktur sieht wie in den meisten Krankenhäusern wie folgt aus: Mehrere Rechnerräume, in denen die Server mit ihren Datenbanken arbeiten, bilden die IT-Infrastruktur (Abbildung 10). Sie sind auf verschiedene Orte verteilt, sodass der Ausfall eines Rechnerraums durch einen zweiten kompensiert werden kann und es zu keinem Datenverlust kommt. Die Rechnerräume sind mit Verteilern (Switch) verbunden, die die Daten auffangen und weiterleiten können. Die Verteiler sind mit vielen Ports (digitalen Eingängen) versehen. Über die Portnummer erkennt die IT-Abteilung das verbundene Gerät und kann dann den Zugang zu den VLAN gewähren. Das Krankenhaus benutzt eine Vielzahl von Netzwerkkomponenten, mit denen weitere Komponenten wie Clients verbunden sind. Ein Client kann ein Arbeitsplatz-Computer oder das Smartphone mit speziellem Zugriffsrecht auf bestimmte Programme; z. B. E-Mail-Client und den Nova-Client sein. Dabei wird ein Lichtwellenleiter mit einem mindestens 10-Gigabit-Ethernet-Eingang verwendet, um längere Strecken zwischen den Switches und den Rechenräumen zu verbinden. Die WLAN-Antenne welches mit einem 1-Gigabit Anschluss Kabel an den Switch verbunden ist, kann von den Endgeräten erkannt werden. Endgeräte, die mit der WLAN-Antenne verbunden sind, bieten einen 300Mbits Verbindung. So kann die Abteilung IT-Technik ein gemeinsames Netzwerk verknüpfen, in dem das ganze Krankenhaus verbunden ist und eine bestimmte Anwendung nutzen kann. Auf diese Weise kann der IT-Techniker auch Teilnetzwerke verknüpfen, wobei eine Abteilung oder ein Hersteller vom eigentlichen Netzwerk getrennt ist und ein eigenes Netzwerk bildet (VLAN). Die Erhaltung der Stromversorgung in einem Krankenhaus ist essentiell. Hierfür werden die Netzwerke mit einem zweiten Netzteil versorgt, um bei einem Stromausfall für einen lückenlosen Übergang der Stromzufuhr zu sorgen.

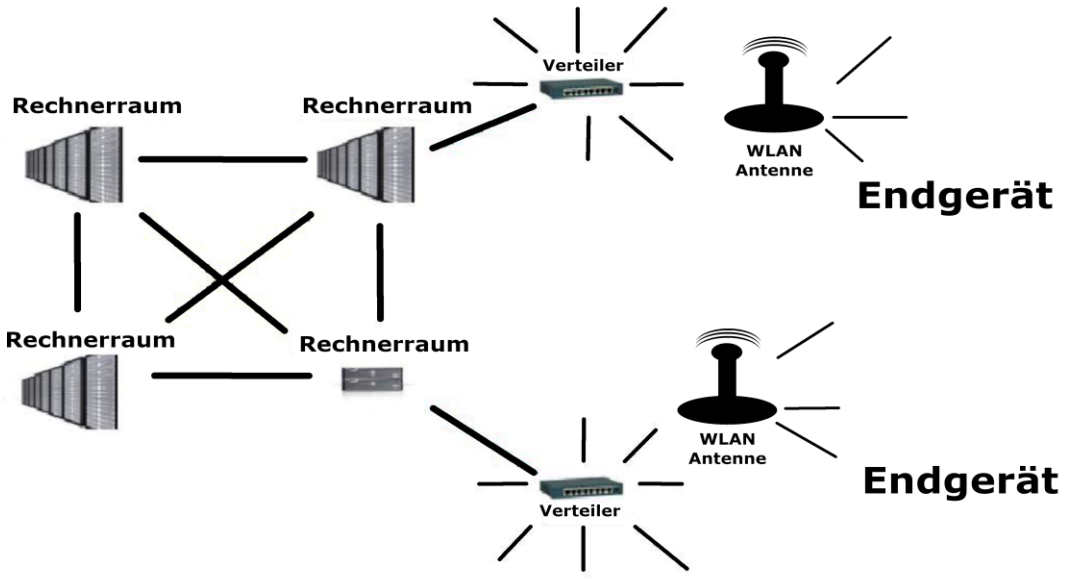

Abbildung 10: Mögliches Krankenhausnetzwerk

3.1.2 Datenstruktur des Teilnetzwerks VScan Air

Das mobile Ultraschallgerät ‚VScan Air' ist nicht ortsgebunden. Es ist handgroß und kann überall hin mitgenommen werden. Daher ist es bedeutsam, dass sein Teilnetzwerk im ganzen Krankenhaus funktioniert. Das Gerät wird über eine VLAN-Verbindung an das Netzwerk angebunden. Eine speziell dafür angelegte Buchse ist daher nicht notwendig. Über das Smartphone wird eine Verbindung zum Netzwerk hergestellt. Dabei ist es wichtig, dass das Gerät sowohl per WLAN als auch per Bluetooth eine Verbindung zum Netzwerk aufbaut, ansonsten ist ein Zugriff nicht möglich. Via KIS werden die Daten des Patienten auf dem Smartphone aufgerufen. Die bei der Untersuchung erstellten Bilder und Videos stellen Rohdaten dar und müssen mit Hilfe von Programmen in das passende DICOM-Format umgewandelt werden. Von den Arbeitsplätzen aus kann der Anwender mit dem entsprechenden Programm die Daten anzeigen lassen und die erstellten Bilder und Videos auswerten. Die Rohdaten werden Parallel in das PACS geladen aus Sicherheitsgründen. Die ausgewerteten Daten werden ebenfalls im Anschluss im PACS archiviert. Somit ist ein Fernzugriff über mehrere Clients an verschiedenen Arbeitsplätzen jederzeit möglich. Diese Prozedur der Worklist ist ein Standard und wird von fast allen anderen Geräten so genutzt. Die VScan Air hingegen kann aber auch anderes arbeiten. In Notfällen kann schnell eine Test-Person angelegt werden und die Daten werden Später dem Patienten zugeordnet. Die Speicherung der Rohdaten auf dem Smartphone ist nur begrenzt möglich, da dessen Speicher von 64GB nach ein Paar Untersuchungen ausgeschöpft ist. Neben der Archivierung der Daten im PACS wird ein Backup der Daten erstellt und auf einem weiteren Rechnerraum-Server gespeichert. Das dient der Sicherung der Daten im Falle einer Störung. (Abbildung 11)

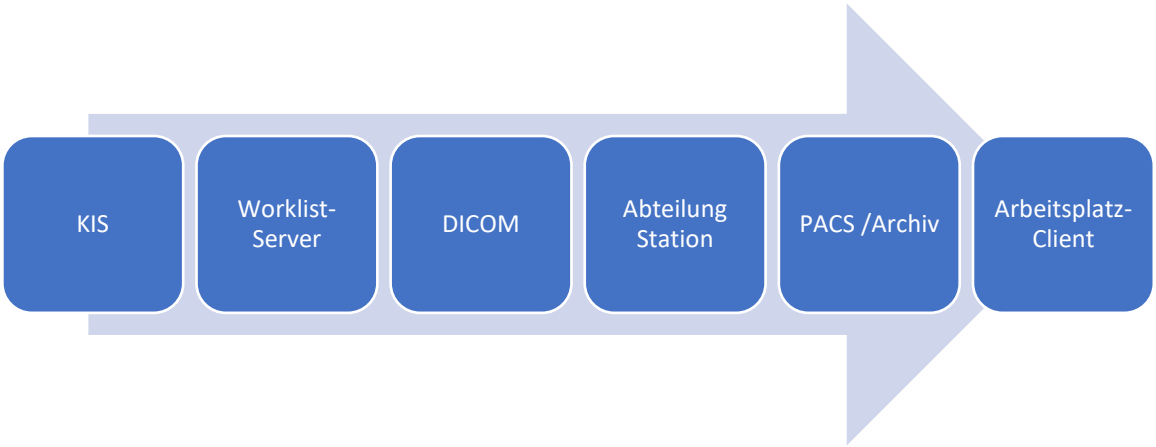

Abbildung 11: Worklist des Teilnetzwerks

3.2 Risikomanagementplan

Die von VScan Air erzeugten Ultraschallbilder und -videos werden kabellos auf das Smartphone übertragen. Dieses ist mit dem PACS verbunden, auf dem die Ultraschallbilder des Patienten gespeichert werden. So können die Aufnahmen auch später aufgerufen werden, um sie in einer Folgeuntersuchung zu vergleichen oder sie auszuwerten. Dabei können über den Arbeits-PC und die passende Software

Befunde erstellt und bearbeitet werden. Die gewonnenen Daten werden dann im KIS bei den behandelten Patienten hinzugefügt. Somit ist die Zweckbestimmung des Geräts die Aufnahme sowie die Erstellung und die Bearbeitung von Ultraschalldaten zur Durchführung der Untersuchung [5, PDF Seite 21].

Der klinische Workflow wird wie folgt koordiniert: Zuerst wird über den Client am Arbeitsplatz im KIS ein Patient angelegt und dazu werden Daten eingepflegt. Der Patient kann über das Smartphone oder das Tablet mit den gespeicherten Informationen aufgerufen werden. Sodann kann die Behandlung mit dem Ultraschallgerät beginnen und die dabei erzeugten Daten werden an das Smartphone oder das Tablet gesendet. Dieses ist mit dem Netzwerk verbunden und die ausgewählten Daten werden im PACS abgespeichert. Die Daten werden zusätzlich im KIS beim Patienten hinterlegt. Sie können dann durch die Ärzte abgerufen und beurteilt werden. Das mobile Ultraschallgerät soll im ganzen Krankenhaus genutzt werden, weshalb eine Netzwerkverbindung überall möglich sein muss.

Probleme beim Workflow entstehen, wenn das Netzwerk ausfällt, während der Behandlung und für längere Zeit nicht zur Verfügung steht. Dann kann eine Behandlung nicht vom Arbeitsplatz gestartet werden, was zu einer Verzögerung des Workflows führt. Zwar kann eine Behandlung auch direkt über das Smartphone gestartet werden, jedoch müssen die Daten nach der Netzwerk Wiederherstellung einem Patienten zugeordnet werden. Hierbei ist der begrenzte Speicher des Smartphones zu betrachten.

Alle Komponenten des medizinischen Teilnetzwerks können Risiken bezüglich der drei Schutzziele Sicherheit, Effektivität, Daten- und Systemsicherheit aufweisen. Die Medizinprodukte, die am Teilnetzwerk angebunden sind, sind im Anhang 3 aufgelistet. Zudem sind die Netzwerkkomponenten des Teilnetzwerks in Anhang 3 dargestellt. Des Weiteren ist eine genügende Bandbreite des Netzwerks sowohl zwischen dessen Komponenten (Switch, WLAN Antenne usw.) als auch am Ende der Kette bei den Medizin- und den Nichtmedizinprodukten von Bedeutung. Ein weiterer Risikofaktor kann die nichtmedizinische Software auf dem Arbeitsplatz sein (Tabelle 9).

Medizinische Software	Nichtmedizinische Software
KIS	Virenscanner
PACS	Internet-Client
Laborinformationssystem	PDF-Reader
Auswertesoftware	E-Mail-Client
	Krankenhaus-Schichtplaner
	Störmeldeportale

Tabelle 9: Anwendungssoftware

Regulär sind die Programme aus Tabelle 9 auch auf einem Arbeitsplatzrechner zu finden. Einige sind essentiell, um die Sicherheit der Arbeitsplätze sowie der Patientendaten zu gewährleisten. In Hinsicht auf das Schutzziel der Daten- und Systemsicherheit ist das Element der Patientendaten wie der Arztbrief sowie persönliche Patientendaten wie die Adresse, Bilder oder Befunde zu beachten und zu beurteilen. Andere Programme hingegen sind auswertungs- oder darstellungsorientiert.

Die Definition der Schutzziele (Patientensicherheit, Effektivität, Daten- und Systemsicherheit) sowie der jeweiligen Risikoakzeptanz ist bedeutsam und ein Teil des Risikomanagementplans. Beim Schutzziel ‚Patientensicherheit' werden alle Gefährdungen im klinischen Workflow betrachtet. Die darin integrierten Komponenten werden stückweise beurteilt. Dabei können das Ultraschallgerät, das Netzwerk, der Anwender und der Patient betrachtet werden. Beim Schutzziel ‚Effektivität' werden alle Gefährdungen gesucht, die den klinischen Workflow beeinträchtigen oder stoppen können. Beispiele sind die physische Zerstörung der Geräte oder die richtige Nutzung der Software. Beim Schutzziel ‚Daten- und Systemsicherheit' werden Gefährdungen der Vertraulichkeit, der Vollständigkeit und der Verfügbarkeit der Daten gesucht. Dabei werden das KIS, das PACS und die Software zur Erstellung und Bewertung der Ultraschallbilder genau betrachtet. Es ist relevant, dass das gesamte Netzwerk stückweise betrachtet wird, um alle möglichen Risiken zu identifizieren.

3.3 VERANTWORTLICHKEITSVEREINBARUNG

Bevor eine Verantwortlichkeitsvereinbarung erstellt wird, müssen Rahmenbedingungen festgelegt werden. Grundlegend müssen zuerst die Parteien benannt werden, für die die Verantwortlichkeitsvereinbarung gilt. Es gibt interne Parteien wie die Abteilungen Medizintechnik, IT-Technik sowie die Anwender, also die Ärzte und die Belegschaft. Des Weiteren müssen die Hersteller als externe Parteien herangezogen werden. Alle Parteien müssen über eine potentielle Gefährdung informiert werden. In der Verantwortlichkeitsvereinbarung werden ihre Pflichten und ihre Aufgaben festgelegt. Diese wurden in den Kapiteln 2.1 und 2.2 beschrieben. Die Verantwortlichkeitsvereinbarung der Agaplesion gAG ist in Anhang 1 dargestellt. Die Verantwortlichkeitsvereinbarung sollte immer vor der Neuanschaffung von medizinischen Geräten ausgefüllt werden. Dabei kann festgelegt werden, dass der Austausch der Informationen zwischen den beiden Parteien (Hersteller und Betreiber) erfolgt oder durch eine externe Firma, die als Vermittler agiert.

Als Erstes wurde Kontakt mit den Herstellern aufgenommen. Diesen wurde kurz erläutert, was das AGAPLESION DIAKONIEKLINIKUM ROTENBURG mit der DIN EN 80001-1 erreichen will und was dafür benötigt wird. Der Hersteller des Vscan Air war einverstanden, weshalb die Dokumente eingereicht wurden. Die ‚AGA FO Verantwortlichkeitsvereinbarung MIT' und die ‚AGA FO MIT Risikoübersicht V7' wurden dann von den Herstellern ausgefüllt retourniert (siehe Anhang 1 und 4). Die angeforderten Informationen, z. B. zu den Fehlerzuständen bei einem Netzwerkausfall, zur kabellosen Übertragung der Daten, zu den Ports sowie zum Virenschutz, werden später für das Risikomanagement benutzt werden.

3.4 Risikoübersicht

Das Dokument ‚AGA FO MIT Risikoübersicht V7' ist das Kernstück zu dem Risikomanagement, aus dem alle Erkenntnisse gewonnen werden. Dabei handelt es sich um zwei Unterdokumente in einer Excel-Datei. Das erste Unterdokument ist eine Legende und dient dem Verständnis des Lesers. Alle

Begrifflichkeiten so wie Abkürzungen werden in dem Dokument erläutert. Somit ist sichergestellt das alle Leser auf dem gleichen Stand sind und die Begriffe nicht fehlinterpretiert werden. Das zweite Dokument ist eine vorgefertigte Tabelle welches von den Herstellern als auch von den MT-IT ausgefüllt werden muss. Eine Erweiterung der Tabelle ist ebenfalls möglich, sollen hierzu neue Erkenntnis sich ergeben. Neben den üblichen Daten wie Firmenname und Kontaktdaten werden auch Gefährdungssituationen dargestellt und der daraus folgende Schaden- und Eintrittswahrscheinlichkeit benannt. Aus denn gelieferten Informationen kann dann der Risikomanager die RPZ-Zahl errechnen. Anschließend wird die Risikominimierung Maßnahmen eingetragen und der RPZ-Zahl wird erneut ausgerechnet. (siehe Anhang 4)

3.5 RISIKOMANAGEMENT

Die Umsetzung einer Aufgabe von der Theorie in die Praxis ist meist mit Schwierigkeiten verbunden. Um ein besseres Verständnis dafür zu entwickeln, werden Sitzungen zwischen den Abteilungen Medizintechnik und IT-Technik abgehalten. Hierbei werden relevante Punkte angesprochen oder kritisiert. Des Weiteren gab es eine externe Schulung, um die Thematik besser zu verstehen. [1] Zwar bestand ein gutes Verständnis, aber die Umsetzung fiel dennoch schwer. Um sie zu bewältigen, wurde zuerst nur ein Teilnetzwerk betrachtet. Durch das Anlegen einer tabellarischen Ansicht und des Teilnetzwerks war es einfacher, das Thema zu verstehen und die Umsetzung einzuleiten. Dazu wurden Gefährdungen, Ursachen, Gefährdungssituationen, Schäden und Maßnahmen tabellarisch aufgeführt. Das daraus resultierende Ergebnis der risikorelevanten Themen ist in Anhang 4 enthalten. Der Risikomanagementprozess wurde an jedem der benannten Punkte der drei Schutzziele Sicherheit, Effektivität und Daten- und Systemsicherheit durchgeführt. Im Folgenden werden anhand von Beispielen die Risikoanalyse und die Risikobewertung dargestellt. Bei der theoretischen Beherrschung des Risikos (Risikobeherrschung) wurden nur die möglichen Maßnahmen benannt, um das Risiko zu minimieren. Es ist relevant, dass anhand einiger Beispiele das Grundprinzip der DIN EN 80001-1 verstanden wird und dann auf alle möglichen Fälle angewandt werden kann. Im Folgenden werden die Begriffe ‚Gefährdung', ‚Ursache', ‚Gefährdungssituation', ‚Schaden' und ‚Risikobewältigung' fortlaufend benutzt, damit alle das gleiche Verständnis haben. Festzuhalten ist auch, dass es sich hierbei um eine Norm handelt, also um eine Empfehlung. Die tatsächliche Umsetzung der Norm kann anders ausfallen. Somit muss nicht jeder Punkt zu 100 % abgedeckt werden, wie sie in der DIN Norm 80001-1 steht. Dies kann verschiede Faktoren haben wie z.B. Ressourcen oder Benutzung der Medizinprodukte.

Durch die bereits integrierten Schritte des Risikomanagements DIN EN 60601-1 im Krankenhaus war ein großer Teil der Arbeit erledigt und darauf konnte zurückgegriffen werden. Die Erstellung des Plans und die Einhaltung der einzelnen Prozessschritte kosteten am meisten Zeit. Auch die für die Schaffung einiger Prozesse notwendige Einholung der Informationen vom Hersteller sowie von den Abteilungen IT-Technik und Medizintechnik bedarf einiger Zeit. Anhand der folgenden Beispiele wird der Prozess

zur Einführung des DIN EN 80001-1 erläutert. Diese Schritte können für alle Folgebeispiele aus Anhang 4 durchgeführt werden.

Beispiel 1: Schutzziel ‚Effektivität' hinsichtlich der Schnittstellen

Bei der Anbindung des VScan Air bestand die größte Schwierigkeit darin, das Gerät bei den einzelnen Schnittstellen freizugeben. Hierfür wird die Software auf das Smartphone geladen, das sich dann mit dem VScan Air verbindet und die Daten ins PACS überträgt. Dabei kann nur die Netzwerkschnittstelle des WLAN genutzt werden. Eine Verbindung per LAN oder Bluetooth ist nicht möglich. Eine Gefährdungssituation, die dabei entstehen kann, ist der Netzwerkausfall. Die Ursache hierfür kann ein Stromausfall sein. Das dabei entstehende Schadensausmaß ist gering und wurde mit dem Wert 2 definiert (Anhang 2). Denn da bei einem Stromausfall das Gerät nicht bedient werden kann, kann kein Patient oder Anwender zu Schaden kommen. Die Wahrscheinlichkeit, dass ein Stromausfall vorkommt, ist sehr gering, da im Krankenhaus alle lebenswichtige Instrumente über eine zweite Stromleitung versorgt sind. Hierfür kommt ein Notfallgenerator zum Einsatz. Der entsprechende Wert von 1 ist aus Anhang 2 zu entnehmen. Die daraus resultierende RPZ ergibt sich aus der Multiplikation des Schadensausmaßes (*S*) und der Eintrittswahrscheinlichkeit (*P*). Diese Rechnung ergab einen Wert von 2. Da die RPZ kleiner als 4 ist, ist eine jährliche Überprüfung der Sicherheitstechnische Kontrolle ausreichend. Weitere Maßnahmen zur Risikobewältigung würden mehr Aufwand und Kosten verursachen, als Risiko reduziert wird. Als allfällig dennoch vorzunehmende Maßnahme wäre die Anbindung auch des Routers an die zweite Stromleitung denkbar, sodass ein Stromausfall ausgeschlossen wird. Die Eintrittswahrscheinlichkeit würde dann 0 betragen und die Gefährdungssituation würde vermieden.

Beispiel 2: Schutzziel ‚Sicherheit' hinsichtlich Login und Logout

Die Verwaltung der Benutzerkonten ist bedeutsam und führt in vielen Fällen zu Problemen. Zum einen ist die Frage der Lizenzen zu klären und zum anderen die Sicherheit der Anwenderkonten. Da im Krankenhaus fünf Geräte des Modells VScan Air angeschafft wurden, beträgt die Mindestanzahl an Lizenzen ebenfalls fünf, für den Fall, dass alle Geräte gleichzeitig zum Einsatz kommen. Da sich bei weniger Lizenzen mehrere Geräte mit dem gleichen Konto anmelden wollen, kann es zur Unterbrechung und Verlust der Daten führen. Des Weiteren ist es relevant, die Konten der Anwender mit einem Passwort vor Fremdzugriffen zu schützen. Diesem Zweck dienen auch Timeout-Funktion, bei denen das Konto automatisch abgemeldet wird, wenn das Gerät über eine bestimmte Zeit nicht genutzt wird. Eine mögliche Gefährdungssituation ist, dass bei einem Konto, auf das mehrere Personen Zugriff haben, nicht erkennbar ist, wer die Daten und die Einstellungen bearbeitet hat. Des Weiteren kann sich die Gefährdungssituation ergeben, dass das Konto nach der Nutzung nicht abgemeldet wird und ein Fremder die Patientendaten einsieht. Die Ursache hierfür ist die unachtsame Nutzung durch den Anwender. Das kann an einem mit Stress verbundenen Tag sehr wahrscheinlich vorkommen. Das Schadensausmaß ist wesentlich und wurde mit dem Wert 4 definiert. Der Eintritt ist sehr unwahrscheinlich und wurde mit

dem Wert 1 bemessen. Somit ergibt sich eine RPZ von 4, was im grünen Bereich liegt. Das Risiko des Fremdzugriffs auf die Patientendaten kann vermieden werden, indem das Gerät nach der Nutzung in einem Schrank eingeschlossen wird. Weiterhin kann bei der Timeout-Funktion eine kürzere Zeit eingestellt werden. Somit könnte der Wert der Wahrscheinlichkeit reduziert werden. Das Schadensausmaß bliebe dabei gleich. Der neue Wert der RPZ würde somit 0 betragen und die Gefährdungssituation würde vermieden.

4 DISKUSSION

Bei der Einführung der DIN EN 80001-1 geht es darum, die DIN Norm am Standort Rotenburg (Wümme) Schritt für Schritt zu etablieren. Die Erkennung der Prozess sowie die Durchführung der Teilschritte der Norm war der erste Schritt. Somit dient dieses Beispiel als Anleitung zur Umsetzung der Norm. Hierzu wurden mehrere Treffen zwischen den Abteilungen IT- und Medizintechnik organisiert, um die Inhalte der Norm zu diskutieren und mögliche Umsetzungen zu klären. Dabei wurden mehrere Dateien erstellt und im Laufe des Prozesses verbessert.
In der DIN EN 80001-1 ist detailliert beschrieben, welche Partei (IT-Abteilung, Medizintechnikabteilung, Hersteller, Geschäftsführer) welche Aufgaben und Verantwortlichkeiten besitzt. Die in der Norm angeführte Dokumentationsstruktur ist umfassend und hilft den Anwendern beim Start der Einführung.

Mit Hilfe der ‚AGA MIT Sicherheitsrichtlinien', welche durch das Krankenhaus vorgegeben ist und der Verantwortlichkeitsvereinbarung wurde grundlegend definiert, welche Aufgabenbereiche wem zufallen (Siehe Anhang 5). Somit sind die Kommunikationswege festgelegt. Sollten Unklarheiten vorliegen, kann in den Dokumenten nachgelesen werden.

Im Verlauf der Bachelorarbeit hat sich das Verständnis über die DIN EN 80001-1 immer mehr verfestigt. Der Anfang war schwer, da der rote Faden gefunden werden musste. Durch die Teilnahme an den Treffen zwischen den Abteilungen IT-Technik und Medizintechnik sowie durch die Schulung hinsichtlich der Norm hat sich die Thematik immer besser eingeprägt und es konnten immer mehr Lösungsansätze verfolgt werden. Die Struktur der Prozesse für die DIN EN 80001-1 ist somit festgelegt. Anzumerken ist, dass diese eine Norm ist. Das heißt, dass es keine feste vorgelegte Struktur gibt, sondern es sich lediglich um Empfehlungen handelt. Dennoch sind die ersten Schritte für die Zukunft geplant und können umgesetzt werden. Der erste Schritt ist die Ernennung des Risikomanagers zur Überwachung der Prozesse. Des Weiteren wird der Risikomanagement Fragebogen an den Hersteller geschickt bei dem das Gerät gekauft wird. Geräte die bereits im Krankenahaus vorhanden sind. werden nach und nach abgearbeitet. Die gesammelten Informationen müssen dann vom Risikomanager bewertet und zur Verfügung gestellt werden.

Die Durchführung des Risikomanagements verlief zunächst gut, da die Struktur und die dafür benötigten Dokumente vorhanden waren. Dennoch muss bei jedem Gerät, für das ein Risikomanagement durchgeführt wird, jeder Punkt diskutiert werden. Daher mussten sich die Abteilungen IT-Technik und Medizintechnik immer wieder treffen. Es ist bedeutsam, dass die Ansicht beider Abteilungen berücksichtigt wird. So konnten Unklarheiten sofort geklärt werden, auch wenn dies manchmal zeitintensiv war.

Die Beschaffung der Informationen für die Netzwerkdokumentation war eines der Hauptprobleme, da die Netzwerkstruktur in Ihrem Aufbau so noch nicht Dokumentiert war. Die Kommunikation zwischen den Abteilungen IT-Technik und Medizintechnik war gut und somit konnten viele Aufgaben sowie Aufgabenbereiche abgearbeitet werden. Zudem hat sich durch die regelmäßigen Treffen zwischen den beiden Abteilungen ein positiver Zusammenhalt ergeben, was die alltäglichen Aufgaben des Krankenhauses verbessert.

Bei der Durchführung des Risikomanagements hat der Betreiber des medizinischen IT-Netzwerks den Vorteil, dass bei einer Anzeige aufgrund eines Schadens Dokumente mit Begründungen vorliegen. Auf dieser Basis wurden Maßnahmen zur Risikominimierung implementiert, auch wenn immer ein Restrisiko vorhanden ist. Somit hat der Betreiber des medizinischen IT-Netzwerks einen Schutz. Des Weiteren kann aufgrund der Beschaffung der Informationen durch das Risikomanagementdokument (Anhang 4) im Vorfeld überprüft werden, ob eine Anbindung des Medizinprodukts an das IT-Netzwerk mit schwerwiegenden Risiken verbunden ist.

Obwohl in der DIN EN 80001-1 beschrieben ist, wer die Kosten bei der Einführung der Norm zu tragen hat, ist die Einschätzung der Gesamtkosten durch den Betreiber des medizinischen IT-Netzwerks schwer. Hinzu kommen Personalkosten, aber auch Ressourcen-Kosten wie Büro- und Lagerkosten. Es hat sich herausgestellt, dass die Durchführung der Norm durch einen Mitarbeiter neben seiner Tätigkeit viel Zeit kostet, da sie einen hohen Aufwand mit sich bringt. Nach dieser Erkenntnis wurde diskutiert, ob ein weiterer Mitarbeiter eingestellt werden soll oder die Durchführung der Norm durch eine externe Firma beauftragt wird.

5 Zusammenfassung und Ausblick

Die DIN EN 80001-1 ist eine Norm, die Anforderungen und Empfehlungen für das Risikomanagement von vernetzten Medizinprodukten festlegt. Ziel ist es, eine sichere Integration von Medizinprodukten in IT-Netzwerke und andere vernetzte Systeme zu gewährleisten. Die Norm gilt für Hersteller, Anwender und Betreiber von Medizinprodukten und fordert, dass die Risiken für Patienten und Anwender bei der Integration von vernetzten Systemen berücksichtigt werden müssen. Dabei müssen auch Datenschutz- und Sicherheitsanforderungen eingehalten werden.

Für den Standort Rotenburg Wümme sind Ansätze der DIN EN 80001-1 teilweise schon vorhanden. Der Prozess des Risikomanagement ist bereits schon eingeführt wurden und kann von der DIN EN Norm übernommen werden. Der Risikomanagement Fragebogen wurde hierzu Normgerecht erweitert. Zu den Ansätzen die noch eingeführt werden müssen, handelt es sich um Strukturelle Ansätze. Die Ernennung des Risikomanagers ist der Schritt zur Durchführung des DIN EN 80001-1 Norm. Dabei ist es wichtig das die Informationen die durch den Risikomanager gesammelt wurden, sowohl von dem Hersteller als auch von der IT-Technik in einem Risikomanagement-Akte kommen. Der Risikomanager kontrolliert und überprüft alle Schritte zur Umsetzung Norm. Zurzeit werden die Aufgaben des Risikomanager von dem Bereichsleiter übernommen, was einen Mehraufwand für die Bereichsleiter bedeutet.
Aus Sicht der DIN EN 80001-1 ist der bereits vorhanden Prozess nicht ausreichen um der Norm gerecht zu werden. Zwar werden die Risiken benannt, aber die Umsetzung der Risikominimierung Maßnahmen fehlen noch, sowie die neue Bewertung des Risikos. Ebenso verhält es sich mit der Verantwortung des Risikomanagers. Da der Hersteller, IT-Technik und Medizintechnik nur ein Teil der Verantwortung übernehmen, ist es wichtig das die gesamt Verantwortung durch den Risikomanagers stets kontrolliert und durchgeführt wird.

Allerdings gibt es Verbesserungspotenziale, die in der DIN EN 80001-1 nicht berücksichtigt werden, aber den Prozess und somit die Norm besser etablieren könnten. Eine Herausforderung besteht darin, dass die Interoperabilität zwischen verschiedenen Herstellern von Medizinprodukten nicht explizit behandelt wird. Dies erschwert die Implementierung von vernetzten Systemen, die aus verschiedenen Komponenten von verschiedenen Herstellern bestehen.
Des Weiteren wäre eine Musterdarstellung des Risikomanagement Fragebogen sehr hilfreich. Das würde denn Risikomanager aber auch den Hersteller des Medizinproduktes Zeit ersparen. Der Fragebogen müsste nur einmal ausgefüllt und online zur Verfügung gestellt werden. Die Individuelle Erweiterung des Fragebogens könnte dann von dem einzelnen Betreiber vorgenommen werden.

Zusammenfassend ist die DIN EN 80001-1 ein wichtiger Schritt in Richtung sicherer und zuverlässiger Integration von vernetzten Medizinprodukten. Durch die Einhaltung der Norm können Hersteller, Anwender und Betreiber von medizinischen Geräten sicherstellen, dass die vernetzten Systeme sicher und zuverlässig funktionieren und keine Gefahr für Patienten und Anwender darstellen.

Abbildungsverzeichnis

Tabellenverzeichnis

LITERATURVERZEICHNIS

[1] El-Madani, M. [unveröffentlichte Präsentation]. Sicherheit, Wirksamkeit und IT-Sicherheit bei der Umsetzung und Anwendung von Vernetzten Medizinprodukten oder Software im Gesundheitswesen, Ort: Rotenburg (Online); Seminar gehalten 13.10.2022 und 14.10.2022.

[2] Ahlbrandt J, Röhrig R, Dehm J, Wrede C, Imhoff M. Risikomanagement für medizinische Netzwerke in der Intensiv-und Notfallmedizin. Gemeinsames Positionspapier zur Norm IEC 80001-1. GMS Med Inform Biom Epidemiol. 2013 Jul;9(3). DOI:10.3205/mibe000137

[3] GE Healthcare. Vscan Air Infomaterial [Internet]. [zitiert am 25. November 2022]. Verfügbar unter: https://vscan.rocks/de/ressourcen

[4] Johner Institut. Schlagwort: IEC 60601-1: Medizinische elektrische Geräte [Internet] [zitiert am 25. November 2022]. Verfügbar unter: https://www.johner-institut.de/blog/tag/iec-60601-1/

[5] GE Vingmed Ultrasounds. Technische Publikation VScan Air [Internet]. 2020 [zitiert am 16. Januar 2022]. Verfügbar unter: https://cdn.shopify.com/s/files/1/0515/3767/4432/files/GE_VScanAirCL_Gebrauchsanweisung_DE__compressed.pdf?v=1624868838

[6] IEC, ISO. IEC 80001-1:2021. Berlin: VDE, 2021.

[7] Medizinprodukte-Kennzeichnung: Neue EU-Verordnung MDR 2017/745 [Internet]. 2020 [zitiert am 16. Januar 2022]. Verfügbar unter: https://www.bluhmsysteme.com/blog/medizinprodukte-neue-eu-verordnung-2017745/

ANHANG 1: VERANTWORTLICHKEITSVEREINBARUNG

AGAPLESION gAG

AGA MIT Verantwortlichkeitsvereinbarung

Vereinbarung über

- ❒ Die Mitarbeit am Risikomanagement
- ❒ Die Weitergabe von Unterlagen und Empfehlungen zur Einbindung betroffener Medizinprodukte

Zwischen der Firma des Medizinproduktes und dem

XXX (Krankenhaus)

Vertreten durch: _____

_____

_____

Hersteller/Importeur _____

_____

_____

Es gelten folgende Bestimmungen:

- Von Seiten der Firma wird bestätigt, dass die betroffenen Medizinprodukte den geltenden Vorschriften, insbesondere denen des MPG (EU-Richtlinie 93/42/EWG), entsprechen.
- Die Firma verpflichtet sich, vor Einbindung des Medizinproduktes den AGA FO MIT Fragebogen zur Risikoidentifizierung auszufüllen und Fragen, die während der Risikobeurteilung auftreten zu beantworten. Hierfür wird ein Ansprechpartner von der Firma benannt.
- Die Firma stellt eine Zweckbestimmung des Medizinproduktes zur Verfügung, die eine Vernetzung rechtfertigt.
- Das Krankenhaus verpflichtet sich, die bereitgestellten Unterlagen der Firma nicht an Dritte weiterzugeben.
- Eine Veröffentlichung über die Ergebnisse bzw. eine Weitergabe der Informationen für die Risikoanalyse bedarf der vorherigen Zustimmung des Krankenhauses.
- Weitergehende Vereinbarungen bedürfen der Schriftform.

Ansprechpartner für die Einbindung von Medizinprodukten: _____

Position: _____ Kontakt: _____

Betreiber / Krankenhaus		Eigentümer / Verleiher	
Unterschrift	_____	Unterschrift	_____
Ort	_____	Ort	_____
Datum	_____	Datum	_____

Mitgeltende Unterlage:

ANHANG 2: LEGENDE DES RISIKOMATRIX UND RPZ

LEGENDE

1. Schutzziele

Folgende Schutzziele müssen für jede Gefährdung betrachtet werden:

Sicherheit
Effektifität
Datenschutz

2. Risikobewertung

	1	2	3	4	5
Schadensausmaß (S)	unbedeutend	gering	erheblich	wesentlich	existenzbedrohend
Eintrittswahrscheinlichkeit (P)	sehr unwahrscheinlich	unwahrscheinlich	möglich	wahrscheinlich	sehr wahrscheinlich

Beschreibung der Risikokategroien

Kategorie	Beschreibung
unbedeutend	Arbeitsablauf wird leicht gestört, Befundung ist unter leicht erschwerten Bedingungen möglich. Das Eintreten des Ereignisses ist
gering	Arbeitsablauf wird gestört, Weiteres Arbeiten unter erschwerten Bedingungen möglich. Das betroffene System kann nur mit Einschränkungen
erheblich	Arbeitsablauf wird gestört, weiteres Arbeiten ist augenblicklich nicht möglich.System fällt für kurze Zeit aus und ist nicht mehr zu nutzen. Das
wesentlich	Arbeitsablauf wird erheblich gestört, es kann zu Fehlfunktionen kommen, die zu Patientenschäden führen können. System fällt für längere Zeit
existenzbedrohend	Geregelter Arbeitsablauf ist nicht mehr möglich, es kommt sehr wahrscheinlich zu Fehlfunktionen, die zu Patientenschäden führen können.

Kategorie	Beschreibung
sehr unwahrschinlich	Auftreten des Problems kann nur durch Verkettung unvorhersehbarer Ereignisse ausgelöst werden
unwahrscheinlich	Problem tritt nur sehr selten auf. Es brauch eine Reihe von Einflussfaktoren, dass der Fehler auftreten kann.
möglich	Problem kann unter ungünstigen Umständen auftreten oder ist bereits vereinzelt aufgetreten
wahrscheinlich	Problem tritt regelmäßig bei nahezu jeder Anwedung des Gerätes/Programmes auf
sehr wahrscheinlich	Fehler tritt bei jeder Anwendung des Gerätes/Programmes auf, häufig auch mehrmals während des Betriebes

3. Wie wird die Risikoprioritätszahl (RPZ) ermittelt?

RPZ = S x P

4. Risikobewertung nach RPZ

	Einrichtungsintern	Verantwortlichkeit
RPZ > 14 und/oder Schadensausmaß = 5	Sofortige Einleitung von Präventivmaßnahmen, Überprüfen der Wirksamkeit, Risiko muss sofort oder ohne schuldhaftes Verzögern abgestellt werden, Bericht an den Vorstand	GF berichtet an den Vorstand
RPZ > 9	Sofortige Einleitung von Präventivmaßnahmen, Realisierung dieser innerhalb von 6 Monaten, Überprüfen der	GF, BL/HL
RPZ > 4	Unterjährige Prüfung, ob RPZ sich verändert, Überprüfen der Wirksamkeit vorhandener Präventivmaßnahmen, ggf.	GF, BL/HL
RPZ 1-4	Jährlich prüfen, u. U. ist auf weitere Überprüfung verzichtbar, in festem Rhythmus beobachten	GF, BL/HL

5. Risikobewältigung

Risikovermeidung:	Auf besonders riskante Handlungen und Tätigkeitsfelder sollte bewusst verzichtet werden.
Risikoreduktion:	Risikoreduktion durch Informationsgewinnung, Schulung und Überwachung von risikobehafteten Tätigkeiten.
Selbsttragung:	Bildung von finanziellen Reserven (Rücklagen) durch Ansatz kalkulatorischer Wagniskosten
Risikostreuung:	Diversifikation in Bezug auf Dienstleistungen, Kunden und Standorte, um nicht abwendbare Risiken zu streuen und damit so klein wie möglich zu halten.
Risikoabwälzung:	Reduzierung finanzieller Konsequenzen durch vertragliche Vereinbarungen (Stichwort Haftungsklauseln), Abwälzung auf Dritte als Leistungserbringer
Schadenverhütung:	Reduktion der Eintrittswahrscheinlichkeit und der Schadenausbreitung durch technische und/oder personelle Vorkehrungen (z.B. Alarmierungsplan)
Risikoübertragung:	Nicht kalkulierbare oder -tragbare Risiken werden auf Versicherungsunternehmen übertragen (z.B. Berufshaftpflicht, Gebäudeversicherung).

6. Risikomatrix

existenzbedrohend	5	10	15	20	25
wesentlich	4	8	12	16	20
erheblich	3	6	9	12	15
gering	2	4	6	8	10
unbedeutend	1	2	3	4	5
	sehr unwahrscheinlich	unwahrscheinlich	möglich	wahrscheinlich	sehr wahrscheinlich

Schadensausmaß

Eintrittswahrscheinlichkeit

7. Abkürzungen der verantwortlichen Abteilungen:

Verantw. zur Umsetzung	Abkürzung
IT-Abteilung	IT
Medizintechnik	MT
Hersteller	Herst.
Technische Abteilung	TA
IT-Abteilung und Medizintechnik	IT,MT
Fachabteilungen könnenergänzt werdedn	

ANHANG 3: NETZWERKKOMPONENTEN DES TEILNETZWERKS

Netzwerkkomponenten des Teilnetzwerk							
Hersteller	**Typ**	**Liefersatum**	**Standort**	**Betriebsystem**	**Software**	**Aufgaben**	**Besonderheiten**
Server							
DELL	Automated Storage	15.06.2013	Rotenburg	WIN	8.1.A	Datenspeicher	
DELL	Automated Storage	07.03.2010	Frankfurt	WIN	8.1.A	Datenspeicher	
DELL	Automated Storage	29.09.2017	Kassel	WIN	8.1.A	Datenspeicher	
Switch							
DELL	DS-SG105	15.06.2013	Intensive		S12.3	Verteiler	
DELL	DS-SG106	07.03.2010	ZNM		S12.3	Verteiler	
DELL	DS-SG107	29.09.2017	OP		S12.3	Verteiler	
WLAN Antenne							
DELL	DW-SG107	15.06.2013	Intensive		1.2.4.w	Verstärker	
DELL	DW-SG108	07.03.2010	ZNM		1.2.4.w	Verstärker	
DELL	DW-SG109	29.09.2017	OP		1.2.4.w	Verstärker	
Client							
GE GmbH		15.06.2013	Intensive	WIN	2.9.c	Kominikation	
GE GmbH		07.03.2010	ZNM	WIN	1.0.3.c	Kominikation	
GE GmbH		29.09.2017	OP	WIN	4.6.c	Kominikation	
Geräte							
GE GmbH	Vscan Air	01.08.2022	Rotenburg	Android	1.X	Ultraschall Aufnahme	
GE GmbH	Vscan Air	02.08.2022	Rotenburg	Android	1.X	Ultraschall Aufnahme	
GE GmbH	Vscan Air	03.08.2022	Rotenburg	Android	1.X	Ultraschall Aufnahme	

ANHANG 4: MEDIZINTECHNIK/IT-TECHNIK RISIKOÜBERSICHT

Der Anhang ist zu groß um es auf der Seite dazustellen und wird als Datei auf dem USB-Stick mitgeschickt

ANHANG 5: AGA MIT SICHERHEITSRICHTLINIE

Der Anhang ist zu groß um es auf der Seite dazustellen und wird als Datei auf dem USB-Stick mitgeschickt