

Risikoanalyse dynamisch vernetzter Medizingeräte

Alexander Mildner
a.mildner@unitransferklinik.de

Inhaltsverzeichnis

1. Einleitung	1
Situation der Geräteintegration heute	2
Ziel: eine offene, dynamische Vernetzung	3
2. Grundlagen	3
Regulatorische Rahmenbedingungen	3
Methoden der Risikoanalyse: Unterschiede zwischen FMEA und Risikoanalyse nach EN ISO 14971	4
3. Lösungsansatz	7
4. Umsetzung	11
Modulare Betrachtung und Delta-Analysen	11
Fehlermöglichkeiten in vernetzten Systemen	14

1. Einleitung

Mediziner müssen sich mit einer immer weiter steigenden Zahl von technischen Systemen auseinandersetzen. Insbesondere die Operationsumgebung für chirurgische Eingriffe ist in den vergangenen Jahrzehnten zunehmend komplexer geworden. Durch die Integration elektronischer medizinischer Geräte in den Operationsablauf werden neue Operationstechniken möglich oder bereits Bekannte verbessert und sicherer gestaltet. Das Spektrum der den Patienten umgebenden Geräte und Funktionalitäten reicht dabei von chirurgischen Schneidinstrumenten und Operationsmikroskopen über 3D-Navigations- und Endoskopiegeräte bis hin zum Krankenhausinformations- und Operationsplanungssystem.

Diese Geräte bzw. Systeme sind mittlerweile ein unentbehrlicher Bestandteil jeder Operation. Durch die zunehmende Verbreitung neuer Technologien und Operationsverfahren steigt die Gerätedichte im Operationssaal stetig an. Immer mehr der Geräte erzeugen medizinisch relevante Daten, welche für fundierte Diagnosen und Behandlungen schnell und sicher miteinander verknüpft und in einen systematischen Zusammenhang gebracht werden können.

Damit steht allerdings nicht mehr nur allein der Patient im Mittelpunkt der Aufmerksamkeit der Chirurgen, Anästhesisten und Assistenten. Zunehmend wird die Komplexitätsbeherrschung der Bedienung der diversen Medizingeräte und Beobachtung der Monitore zum Thema.

Durch eine Integration der Geräte in das Krankenhaus-Informationssystem und eine Vernetzung untereinander können Daten besser verknüpft werden und Funktionen verschiedener Geräte zusammengeführt werden. Eine Vernetzung der Geräte untereinander ermöglicht beispielsweise eine Daten- und Funktionsübergabe an andere Geräte, wodurch neue Funkti-

onalitäten geschaffen werden können und auch eine direkte Verringerung von Bedienaktuatorik und Messsensorik möglich wird. Durch die Zusammenführung von Datensätzen aus mehreren Geräten steigt die Qualität von Diagnosen, da alle Daten zentral dargestellt werden können.

Durch diese Möglichkeiten können Arbeitsabläufe vereinfacht und effizienter gestaltet werden, durch eine verbesserte Usability des Geräteverbundes im Vergleich zu Einzelgeräten wird das Personal entlastet und die Patientensicherheit steigt.

Situation der Geräteintegration heute

Um eine erleichterte Bedienung zu ermöglichen, bieten verschiedene Medizintechnikhersteller integrierte OP-Systeme an. Das System OR1 von Karl Storz ist ein vollständig integrierter Operationssaal für minimal-invasive Eingriffe mit einer Schnittstelle zur Anbindung an Krankenhaus-Informationssysteme und telemedizinische Kommunikation [1]. Die OP-Umgebung kann zentral über einen Touchscreen oder eine Sprachsteuerung bedient werden. Richard Wolf bietet mit dem core nova System [2] eine zentrale Steuerung in das System integrierter Medizingeräte verschiedener Hersteller in der minimal-invasiven Chirurgie an. Auch dieses System ist mit einer Schnittstelle zum PACS und einer Telemedizinlösung ausgestattet und wird ebenfalls über einen zentralen Touchscreen oder eine Sprachsteuerung bedient. Olympus bietet mit dem System Endoalpha eine vergleichbare integrierte OP-Lösung mit ähnlichem Funktionsumfang an, also einer zentralen Steuerung, Kommunikation und Dokumentation [3]. Die i-Suite des Herstellers Stryker ist eine Familie unterschiedlicher Konfigurationen integrierter Operationssäle, welche den unterschiedlichen Anforderungen verschiedener chirurgischer Disziplinen angepasst ist, und bietet ähnliche Vorteile wie die anderen integrierten OP-Systeme [4]. Das vorrangige Ziel der insoweit bereits existierenden Systeme ist eine Verringerung der Bedienelemente und eine zentrale Steuerung aller an der Operation beteiligter Geräte. Auf der anderen Seite ist auch eine Einbindung der Krankenhaus-Informationssysteme ein gemeinsames Anliegen.

Die heute übliche proprietäre Vernetzung von Medizingeräten basiert auf firmenspezifischen Schnittstellen und definierten Netzwerkverbindungen der Geräte, einer geschlossenen Vernetzung - es existieren jedoch keine gemeinsamen Standards für die Vernetzung und den Austausch von Daten von medizinischen Geräten sowie zu den angrenzenden (Krankenhaus-) IT-Systemen. Systemfremde, nicht in die proprietäre Lösung eingebundene Geräte können nicht oder nur mit großem Aufwand in einen proprietären Geräteverbund integriert werden.

Die Zulassung proprietär vernetzter Medizingeräte folgt dem Prinzip, dass durch die Vernetzung zweier Medizingeräte ein System aus Medizingeräten, welches als neues Medizingerät zugelassen wird, gestaltet wird. Für dieses System übernimmt dann einer der beiden Medizingerätehersteller als Systemführer und Inverkehrbringer die Verantwortung für das gemeinsame Funktionieren der Medizingeräte, bestätigt die Konformität und stellt die notwendigen Belange des Risikomanagements samt Test des Gerätesystems sicher. Dabei bedient sich der federführende Medizingerätehersteller der Zusammenarbeit mit dem Hersteller des anderen Medizingerätes unter Nutzung von dessen dokumentierter Spezifikationen und Risikobetrachtungen, die die Schnittstelle beschreiben und dokumentieren.

Diese Systematik passt jedoch nicht für dynamisch vernetzte Systeme unter Nutzung von Krankenhaus-IT-Netzwerken, insoweit diese der Verantwortung des Betreibers der Krankenhaussysteme unterliegen. Eine Medizingerätevernetzung unter Nutzung von Krankenhaus-Netzwerken folgt bis heute der Grundlage, dass der Betreiber dann zum Hersteller eines Medizingerätesystems wird. Der Betreiber ist dabei allerdings oft überfordert und nicht Willens, solche Systemherstellerepflichten zu übernehmen, abgesehen davon, dass die Koordination von drei Partnern für ein System hohe Transaktionskosten der Vernetzungsabstimmung mit sich bringt.

Insoweit zwingt die Ist-Situation Klinikbetreiber, sich entweder auf die proprietäre Lösung eines Herstellers zu beschränken oder nicht vernetzte Medizingeräte einzusetzen. Im ersten Fall ist es für den Betreiber nicht möglich, die für seinen Einsatzzweck optimale Kombination von Medizingeräten einzusetzen, wenn diese nicht in der proprietären Lösung mit eingebunden sind, im zweiten Fall können die Vorteile einer integrierten und vernetzten Operationsumgebung nicht ausgenutzt werden.

Ziel: eine offene, dynamische Vernetzung

Das Ziel muss also sein, einen Standard zu schaffen, welcher eine dynamische und offene Vernetzung und Integration von Medizingeräten erlaubt, ohne dass diese zum Zeitpunkt der Zulassung einander bekannt sind. Ebenso sollen die Systemherstellerepflichten nicht auf den Betreiber übertragen werden.

Eine solche Vernetzung wäre sowohl für Klinikbetreiber als auch Hersteller vorteilhaft. Die Klinikbetreiber können durch eine flexible, modulare Zusammenstellung der medizinischen Geräte eine Gerätekombination zusammenstellen, welche den spezifischen Operationsablauf optimal unterstützt. Bei Herstellern vernetzter Systeme wird mittels einer offenen Vernetzung die Reichweite des Vertriebs durch neue Möglichkeiten der Gerätezusammenstellung erhöht. Der Wegfall proprietärer Schnittstellen durch eine vereinfachte Zulassung und weniger benötigtes Expertenwissen bei der Schnittstellenkonfiguration führt zu Einsparpotenzialen. Unternehmen, welche bis jetzt keine vernetzbaren Medizingeräte herstellen, erreichen ebenfalls eine Erhöhung ihrer Vertriebsreichweite und eine steigende Attraktivität ihrer Geräte, wenn diese in einen vernetzten Operationssaal integriert werden können.

2. Grundlagen

Regulatorische Rahmenbedingungen

Der Hersteller eines Medizinprodukts ist dafür verantwortlich, dass sein Produkt für die festgelegte Zweckbestimmung zugelassen ist und das alle mit seiner Anwendung (nach Zweckbestimmung) verbundenen Risiken nach Abwägung gegen den klinischen Nutzen vertretbar sind. Er muss bei der Zweckbestimmung seines eigenen Medizinprodukts darauf achten, dass er keine Zusammenstellungen zulässt, für die er die Sicherheit nicht bestätigen kann.

Die heute übliche proprietäre Vernetzung von Medizingeräten folgt dem Prinzip, dass durch die Vernetzung zweier Medizingeräte ein Medizinsystem gestaltet wird, für das einer der Hersteller als System-Inverkehrbringer die Verantwortung für das Funktionieren des Systems

aus Medizinprodukten übernimmt; er erklärt also die Konformität des Systems und stellt die Belange des Risikomanagements samt Tests des Gerätesystems sicher.

Gleiches gilt wenn der Betreiber die Vernetzung vornimmt. In diesem Fall nimmt er eine Eigenherstellung nach §12 des Medizinproduktegesetzes vor. Die Betreiberorganisation ist verantwortlich dafür, vor der Verwendung des „neuen“ Produkts die Erfüllung der grundlegenden Anforderungen nachzuweisen [5].

Bei einer Zulassung einer Verbindung von Medizinprodukt und Zubehör verhält es sich ähnlich. Hier erklärt der Medizinprodukt-Hersteller die Konformität des Gesamtsystems und stellt die Belange des Risikomanagements sicher.

Zubehör ist nach der Richtlinie 93/42 EWG Anhang IX Regel II, 2.2 unabhängig von dem Produkt, mit dem es verwendet wird, gesondert zu klassifizieren. Somit ist beispielsweise ein Fußschalter, der ein Medizingerät steuert, als Zubehör analog zu einem Klasse 1-Produkt zu klassifizieren. Die Klassifizierung ergibt sich aus einer Zweckbestimmung der Steuerung eines anderen Medizinprodukts. Zusätzlich müssen Informationen an den Hersteller des Medizinprodukts zur korrekten Verwendung und Einbindung des Zubehörs gegeben werden. Dieser relativ einfache Weg der Zulassung eines Zubehörs ist allerdings nur bei analogen Ausgangssignalen wie beispielsweise des Schließens eines Stromkreises möglich.

Bei einer digitalen Signalübertragung enthält das Zubehör notwendigerweise Software. Es trifft die weitere Regel der 93/42 EWG zu. Anhang IX, Regel II, 2.3 besagt, dass Software, welche ein Medizingerät steuert oder dessen Anwendung beeinflusst, automatisch derselben Klasse wie das Medizingerät zuzuordnen ist. Auch die Einbindung in das Risikomanagement und die zu übergebende Dokumentation und Begleitpapiere werden umfangreicher. Somit ist beispielsweise ein Fußschalter, welcher über ein Übertragungsprotokoll mit dem Medizingerät kommuniziert, in die gleiche Risikoklasse wie das gesteuerte Gerät einzuordnen.

Methoden der Risikoanalyse: Unterschiede zwischen FMEA und Risikoanalyse nach EN ISO 14971

Die Fehlermöglichkeits- und Einflussanalyse FMEA ist eine Methode zur Risikoanalyse, -bewertung und -beherrschung und findet zunehmend auch in der Medizintechnik Verbreitung. In der FMEA werden die Folgen eines Versagensmodus systematisch untersucht und bewertet. Es stellt sich immer die Frage „was passiert wenn...“. Die FMEA folgt einem „bottom-up“-Ansatz, was bedeutet, dass eine auslösende Ursache und die Fehlerfortpflanzung zur nächsten Ebene des Funktionssystems betrachtet werden; der Fehler bei einer Bauteilkomponente verursacht eine Störung des Bauteils, diese setzt sich fort bei der Baugruppe usw.. Eine genaue Beschreibung der Methode findet sich in der IEC 60812 [6]. Eine Risikoanalyse mittels FMEA kann nicht nur für funktionale Baugruppen, sondern auch für Prozesse (Prozess-FMEA) und Anwendungsfehler (Human-FMEA) erstellt werden. Wenn im Folgenden von einer FMEA gesprochen wird, ist allerdings immer die technische Design-FMEA für funktionale Baugruppen/-teile etc. gemeint.

Eine FMEA besteht aus den drei Teilen der Risikoanalyse, Risikobewertung und Risikobeherrschung. In der Risikoanalyse werden Fehlerquellen identifiziert und davon ausgehende mögliche Störungen oder Ausfälle identifiziert. In der Risikobewertung werden diese technischen Risiken mit Zahlenwerten zur Auftretenswahrscheinlichkeit des Versagens einer Kom-

ponente, Schweregrad der Auswirkung und Entdeckungswahrscheinlichkeit des Fehlers belegt. Diese werden in der Regel mit Zahlenwerten zwischen 1-10 bewertet, wobei 10 immer der Worst Case ist. Also bedeutet eine hohe Bewertung eine hohe Auftretenswahrscheinlichkeit, einen hohen Schweregrad und eine geringe Entdeckungswahrscheinlichkeit. Diese Zahlenwerte werden multipliziert und bilden so die Risikoprioritätszahl (RPZ). Je höher diese ist, desto kritischer ist der Versagensmodus anzusehen. In der Regel liegen akzeptable Risiken bei Werten von 0-120, kritische Risiken bei etwa 120-300 und nicht akzeptable Risiken bei 300-1000. In der anschließenden Risikokontrolle werden Maßnahmen zur Risikobeherrschung getroffen. Nach deren Umsetzung erfolgt eine Neubewertung.

Im regulatorischen Umfeld von Medizinprodukten ist die zu erfüllende Norm die EN ISO 14971 [7], welche ein Risikomanagement über den gesamten Produktlebenszyklus vorgibt. Ein Teil der Norm beschäftigt sich mit einem Risikoanalyse-, Risikobewertungs- und Risikobeherrschungsverfahren. Dieses Verfahren ist ähnlich einer FMEA aufgebaut. Es gibt aber auf der anderen Seite auch klare Unterschiede zwischen einer Risikoanalyse nach 14971 und einer technischen FMEA, welche im Folgenden benannt werden:

1. Die FMEA ist eine Methodik für technische Risikoanalysen. Daraus folgt, dass zu einer Fehlermöglichkeit der direkte Einfluss auf die nächsthöhere Baugruppe betrachtet wird. Die Risikoanalyse nach EN ISO 14971 betrachtet als Schaden immer die Schädigung von Patienten, Anwender oder Umgebung, also die letzte Konsequenz der Schadensursache; ein Fehler eines Bauteils führt ggf. zu Fehlern auf höheren technischen Ebenen (FMEA) bis hin ggf. zur Beeinträchtigung einer Gerätefunktion, die dann einen Schaden verursachen kann (Risikoanalyse nach EN ISO 14971).
2. Die FMEA betrachtet die Auftretenswahrscheinlichkeit des Fehlers einer Komponente und die Entdeckungswahrscheinlichkeit dieses Fehlers. Diese ziehen einen Fehlereinfluss eines bestimmten Schweregrades nach sich. Die EN ISO 14971 betrachtet diese Faktoren aus einer anderen Sichtweise. Hier wird nicht die Auftretenswahrscheinlichkeit eines Fehlers, sondern die des resultierenden Schadens betrachtet. Das Risiko setzt sich zusammen aus Auftretenswahrscheinlichkeit des Schadens und Schadensausmaß.
3. In der technischen FMEA wird zwischen Vermeidungsmaßnahmen und Entdeckungsmaßnahmen unterschieden. Vermeidungsmaßnahmen senken die Auftretenswahrscheinlichkeit und/oder den Schweregrad, Entdeckungsmaßnahmen steigern die Entdeckungswahrscheinlichkeit, um in diesem Fall geeignete Maßnahmen zur Fehlerfortsetzung auf höheren Ebenen ergreifen zu können. Die EN ISO 14971 unterscheidet hingegen zwischen Maßnahmen zur inhärenten Sicherheit, Schutzmaßnahmen und Warnhinweisen. Maßnahmen zur inhärenten Sicherheit können hier den Schweregrad vermindern, Schutzmaßnahmen und Warnhinweise hingegen die Auftretenswahrscheinlichkeit.

Nach der harmonisierten Norm EN ISO 14971 muss für jedes Medizinprodukt und System aus Medizinprodukten eine Risikoanalyse mit dem Endpunkt des Schadens des Patienten oder Anwenders durchgeführt werden. Die aus der Risikoanalyse abgeleiteten Restrisiken müssen gegen den klinischen Nutzen abgewogen werden. Aufgrund des Harmonisierungscharakters der Norm gilt die Konformitätsvermutung, wenn die Norm in allen Belangen ein-

gehalten wurde. Es wird insoweit vermutet, dass das Medizinprodukt den grundlegenden Anforderungen im Bereich des Risikomanagements entspricht. Wenn eine andere Methode als die in der Norm beschriebenen zur Risikoanalyse, -bewertung und -beherrschung angewandt wird, ist für eine Zulassung des Medizinprodukts zu begründen, aus welchem Grund dieses angewandt wurde.

Ein Beispiel für eine solche Verfahrensänderung für die Risikobetrachtung ist die Zulassung eines Fußschalters als Zubehör zu einem Medizingerät. Für die Funktionsausgänge des Fußschalters als Steuersignale des Medizingeräts kann insoweit keine Risikoanalyse mit dem Endpunkt Patientenschädigung durchgeführt werden, als das der Fußschalterhersteller diese Risiken nicht kennen kann. Der mögliche Schaden am Patienten oder Anwender stellt erst die letzte Konsequenz einer Ursachenkette dar, an deren Ende der Funktionsausgang des die Funktion ausführenden Medizingerätes steht.

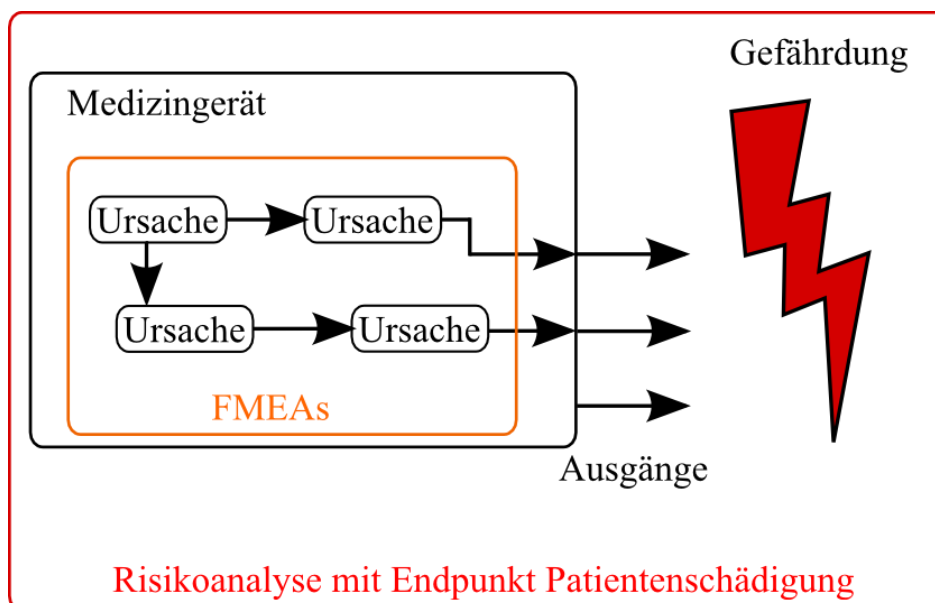


Abbildung 1: Risikoanalysen Geräteintern und -extern

Innerhalb dieser Ursachenkette, in der in diesem Beispiel auch der Fußschalter steht, werden lediglich technische Risiken des Ausfalls der nächsthöheren Baugruppe analysiert und bewertet. Eine Risikoanalyse mit dem Endpunkt Patientenschädigung, welche die EN ISO 14971 beschreibt, ist erst am Funktionsausgang, an welchem eine Wechselwirkung mit der Umgebung auftritt, durchzuführen. Damit ist für den Fußschalterhersteller für die Risikoanalyse seiner Steuersignale eine technische Risikoanalyse nach dem FMEA-Vorgehen angemessen. Die aus dieser Risikoanalyse hervorgehenden Fehlermöglichkeiten werden an den Hersteller des gesteuerten Medizingeräts kommuniziert und am Ende der Ursachenkette auf eine mögliche Patientenschädigung betrachtet.

3. Lösungsansatz

Da die dynamische Vernetzung erhebliche Vorteile für medizinische Anwendungsszenarien hat, muss eine neue Logik und Vorgehensweise für das Zulassungs- und Risikomanagement erarbeitet werden. In erster Linie betreffen diese eine Erfassung und methodische Bearbeitung von aus der Vernetzung hervorgehenden neuen Anforderungen und Risiken.

Ausgehend von der proprietären Vernetzungs-Vorgehensweise sind vier logische Betrachtungsebenen für die dynamische Vernetzung zu adressieren. Diese sind in Abbildung 2 abgebildet und werden im Weiteren erläutert.

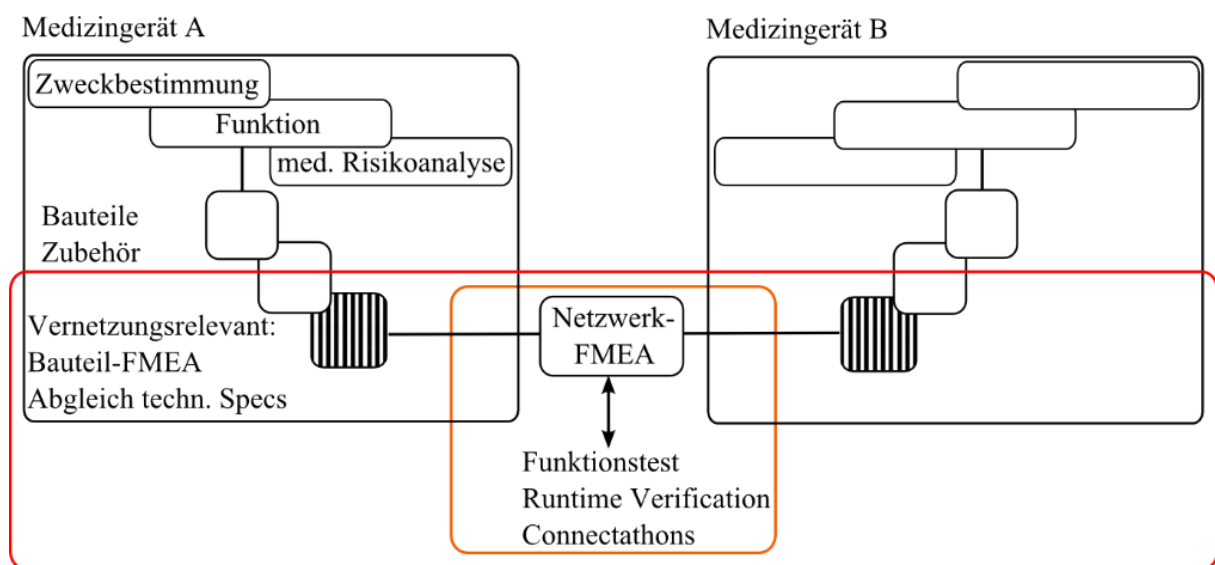


Abbildung 2: Betrachtungsebenen der Gerätevernetzung

Zweckbestimmungs-/Funktionsebene:

Jedes Medizingerät und jede Kombination von Medizingeräten hat Anwendungsanforderungen zu erfüllen, die in der medizinischen Zweckbestimmung der Geräte definiert sind, aus der sich dann sekundär funktionale und tertiär technische Geräte-Anforderungen bzw. -Spezifikationen ableiten lassen.

Die medizinische Zweckbestimmung beinhaltet alles, was mit dem Medizinprodukt medizinisch im Sinne einer Diagnose, Therapie oder Überwachung von Krankheiten und Verletzungen erreicht werden soll [5, p. 09001]. In der medizinischen Zweckbestimmung sollten folgende Aspekte betrachtet werden:

- Medizinische Anwendung (Art der Diagnose/Therapie, Indikation,...)
- Patientenpopulation (Alter, Geschlecht, Gewicht, behandelte Organe,...)
- Anwender (Ausbildung, Kenntnisse, erforderliche Einweisung,...)
- Anwendung (Anwendungsdauer, Umgebungsbedingungen, Art der Anwendung,...)

Aus der medizinischen Zweckbestimmung leitet sich die Risikoklassifizierung ab und es bildet die Grundlage des Risikomanagements. Die medizinische Zweckbestimmung bildet den

Kern des Lastenhefts, welches diese um die Definition der Produktidee und einer anwender-induzierten Beschreibung der Funktionalität und des gewünschten Nutzens des Produktes ergänzt. Das Pflichtenheft setzt nun all diese Funktionsanforderungen in technische Geräte-Anforderungen und –Spezifikationen um [8] [5].

In der Regel werden bei einer Medizingerätevernetzung die medizinischen Zweckbestimmungen der zu vernetzenden Medizingeräte nicht tangiert. So ergibt sich zum Beispiel bei der Vernetzung eines Operationsmikroskopes und eines chirurgischen Schneidgerätes im Hinblick auf die gemeinsame Nutzung von Bedien- und Anzeigeelementen des Mikroskopsystems (Fußschalter, Handschalter, Anzeige von Einstellungsparametern), dass durch die Vernetzung die jeweiligen medizinischen Zweckbestimmungen der Geräte nicht geändert sind. Ebenso wenig werden die aus der Zweckbestimmung ableitbaren notwendigen Funktionen beider Geräte zur Realisierung der medizinischen Zweckbestimmung, also die Bedienung und Anzeige von Einstellungsparametern, funktional nicht verändert. Die Vernetzung besteht lediglich in der anderen technischen Realisierung der Funktionen; statt des eigenen Fußschalters des Schneidgerätes wird der andere Fußschalter des OP-Mikroskops benutzt, das eine Zubehör also durch das andere ersetzt. Natürlich müssen dabei die technischen Anforderungen bzw. Spezifikationen der Bedienelemente und Anzeigeeinstellungen des einen Gerätes (chirurgisches Schneidgerät) mit den Spezifikationen der Bedieneinheiten des anderen Gerätes, mit dem es vernetzt werden soll (Mikroskopsystem), kompatibel sein und insoweit auch auf mögliche technischen Risiken überprüft werden.

In der Konsequenz bedeutet dies, dass im Falle dynamischer Vernetzung von Geräten die zur Verfügungstellung von Diensten an bzw. Nutzungsmöglichkeit von Diensten von anderen Geräten in die technische (nicht medizinische) Zweckbestimmung aufgenommen werden muss. Auch muss dieser Umstand jeweils im Hinblick auf eine mögliche Veränderung der jeweils medizinischen Zweckbestimmung und der Funktionen zur Realisierung dieser medizinischen Zweckbestimmungen überprüft werden. Da aber üblicherweise die medizinische Hauptzweckbestimmung der Geräte nicht tangiert ist, finden Erweiterungen in einem Zusatz zur medizinischen Zweckbestimmung oder als Änderungen im Bereich technischer Spezifikationen im Hinblick auf die Bau-/ Zubehöerteile, die die Gerätefunktion unterstützen, statt. Dies betrifft beispielsweise die Nutzung von Bedienelementen, Anzeigemöglichkeiten von Parametern oder der Messwertnutzung anderer Geräte.

Sollten sich dennoch Veränderungen auch auf der medizinischen Zweckbestimmungsebene und der dafür notwendigen Funktionen ergeben, so müssten diese in die Risikoanalyse mit dem Endpunkt möglicher Patientengefährdungen einfließen. Dies wird üblicherweise bei der Vernetzung von Medizingeräten nicht der Fall sein, weil diese sich „nur“ auf der Ebene der technischen Realisierung der Funktionen abspielen wird, nicht jedoch durch Funktionsänderungen als solche. Erst wenn eine Vernetzung von Medizingeräten auf Ebene ihrer medizinischen Funktionen stattfindet, typischerweise bei automatisierten Funktionssteuerungen ohne Eingriff des medizinischen Anwenders werden weiterreichende Risikobetrachten bis hin zu klinischen Bewertungen durchgeführt werden müssen.

Spezifikationsebene:

Bei unveränderter medizinischer Zweckbestimmung und diesbezüglicher Funktionen zur Realisierung derselben muss im Hinblick auf die Vernetzung ein Abgleich der Spezifikationen der für die Umsetzung der Funktionen eingesetzten Bau-/Zubehöerteile sichergestellt werden. Nur wenn gegenseitig die Spezifikationsanforderungen erfüllt werden, dürfen Geräte vernetzt werden.

Die Vernetzung über ein Krankenhaus-IT-Netzwerk ist notwendigerweise digital, so dass sich die technischen Spezifikationen im Hinblick auf die Übertragung digitaler Parameter in einer Schnittstellenbeschreibung abbilden lassen. Wenn also gegenseitig sichergestellt werden kann, dass die digitalen Signale gemäß der Schnittstellenbeschreibung gesendet und empfangen werden, kann von sicherer Vernetzungsfähigkeit ausgegangen werden. Natürlich muss dies Gegenstand einer Risikobetrachtung werden (vgl. unten).

Im Übrigen ist auch die Sicherheit und Zuverlässigkeit der jeweiligen Bau- und Zubehöerteile sicherzustellen, insbesondere im Hinblick auf Usability. Dabei ist eine Gerätevernetzung in dieser Hinsicht jedoch zunächst als positiv anzunehmen und dann zu bestätigen, weil die Gerätevernetzung typischer Weise ja eben gerade im Bereich der Usability für den Anwender einen Vorteil realisiert und es insoweit überhaupt den Anlass zur Vernetzung von gibt.

Die Sicherheit und Zuverlässigkeit der betreffenden Bau-/Zubehöerteile im Rahmen der Gerätevernetzung wird durch technische Risikoanalysen mit der hierfür geeigneten Methodik der Fehlermöglichkeits- und Einflussanalyse (FMEA) getrennt jeweils auf Seiten der zu vernetzenden Geräte analysiert; im Beispiel haben die zu vernetzenden Geräte beide einen Fußschalter in ihrer Gerätekonfiguration, deren mögliche Fehlfunktionen bereits in der medizinischen Risikoanalyse betrachtet werden mussten: "welcher Schaden am Patienten kann auftreten, wenn das Bedienelement Fußschalter ausfällt ... (o.ä.)" Auch sollten darunter liegende technische Risikoanalysen (FMEA) ggf. von Fußschalterherstellern vorliegen. Diese FMEA der Hersteller können deshalb ergänzend zum Abgleich der eigentlichen technischen Spezifikationen zum Abgleich der Risikobetrachtungen herangezogen werden.

Vernetzungsebene:

Im Szenario der dynamischen Vernetzung sind die zu vernetzenden Medizingeräte unabhängig vom Netzwerk des jeweiligen Krankenhausbetreibers zu sehen. Gleichwohl bestehen von beiden Herstellern der zu vernetzenden Medizingeräte aufgrund der jeweiligen technischen Spezifikationen auch Anforderungen an das Netzwerk. Insoweit das Netzwerk Fehlermöglichkeiten im Hinblick auf die Übertragung von notwendigen digitalen Signalen zwischen den Medizingeräten bergen kann, ist eine entsprechende Risikobetrachtung der möglichen Fehlerverursachung durch das Netzwerk notwendig.

Diese Risikobetrachtung kann wiederum durch die technisch orientierte FMEA durchgeführt werden, insoweit „höher liegende“ Folgen möglicher Funktionseinschränkungen bereits jeweils auf Medizingeräteebene im Rahmen der dortigen medizinischen Risikoanalysen (nach EN ISO 14971) betrachtet sind.

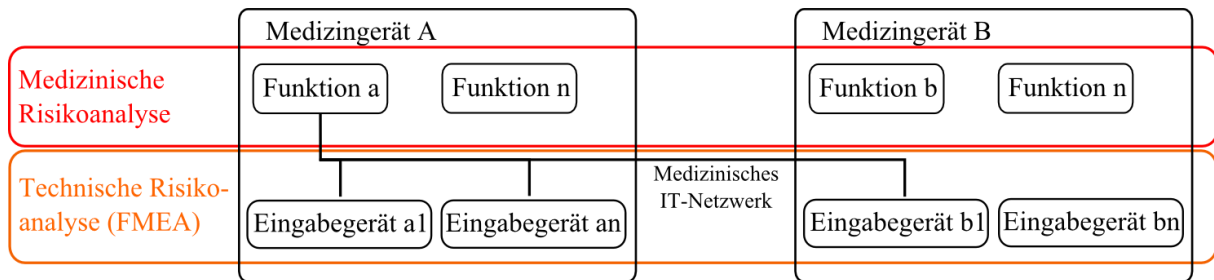


Abbildung 3: Ebenen der Risikoanalyse

Insoweit nun die Fehlermöglichkeiten aus einem Netzwerk heraus „endlich“ sind, kann eine standardisierte „Vernetzungs-FMEA“ - es werden alle Übertragungs-Fehlermöglichkeiten von Netzwerken generell betrachtet - zugrunde gelegt werden, die gleichermaßen von Medizingeräte-Herstellern auf jeweils ihrer Seite in Verbindung mit der jeweils technischen Risikoanalyse betreffend Bau-/Zubehöerteile herangezogen werden kann. Sofern sich aus dem Abgleich des Herstellers mit der Standard-Vernetzungs-FMEA keine zusätzlich zu betrachtenden Risiken ergeben, kann davon ausgegangen werden, dass die Vernetzung im Hinblick auf die jeweiligen funktionalen und damit patientenorientierten Anforderungen unschädlich ist. Wenn sich jedoch aus dem Abgleich mit der Vernetzungs-FMEA zusätzliche Aspekte ergeben, müssen diese im Einzelfall weiter geklärt werden.

Testverfahren:

Im Fall proprietärer Vernetzungen zweier definierter Medizingeräte sind umfangreiche Tests der Vernetzung möglich, die dann bei unveränderten Spezifikationen auf beiden Seiten der Geräte den Nachweis der generellen Sicherheit und Zuverlässigkeit des Systems erbringen. Gleichwohl wird bei solchen Systemen im Einzelfall ein einfacher Funktionstest vor dem ersten Einsatz durchgeführt.

Im Fall dynamischer Vernetzungen wird aus dem Kompatibilitätsabgleich technischer Spezifikationen sowie technischer Risikoanalysen von Bau-/Zubehöerteilen und des Netzwerks abgeleitet werden können, dass eine sichere Vernetzungsfähigkeit gegeben ist. Auch diese muss im ersten Einsatzfall bei Einrichtung der Gerätevernetzung natürlich einem Funktionstest standhalten.

Darüber hinaus können weitere Verfahren der Runtime-Verification (Testverfahren im laufenden Betrieb) und Konnektivitätstests (Connectathons) ergänzt werden, die dann gemeinsam den proprietären Konnektivitätstest ersetzen.

Risikomanagement:

In diesem Szenario des Abgleichs von Anforderungen an Spezifikationen und technische Risikoanalysen kommt dem Betreiber des Netzwerkes dann die Aufgabe zu, auf Basis jeweils zugelieferter Dokumente die Kompatibilität der Geräte auf Basis seines gegebenen Netzwerkes festzustellen.

Regulatorisch betrachtet wird jedoch kein Gerätesystem adressiert, sondern die Ergänzung jeweils eines Medizingerätes im Sinne von Zubehör durch ein Bauteil bzw. das Zubehör ei-

nes anderen Gerätes, welcher durch ein vom Krankenhausbetreiber zur Verfügung gestellten Netzwerks angebunden wird.

Aus den vorgenannten Überlegungen ergeben sich für den Vernetzungspartner, welcher Bauteile in Verbindung mit dem Netzwerk eines anderen Medizingerätes nutzt, keine Veränderungen der medizinischen Zweckbestimmung. Die jeweils mit Risikoanalysen betrachteten und spezifiziert zugesicherten Eigenschaften der Bau-/Zubehörteile bzw. des Netzwerks und die damit verbundenen Haftungen bleiben unbenommen.

Da die dynamische Vernetzung insoweit in der Regel auch keine Veränderung der medizinischen Zweckbestimmungen der vernetzten Geräte adressiert, beschränken sich die Änderungen an zulassungsrelevante Dokumentationen auf Ergänzungen der technischen Zweckbestimmung (technischen Spezifikation) und diesbezügliche technische Risikoanalysen.

Die Risikoanalyse mit dem Endpunkt Patientenschädigung (Risikoanalyse nach EN ISO 14971) muss nicht erweitert werden, wenn sich aus den darunterliegenden FMEA keine Anhaltspunkte dafür ergeben. Für die technische Risikobetrachtung ist eine Fehlermöglichkeiten-Einflussanalyse ohne Bezug zur potentiellen Schädigung des Patienten oder Anwenders zunächst angemessen. Die Betrachtung der Patientenschädigung liegt bei der Zulassung von Medizinprodukt und Zubehör auch im heutigen Usus weiterhin beim gesteuerten Gerät. Diese Vorgehensweise entspricht der in Kapitel 2 beschriebenen Zulassung eines Zubehörproduktes, da der Hersteller des Vernetzungspartners, welches Funktionen des anderen steuert, nicht wissen kann, was das gesteuerte Gerät im Detail am Patienten oder Anwender bewirkt und welche Schädigungen auftreten können.

4. Umsetzung

Modulare Betrachtung und Delta-Analysen

Aus den in Kapitel 3 beschriebenen Ebenen lassen sich Anforderungen an den Aufbau einer Zulassungs- und Risikomethodik-Strategie ableiten. Auf den einzelnen Ebenen sind verschiedene Zusatzarbeiten im Vergleich zu unvernetzten Medizingeräten notwendig, welche bereits im vorigen Kapitel adressiert wurden. Diese Zusatzarbeiten werden für beide Geräte durchgeführt und, je nachdem ob eine Wechselwirkung zum Vernetzungspartner besteht, einer Delta-Analyse unterzogen oder in einem Geräteprofil erfasst.

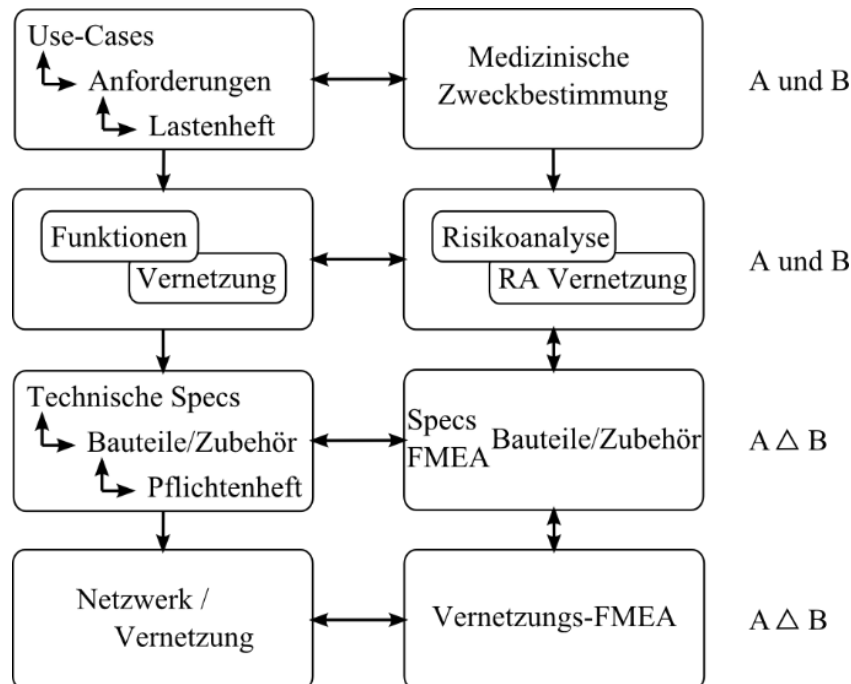


Abbildung 4: Abbildung der zulassungsrelevanten Änderungen im Entwicklungsprozess

Zweckbestimmungs-/Funktionsebene:

Typischer Weise werden die medizinischen Hauptzweckbestimmungen bei einer Vernetzung von Medizingeräten nicht tangiert. Gleichwohl muss eine Prüfung durchgeführt werden, ob eine Ergänzung der medizinischen Zweckbestimmung durchgeführt werden muss. Wenn ein Medizingerät zusätzlich zu seiner Haupt-Zweckbestimmung als Zubehör zu einem anderen fungiert und dessen Funktionen (auf technischer Umsetzungsebene) übernimmt, dann kann diese zusätzliche Funktionalität in einem Zusatz zur Zweckbestimmung Berücksichtigung finden.

Die medizinische Zweckbestimmung des Vernetzungspartners, welcher Bedienfunktionen, Anzeigedaten oder Messwerte zur Verfügung stellt, wird in der Regel nicht geändert. Sollten sich aus den tieferliegenden Risikobetrachtungen Änderungen im Bereich der zur Erfüllung der medizinischen Zweckbestimmung notwendigen Funktionen ergeben, muss die Risikoanalyse mit dem Endpunkt Patientenschädigung des entsprechenden Gerätes erweitert werden.

Die Überprüfung erfolgt auf jeder Seite der zu vernetzenden Geräte isoliert und wird in dem jeweiligen Geräteprofil dokumentiert. Auf der Funktionsebene findet ebenfalls die Definition von Vernetzungsszenarien statt. Wenn beide Vernetzungspartner die jeweilige Seite des Vernetzungsszenarios abbilden, kann eine Vernetzung stattfinden.

Spezifikationsebene:

Im Hinblick auf die zur Umsetzung der Funktionen, die die Zweckbestimmung erfüllen, notwendigen Bau-/Zubehöerteile müssen Spezifikationsanforderungen gestellt und eine technische Risikoanalyse in Form einer FMEA durchgeführt werden. Insoweit unterscheiden sich

ein Vernetzungspartner und das überbrückende Netzwerk nicht von bei einem Medizingerät zugelassenen Bau-/Zubehörteilen.

Die Anforderungen an technische Spezifikationen des Vernetzungspartners umfassen sowohl technische Parameter als auch User-Interface-Anforderungen. Da die Vernetzung über ein Krankenhaus-Netzwerk digital ist, bestehen technische Spezifikationen an die Schnittstelle des Vernetzungspartners notwendigerweise aus Anforderungen an digitale Parameter und Modalitäten der Verbindung, beispielsweise die verwendeten Protokollversionen oder Datentypen des Vernetzungspartners oder Quality of Service-Anforderungen an die Verbindung. User-Interface-Anforderungen stellen Bedingungen an die Ein- und Ausgabegeräte sowie Interaktionselemente. Die Sicherheit der die Vernetzung betreffenden Bau-/Zubehörteile wird durch eine technische Risikoanalyse typischerweise mittels einer FMEA erfasst und sichergestellt.

Im Vorfeld einer Gerätevernetzung müssen die Spezifikationsanforderungen und Ergebnisse der technischen Risikoanalysen im Rahmen einer Delta-Analyse durch den Betreiber verglichen werden, um eine sichere Vernetzungsfähigkeit sicherzustellen. Die Vernetzungsfähigkeit besteht aus technischer Sicht dann, wenn die Spezifikationsanforderungen gegenseitig erfüllt werden, also Kompatibilität gegeben ist. Ein sicherer Betrieb wird weiter durch den Vergleich der jeweiligen FMEA durch den Betreiber ermöglicht. Erst wenn sich im Rahmen der FMEA eines Medizingeräts Aspekte ergeben, welche Auswirkungen auf die Funktionalität des Vernetzungspartners bergen und dort noch nicht berücksichtigt sind, muss überprüft werden, ob im Einzelfall zusätzliche Gegenmaßnahmen implementiert werden müssen. Um diese Vergleichbarkeit zu erleichtern ist es sinnvoll, einen Katalog aus Fehlermöglichkeiten aus der dynamischen Vernetzung zu erarbeiten.

Vernetzungsebene:

In der dynamischen Vernetzung von Medizingeräten sind diese unabhängig vom Netzwerk des jeweiligen Krankenhausbetreibers zu sehen, stehen aber gleichwohl in Abhängigkeit zu diesem, da der Datentransfer über das Netzwerk abgewickelt wird. Für einen Regelbetrieb können Quality of Service-Anforderungen an das Netzwerk gestellt werden (siehe unten), welche die Grundanforderungen an einen reibungslosen Betrieb der vernetzten Medizingeräte stellen. Für den Fehlerfall ist eine netzwerkspezifische technische Risikoanalyse in Form einer FMEA notwendig. Die Risikoanalyse mit dem Endpunkt Patientenschädigung des jeweiligen Geräts wird nicht tangiert, insoweit beispielsweise ein Netzwerkausfall lediglich eine Fehlermöglichkeit des Ausfalls einer Komponente darstellt.

Aufgrund endlicher Fehlermöglichkeiten aus dem Netzwerk kann ein Katalog aus Fehlermöglichkeiten erarbeitet werden, welcher jeweils von beiden Medizingeräteherstellern zur Erstellung einer Vernetzungs-FMEA verwendet werden kann. Die Ergebnisse der Vernetzungs-FMEA beider Hersteller werden vom Betreiber in einer Delta-Analyse verglichen und auf zusätzlich zu betrachtende technische Risiken überprüft. Wenn sich in dieser Überprüfung neue Aspekte ergeben, müssen diese ebenfalls im Einzelfall überprüft werden.

Die Randbedingungen, Spezifikations- und Netzwerkanforderungen sowie Ergebnisse der Risikoanalysen können in einem Geräteprofil zusammengefasst werden. Vor einer Vernetzung zweier Geräte zeigt ein Vergleich der Geräteprofile die Machbarkeit einer sicheren Vernetzung. Der Betreiber, welcher die Verbindung etabliert, fertigt nach einem Verbindungs-

checkup ein Vernetzungsprotokoll an und dokumentiert somit die Funktionsfähigkeit der Verbindung, ohne jedoch zulassungstechnisch ein neues Medizinprodukt zu schaffen

OR.NET-Geräteprofil	Beschreibung
Vernetzungsszenario (Funktionalitäten, evtl. Erweiterung der Zweckbestimmung)	Nutzungskontext des Geräts, welche Funktionen werden übernommen, z.B. OP-Mikroskop steuert US-Leistung, Absaugleistung, Spülmenge und Auslösezustand (koaguliere/schneiden) eines HF-Schneidgeräts und zeigt dessen Einstellungswerte an
Technische Spezifikationen	Protokollversion, Datentypen, Wertebereiche, Verweis auf Ergebnisse der FMEA (über die an der Vernetzung beteiligten Bauteile)
User-Interface-Daten	Anforderungen an Eigenschaften der Ein- und Ausgabeelemente sowie Interaktionselemente, Umgebungsbedingungen,...
Netzwerk	Anforderungen an das Netzwerk, z.B. Quality of Service-Anforderungen, Risikosicherung nach IEC 80001, Verfügbarkeit, ... Fehlermöglichkeiten aus VernetzungsfMEA

Tabelle 1: Aufbau eines Geräteprofils (verändert übernommen von A. Janss)

Fehlermöglichkeiten in vernetzten Systemen

Für vernetzte Medizingeräte müssen zusätzlich zu den regulären Risikobetrachtungen Ursachen für Gefährdungen festgestellt, bewertet und mit Gegenmaßnahmen aufgefangen werden, die aus der Vernetzung der Medizingeräte miteinander hervorgehen. Zu diesen gehören zum einen Risiken der Datenübertragung wie eine Schnittstellenüberlastung oder auch eine Laufzeitverzögerung; bei in das Krankenhausnetzwerk integrierten Geräten aber auch auf dieses bezogene Risiken wie Netzwerkausfall oder Infizierung mit/Datenverfälschung durch Malware.

FMEA für Bau-/Zubehörteile

Eine grundlegende Aufzählung von zu betrachtenden Risikofeldern ist in der EN 60001-1:2006 im Kapitel 14.6.1 [9] zu finden. Die Aufzählung adressiert folgende Gebiete Ursachen von Gefährdungen, welche bei einer Vernetzung von Medizingeräten zusätzlich zur den Angaben in EN ISO 14971, Anhang D, betrachtet werden sollten [7] und wurde durch eigene Überlegungen zur dynamischen Vernetzung von Medizingeräten ergänzt:

- Netzwerk/Datenverbund ist nicht in der Lage, die notwendigen Merkmale für das PEMS (Programmierbares elektrisches Medizingerät) zu liefern, damit dieses seine Basissicherheit oder wesentlichen Leistungsmerkmale erzielen kann
- Unerwünschte Rückwirkung (physikalisch und datentechnisch)

- Nicht verfügbare Daten
- Fehlende Datenintegrität
- Falsche Daten
- Falsche zeitliche Datenzuordnung
- Unbeabsichtigte Wechselwirkungen innerhalb und zwischen PESS (Programmierbares elektronisches Subsystem)
- Unbekannte Aspekte oder Qualität der Software Dritter
- Unbekannte Aspekte oder Qualität der PESS Dritter
- Fehlende Datensicherheit, insbesondere Anfälligkeit für Verfälschung, unerwünschte Wechselwirkung mit anderen Programmen und Viren
- Schnittstellenausfall/Schnittstellenüberlastung eines Vernetzungspartners
- Übertragene Werte außerhalb des Wertebereichs
- Schnittstellenverträglichkeit
- Verbindungen (Modifikation der Hardware, Datenformate)
- Inkonsistenz der der Schnittstellen, die zu Datenverlusten bei Übertragung führen können
- Möglichkeit der gleichzeitigen Funktionsausführung an verschiedenen Eingabegeräten

Anforderungen an das Netzwerk/Vernetzungs-FMEA

Aufgrund der zu betrachtenden technischen Risiken bei einer Vernetzung über das Krankenhausnetzwerk muss dieses Netzwerk insgesamt ebenfalls einer Risikobetrachtung unterzogen werden. Zurzeit erhältliche vernetzte Medizingeräte oder bereits am Markt erhältliche integrierte OP-Lösungen beruhen auf proprietären Schnittstellen und agieren in weitestgehend abgeschlossenen Netzwerken. Durch diese geschlossenen Netzwerke werden Risikobetrachtungen für die Vernetzung der Medizingeräte minimiert und vereinfacht. Auf der anderen Seite können nicht in den Verbund einbezogene Medizingeräte allerdings auch nicht ohne weiteres integriert werden.

Die Grundlage für eine Vernetzung von Medizingeräten mittels offener Netzwerke liefert die EN 80001-1 [10]. Diese Norm beschreibt einen Ansatz für das Risikomanagement in medizinischen Netzwerken. Die Empfehlungen der Norm richten sich vor allem an die Betreiber von Krankenhäusern und beschreiben die Rollenverteilungen und Verantwortlichkeiten in der Betreiberorganisation und deren Interaktionen.

Die Norm beschreibt im Weiteren den Ablauf des Risikomanagements für das medizinische IT-Netzwerk. Jede gefundene Fehlermöglichkeit wird analysiert und nach ihrer Eintrittswahrscheinlichkeit und ihren angenommenen Folgen bewertet (Analog FMEA-Vorgehen). Im Anschluss wird festgelegt, ob das Restrisiko tragbar ist und, wenn nicht, wie Gegenmaßnahmen implementiert werden können. Es ist eine Risikodokumentation und ein fortlaufendes Risikomonitoring vorgesehen. Damit schlägt die Norm einen Risikomanagement-Prozess vor, der analog zu dem „konventioneller“ Medizinprodukte aufgebaut ist und setzt diesen auf ein medizinisches Netzwerk um.

Mittels eines durch ein solchen risikobetrachteten Netzwerks können für eine Vernetzung von Medizingeräten Quality of Service-Anforderungen an das Netzwerk gestellt werden.

Diese bestehen in IP-Netzwerken neben allgemeinen Anforderungen wie einer stabilen Kommunikationsverbindung, verlässlichen Zustellung von Nachrichten und einer fehlerlosen Nachrichtenübertragung üblicherweise aus:

- Latenzzeit: Verzögerung der Ende zu Ende Übertragung
- Jitter: Varianz der Latenzzeit vom Mittelwert
- Paketverlustrate: Wahrscheinlichkeit, dass IP-Pakete verloren gehen
- Datenübertragungsrate: Pro Zeiteinheit im Mittel übertragene Datenmenge

Je nach Zeitkritikalität der Kommunikation und des möglichen Schweregrads bei einer Fehlfunktion können so Anforderungen an das Netzwerk, welches üblicherweise in der Verantwortung des Betreibers liegt, gestellt werden. Bei stark belasteten Netzwerken besteht die Möglichkeit, Verbindungen mittels Quality of Service in Prioritätsklassen einzuteilen und so zeitkritische Nachrichten bevorzugt weiterzuleiten. Dieses Vorgehen wird bereits in verschiedenen Bereichen angewandt [11].

Auf Grundlage der in der Norm 60601-1 aufgeführten Ursachen von Gefährdungen und der Möglichkeit, Quality of Service-Anforderungen an ein risikobetrachtetes Netzwerk zu stellen, wurde in diesem Kontext eine erste Zusammenstellung von zu betrachtenden Ursachen von Fehlermöglichkeiten aufgrund des Datenaustauschs betrachtet werden:

- Keine Datenübertragung
 - o Verfügbarkeit des Netzwerks durch geplante/nicht geplante Wartung
 - o Netzwerkkonfiguration falsch (Nachrichten werden an falsches Gerät geroutet)
 - o Netzwerkausfall
 - o Datenpaketverlust
- Verzögerte Datenübertragung
 - o Überlastung des Netzwerks im Regel- oder Spitzenbetrieb
 - o Ungeeignete Datenzuordnung durch Laufzeitverzögerung
- Senden/Empfangen verfälschter Daten
 - o Verfälscht durch Malware/Datenkorruption
 - o Verfälscht durch physikalische Effekte (z.B. Strahlung)
 - o Falsche Datentypen oder falsches Format der Parameter

Literaturverzeichnis

- [1] „Karl Storz OR1,“ [Online]. Available: <https://www.karlstorz.com/cps/rde/xchg/SID-50D8E497-9492B3E9/karlstorz/hs.xsl/10382.htm>. [Zugriff am 07 04 2014].
- [2] „Richard Wolf core nova,“ [Online]. Available: <http://www.richard-wolf.com/integration/integrierter-op/geraetesteuerung.html>. [Zugriff am 07 04 2014].
- [3] „Olympus Endoalpha,“ [Online]. Available: http://www.olympus-owi.de/front_content.php?idcat=14. [Zugriff am 07 04 2014].
- [4] „Stryker i-Suite,“ [Online]. Available: http://www.europe.stryker.com/i-suite/de/index/ms_pag_what-matters/ms_pag_solutions.htm. [Zugriff am 07 04 2014].
- [5] A. Hermeneit, A. Steffen und J. Stockhardt, Der CE- Routenplaner - Medizinprodukte planen, entwickeln, realisieren, Köln: TÜV Media GmbH, 12.2013.
- [6] *DIN EN 60812:2006-11: Analysetechniken für die Funktionsfähigkeit von Systemen - Verfahren für die Fehlzustandsart- und -auswirkungsanalyse (FMEA).*
- [7] *DIN EN ISO 14971:2009-10: Medizinprodukte - Anwendung des Risikomanagements auf Medizinprodukte (ISO 14971:2007, korrigierte Fassung 2007-10-01).*
- [8] o. GmbH, *Kurs Manager/in Regulatory Affairs*, Lübeck, 2013.
- [9] *DIN EN 60601-1: Medizinische elektrische Geräte - Teil 1: Allgemeine Festlegungen für die Sicherheit einschließlich der wesentlichen Leistungsmerkmale (IEC 60601-1:2005).*
- [10] J. Ahlbrandt, J. Dehm, R. Röhrig, C. Wrede und M. Imhoff, „Risikomanagement für medizinische Netzwerke in der Intensiv- und Notfallmedizin: Gemeinsames Positionspapier zur Norm IEC 80001-1,“ DGMBT - Deutsche Gesellschaft für Biomedizintechnik im VDE, Frankfurt am Main, 2012.
- [11] „IT Administrator - Das Magazin für professionelle System. und Netzwerkadministration,“ Heinemann Verlag GmbH, [Online]. Available: http://www.it-administrator.de/lexikon/quality_of_service.html. [Zugriff am 23 04 2014].
- [12] *IEC 80001-1: Anwendung des Risikomanagements für IT-Netzwerke mit Medizinprodukten; Teil 1: Aufgaben, Verantwortlichkeiten und Aktivitäten.*
- [13] M. Hausherr und G. Dominik, „Seminarbericht Design by Contract in Java,“ Fachhochschule Nordwestschweiz, 2006.