Andreas Zangl, BSc

Risikomanagement – Aspekte für eine mobile medizinische Software

MASTER'S THESIS

to achieve the university degree of

Diplom-Ingenieur

Master's degree programme: Biomedical Engineering

submitted to

Graz University of Technology

Supervisor

Assoc.Prof. Dipl.Ing. Dr.techn. Jörg Schröttner

Institute of Health Care Engineering

Graz, January 2019

EIDESSTATTLICHE ERKLÄRUNG

AFFIDAVIT

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

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

_____ _____

Datum / Date Unterschrift / Signature

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

Kurzfassung

Die Anwendung von Software ist heute in der Medizin nicht mehr wegzudenken. Insbesondere spielt Software für mobile Anwendungen eine immer wichtigere Rolle. Hierbei ist zu beachten, dass für Software als Medizinprodukt ein adäquates Risikomanagement im Rahmen der Entwicklung und Marktzulassung unumgänglich ist. Daher war es Ziel dieser Arbeit die wesentlichen Aspekte des Risikomanagements für eine mobile Softwarelösung zu analysieren und zu bewerten.

Im Zuge dieser Ausarbeitung konnte zusammengefasst werden, wie mit geeigneten Methoden (u.a. FMEA, FTA, SWIFT) Risikoanalysen durchgeführt, die dabei identifizierten Risiken bewertet und wie daraufhin mit Risikobeherrschungsmaßnahmen inakzeptable Risiken minimiert werden können. Ebenso wird der Zusammenhang mit weiteren zu beachtenden relevanten Normen erläutert.

Mit den durchgeführten Risikoanalysen konnten 109 Einzelrisiken identifiziert und bewertet werden, wobei 27 Risiken als inakzeptabel eingestuft werden mussten. Für diese inakzeptablen Risiken wurden Risikobeherrschungsmaßnahmen definiert und implementiert, damit diese auf ein akzeptables Niveau gebracht werden konnten.

Durch die in dieser Arbeit durchgeführten Risikoanalysen und die eingeführten Risikobeherrschungsmaßnahmen konnte die betrachtete mobile Software von Seiten des Risikomanagements zur Freigabe vorbereitet werden.

Stichworte

Software, Medizinprodukt, EN ISO 14971, regulatorische Anforderungen, Marktzulassung

Abstract

Nowadays it is impossible to imagine medicine without the use of software. In particular for mobile applications software plays an important role. For software as a medical product, adequate risk management is essential in the context of development and market approval. Therefore, the aim of this thesis was to analyze and evaluate the essential aspects of risk management for a mobile software application.

In this thesis it was possible to summarize how risk analyses could be carried out with suitable methods (e.g. FMEA, FTA, SWIFT), how the identified risks could be evaluated and how unacceptable risks could be minimized with risk control measures. Also the connection to other relevant standards is described.

Through the risk analyses 109 individual risks could be identified and assessed, 27 of which had to be classified as unacceptable. Risk control measures were defined and implemented for these unacceptable risks to improve product safety.

The risk analyses carried out in this thesis and the risk control measures taken form the basis of the risk management procedure for a final release of the mobile software application.

Keywords

Software, medical device, EN ISO 14971, regulatory affairs, market approval

Inhalt

1 Einleitung

Die Digitalisierung in ihren verschiedenen Ausprägungen hat in allen Bereichen unseres Alltags und unseres Berufslebens Einhalt gefunden. Die Informationstechnik ist hier eine Schlüsseltechnologie in der Zeit der Digitalisierung und durch ihre rasant fortschreitende Entwicklung ein Wachstumstreiber für neue Geschäftsmodelle.

In vielen Branchen beginnt der Einzug der Digitalisierung aber erst bzw. erfolgt der Fortschritt aus verschiedenen Gründen nur schleppend. Zu diesen Branchen gehört auch das Gesundheitswesen in Europa. Vielerorts möge der Digitalisierungsgrad im Gesundheitswesen, hier speziell in Krankenanstalten schon hoch sein, im Gesamten betrachtet hinkt er aber der Allgemeinheit hinterher [1]. Der Grund dieses Hinterherhinkens der Digitalisierung im Gesundheitsapparat hat vielfältige Gründe. So müssen oft praxiserprobte Arbeitsweisen oder Prozesse unter Anwendung von digitalen Hilfsmitteln ‚umgebaut' werden. Oft scheitert die Implementierung digitaler Arbeitsweisen an der dafür benötigten IT-Infrastruktur, manchmal schlicht an der Finanzierung oder durch unterschiedliche Interessenslagen der involvierten Entscheider. Die Komplexität vieler digitaler Anwendungen im Gesundheitswesen trägt bei der Anwenderakzeptanz eine wichtige Rolle – Erfahrungen zeigen, dass komplexe Systeme selten und ungern angewandt werden, und damit rasch implementiert werden. [1] Weitere Gründe für die langsame Entwicklung im Gesundheitswesen sind die hohen Sicherheitsanforderungen, stark differenzierte, in der Praxis seit langem erprobte Abläufe, sowie die große Anzahl an unterschiedlichen Geräten und Softwarelösungen. Auch die versuchten nationalen Anläufe (Elektronische Fieberkurve, e-Health Digitalisierungsinitiative, etc.) mangeln an deren Umsetzung bzw. sind gerade in Pilotphasen.

Dabei ist die Digitalisierung von Prozessen oder Arbeitsabläufen gerade im Gesundheitswesen von zentraler Bedeutung.

Um einen Beitrag zum Fortschritt der Digitalisierung im Gesundheitswesen zu leisten, bzw. um Hindernisse, die dazu führen, dass der Fortschritt langsam verläuft zu überwinden, wurde das System ‚*ilvi*' entwickelt. Das System ‚*ilvi*' dient als Schnittstelle zwischen Pflegepersonal und Krankenhausinformationssystem (KIS) bzw. einer schon vorhandenen digitalen Fieberkurve oder digitalen Patientenakte.

Es soll den Weg der Gesundheitsparameter oder Vitalwerte, die regelmäßig durch das Pflegepersonal gemessen oder erfasst werden, in das Zielsystem (z.B.: KIS) erleichtern. Ursprünglich wurden diese Daten in die klassische Fieberkurve handschriftlich eingetragen. Diese Fieberkurve wurde anschließend an das Bettende des betreffenden Patienten gehängt. Eine Folge der fortschreitenden Digitalisierung ist der Datenschutz. So wurde es (verständlicherweise) verboten, die ‚klassische' Fieberkurve mit allen patientenbezogenen Daten an das öffentlich einsehbare Bettende zu hängen. Da aber bei Inkrafttreten der Datenschutzrelevanten Gesetzgebung in den meisten Krankenanstalten keine digitale Patientenakte vorhanden war, ging man dazu über, die Patientenakten bzw. Fieberkurven im nichtöffentlichen Teilen der Krankenanstalt zu lagern. Folglich müssen das Personal die erfassten Daten ‚zwischenspeichern' – oft auf einer trivialen Haftnotiz – und die Werte anschließend in die Fieberkurve – noch immer handschriftlich –

nachtragen. Diese Vorgehensweise impliziert eine hohe Fehleranfälligkeit und einen hohen Arbeitsaufwand für die Bediensteten.

Unter der Annahme, dass eine digitale Patientenakte in einer Krankenanstalt implementiert ist bzw. wurde muss diese ebenfalls mit Daten befüllt werden. Vielfach sind Medizinprodukte am Markt verfügbar, die ihre Messwerte, Messergebnisse via Vernetzung in der IT-Infrastruktur der Patientenakte zur Verfügung stellen. Andererseits werden aber eine große Anzahl an medizinischen Messgeräten, wie z.B.: Messgeräte zur Blutdruckmessung, Sauerstoffmessung, Blutzuckermessung, etc. eingesetzt, die keine Anbindung an das IT-Netz der Krankenanstalt ermöglichen. In Diesem Fall muss das Pflegepersonal die Messergebnisse wiederum dezidiert nach der Messung manuell (via Zugangsterminal zur Patientenakte) eintragen. Dies kann im Idealfall mittels eines mobilen Terminals in Form eines Laptops, PC, oder Tablet-PC erfolgen – wiederum mit der Fehlerquelle bei der manuellen Eingabe.

Das System *ilvi* soll diese Arbeitsweisen neu definieren und den Arbeitsaufwand mit den darin liegenden Fehlerquellen minimieren.

1.1 Mobiles System zur Erfassung von Vital- und Gesundheitswerten und Weiterleitung an ein KIS

Das System *ilvi* (Abbildung 1) des Herstellers Berger Medizintechnik GmbH ist ein Softwaresystem zur einfachen, gebrauchstauglichen Erfassung von verschiedenen Gesundheits- und Vitalwerten direkt am Krankenbett des Patienten und zur anschließenden Weiterleitung der Daten an ein KIS oder an eine digitale Patientenakte. Das System besteht aus einer Hardware mit darauf laufender Software. Als Hardware wird ein Handheld-Computer genutzt, der eine mobile, netzunabhängige Anwendung ermöglicht. Das System ermöglicht eine Kommunikation mit vorhandenen Medizinprodukten/Messgeräten und dem KIS bzw. der digitalen Patientenakte. So können die erfassten Daten ‚in Echtzeit', also ohne weitere Zwischenschritte direkt an das Zielsystem übertragen werden. Um dies zu gewährleisten muss ein Krankenhausinformationssystem oder eine digitale Patientenakte in der Krankenanstalt implementiert sein. Ebenfalls muss ein drahtloses Netzwerk vorhanden sein, über welches die Kommunikation mit dem KIS von statten geht. In der ersten Version des Systems werden verschiede Daten erfasst werden können. Diese Daten können einerseits direkt von einem Messgerät stammen (Blutdruck, Sauerstoffsättigung, Blutzucker, Temperatur) , andererseits über ein Gespräch mit dem Patienten generiert werden (Schmerzempfinden). Der Vorteil in der Verwendung dieses Systems besteht in der Reduktion der Arbeitsschritte, bis die geforderten Daten oder Werte im KIS sind, in der Vermeidung bzw. Minimierung von Fehlerquellen resultierend aus der manuellen Datenübertragung bzw. Dateneintragung und der dadurch gesteigerten Dokumentationsqualität.

Am Beginn der Anwendung muss sich der Anwender am Gerät anmelden. Dies kann entweder mit einer digitalen Authentifizierung via Barcode oder NFC-Chip geschehen oder der Anwender meldet sich mittels Eingabe von Benutzernamen und Passwort an. Der nächste Schritt ist die Identifikation eines Patienten, welche über einen entsprechenden Barcode (z.B. vom Patientenarmband) erfolgt. Sind diese zwei Schritte erledigt, kann die Erfassung von Daten mit *ilvi* beginnen. Es besteht die Möglichkeit, Vitalparameter des Patienten über zwei Wege in *ilvi* zu übertragen. Der erste Weg ist die manuelle Eingabe der Daten/Parameter über eine Tastatur am Touchscreen des Handheld-Computer. Dazu stellt der ‚Hauptbildschirm' jeden möglichen Parameter der erfasst werden kann, als ‚Kachel' dar. Ein ‚Eingabeassistent' sorgt dafür, dass mögliche Falscheingaben verhindert werden. So erlaubt dieser nur die Eingabe von Werten, die plausibel erscheinen (z.B. ist es nicht möglich, eine Körpertemperatur von über 50°C einzugeben). Dies ist auch schon ein Beispiel für eine Risikobeherrschungsmaßnahme, wie sie in dieser Arbeit beschrieben werden. Ein weiterer Weg, um Daten auf *ilvi* zu bekommen ist eine automatische Datenübertragung von einem Messgerät via Bluetooth. Voraussetzung dafür ist das Vorhandensein eines Bluetooth-fähigen Messgerätes (z.B. Blutdruckmessgerät). Bei Parametern, die nicht durch ein Gerät ermittelt werden, ist dieser Weg nicht vorgesehen (z.B. Schmerzempfinden). Eine weitere Funktion von *ilvi* ist die Aufnahme von Fotografien zu Dokumentationszwecken. Dazu verwendet man die in der Hardware vorhandene Kamera. Eine Bearbeitung der Fotos ist nicht vorgesehen. Nachdem alle notwendigen Parameter erfasst wurden (es müssen nicht alle verfügbaren Werte erfasst werden), können diese nach einer Bestätigung an das KIS übertragen werden. Nutzt der selbe Anwender das Gerät weiter, muss er lediglich einen ‚neuen' Patienten identifizieren um die Anwendung fortsetzen zu können.

Abbildung 1: ilvi

1.2 Eigenschaften und Besonderheiten dieses Systems

Im Vergleich mit ‚klassischen' Medizinprodukten, wie z.B. ein Skalpell oder auch ein EKG-Gerät, unterscheidet sich *ilvi* dadurch, dass es sich um Software handelt, die aber im regulatorischen Umfeld als Medizinprodukt behandelt werden muss. Mehr dazu wird im Folgekapitel beschrieben. Ebenfalls ist es eine Besonderheit, dass *ilvi* nicht auf einem PC betrieben wird, sondern auf einem Handheld-Computer, der sich u.a. durch seine Schnittstellen, Bedienung und auch im Betriebssystem davon unterscheidet. Auch die Funktion an sich ist besonders, da sie keine direkte medizinische Diagnose liefert, wie es manch andere Software als Medizinprodukt macht. So ist *ilvi* eher als eine weitere Sicherheitsstufe in der Pflegedokumentation zu sehen, wie es ein klassisches Diagnosegerät es sein würde. Wie schon beschrieben, sind die Schnittstellen des Systems eine Eigenschaft, die besonders ist. So ist es mit *ilvi* möglich, Parameter, welche durch andere (externe) Mess- bzw. Medizingeräte gemessen werden, zu erfassen. Dabei beschränkt sich die Vielfalt dieser Daten aber nicht auf die Messgerättypen, sondern auf die dazu verwendeten Schnittstellen. Diese Schnittstellen sind für *ilvi* die manuelle Eingabe durch den Anwender und die automatische Übertragung durch Bluetooth. Durch die Einschränkung bzw. eindeutige Definition der verwendeten Übertragungsprotokolle wird eine gewisse Unabhängigkeit der Messgeräte erreicht. Dabei ist natürlich (im Zuge des Risikomanagements) zu achten, dass diese Messgeräte durch *ilvi* nicht negativ in deren Grundfunktion bzw. Leistung beeinflusst werden. Beachtenswert ist auch die für manchen Benutzer ungewohnte Bedienung via Touchscreen, und nicht via Tastatur und Maus, wie man es von einem PC gewohnt ist.

Durch diese Besonderheiten ergeben sich Szenarien, im Entwicklungs- und Zulassungsumfeld, die besondere Beachtung erfordern. Diese Besonderheiten werden unter anderem in dieser Arbeit betrachtet und deren Ergebnisse dargestellt.

2 Software als Medizinprodukt

Um die regulatorischen Rahmenbedingungen vor Beginn der Entwicklung festlegen zu können, muss die Frage geklärt werden, ob es sich bei dem zu entwickelnden Produkt um ein Medizinprodukt handelt, oder möglicherweise andere Standards und Richtlinien (z.B. Maschinenrichtlinie 2006/42/EG [2]) eingehalten oder angewandt werden müssen. Anhand der Zweckbestimmung des Systems, muss geklärt werden, ob es sich bei dem System um ein Medizinprodukt nach Definition der Medizinproduktrichtlinie 92/43/EWG (MDD) [3] handelt, oder nicht. Diese Entscheidung ist ausschlaggebend für die regulatorischen Rahmenbedingungen unter welchen das Produkt entworfen, produziert und vermarktet wird. Es ist naheliegend, dass ein Produkt bzw. eine Software im Umfeld des Gesundheitswesens ein Medizinprodukt sein könnte und somit die Anforderungen der Medizinproduktrichtlinie erfüllen muss.

Die MDD bildet europaweit den Rahmen der regulatorischen Anforderungen für Medizinprodukte. Für in-vitro Diagnostika (IVD) und implantierbare aktive Medizinprodukte existieren noch weitere Richtlinien – 98/79/EG für IVD [4] und 90/385/EWG für implantierbare aktive Medizinprodukte [5]. Für eine Software als

Medizinprodukt ist die MDD anzuwenden. Es gilt nun zu klären, ob eine bzw. welche der genannten europäischen Richtlinien zur Anwendung kommt.

Dazu muss man die Definition eines Medizinproduktes gemäß der MDD kennen:

‚Ein Medizinprodukt sind alle einzeln oder miteinander verbunden verwendeten Instrumente, Apparate, Vorrichtungen, Software, Stoffe oder andere Gegenstände, einschließlich der von Hersteller speziell zur Anwendung für diagnostische und/oder therapeutische Zwecke bestimmten und für ein einwandfreies Funktionieren des Medizinproduktes eingesetzten Software, die vom Hersteller zur Anwendung für Menschen für folgende Zwecke bestimmt sind:

- *Erkennung, Verhütung, Überwachung, Behandlung oder Linderung von Krankheiten,*
- *Erkennung, Überwachung, Behandlung, Linderung oder Kompensierung von Verletzungen oder Behinderungen,*
- *Untersuchung, Ersatz oder Veränderung des anatomischen Aufbaus oder eines physiologischen Vorgangs,*
- *Empfängnisregelung*

und deren bestimmungsgemäße Hauptwirkung im oder am menschlichen Körper weder durch pharmakologische oder immunologische Mittel noch metabolisch erreicht wird, deren Wirkungseise aber durch solche Mittel unterstützt werden kann.‘ Zitiert aus [3]

Der allererste Schritt muss also die Festlegung der Zweckbestimmung des Systems sein. Anhand dieser Zweckbestimmung und des damit in Zusammenhang liegenden bestimmungsgemäßen Gebrauchs lässt sich klären, ob das betreffende Produkt oder System unter die oben genannte Definition fällt. Bei der Erstellung der Zweckbestimmung muss beachtet werden, dass über die Definition der Funktionsweise des Produkts auch der bestimmungsgemäße Gebrauch beschrieben wird. Daher ist der Mindestinhalt einer Zweckbestimmung die Beschreibung, wie das Produkt funktioniert, bei einem möglichen Medizinprodukt, die medizinische Wirkung zur Therapie, Diagnose, Überwachung von Vitalparametern, etc. (ein Vergleich mit der Definition eines Medizinproduktes nach MDD ist hier sinnvoll). Zusätzlich sollte die vorgesehene Patientenpopulation, deren Alter und Gesundheitszustand, an welcher das Produkt zur Anwendung kommt beschrieben werden. Ebenfalls muss die Zweckbestimmung, die Anwendergruppe und das Umfeld der Anwendung spezifizieren.

Um diese Entscheidung, welche Richtlinie für das System *ilvi* anwendbar ist zu fällen, zieht man dessen Zweckbestimmung heran, welche wie folgt lautet:

2.1 Zweckbestimmung des Systems ‚*ilvi*'

Das System ilvi dient als Schnittstelle zur Datenerfassung, Anzeige der erfassten Daten und Weiterleitung der Daten zur Archivierung (z.B. an ein Krankenhausinformationssystem). Das System ermöglicht die Erfassung von Gesundheits- und Vitalwerten von Patienten in Anstalten des Gesundheitswesens. Die erfassten Vitalwerte können nachfolgend zur Unterstützung der Therapieplanung herangezogen werden. Das System ilvi analysiert die erfassten Vitalwerte und liefert Informationen zur Unterstützung der Diagnose und Therapie. Der Einsatz des Systems ilvi erfolgt an Patienten, unabhängig deren Alter und Geschlechts.

Folgende Vitalwerte können erfasst werden:

- Sauerstoffsättigung
- Temperatur
- Blutzucker
- Blutdruck
- Puls

Das System ilvi analysiert die erfassten Werte und liefert Informationen zur Unterstützung der Diagnose und Therapie. Zur leichteren Erkennung dieser Informationen werden die Daten entsprechend aufbereitet und dargestellt. Folgende Vitalwerte werden auf Grenzwerte geprüft. Die dargestellten Grenzwerte sind Default-Werte und können vom Anwender spezifisch bestimmt werden:

- Sauerstoffsättigung:
  - < 94% = "Achtung niedrige Sauerstoffsättigung"
- Temperatur:
  - < 36,3°C = "Niedrige Körpertemperatur"
  - > 37,4°C = "Erhöhte Körpertemperatur"
- Blutzucker
  - < 70 mg/dl
  - > 190 mg/dl
- Blutdruck:
  - Systolisch< 100 mmHg oder diastolisch < 60 mmHg = "Achtung niedriger Blutdruck"
  - Systolisch > 140 mmHg oder diastolsch > 100 mmHg = "Achtung erhöhter Blutdruck"
- Puls
  - < 60 bpm = "Achtung niedriger Puls"
  - > 150 bpm = "Achtung erhöhter Puls"

Zusätzlich zu den Vitalwerten ermöglicht das System die Erfassung von Gesundheitswerten zwecks Dokumentation. Ebenfalls möglich ist die Aufnahme von Bildern für die Fotodokumentation.

Der Betrieb des Systems ilvi erfolgt auf einem mobilen Handheld-Gerät und ist nur für den Gebrauch in geschlossenen Räumen vorgesehen. Dabei bilden die ortsüblichen Eigenschaften der Anstalten des Gesundheitswesens die arbeitstechnischen Rahmenbedingungen des Systems. Die Installation der Software ilvi erfolgt ausschließlich durch den Hersteller oder die von ihm autorisierte Personen.

ilvi fungiert auch als User-Schnittstelle mit folgenden grundlegenden Funktionalitäten:

- Authentifizierung des Benutzers
- Eingabe von Daten per Touchscreen
- Anzeige der erfassten Daten
- Erfassung von Daten über Eingangsschnittstelle
- Weiterleitung von Daten über Ausgangsschnittstelle
- Fokus auf einer einfachen und leicht verständlichen Bedienung
- Große Bedienelemente
- Grafische und farbliche Darstellung
- Verwendung eines hohen Kontrastes
- Übersichtliches Menü in Kachelform
- Eingabeassistent zur leichteren und fehlerfreien Eingabe

Der Benutzer wird durch folgende Punkte auf den richtigen Gebrauch hingewiesen:

- Einschulung des Benutzers vor erstmaligem Gebrauch
- Anzeigen der durchzuführenden Schritte am Screen während Betrieb
- Gebrauchsanweisung

Bei Versagen des Systems ilvi müssen die Daten vom Benutzer manuell abgelegt werden.

Charakterisierung der Anwender:

Die vorgesehenen Anwender sind Ärzte und Pflegepersonal im Rahmen der Patientenbetreuung.

Folgende Eigenschaften müssen die vorgesehenen Anwender erfüllen:

- Unabhängig von Alter und Geschlecht
- Die körperliche und sprachliche Eignung zur Bedienung des Systems Q-PDA muss gegeben sein
- Ausbildung mindestens auf Stand eines Pflegehelfers/Pflegehelferin
- Keine Erfahrung in Bezug auf das System ilvi notwendig

Charakterisierung der Gebrauchsumgebung

Das System Q-PDA ist nur für den Gebrauch in geschlossenen Räumen vorgesehen. Dabei bilden die ortsüblichen Eigenschaften der Anstalten des Gesundheitswesens die arbeitstechnischen Rahmenbedingungen des Systems.

Der Betrieb des Systems Q-PDA erfolgt auf einem mobilen Handheld-Gerät mit dem Betriebssystem Android.

Durch diese Zweckbestimmung wird es möglich, das zu entwickelnde System einer Richtlinie zuzuordnen. Anhand der Festlegungen der Zweckbestimmung für ilvi ist es naheliegend, dass die MDD zur Anwendung kommen wird, daher wird in Folge auch diese Richtlinie näher betrachtet.

Anzumerken ist, dass bei gewissen Produkten, vor allem Software im Bereich der Datenverarbeitung und –erfassung, die Frage ob ein Medizinprodukt vorliegt oder nicht, von der Beschreibung in der Zweckbestimmung abhängt. Diese Beschreibung darf der Hersteller wählen. Dient eine Software beispielsweise zur Erfassung von

Vitalparametern, kann der Hersteller festlegen, dass diese Erfassung lediglich der Dokumentation dient; in diesem Fall wäre die Software kein Medizinprodukt.

Beschreibt der Hersteller jedoch, dass die Werte zur Therapie oder Diagnose herangezogen werden können, wäre diese Software sehr wohl ein Medizinprodukt – bei selber Funktion [6].

Einen Leitfaden zur Umsetzung der MDD-Anforderungen stellen die MEDDEV-Dokumente dar. MEDDEV (MEDical DEVices) Dokumente sind unterstützende Dokumente, welche die Anwendung der Richtlinie 93/42/EWG (MDD –Medical Device Directive)[3] und den harmonisierten Normen erleichtern sollen. Diese Dokumente werden von Expertengruppen aus dem Umfeld der EU-Kommission erstellt, sind aber nicht verbindlich [7]. Um nun die Frage beantworten zu können, ob das Produkt bzw. die Software unter die Definition eines Medizinproduktes nach MDD 93/42/EWG fällt, kann man das MEDDEV Dokument 2.1/6 heranziehen, welches unter anderem die Fragestellung speziell für Software behandelt, wann eine Software ein Medizinprodukt ist, und wann nicht [8]. Dazu beinhaltet das Dokument einen Entscheidungsbaum, anhand dessen man auf Basis der Zweckbestimmung zur Beantwortung der oben genannten Frage kommt. Dieser Entscheidungsbaum ist in Abbildung 2 dargestellt. Zusätzlich wurden in diesem Entscheidungsbaum die Antworten auf die betreffenden Fragen für die Software von *ilvi* beantwortet.

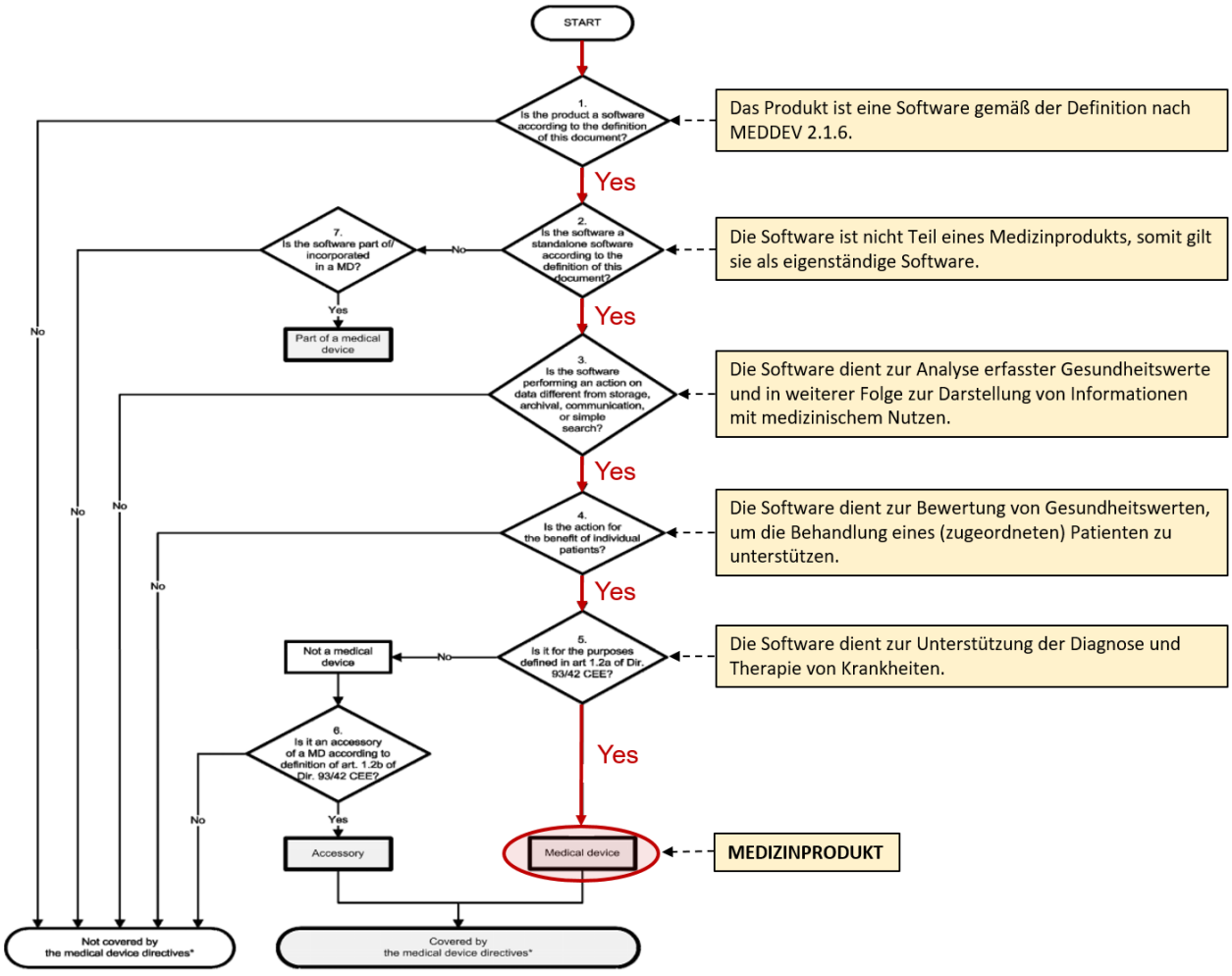


Abbildung 2: Entscheidungsbaum aus MEDDEV 2.1/6 mit Beantwortung der Fragen für ilvi [8]

Schritt 1: Fällt die zu behandelnde Software unter die Definition von Software gemäß des Dokumentes MEDDEV 2.1/6? Im Falle von *ilvi*: Ja, es ist ein Set aus Befehlen, die einen Input in einen Output eines Systems führen.

Schritt 2: Ist die Software Teil eines anderen Medizinproduktes? Im Falle von *ilvi*: Nein, die Software funktioniert eigenständig (abgesehen von der zu verwendenden Hardware) und ist somit eine Stand-alone Software.

Schritt 3: Dient die Software zur weiteren Verarbeitung von Daten, abgesehen von Archivierung, Speicherung, einfacher Suche oder Kommunikation? Im Falle von *ilvi*: Ja, die erfassten Daten werden auf Unter- oder Überschreitung von Grenzwerten untersucht und dessen Ergebnis dargestellt (siehe Zweckbestimmung von *ilvi*).

Schritt 4: Dient die Verarbeitung der Daten einem bestimmten Patienten? Im Falle von *ilvi*: Ja, das Ergebnis wird einem eindeutig identifizierten Patienten zugeordnet.

Schritt 5: Fällt die Funktion unter die Definition der MDD? Im Falle von *ilvi*: Ja, die Daten dienen der Unterstützung der Therapie und der Diagnose.

Anhand dieses Entscheidungsbaumes steht nun fest, dass das Produkt *ilvi* eine Software als Medizinprodukt darstellt, und die MDD 93/42/EWG zur Anwendung gebracht werden muss. Dabei ist das ‚Produkt' ein System aus der Stand-alone Software und der Hardware, auf der die Software installiert wird.

Ziel der MDD ist es, sichere Produkte in Bezug auf Patienten, Anwender und der Umwelt zu schaffen. Dazu fordert die MDD die Einhaltung der ‚grundlegenden Anforderungen', welche in Anhang I der MDD beschrieben werden. Diese werden dabei in ‚Allgemeine Anforderungen' und ‚Anforderungen an die Auslegung und Konstruktion' unterteilt. Die allgemeinen Anforderungen müssen von jedem Medizinprodukt erfüllt werden, die speziellen Anforderungen müssen erfüllt werden, wenn sie zutreffen.

Um diese grundlegenden Anforderungen zu erfüllen, muss das Medizinprodukt unter anderem nach dem ‚Stand der Technik' entwickelt und produziert werden. Diesen ‚Stand der Technik' repräsentieren die mit der MDD harmonisierten Normen. In Bezug zu Software als Medizinprodukt legen die grundlegenden Anforderungen vor allem Augenmerk auf folgende Aspekte:

- Qualitätsanforderungen
- Risikomanagement
- Software-Lebenszyklus
- Gebrauchstauglichkeit

Wie schon erwähnt, stellen die harmonisierten Normen den Stand der Technik dar, welcher eingehalten und nachvollziehbar dokumentiert werden muss. Für die genannten Aspekte der MDD sind dies folgende Normen:

- EN ISO 13485 für das Qualitätsmanagement bei Medizinprodukten [9]
- EN ISO 14971 für das Risikomanagement [10]
- EN 62304 betreffend den Software-Lebenszyklus [11]
- EN 62366 für die Gebrauchstauglichkeit von Medizinprodukten [12]

Wird zur Software auch eine Hardware benötigt oder entwickelt, so muss darüber hinaus auch die Normenfamilie EN60601 [13] angewandt bzw. beachtet werden.

Diese Normen stellen somit die Basis zur Erfüllung der grundlegenden Anforderungen der MDD dar. Die Normen verweisen dabei auch auf sich gegenseitig, so empfiehlt die EN ISO 13485 die Durchführung eines Risikomanagements nach EN ISO 14971. Ebenso verweist die EN 62304 auf ein Risikomanagement gemäß EN ISO 14971 sowie auf ein Qualitätsmanagementsystem nach EN ISO 13485. Auch die EN 62366 fordert ein Risikomanagement nach EN ISO 14971. Eine grafische Darstellung der gegenseitigen Referenzen dieser Normen untereinander ist in Abbildung 3 dargestellt.

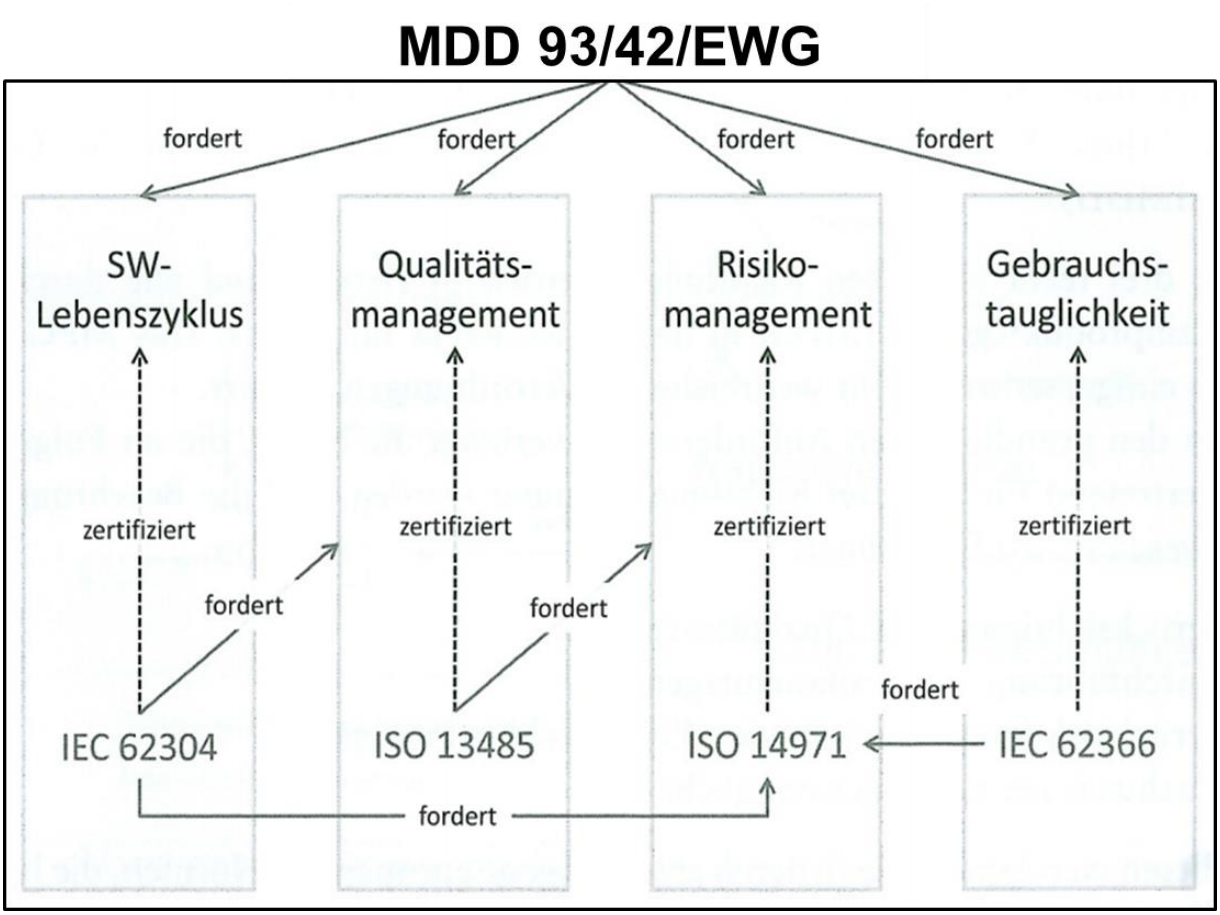


Abbildung 3: Übersicht der anzuwendenden Normen für Software als Medizinprodukt nach [16]

Die Regulatorischen Rahmenbedingungen stehen nun also fest. Um ein Medizinprodukt vermarkten zu dürfen bzw. eine Markteinführung durchführen zu können, muss das Medizinprodukt CE-gekennzeichnet sein. Um diese CE-Kennzeichnung am Medizinprodukt anbringen zu dürfen, muss der Hersteller einen Nachweis erbringen, dass die grundlegenden Anforderungen der MDD erfüllt sind. Diesen Nachweis erbringt der Hersteller mit einem geeigneten Konformitätsbewertungsverfahren. Gemäß der MDD gibt es verschiedene Konformitätsbewertungsverfahren, abhängig von der Risikoklasse des entsprechenden Produkts. Der nächste Schritt im Produktlebenslauf ist nun also die Klassifizierung – die Zuordnung des Produkts zu einer Risikoklasse.

2.2 Klassifizierung

Das Medizinprodukt bzw. die Software als Medizinprodukt muss demnach einer Risikoklasse zugeordnet werden, damit sich der Hersteller für ein geeignetes Konformitätsbewertungsverfahren entscheiden kann.

Die MDD sieht folgende Risikolassen für Medizinprodukte vor, welche im Anhang IX der MDD beschrieben sind: [3]

- Klasse I mit den Sonderformen für sterile Produkte und Produkte mit Messfunktion Is und Im
- Klasse IIa
- Klasse IIb
- Klasse III

Aufsteigend mit den Klassen steigt auch das methodische Risiko, der Invasivitätsgrad und die Anwendungsdauer.

Der Anhang IX der MDD beschreibt auch Regeln, anhand derer man das entsprechende Produkt klassifizieren kann bzw. muss. Dabei nutzt man wieder die Zweckbestimmung des Produktes um die entsprechenden Regeln anzuwenden. Es ist dabei die Aufgabe des Herstellers die Klassifizierung durchzuführen. Um diese Regeln auf Software anzuwenden, muss klargestellt werden, dass alleinstehende (stand-alone) Software als ‚aktives Medizinprodukt' gilt [3]. Wird Software als Zubehör zu einem Medizinprodukt (Hardware) in Verkehr gebracht, so ist die Risikoklasse des 'Hauptprodukts' jene der Software. Beispielsweise wäre hier Software zur Steuerung eines Röntgenapparats zu nennen. Im Falle der Software *ilvi* handelt es sich um eine Stand-alone Software. Unterstützend zur Klassifizierung kann hier das MEDDEV Dokument 2.4/1 in der aktuellen Revision 9 herangezogen werden [14]. Unter anderem werden darin die 18 Klassifizierungsregeln der MDD, Anhang IX in Entscheidungsbäumen dargestellt, welche die Anwendung der Regeln erleichtern kann.

Die Regeln, welche aktive Medizinprodukte klassifizieren, sind speziell die Regeln 9 bis 12. Regeln 1 bis 8 dienen der Klassifizierung von invasiven und nicht-invasiven Produkten, Regel 13 bis 18 behandelt besondere Produktkategorien. In Abbildung 4 ist der Entscheidungsbaum der zusätzlichen Regeln für aktive Medizinprodukte dargestellt.

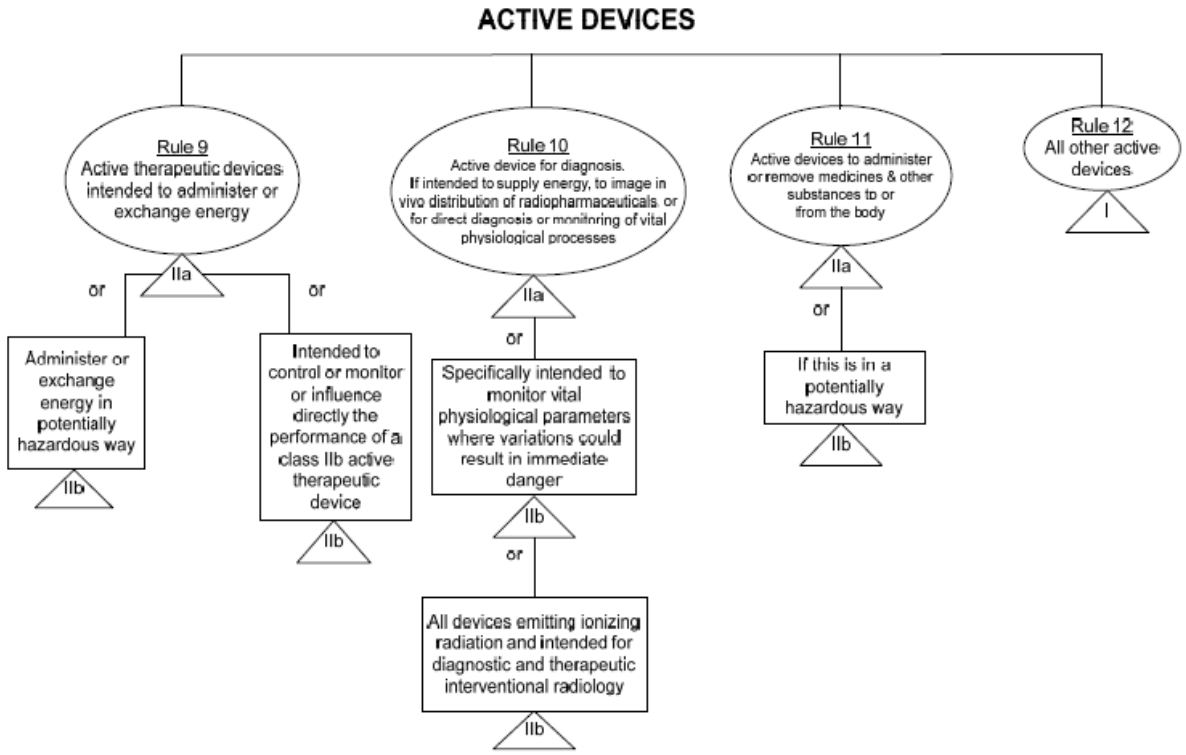


Abbildung 4: Klassifizierungsregeln für aktive Medizinprodukte aus [14]

Regel 9 besagt: „Alle aktiven therapeutischen Produkte, die zu Abgabe oder Austausch von Energie bestimmt sind, gehören zur Klasse IIa, es sei denn, die Abgabe oder der Austausch von Energie an den bzw. mit dem menschlichen Körper kann unter Berücksichtigung der Art, der Dichte und des Körperteils, an dem die Energie angewandt wird, aufgrund der Merkmale des Produktes eine potentielle Gefährdung darstellen; in diesem Fall sin sie (die Produkte) der Klasse IIb zugeordnet.“ [3] Auf Software trifft diese Regel normalerweise nicht zu, da Software üblicherweise keine Energie abgibt oder austauscht.

Regel 10 besagt: „Alle aktiven diagnostischen Produkte gehören zur Klasse IIa, wenn sie dazu bestimmt sind, Energie abzugeben, die vom menschlichen Körperabsorbiert wird – mit Ausnahme von Produkte, deren Funktion es ist, den Körper des Patienten im sichtbaren Spektralbereich auszuleuchten;

wenn wie zur In-vivo Darstellung der Verteilung von Radiopharmaka bestimmt sind;

wenn sie dazu bestimmt sind, eine direkte Diagnose oder Kontrolle von vitalen Körperfunktionen zu ermöglichen, es sei denn, sie sind speziell für die Kontrolle von vitalen physiologischen Parametern bestimmt, bei denen die Art der Änderung zu einer unmittelbaren Gefahr für den Patienten führen könnte, z.B.: Änderung der Herzfunktion, der Atmung oder Aktivität des zentralen Nervensystems; in diesem Fall werden sie der Klasse IIb zugeordnet.“[3]

Diese Regel ist für die Software *ilvi* anwendbar, besonders in Hinblick auf direkte Diagnose oder Kontrolle von Vitalparametern. Hierbei gibt das MEDDEV-Dokument 2.4/1 Hilfestellung. Eine direkte Diagnose erfolgt anhand der Messung von Vitalparametern.

Wird diese Messung kontinuierlich durchgeführt, wird das Produkt der Klasse IIb zugeordnet, erfolgt die Messung (und nachfolgende Anzeige) der Vitalparameter sporadisch bzw. nicht-kontinuierlich, wird das Produkt der Klasse IIa zugeordnet. Da ‚*ilvi*' weder kontinuierlich noch sporadisch selbst Vitalparameter misst und anzeigt, kann diese Regel nicht angewandt werden. Entsprechend der Zweckbestimmung misst *ilvi* keine Vitalparameter, sondern zeigt lediglich Parameter von anderen Messgeräten an und überträgt diese an ein KIS.

Regel 11 besagt: „Alle aktiven Produkte, die dazu bestimmt sind, Arzneimittel, Körperflüssigkeiten oder andere Stoffe an den Körper abzugeben und/oder aus dem Körper zu entfernen, werden der Klasse IIa zugeordnet, es sei denn, dass die Vorgehensweise unter Berücksichtigung der Art der betreffenden Stoffe, des betreffenden Körperteils und der Art der Anwendung eine potentielle Gefährdung darstellt; in diesem Fall werden sie der Klasse IIb zugeordnet." [3]

Auch diese Regel ist mit Software, speziell ‚*ilvi*' nicht anzuwenden.

Somit muss die Regel 12 zur Klassifizierung angewandt werden, welche lautet:

„Alle anderen Produkte sind der Klasse I zugeordnet." [3]

Der Entscheidungsbaum für aktive Medizinprodukte mit den Entscheidungen für die Software *ilvi* ist in Abbildung 5 dargestellt. Dabei kommt es für *ilvi* zu einer Zuordnung der Klasse I, ausschlaggebend ist die Regel 12.

Grund dafür ist, dass *ilvi* keine ‚direkte' Diagnose ermöglicht, sondern die Diagnose- oder Therapieentscheidung unterstützen kann (vergleiche Zweckbestimmung von *ilvi*).

Auf Basis der Risikoklasse des Produkts kann der Hersteller nun ein geeignetes Verfahren wählen, um die Konformität (Erfüllung der grundlegenden Anforderungen der MDD) nachweisen zu können – die verschiedenen Konformitätsbewertungsverfahren.

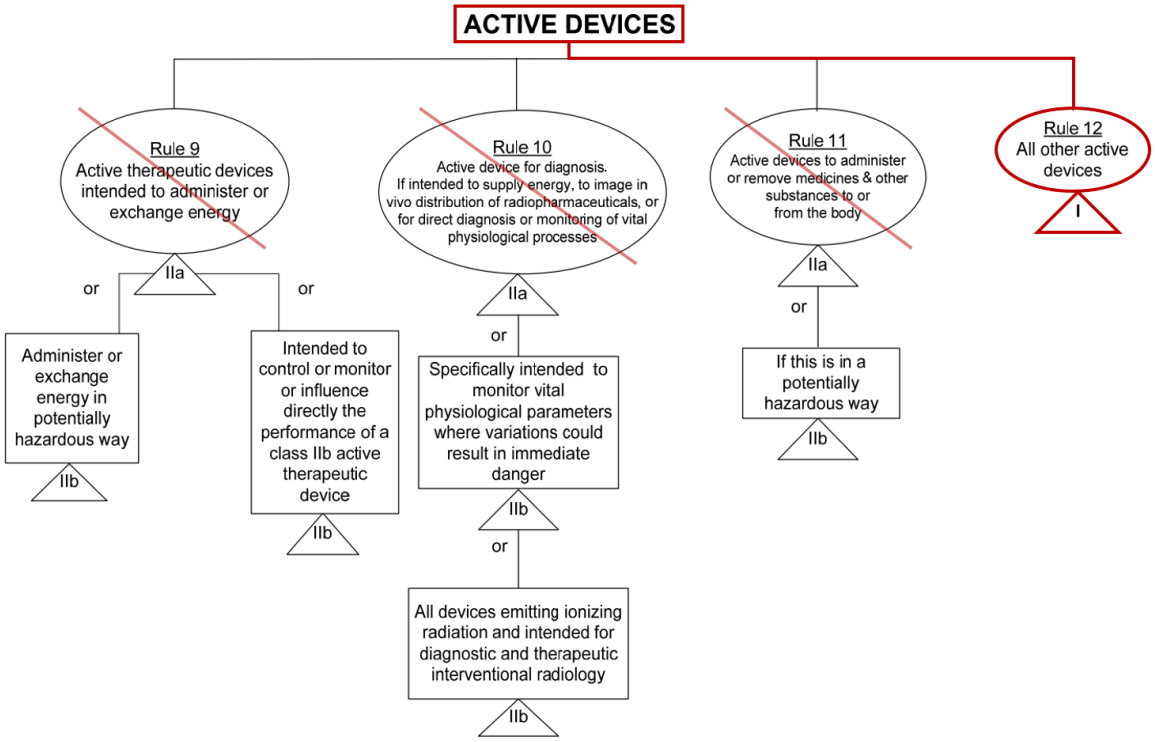


Abbildung 5: Klassifizierungsregeln für aktive Medizinprodukte aus [14] mit Entscheidungen für ‚ilvi'.

2.3 Konformitätsbewertung

Ziel jedes Herstellers ist es, oder sollte es sein, sein Produkt zu vermarkten. Für Medizinprodukte ist dafür eine CE-Kennzeichnung Voraussetzung. Um ein CE-Kennzeichen an einem Medizinprodukt anbringen zu dürfen, muss durch den Hersteller nachgewiesen werden können, dass die Anforderungen der MDD erfüllt werden (wie schon beschrieben) [3]. Dies gelingt mit einem entsprechenden Konformitätsbewertungsverfahren. Die MDD sieht dafür verschiedenen Verfahren vor, wobei der Hersteller wählen kann, welches Verfahren für sein Produkt angewandt wird. Limitiert wird diese Entscheidung von der vorab bestimmen Risikoklasse des Produktes. Eine Darstellung der zur Verfügung stehenden Verfahren bzw. Konformitätsmodulen in Abhängigkeit der Risikoklasse ist in Abbildung 6 dargestellt. Die MDD unterscheidet dabei Verfahrensmodule für die Entwicklung bzw. den Entwurf eines Produkts und Verfahrensmodule für die Produktion dessen. Diese verschiedenen Verfahren werden in den Anhängen II bis VIII der MDD beschrieben, wobei beachtet werden muss, dass einige Verfahren bzw. Konformitätsmodule nur in Verbindung mit einem anderen Verfahren bzw. Konformitätsmodul anwendbar sind. Ziel der MDD ist es, damit die Produktauslegung sowie die Produktherstellung abzudecken.

Die zur Verfügung stehenden Konformitätsverfahrensmodule sind:

- Vollständiges QM-System nach Anhang II

  Hierbei wird ein vollumfassendes Qualitätsmanagement-System (QMS) beim Hersteller eingeführt und durch eine benannte Stelle oder akkreditierte Prüfstelle zertifiziert. Das QMS umfasst dabei den gesamten Produktlebenszyklus von der Entwicklung, der Fertigung, der Endkontrolle bis hin zur nachgelagerten Phase (Marktüberwachung). Dieses Konformitätsmodul kann alleine, ohne Anwendung eines weiteren Moduls angewandt werden.

- EG-Baumusterprüfung nach Anhang III

  Hierbei erfolgt die Prüfung der Konformität es Produktes anhand eines Prüfmusters und der dazugehörigen technischen Dokumentation durch eine benannte Stelle. Die Anwendung dieses Moduls ist nur in Verbindung mit einem weiteren, qualitätssichernden Modul möglich.

- EG-Prüfung nach Anhang IV

  Dieses qualitätssichernde Modul dient der Fertigungsendkontrolle. Durchgeführt wird diese Kontrolle von einer benannten Stelle, indem der Hersteller ein fertig hergestelltes Produkt zur Verfügung stellt. Dieses Modul kommt in Verbindung mit einer EG-Konformitätserklärung (VII) oder einer EG-Baumusterprüfung (III) zu Anwendung.

- Qualitätssicherung – Produktion nach Anhang V

  Bei diesem Modul führt der Hersteller ein QMS ein, welches die Bereiche des gesamten Herstellungsprozesses inklusive einer Herstellungsendkontrolle abdeckt. Die Tätigkeiten finden beim Hersteller statt, eine benannte Stelle prüft und zertifiziert das QMS. In Verbindung mit einer EG-Baumusterprüfung oder einer EG-Konformitätserklärung kann dieses Modul angewandt werden.

- Qualitätssicherung – Produkt nach Anhang VI

  Auch bei diesem Modul führt der Hersteller ein QMS ein, dieses deckt jedoch nur den Bereich der Herstellungsendkotrolle ab. Eine benannte Stelle prüft und zertifiziert dieses QMS.

- EG-Konformitätserklärung nach Anhang VII

  Bei Anwendung dieses Moduls führt der Hersteller eine interne Entwurfs- und Fertigungsendkontrolle durch. Dies erfolgt ohne Einbeziehung einer benannten Stelle, sofern das Produkt der Klasse I zugeordnet wird, bei höherklassigen Produkten muss ein qualitätssicherndes Modul zusätzlich angewandt werden.

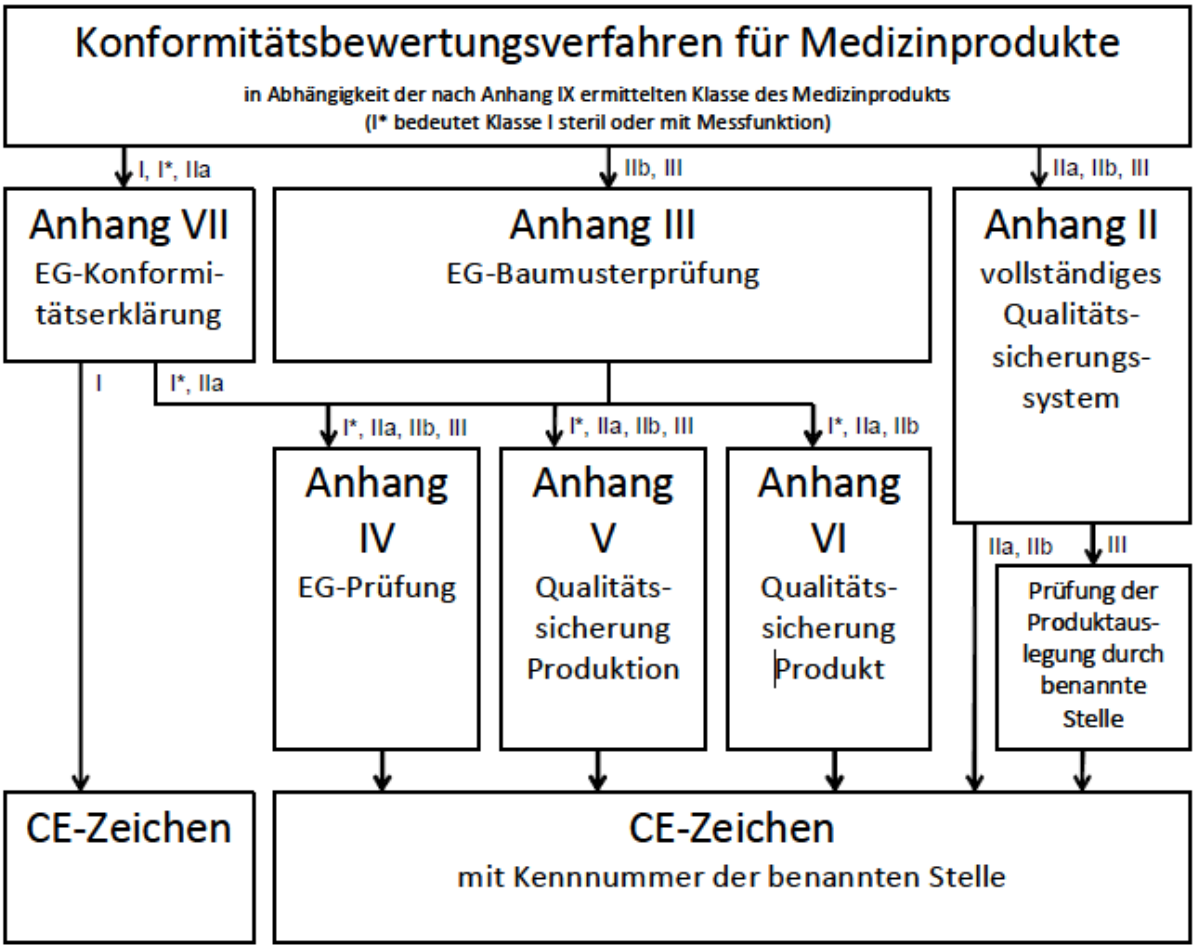


Abbildung 6: Konformitätsbewertungsverfahren nach MDD aus [15]

Abhängig von der Klasse des Produktes können also folgende Module gemäß den Anhängen der MDD angewandt werden – wie in Tabelle 1 dargestellt.

Bei Produkten der Klasse Im und Is müssen die Komponenten mit Messfunktion oder welche die Sterilität von Produkten betreffen durch eine benannte Stelle geprüft werden.

Für Produkte und somit auch Software der Klasse I ist es ausreichend, wenn der Hersteller ein Konformitätsbewertungsverfahren bzw. Konformitätsmodul nach Anhang VII durchführt. Dazu muss der Hersteller eine technische Dokumentation erstellen, anhand derer der Nachweise erbracht wird, dass die Anforderungen der MDD erfüllt werden. Eine Einbeziehung einer benannten Stelle ist bei diesem Konformitätsmodul nicht notwendig, wobei eine Baumusterprüfung nach Anhang III freiwillig möglich ist. Die CE-Kennzeichnung des Produktes erfolgt mit diesem Modul eigenverantwortlich durch den Hersteller.

Für Produkte höherer Risikoklassen müssen wie schon beschrieben, mindestens 2 Module angewandt werden, um einen Konformitätsnachweis erbringen zu können. Eine Ausnahme stellt hier der Anhang II (vollständiges QMS) dar.

Risikoklasse	Konformitätsbewertungsverfahren
I	Anhang VII
IIa	Anhang II oder Anhang VII mit - Anhang IV - Anhang V - Anhang VI
IIb	Anhang II oder Anhang III mit - Anhang IV - Anhang V - Anhang VI
III	Anhang II oder Anhang III mit - Anhang IV - Anhang V

Tabelle 1: Übersicht der anwendbaren Konformitätsmodule abhängig von der Risikoklasse

2.3.1 Konformitätsbewertungsverfahren für Hersteller von Software

In Anbetracht der Eigenschaften von Stand-alone Software, können die beschriebenen mehrstufigen Konformitätsbewertungsverfahren nur schwer implementiert werden. Es wird einem Softwarehersteller schwer gelingen eine klar dokumentierte Trennung zwischen Entwicklung (Entwurf) und Herstellung des Produktes zu schaffen. Eine eigentliche ‚Herstellung' im Sinne einer Produktion findet bei Software nicht statt. Im besten Fall fielen darunter die Produktion bzw. Beschreibung von Datenträgern mit der Software.

Somit kommen die mehrstufigen Konformitätsmodule für Softwarehersteller nicht in Frage. Ausgenommen davon sind Hersteller von Software der Klasse I. Wie bei ‚klassischen Medizinprodukten' erstellt der Hersteller eine technische Dokumentation, welche den Nachweis erbringt, dass die grundlegenden Anforderungen der MDD erfüllt sind. Es ist auch empfehlenswert, ein zumindest ‚rudimentäres' QMS bei Klasse I Software zu etablieren, dies erleichtert eine nachvollziehbare Selbstdeklaration der Konformität. Bei Klasse I Produkten muss ein QMS jedoch nicht zertifiziert werden. Es ist jedoch empfehlenswert von Anfang der Entwicklung ein zertifiziertes QMS zu etablieren und zu betreiben, da in Zukunft aufgrund geänderter regulatorischen Anforderungen oder zusätzlichen Softwarefunktionen das Endprodukt in eine höhere Risikoklasse eingestuft werden muss. So wurde auch zur Entwicklung der Software ‚*ilvi*' ein zertifiziertes QMS

eingeführt, um für die zukünftigen (regulatorischen und funktionellen) Herausforderungen gerüstet zu sein.

Ab der Risikoklasse IIa kommt für Softwarehersteller eigentlich nur noch ein vollständiges QMS nach Anhang II in Frage. Dies resultiert aus der oben beschriebenen Eigenschaft von Software. Der Anhang II sieht eine Einführung und Aufrechterhaltung eines vollständigen QMS beim Hersteller vor. Dabei spezifiziert die MDD nicht wie oder welches QMS dabei eingeführt werden muss, sondern verweist auf Punkte bzw. Bereiche aus dem Produktlebenszyklus, die mit dem QMS abgedeckt werden müssen. Da zum Nachweis der Erfüllung der grundlegenden Anforderungen der ‚Stand der Technik' Beachtung finden muss, ist es naheliegend, dass man einen Standard nutzt, der passend für diese Anforderung ist. Die EN ISO 13485 ist hierzu eine Norm, die ein Qualitätsmanagement für Medizinprodukte beschreibt.

3 Qualitätsmanagement nach EN ISO 13485

Die Norm EN ISO 13485, der vollständige Titel lautet „Medizinprodukte – Qualitätsmanagementsysteme – Anforderungen für regulatorische Zwecke" [9], stellt die Anforderungen für ein QMS dar, wie es für Hersteller von Medizinprodukten eingeführt werden muss, damit eine Konformität gegeben sein kann. Die Norm richtet sich darüber hinaus an alle Organisationen, die Medizinprodukte zur Verfügung stellen', also auch an Händler, Zulieferer oder Importeure.

Die ISO 13485 ist ähnlich der QM-Norm ISO 9001, spezifiziert ihre Anforderungen jedoch speziell auf einen risikobasierten Ansatz [15]. Hintergrund dafür ist die Sicherheit der produzierten Produkte in Hinblick auf den Patienten, den Anwender und Dritte. Hierbei wird auf ein adäquates Risikomanagement verwiesen, wie es die harmonisierte Norm EN ISO 14971 darstellt. Die EN ISO 13485 verfolgt auch einen prozessorientierten Ansatz. Die in der Norm geforderten Prozesse funktionieren nur im Zusammenspiel aller als Gesamt (Qualitätsmanagement-)-System.

Wie ein QMS gemäß der EN ISO 13485 aufzubauen ist, wird in den Kapiteln 4 bis 8 der Norm beschrieben. In Kapitel 4 stehen allgemeine Anforderungen an das QMS, speziell die Dokumentationsanforderungen. Zentrales Dokument ist hier das Qualitätsmanagement-Handbuch.

In Kapitel 5 werden die Anforderungen an die oberste Leitung festgelegt. Darunter fallen die Definition einer Qualitätspolitik sowie Qualitätszielen ebenso, wie die Durchführung von regelmäßigen Managementbewertungen und internen Audits. Um Input für diese Tätigkeiten zu erlangen, muss die oberste Leitung einen Qualitätsmanagement-Beauftragten ernennen, welcher die erforderlichen Tätigkeiten zur Etablierung und Aufrechterhaltung des QMS durchführt. Aus den Ergebnissen der Managementbewertungen werden folgend gegebenenfalls Korrekturmaßnahmen gesetzt. Diese Anforderungen werden in den ‚Managementprozessen' (siehe Abbildung 8) umgesetzt.

Kapitel 6 der EN ISO 13485 beschreibt das Management von Ressourcen. Dabei muss die oberste Leitung die nötigen Ressourcen zur Verfügung stellen, um die im QMS

beschriebenen Verfahren anwenden und durchführen zu können. Darin enthalten sind auch die notwendige Qualifikation und Schulungsmaßnamen der Mitarbeiter als auch die Anforderungen an die Infrastruktur bzw. die Arbeitsumgebung. Die Anforderungen aus Kapitel 6 werden zum Teil durch die ‚unterstützenden Prozesse' erfüllt.

In Kapitel 7 werden die Anforderungen an die Produktentwicklung bzw. Produktrealisierung gestellt. Diese Anforderungen betreffen den gesamten Produktlebenszyklus, im Falle von Software den Softwarelebenszyklus. Es wird die Einbindung von Kunden gefordert, dessen Anforderungen an das Produkt erfüllt werden müssen. Dies ist in Abbildung 8 gut erkenntlich dargestellt. Zusätzlich fordert dieses Kapitel der Norm Verfahren für die Beschaffung, die Produktion, den Umgang mit Kundeneigentum, die Überwachung von Messmitteln, beschreibt Anforderungen an das Design und die Entwicklung. Ebenso fordert die Norm in diesem Kapitel ein Risikomanagement und empfiehlt dabei die Durchführung dessen nach der ISO 14971. In den ‚Kernprozessen' des QMS werden diese Anforderungen umgesetzt.

Schließlich beschreibt das Kapitel 8 der EN ISO 13485 notwendige Verfahren, um die Wirksamkeit des QMS zu bewerten.

Im Zuge der Anwendung der Norm gilt nur, was auch beschrieben und dokumentiert ist. Daher beschreibt die Norm auch, welche Prozesse und Dokumente wie zu dokumentieren sind.

Als übergeordnetes Dokument dient das Qualitätsmanagement-Handbuch (QMH), gefolgt von den prozessbeschreibenden Verfahrensanweisungen (VA) und den dazugehörigen Arbeitsanweisungen (AA). Formblätter (FB), Checklisten (CL), Listen (LI) und Festlegungen (FL) sind immer in Verbindung mit einer Verfahrens- oder Arbeitsanweisung auszufüllen oder durchzuführen, und sind danach Aufzeichnungen.

Diese Dokumentenhierarchie ist in Abbildung 7 dargestellt.

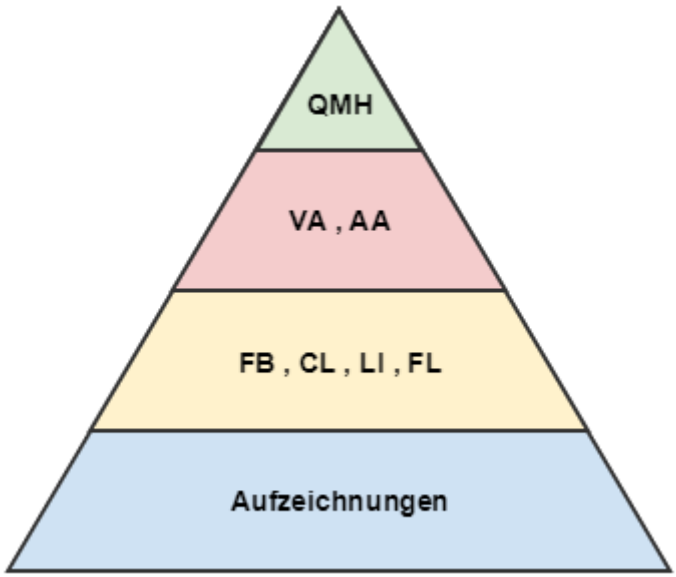


Abbildung 7: Dokumentenhierarchie eines QMS.

Der Inhalt des Qualitätsmanagementhandbuches wird in der EN ISO 13485 geregelt. Darin ist der Anwendungsbereich des QMS, die dokumentierten Verfahren (VA's), oder Verweise darauf sowie die Wechselwirkung der Prozesse des QMS zu dokumentieren.

Zur Darstellung der Wechselwirkung der Prozesse zum Gesamt-QM-System eignet sich eine Prozesslandschaft, in der grafisch das Zusammenspiel aller Prozesse/Verfahrensanweisungen dargestellt wird. Am Beispiel des QMS zur Entwicklung von *ilvi* sieht diese Prozesslandschaft wie in Abbildung 8 dargestellt aus.

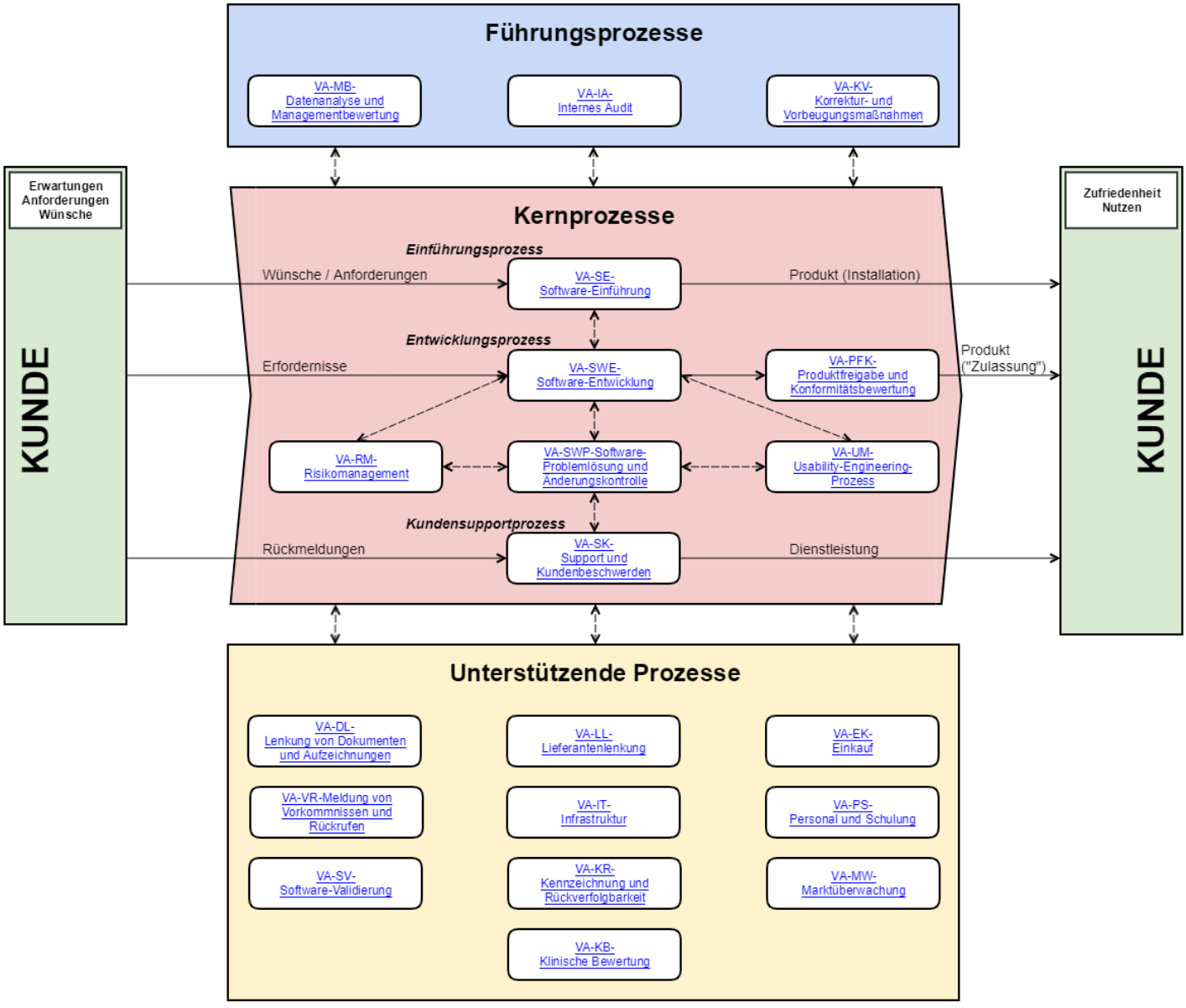


Abbildung 8: Prozesslandschaft im Qualitätsmanagementhandbuch.

In dieser Prozesslandschaft sind sämtliche erstellten und dokumentierten Verfahrensanweisungen, welche einem Prozess entsprechen, dargestellt. Sie bildet das gesamte QMS grafisch ab. Es wird hierbei zwischen Kernprozessen, unterstützenden Prozessen und Führungsprozessen unterschieden.

Die Kernprozesse beschreiben alle notwendigen Tätigkeiten, damit ein konformes Endprodukt an einen Anwender bzw. Kunden ausgeliefert wird. Zentraler Prozess dabei ist der ‚Software-Entwicklungs-Prozess'. Um jedoch ein konformes Produkt zu entwickeln, bedarf es weiterer Kernprozesse, die den Umgang mit Softwareproblemen (SW-Problemlösungs- und Änderungskontrolle), die Gebrauchstauglichkeit (Gebrauchstauglichkeitsprozess), das Risikomanagement (Risikomanagement-Prozess), die Tätigkeiten zur SW-Einführung beim Kunden (SW-Einführungsprozess), den Umgang mit Beschwerden und Supportanfragen sowie schlussendlich die Konformitätsbewertung regeln.

Ein QMS bzw. die darin geregelten Tätigkeiten funktionieren jedoch nur mit weiteren Verfahren, wie es die unterstützenden Prozesse darstellen. Diese Prozesse definieren folgende Anforderungen und Tätigkeiten:

Dokumentenlenkung: Diese Verfahrensanweisung beschreibt die Struktur der QM-Dokumentation mit den darin benötigten Tätigkeiten, um diese Dokumente und Aufzeichnungen korrekt zu lenken.

Meldung von Vorkommnissen und Rückrufen: Beschreibt den Prozess, wie der Hersteller mit Meldungen von Vorkommnissen, betreffend der hergestellten Produkte umzugehen hat. Ebenso wird darin der Prozess beschrieben, wie Produktrückrufe durchzuführen sind.

SW-Validierung: Darin ist festgehalten, wie Software, die die Produktqualität beeinflussen kann, validiert und freigegeben wird. Bei dieser Software handelt es sich nicht um das Endprodukt, sondern um die notwendige Software, um dieses Endprodukt zu entwickeln.

Lieferantenlenkung: Definiert, wie der Hersteller Lieferanten auswählt und bewertet, um konforme und vor allem sichere Produkte bzw. Software herzustellen.

Einkauf: Darin wird die Tätigkeit beschrieben, wie bei gelenkten Lieferanten Produkte oder Dienstleistungen bezogen werden.

Infrastruktur: Beschreibt die notwendige IT-Infrastruktur und die periphere Infrastruktur, die zur Entwicklung notwendig ist.

Kennzeichnung und Rückverfolgbarkeit: Definiert die Anforderungen zur Kennzeichnung der Produkte während des gesamten Produkt-Lebenszyklus sowie die Gewährleistung der Rückverfolgbarkeit derer.

Klinische Bewertung: Definiert die Tätigkeiten, die notwendig sind, um die klinische Bewertung eines Produktes zu erstellen. Diese wird benötigt, um die medizinische Leistung eines Produktes zu bewerten.

Marktüberwachung: Darin wird beschrieben, wie die nachgelagerte (nach der Entwicklung) Marktüberwachung zu erfolgen hat.

Personal und Schulung: Darin enthalten sind die Anforderungen an das Personal, welches dem QMS unterliegt und ebenso, wie dieses Personal korrekt gelenkt und geschult werden muss.

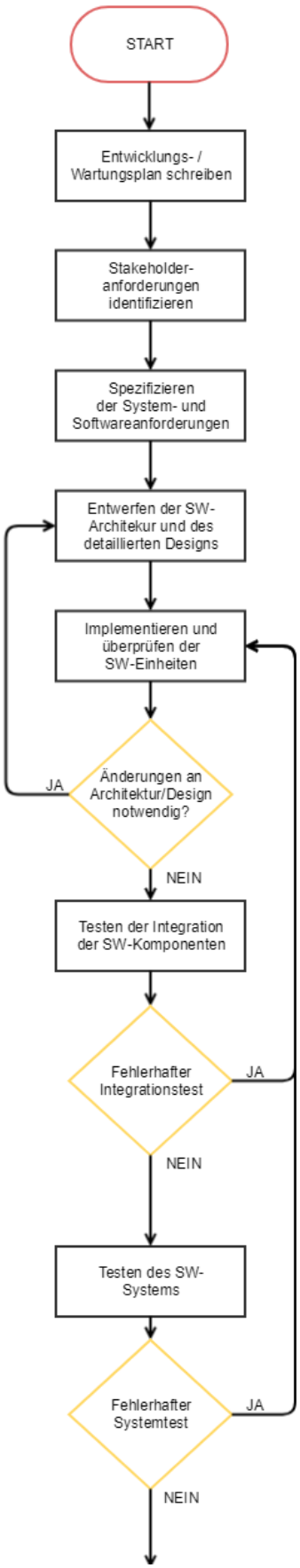
Die EN ISO 13485 fordert explizit die Einbindung bzw. Verantwortung der ‚obersten Leitung', also der Geschäftsführung in das QMS. Diese Einbindung und die damit verbundenen Tätigkeiten werden in den Führungsprozessen beschrieben. Im Zuge einer Managementbewertung wird die Wirksamkeit des QMS geprüft und bewertet. Hinzu kommt die Anforderung zur Untersuchung nach den anwendbaren regulatorischen Anforderungen, um sicherzustellen, dass geänderte Regularien beachtet werden. Ebenso werden hier die notwendigen internen Audits beschrieben. Schließlich wird hier auch der Umgang bei festgestellten Abweichungen der Anforderungen im Prozess der Korrektur- und Vorbeugemaßnahmen definiert.

Die in der dargestellten Prozesslandschaft enthaltenen Verfahren bilden jedoch nicht allein die Anforderungen der EN ISO 13485 ab, sondern beinhalten auch Verfahren aus den weiteren relevanten und harmonisierten Normen. Der Zusammenhang wurde schon in Abbildung 3 dargestellt. Im Falle einer Softwareentwicklung sind diese Normen die ISO 14971 über das Risikomanagement, die EN 62304 über den Software-Lebenszyklus und die ISO 62366 über die Gebrauchstauglichkeit.

4 Zusammenhang mit anderen Normen

4.1 Software-Lebenszyklus nach EN 62304

Um den Produkt-Lebenszyklus auf Software als Medizinprodukt anwenden zu können, muss die EN 62304 umgesetzt werden [11]. Im hierbeschriebenen QMS werden die Anforderungen aus dieser Norm in mehreren Verfahren erfüllt. Zentraler Prozess ist dabei der Software-Entwicklungsprozess. Weitere Prozesse, die diese Norm betreffen ist die Software-Einführung, die Produktfreigabe mit der Konformitätsbewertung und die Problemlösungs- und Änderungskontrolle. Darüber hinaus fordert die Norm ein adäquates Risikomanagement und verweist dabei explizit auf ein Risikomanagement gemäß der EN ISO 14971 [10]. Schließlich empfiehlt die Norm auch noch ein geeignetes QMS in Form der EN ISO 13485 [9]. Als zentraler Prozess wird in Abbildung 9 der Software-Entwicklungsprozess als Flussdiagramm dargestellt. Hierbei sind auch die Zusammenhänge zu anderen Normen dargestellt. So müssen die ‚Kernaufgaben' der Software gemäß der EN 62304 beschrieben werden, anhand derer eine Risikoanalyse betreffend diese Kernaufgaben durchgeführt werden muss. Hier gibt es eine Verbindung zur EN ISO 14971 bzw. dem Risikomanagement. Das Gebiet der Gebrauchstauglichkeit betrifft auch die Tätigkeit der Softwarevalidierung. In die Systemtests wiederum ist wiederum das Risikomanagement mit einbezogen, um Beherrschungsmaßnahmen zu verifizieren.

Prozessablauf	Zugehörige Informationen	VW	MW	ZI
	Nennen von Personen und Terminen. Kernaufgaben beschreiben Stakeholder-Anforderungen ableiten Verifizierung und Genehmigung Benutzungsszenarien System als Blackbox RM Sicherheitsklassen Planung Systemtest Verifizierung und Genehmigung Planung Integrationstest Implementierung Verifizierung und Genehmigung Modultests Durchführung des Integrationstests und Berichterstellung Durchführung und Berichterstellung Formative Evaluierung der Gebrauchstauglichkeit	PL PL PL SWA SWE SWA SWT SWT SWT	 Team UMB RMB Team RMB SWA SWE SWE RMB	 Team SWE PL EL EL PL PL EL PL EL PL EL PL EL

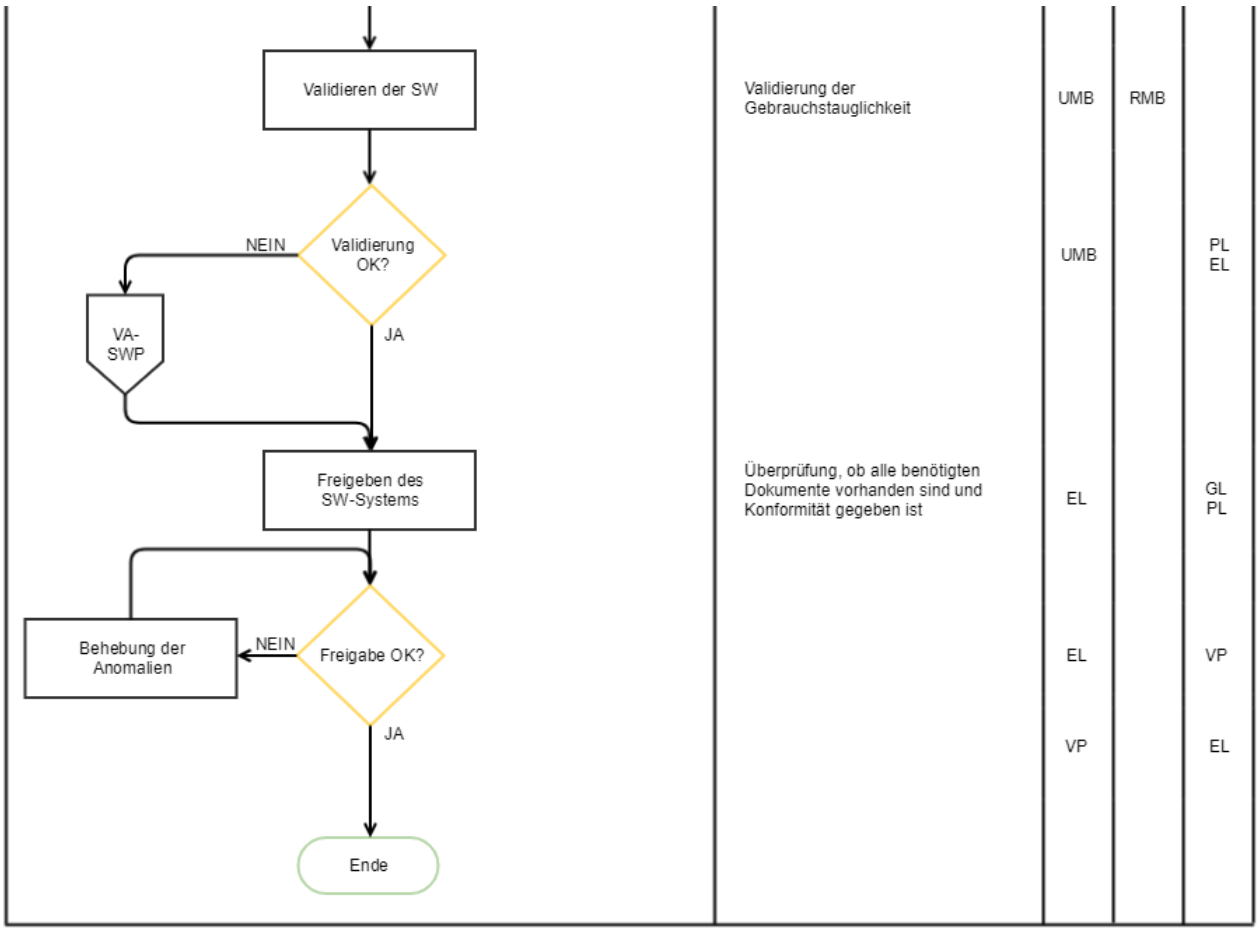


Abbildung 9: Software-Entwicklungsprozess.

In Bezug auf das Risikomanagement fordert diese Norm eine Klassifizierung der Software bzw. der Softwarekomponenten. Diese Klassifizierung ist nicht zu verwechseln mit der Klassifizierung in Risikoklassen in Bezug auf die MDD – eine Klassifizierung in Sicherheitsklassen erfolgt hier ‚nur' bei Software als Medizinprodukt. Im Gegensatz zur EN ISO 14971, welche das ‚Produktrisikomanagement' behandelt, bei dem immer eine Eintrittswahrscheinlichkeit eines Schadens beachtet werden soll, verlangt die EN 62304 die Beachtung der Wahrscheinlichkeit nicht. Im Gegenteil, sie fordert die Annahme der Eintrittswahrscheinlichkeit von 1 bzw. 100%. Unter dieser Annahme erfolgt die Klassifizierung in folgende Klassen:

- A: Durch die Software sind keine Verletzungen oder Gefährdungen möglich
- B: Es sind keine schwerwiegenden Verletzungen möglich
- C: Es sind schwerwiegende Verletzungen oder der Tod möglich.

Für die Software *ilvi* wird diese Klassifizierung im Zuge des Risikomanagements im entsprechenden Kapitel beschrieben.

4.2 Gebrauchstauglichkeit gemäß EN 62366

Einen engen Zusammenhang haben die EN 62366 und die EN ISO 14971. Die Norm EN 62633 behandelt die Aspekte der Gebrauchstauglichkeit von Medizinprodukten, hier vor allem sicherheitsrelevante Aspekte. In Bezug auf das Risikomanagement behandelt diese Norm vor allem Risiken und Gefährdungen, welche aus einer unzureichenden Gebrauchstauglichkeit resultieren. Um nun eine gute Gebrauchstauglichkeit zu schaffen, muss ein Prozess geschaffen werden. Die dazu notwendigen Tätigkeiten werden über den Gebrauchstauglichkeitsprozess abgebildet. Am Beispiel des QMS für Software-Herstellung wird dieser Prozess in Abbildung 10 dargestellt. Die enge Beziehung zum Risikomanagement ist hier ersichtlich. Diese Beziehungen spiegeln sich auch in einzelnen Kapiteln beider Normen wider. So fordert die EN 62366 in Kapitel 5.1 [12] und die EN ISO 14971 in Kapitel 4.2 [10] eine Identifizierung von Sicherheitsbezogenen Merkmalen. Die EN 62366 fordert in Kapitel 5.3.2 die Erkennung von Gefährdungen und Gefährdungssituationen in Bezug auf die Gebrauchstauglichkeit, ebenso wie die ISO 14971 in Kapitel 4.3. Sind Maßnahmen zur Erhöhung der Gebrauchstauglichkeit notwendig, müssen diese auf daraus resultierenden Gefährdungen untersucht werden. Schließlich fordern beide Normen eine Beurteilung des Restrisikos sowie eine Abwägung des Nutzens zum Restrisiko [16]. Die Abbildung 10 auf der Folgeseite zeigt einen Gebrauchstauglichkeitsprozess wie er für Softwareentwicklungen angewandt wird.

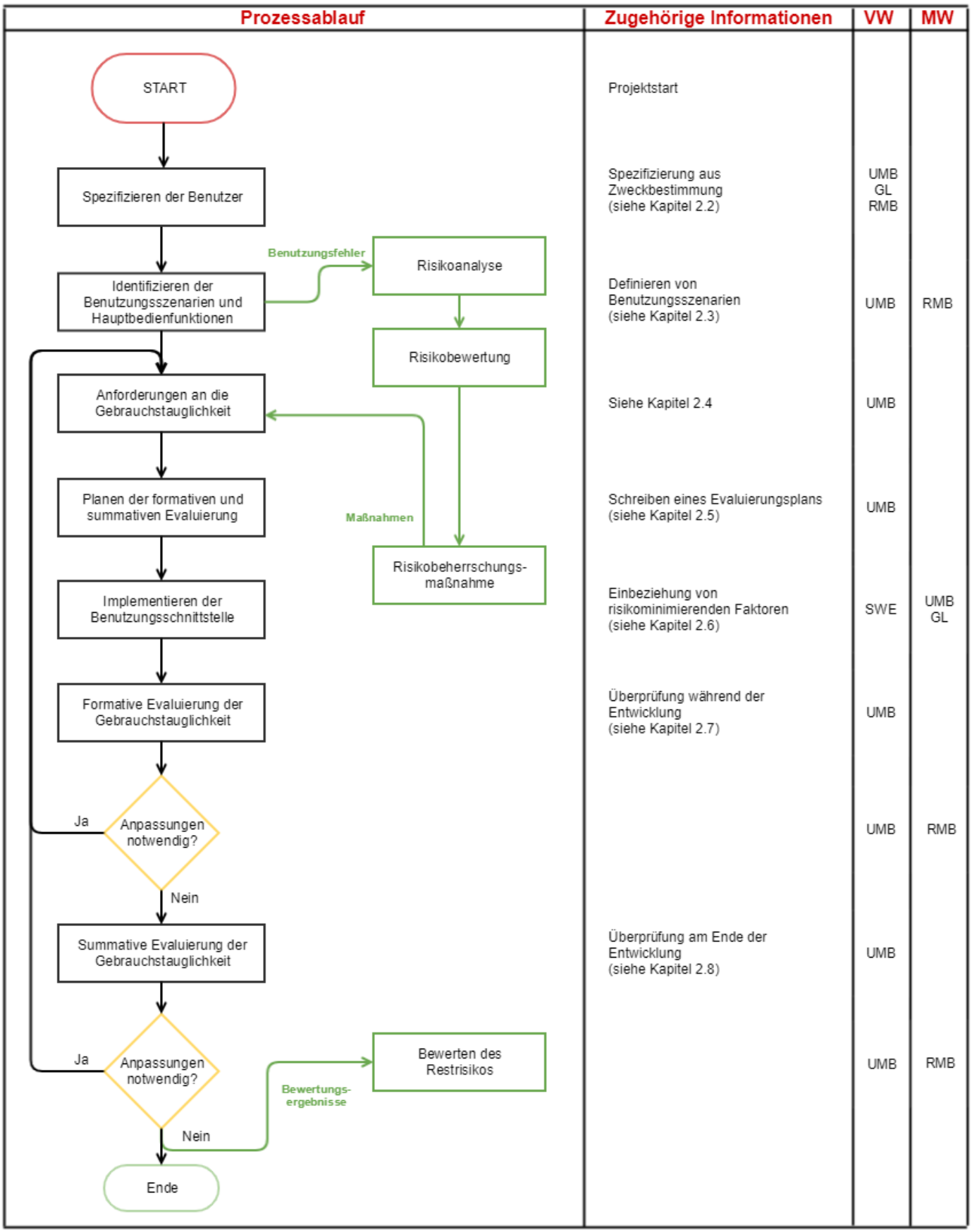


Abbildung 10: Gebrauchstauglichkeitsprozess.

Wie in vielen Prozessen der Produktentwicklung, beginnt auch der Gebrauchstauglichkeitsprozess mit der Definition bzw. aufbauend auf der Zweckbestimmung. Inhaltlich muss die Zweckbestimmung die vorgesehenen Benutzergruppen darstellen, aus denen über den Gebrauchstauglichkeitsprozess die sogenannten Benutzungsszenarien und Hauptbedienfunktionen für jede Benutzergruppe aus den Kernaufgaben abgeleitet werden müssen. Im Falle von *ilvi* sind die Benutzergruppen das Pflegepersonal und Ärzt/innen. Ausgehend von diesen Benutzergruppen können die Benutzungsszenarien abgeleitet werden, welche für *ilvi* wie folgt in Tabelle 2, 3, 4 und 5 dargestellt sind. Dabei wurden vorab die Kernaufgaben (KA) identifiziert, wobei diese für beide Benutzergruppen gelten:

- Benutzeranmeldung und identifizieren von Patienten
- Erfassung von gemessenen Vitalwerten
- Abfrage und Dokumentation von Gesundheitswerten
- Dokumentation der Wundheilung

Zu diesen Kernaufgaben werden in Folge die Benutzungsszenarien abgeleitet und beschrieben. Ebenso werden die dazugehörigen Bildschirmdesigns dargestellt.

Benutzeranmeldung und identifizieren von Patienten			
Vorbedingung:	Es bedarf einer Aktion am Patienten unter Einbeziehung des Systems.		
Nachbedingung:	Der Benutzer sowie der Patient wurden korrekt authentifiziert bzw. identifiziert / Der Benutzer und der Patient sind erfolgreich vom System abgemeldet.		
Aufgaben	**Häufig/Sicherheitsbezogen**	**Aktion des Benutzers**	**Reaktion des Systems**
Anmeldung am System	Häufig benutzt: Ja Sicherheitsbezogen: Nein	keine	Das System zeigt dem Benutzer, wie er sich am System anmelden kann.
		Der Benutzer meldet sich am System an.	Das System überprüft, ob der Benutzer gültig ist. Wenn ja: Das System zeigt den Titel und Namen des Benutzers an. Wenn nein: Das System gibt eine entsprechende Fehlermeldung aus.

Identifizieren des Patienten	Häufig benutzt: Ja Sicherheitsbezogen: Ja	keine	Das System zeigt dem Benutzer, wie er einen Patienten identifizieren kann.
		Der Benutzer identifiziert am System einen Patienten.	Das System überprüft, ob der Patient gültig ist. Wenn ja: Das System zeigt Name und Geburtsdatum des Patienten an. Wenn nein: Das System gibt eine entsprechende Fehlermeldung aus.
Detaillierte Informationen einsehen	Häufig benutzt: Ja Sicherheitsbezogen: Ja	Der Benutzer wählt Informationsfenster am System aus.	Das System zeigt detaillierte Daten über Patienten und Benutzer.
Patient abmelden	Häufig benutzt: Nein Sicherheitsbezogen: Ja	keine	Das System bietet im Informationsfenster die Möglichkeit, den Patienten abzumelden.
		Der Benutzer wählt am System die Patientenabmeldung aus.	Das System warnt vor bevorstehender Abmeldung des Patienten und bietet die Möglichkeit zum Abbruch der Aktion.
		Der Benutzer verifiziert die Abmeldung.	Das System meldet den Patienten ab.

Benutzer abmelden	Häufig benutzt: Ja Sicherheitsbezogen: Nein	keine	Das System bietet im Informationsfenster die Möglichkeit, den Benutzer abzumelden.
		Der Benutzer wählt am System die Benutzerabmeldung aus.	Das System warnt vor bevorstehender Abmeldung des Benutzers und bietet die Möglichkeit zum Abbruch der Aktion.
		Der Benutzer verifiziert die Abmeldung.	Das System meldet den Benutzer ab und zeigt den Startscreen.

Tabelle 2: Benutzungsszenario aus der KA Benutzeranmeldung und identifizieren von Patienten

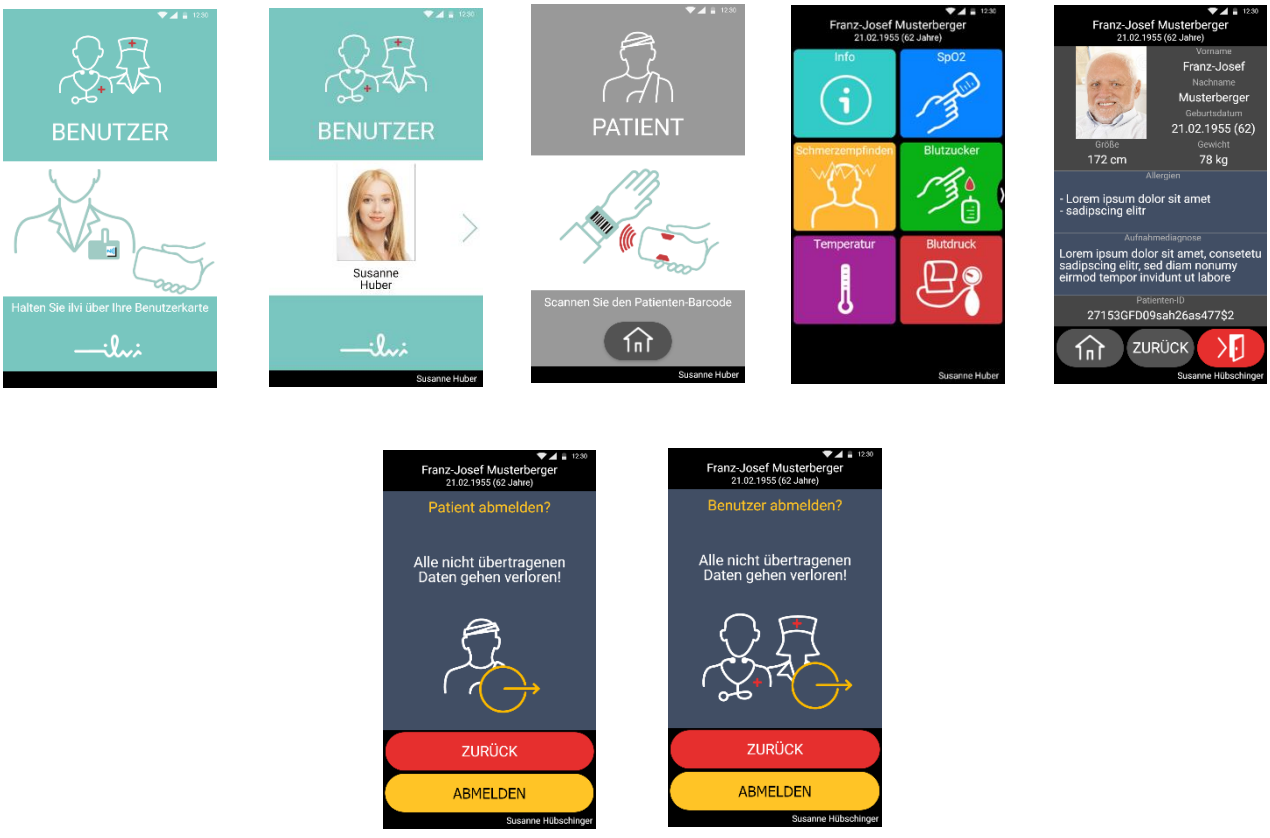


Abbildung 11: GUI aus der Kernaufgabe 'Anmeldung'

Erfassen von Vitalparametern			
Vorbedingung:	Es liegen Daten einer Messung vor. Benutzer ist am System autorisiert. Patient ist am System identifiziert.		
Nach-bedingung:	Die Pflegekraft hat die korrekten Daten korrekt abgelegt.		
Aufgaben	**Häufig/Sicherheitsbezogen**	**Aktion des Benutzers**	**Reaktion des Systems**
Automatische Übertragung der Werte auf das System	Häufig benutzt: Ja Sicherheitsbezogen: Ja	Der Benutzer wählt am System aus, dass er Daten erhalten möchte.	Das System zeigt die empfangenen Werte an und bietet dem Benutzer die Möglichkeit, die Daten zu übernehmen oder die empfangenen Daten zu verwerfen. Gleichzeitig führt das System eine Plausibilitätsprüfung der Werte durch.
		Der Benutzer übernimmt die Daten am System.	Das System zeigt die bestätigten Werte an.
Manuelle Erfassung der abgelesenen Vitalparameter	Häufig benutzt: Ja Sicherheitsbezogen: Ja	keine	Das System zeigt eine Auswahl der zu erfassenden Vitalparameter an.
		Der Benutzer wählt am System den gewünschten Parameter aus.	Das System zeigt das zum Vitalparameter zugehörige Fenster an.
		Der Benutzer trägt am System die vom Medizinprodukt abgelesenen Werte manuell ein.	Das System zeigt die Eingaben des Benutzers und bietet die Möglichkeit, die Eingaben zu bearbeiten/löschen. Das System überprüft die eingegebenen Daten auf Plausibilität.

		Der Benutzer bestätigt die eingegebenen Werte.	Das System speichert die eingegebenen Werte und zeigt diese an.
Löschen von bereits bestätigten Vitalwerten	Häufig benutzt: Nein Sicherheitsbezogen: Ja	Der Benutzer wählt am System das Löschen eines Wertes aus.	Das System erfordert die Bestätigung zum Löschen der Daten.
		Der Benutzer bestätigt am System das Löschen.	Das System löscht den gewünschten Parameter.
Übertragen der Daten an das Informations-system der Kranken-anstalt	Häufig benutzt: Ja Sicherheitsbezogen: Ja	Der Benutzer wählt am System aus, dass er die empfangenen/eingegebenen Vitalparameter übertragen möchte.	Das System erfordert die Bestätigung zum Übertragen der Daten.
		Der Benutzer bestätigt am System das Übertragen.	Das System überträgt die Daten an das KIS der Krankenanstalt.

Tabelle 3: Benutzungsszenario aus der KA Erfassen von Vitalparameter

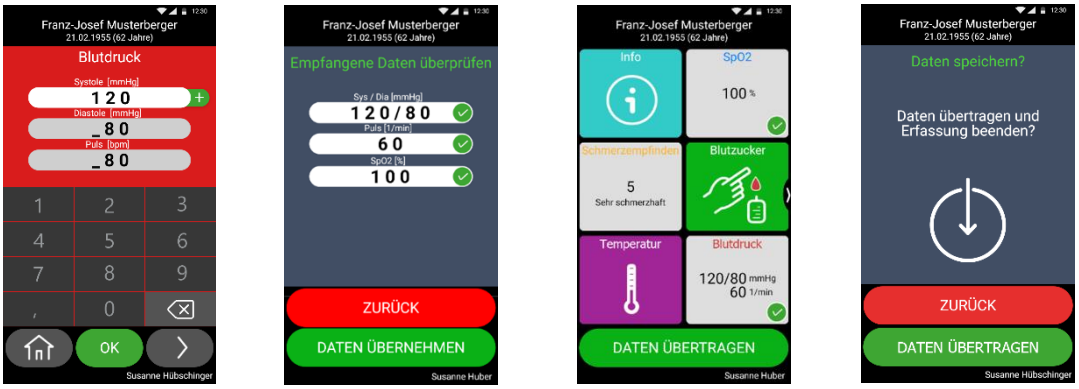


Abbildung 12: GUI aus 'Erfassen von Vitalparametern

Erfassen von weiteren Gesundheitswerten			
Vorbedingung:	Patient muss ansprechbar und mental in der Lage sein, auf die Fragen des Pflegepersonals zu antworten. Benutzer ist am System autorisiert. Patient ist am System identifiziert.		
Nachbedingung:	Die Pflegekraft hat die korrekten Daten korrekt abgelegt.		
Aufgaben	**Häufig/Sicherheitsbezogen**	**Aktion des Benutzers**	**Reaktion des Systems**
Manuelle Erfassung der aufgenommenen Gesundheitswerte	Häufig benutzt: Ja Sicherheitsbezogen: Ja	keine	Das System zeigt eine Auswahl der möglichen Gesundheitswerte an, welche erfasst werden können.
		Der Benutzer wählt am System den gewünschten Gesundheitswert aus.	Das System zeigt das zum Gesundheitswert zugehörige Fenster an.
		Der Benutzer trägt am System den Gesundheitswert des Patienten ein.	Das System zeigt die Eingaben des Benutzers und bietet die Möglichkeit, die Eingaben zu bearbeiten/löschen. Das System überprüft ggf. die eingegebenen Daten auf Plausibilität.
		Der Benutzer bestätigt den eingegebenen Wert.	Das System speichert den eingegebenen Wert und zeigt diesen an.

Löschen von bereits bestätigten Gesundheitswerten	Häufig benutzt: Nein Sicherheitsbezogen: Ja	Der Benutzer wählt am System das Löschen eines Wertes aus.	Das System erfordert die Bestätigung zum Löschen der Daten.
		Der Benutzer bestätigt am System das Löschen.	Das System löscht den gewünschten Wert.
Übertragen der Daten an das Informationssystem der Krankenanstalt	Häufig benutzt: Ja Sicherheitsbezogen: Ja	Der Benutzer wählt am System aus, dass er die eingegebenen Gesundheitswerte übertragen möchte.	Das System erfordert die Bestätigung zum Übertragen der Daten.
		Der Benutzer bestätigt am System das Übertragen.	Das System überträgt die Daten an das Informationssystem der Krankenanstalt.

Tabelle 4: Benutzungsszenario aus der KA Abfrage und Dokumentation von Gesundheitswerten

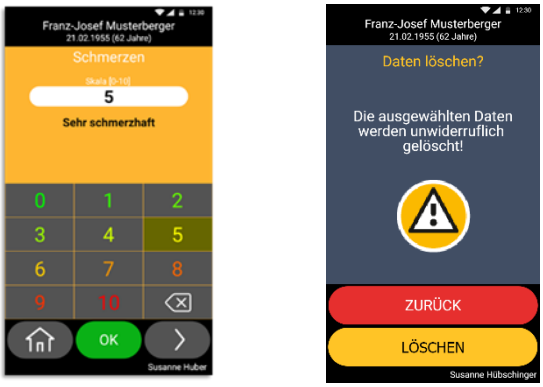


Abbildung 13: GUI aus 'Erfassen von Gesundheitswerten'

Wunddokumentation			
Vorbedingung:	Ein Patient muss am System identifiziert sein. Der Patient muss eine Wunde haben.		
Nachbedingung:	Der Benutzer hat die korrekten Foto-Dateien korrekt abgelegt.		
Aufgaben	**Häufig/Sicherheits-bezogen**	**Aktion des Benutzers**	**Reaktion des Systems**
Wunddokumentation starten	Häufig benutzt: Ja Sicherheitsbezogen: Nein		Das System bietet eine Auswahlmöglichkeit zum Starten der Wunddokumentation.
		Der Benutzer wählt am System die Wunddokumentation aus.	Das System startet die Kamera und zeigt den dazugehörigen Bildschirm.
Foto aufnehmen	Häufig benutzt: Ja Sicherheitsbezogen: Ja	Der Benutzer wählt am System aus, dass er ein/mehrere Foto(s) machen möchte.	Das System fokussiert die Kamera und schießt ein Foto. Das System zeigt eine Aufnahme des Fotos. Das System erfordert die Bestätigung zum Speichern des Fotos
		Der Benutzer bestätigt am System das Speichern.	Das System speichert das/die aufgenommene(n) Foto(s) und ordnet es/sie dem Patienten zu (Benamung des Fotos mit Namen/Fall-ID u.ä.).
Foto(s) übertragen	Häufig benutzt: Ja Sicherheitsbezogen: Ja	Der Benutzer wählt am System aus, dass er die aufgenommenen Fotos übertragen möchte.	Das System erfordert die Bestätigung zum Übertragen der Daten.
		Der Benutzer bestätigt am System das Übertragen.	Das System überträgt die Daten an das Informationssystem der Krankenanstalt.

Tabelle 5: Benutzungsszenario aus der KA Dokumentation von Wundheilung

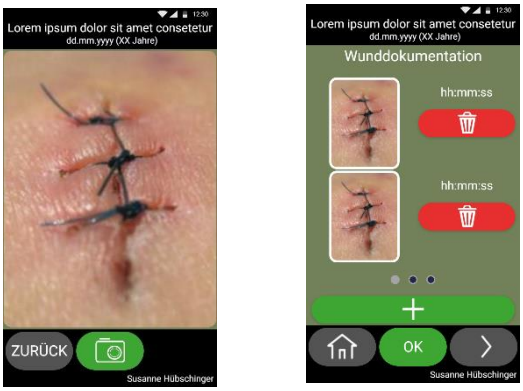


Abbildung 14: GUI der Wunddokumentation

In diesem Schritt des Gebrauchstauglichkeitsprozesses besteht eine enge Verknüpfung mit dem Risikomanagement. Für jedes Benutzungsszenario muss bewertet werden, ob es einen Einfluss auf die Sicherheit der Software hat. Dies ist in den oben dargestellten Tabellen ersichtlich. Im Zuge des Risikomanagement-Prozesses, der im Folgekapitel beschrieben wird, erfolgt zu den Benutzungsszenarien auch eine Risikoanalyse. Die Ereignisse dieser Risikoanalyse bzw. gegebenenfalls erforderliche Risikobeherrschungsmaßnahmen fließen in den Gebrauchstauglichkeitsprozess ein, indem sie Anforderungen dazu darstellen (Sicherheitsbezogene Merkmale). Über den SW-Entwicklungsprozess werden diese Gebrauchstauglichkeits-Anforderungen in die Software implementiert, gefolgt von einer formativen Evaluierung des Systems. Schließlich wird unter Einbeziehung der vorgesehenen Benutzergruppen das System summativ evaluiert, woraus sich wiederum Änderungen ergeben können. Auch hier kommt es wieder zu einer Verknüpfung zum Risikomanagementprozess, über welchen das Restrisiko des Systems bewertet werden muss. Im Zuge dieser Arbeit wird der Gebrauchstauglichkeitsprozess bzw. seine Anwendung nicht näher beschrieben, dies würde den Rahmen dazu sprengen. Verknüpfungen zum Risikomanagementprozess werden detaillierter im entsprechenden Kapitel behandelt.

5 Risikomanagement nach EN ISO 14971

5.1 Einführung

Die MDD fordert in den grundlegenden Anforderungen, dass Medizinprodukte so ausgelegt und hergestellt werden müssen, „*dass ihre Anwendung unter den vorgesehenen Bedingungen und zu den vorgesehenen Zwecken weder den klinischen Zustand und die Sicherheit der Patienten noch die Sicherheit und die Gesundheit der Anwender oder gegebenenfalls Dritter gefährdet, wobei etwaige Risiken im Zusammenhang mit der vorgesehenen Anwendung gemessen am Nutzen für den Patienten vertretbar und mit einem hohen Maß an Gesundheitsschutz und Sicherheit vereinbar sein müssen*.“ Zitiert aus [3]

Dies impliziert im regulatorischen Rahmen der MDD die Anwendung der Risikomanagement-Norm EN ISO 14971 [10], damit ein konformes Produkt entwickelt werden kann. Unter Anwendung dieser Norm wird es möglich, dass etwaige Risiken erst erkannt bzw. identifiziert, diese bewertet und gegebenenfalls Beherrschungsmaßnahmen eingeführt werden, um Risiken zu minimieren. Das Risikomanagement spielt somit im Zusammenhang mit den weiteren relevanten Normen eine zentrale Rolle, um qualitativ sowie sicherheitstechnisch konforme Produkte zu vermarkten. Eine Übersicht, welche diese zentrale Rolle verdeutlicht, wird in Abbildung 15 dargestellt.

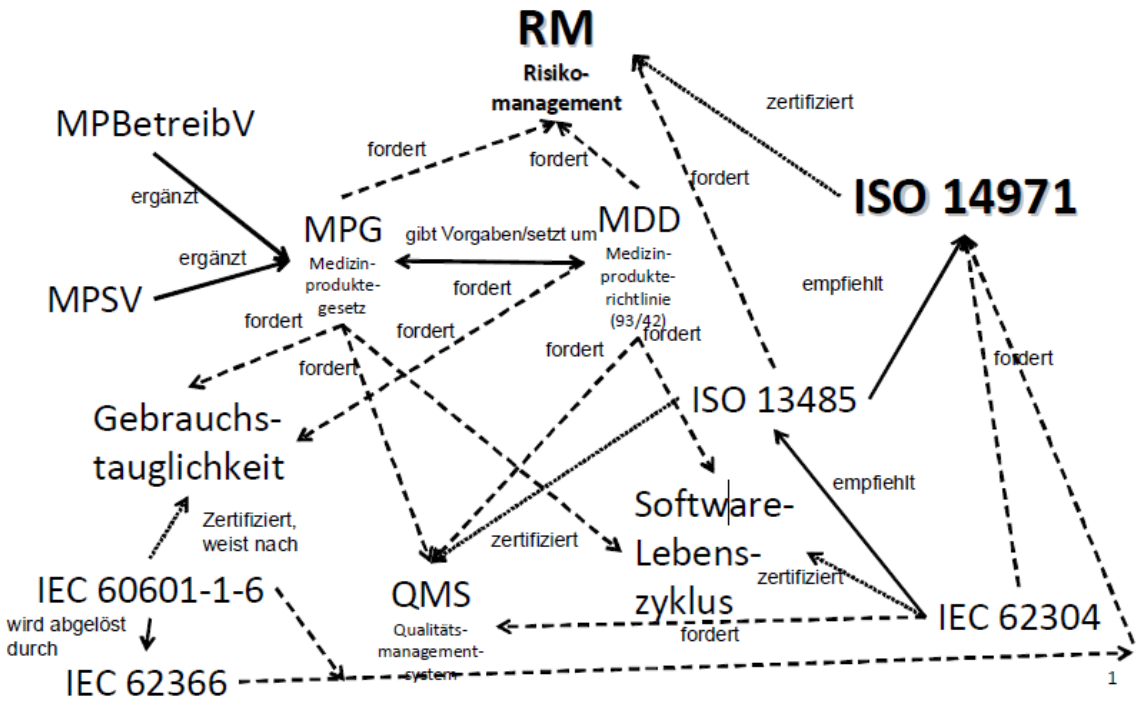


Abbildung 15: Übersicht der regulatorischen Verknüpfungen zum Risikomanagement [15]

5.2 Der Risikomanagement-Prozess

Die Dokumentation der Tätigkeiten rund um das Risikomanagement erfolgt im Rahmen des Qualitätsmanagements. In Bezug auf das Risikomanagement ist dies der Risikomanagement-Prozess, dessen Ziel es ist, alle Gefährdungen und damit verbundenen Risiken zu identifizieren, zu bewerten und gegebenfalls zu minimieren. So soll eine hohe Sicherheit hinsichtlich der Patienten, Anwender und Dritten erreicht werden. Ebenso sollen aber Risiken in Bezug auf die Umwelt oder Eigentum [17] über diesen Prozess behandelt werden. Die EN ISO 14971 beschreibt diesen Prozess, welcher über folgende Hauptelemente verfügt:

- *Risikoanalyse*
- *Risikobewertung*
- *Risikobeherrschung*
- *Informationen aus der Herstellung und der Herstellung nachgelagerten Phasen* [10]

Diese vier Hauptelemente werden in folgender Abbildung 16 zum Risikomanagementprozess zusammengeführt. Die Risikoanalyse und –bewertung werden zur Risikobeurteilung zusammengefasst. Das gesamte Risikomanagement umfasst dazu auch die Risikobeherrschung und die Tätigkeiten in der nachgelagerten Phase.

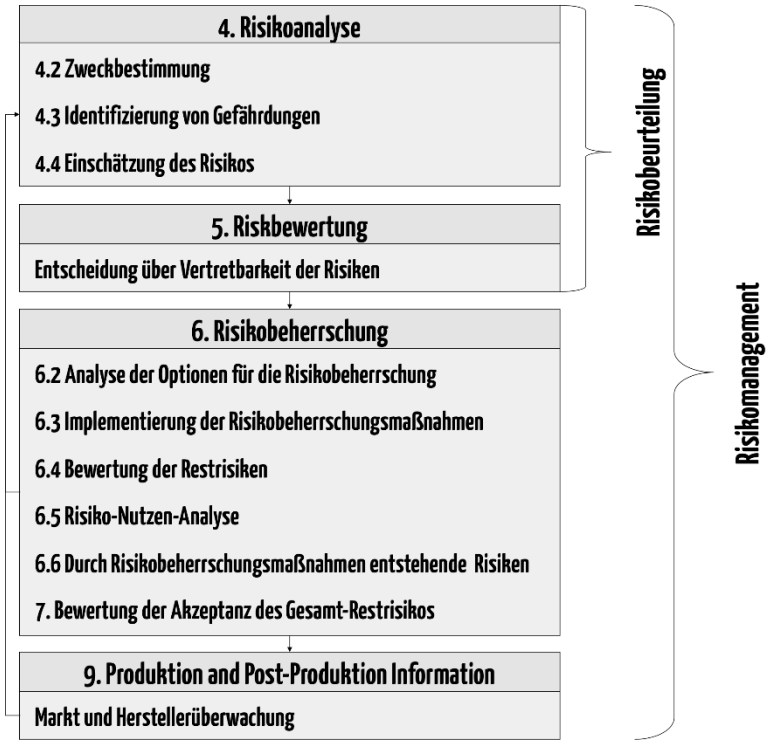


Abbildung 16: Die Hauptelemente des Risikomanagements im Risikomanagementprozess aus [20]

Neben der Etablierung dieses Risikomanagementprozesses sieht die EN ISO 14971 auch die Dokumentation bzw. Erstellung von weiteren Dokumenten betreffend des Risikomanagement vor.

Diese sind ein Risikomanagement-Plan, die Beschreibung der „Verantwortung der Leitung“ [10] betreffend des Risikomanagement, ein Nachweis der Qualifikation des Personals, welche das Risikomanagement durchführen sowie einen abschließenden

Risikomanagement-Bericht. Diese Dokumente werden in den Folgekapiteln näher betrachtet.

Im Zuge der Software-Entwicklung von *ilvi* wurde der Risikomanagementprozess (RM-Prozess) laut Abbildung 16 um diese Tätigkeiten erweitert, sodass sich ein Prozess ergibt, wie es ihn Abbildung 17 zeigt.

Der erste Schritt betrifft hierbei schon die oberste Leitung, welche eine Risikopolitik bzw. Risikoakzeptanzkriterien definieren muss. Dabei wird beschrieben, welche Risiken aus Sicht des Herstellers als akzeptabel eingestuft werden können und welche Risiken nicht akzeptabel sind. Diese Definitionen dienen als Grundlage zur Erstellung einer sog. Risikomatrix, können aber auch allgemein – nicht auf ein Produkt spezifiziert sein. In diesem Fall müssen die produktbezogenen Kriterien in der Risikomanagement-Akte enthalten sein.

In Folge dessen wird das Risikoteam gebildet, welches mit der Durchführung des Risikomanagements beauftragt wird. Die EN ISO 14971 beschreibt dabei in Kapitel 3.3 welche Anforderungen an dieses Personal gestellt werden. In Bezug auf Software, aber auch im Allgemeinen sollte das Risikomanagement niemals von einer Einzelperson durchgeführt werden. Für die korrekte Durchführung müssen Kenntnisse aus mehreren Disziplinen vorhanden sein. Daher benennt man ein Risikoteam, welches durch den Risikomanagementbeauftragen (RMB) geleitet wird. Durch eine Abdeckung von mehreren Disziplinen soll gewährleistet werden, dass keine Risiken ‚übersehen' werden. So soll das Risikoteam über Kenntnisse der SW-Erstellung (Programmierung), Softwarearchitektur, Softwaretesting, aber auch über den Gebrauch der Software und eben auch regulatorische Kenntnisse (vor allem im Sinne des Risikomanagements) verfügen [16]. Die Norm definiert die erforderlichen Kenntnisse auf folgende gebiete:

- *„wie das Medizinprodukt aufgebaut ist;*
- *wie das Medizinprodukt funktioniert;*
- *wie das Medizinprodukt hergestellt wird;*
- *wie das Medizinprodukt gegenwärtig verwendet wird;*
- *wie der Risikomanagement-Prozess anzuwenden ist."* [10]

Kann eine einzelne Person dieses Wissen nicht nachweisen, ist es naheliegend, dass mehre Personen am Risikomanagement beteiligt sein müssen. Idealerweise können diese Kenntnisse dokumentiert nachgewiesen werden.

Der nächste Schritt im RM-Prozess behandelt ein Hauptelement der EN ISO 14971, die Risikoanalyse im Sinne einer Gefährdungsanalyse. Eine Beschreibung des Unterschieds von Risiko und Gefährdung wird in einem Folgekapitel beschrieben. Dieser Schritt impliziert die Anwendung geeigneter Methoden, um die gegebenen Gefährdungen zu erkennen. Auch diese Methoden werden in Folge genauer betrachtet.

Nachdem Gefährdungen und die damit verbundenen Risiken identifiziert wurden, müssen diese bewertet werden, damit eine Beurteilung aufgrund der vorhin definierten Akzeptanzkriterien erfolgen kann. Anhand der bewerteten Risiken kann bzw. muss nun entschieden werden, ob und welche Risikobeherrschungsmaßnahmen getroffen werden müssen.

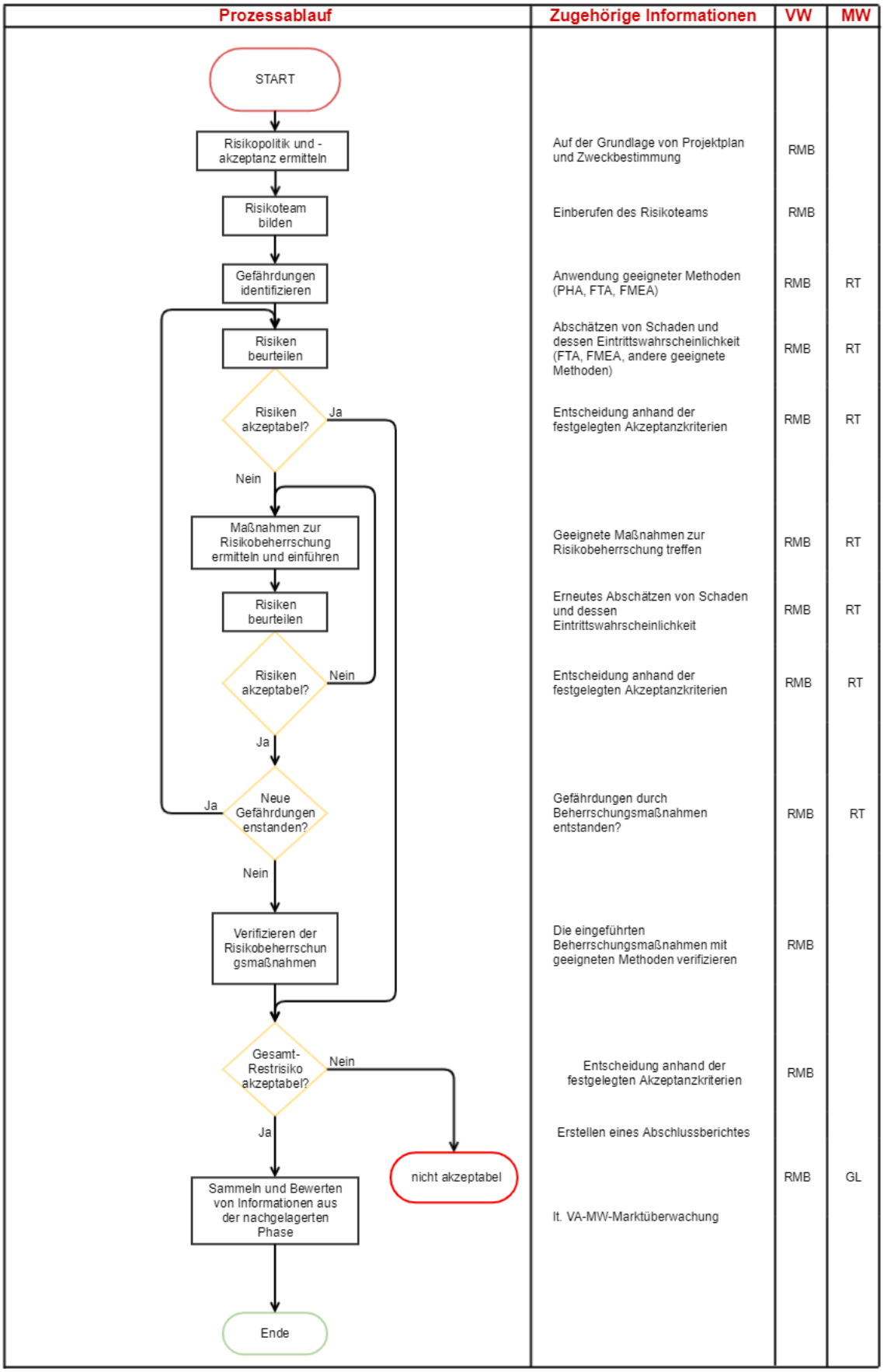


Abbildung 17: Beispiel eines Risikomanagementprozess zur Software-Entwicklung

Die gegebenenfalls eingeführten Beherrschungsmaßnahmen können wiederum neue Risiken beherbergen bzw. hervorrufen. Diese neuen Risiken bedürfen wiederum einer Bewertung nach den Akzeptanzkriterien.

Wurden Risikobeherrschungsmaßnahmen definiert, müssen diese auch implementiert und verifiziert werden. Dabei muss nachgewiesen werden, dass die Beherrschungsmaßnahmen schließlich wirklich implementiert und auch geeignet sind, das betreffende Risiko zu verringern.

Der letzte Schritt, welcher im Zuge der Entwicklung durchgeführt wird, ist die Bewertung des Gesamt-Restrisikos. Hierbei wird wieder anhand der Akzeptanzkriterien das resultierende Gesamtrisiko (nach der Durchführung von Beherrschungsmaßnahmen) bewertet und mit dem Nutzen des Produktes verglichen. Dabei soll der Nutzen naturgemäß dem Restrisiko überwiegen.

Der RM-Prozess endet aber nicht mit dem Ende der Entwicklung, sondern zieht sich über den gesamten Produkt-Lebenszyklus. So muss über die Dauer dessen Informationen aus der der Entwicklung nachgelagerten Phase in den RM-Prozess einfließen. Hier kann es zu Anpassungen der schon entdeckten Risiken kommen, oder es können daraus auch neue Risiken identifiziert werden. Die Informationen dazu kommen aus einer aktiven Informationseinholung bei den Anwendern, aus Reklamationen, Meldungen von Zulieferern, zudem können auch Änderungen von Normen und anderen regulatorischen Dokumenten eine Neubewertung von Risiken zur Folge haben.

Der RM-Prozess endet somit erst mit dem ‚Vom Markt nehmen' des letzten betreffenden Produktes.

5.3 Begriffe aus dem Risikomanagement

Wie schon vorhin beschrieben, behandelt das Risikomanagement die Erkennung und Minimierung von Risiken bei und nach der Entwicklung von Medizinprodukten. Um Klarheit über die darin verwendeten Begriffe zu schaffen, werden diese hier wie in der Norm beschrieben.

Schaden: Die physische Verletzung oder Schädigung der menschlichen Gesundheit oder Schädigung von Gütern oder der Umwelt [10].

Ein Schaden ist also als Resultat des Eintretens eines Risikos anzusehen.

Gefährdung: potentielle Schadensquelle [10].

Eine Gefährdung ist also gegeben, wenn durch Verkettung ungünstiger Ereignisse ein Schaden eintreten kann.

Gefährdungssituation: Umstände, unter denen Menschen, Güter oder die Umwelt einer oder mehreren Gefährdungen ausgesetzt sind [10].

Dabei kann die Kombination von ungünstigen Ereignissen, die einen Schaden zur Folge haben können, eine Gefährdungssituation darstellen.

Schweregrad: Maß der möglichen Auswirkung einer Gefährdung [10].

Dies kann z.B.: von einer ‚Unannehmlichkeit' bis hin zum Tod von Personen reichen.

Risiko: Kombination der Wahrscheinlichkeit des Auftretens eines Schadens und des Schweregrades dieses Schadens [10].

Ein Risiko besteht damit nicht allein aus einem aus einer Gefährdung resultierenden Schaden, sondern es muss auch die damit verbundene Eintrittswahrscheinlichkeit mit betrachtet werden.

Um den Zusammenhang zwischen diesen Begriffen besser darstellen zu können, zeigt Abbildung 18, wie es ausgehend von einer Gefährdung schließlich zu einem Risiko kommt. Dabei ist P1 die Wahrscheinlichkeit des Auftretens einer Gefährdungssituation, P2 die Wahrscheinlichkeit einer Gefährdungssituation, die zum Schaden führt [10].

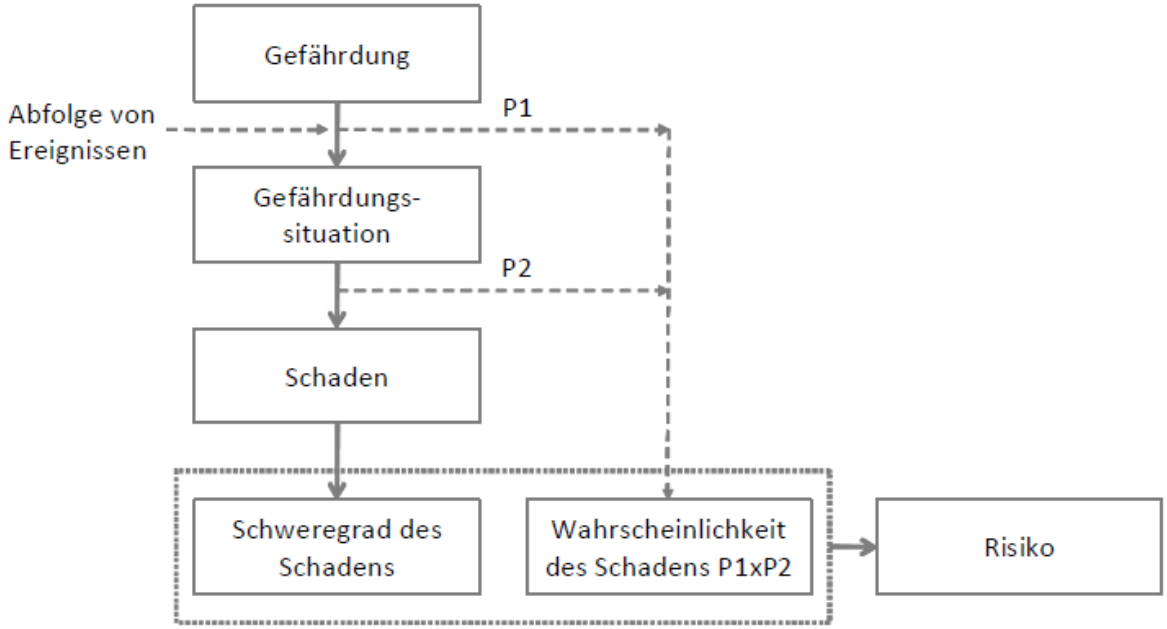


Abbildung 18: Zusammenhang zwischen den Begriffen des Risikomanagements aus [16]

5.4 Die Risikomanagement-Akte

Die Risikomanagement-Akte ist das zentrale Dokument, in welchem alle Tätigkeiten und Erkenntnisse bzw. Ergebnisse aus dem Risikomanagement aufgezeichnet und dokumentiert werden. Dabei müssen die nötigen Dokumente jedoch nicht direkt darin enthalten sein, sondern es kann darauf verwiesen werden. Um die gesamten Anforderungen der EN ISO 14971 abzubilden, muss die Risikomanagement-Akte folgende Dokumente bzw. Verweise darauf beinhalten. [16] schlägt dabei folgende Gliederung dieser Akte vor:

Kapitel der EN ISO 14971	Inhalt
3.1 RM-Prozess	Prozessdarstellung, ggf. Verweis auf das QMS
3.2 Verantwortung der Leitung	Verweis auf das QMH, Risikopolitik mit Risikoakzeptanzkriterien
3.3 Qualifikation des Personals	Schulungsnachweise bzw. Verweise darauf (QMS, Personal und Schulung)
3.4 Risikomanagementplan	Verweis auf das entsprechende Dokument
3.5 Risikomanagement-Akte	-
4.2 Zweckbestimmung	Verweis auf das Dokument oder Dokumente (Sicherheitsmerkmale gemäß Gebrauchstauglichkeitsprozess)
4.3 Gefährdungen	Liste der identifizierten Gefährdungen
4.4 Einschätzen von Risiken	Beurteilung der Eintrittswahrscheinlichkeit und des Schweregrades einer Gefährdung(-situation)
5 Risikobewertung	Bewertung, ob eine Beherrschungsmaßnahme erforderlich ist. Mit Bezug auf die Akzeptanzkriterien
6.2 und 6.3 Analyse und Umsetzung der Maßnahmen	Definition der Maßnahmen und Nachweis der Umsetzung
6.4 Analyse des Restrisikos	Beurteilung der Risiken nach Einführung der Beherrschungsmaßnahmen
6.5 Risiko-Nutzen-Analyse	Diskussion unter Beachtung der Akzeptanzkriterien
6.6 Neue Risiken durch Beherrschungsmaßnahmen	Behandlung der Risiken, welche durch Beherrschungsmaßnahmen hervorgerufen werden.
6.7 Vollständigkeit	Nachweis, dass alle Gefährdungssituationen beachtet wurden
7 Bewertung des Gesamt-Restrisikos	Unter Beachtung der Akzeptanzkriterien
8 Risikomanagement-Bericht	Abschließender Bericht, über die Tätigkeiten
9 Nachgelagerte Phase	Mit Verweisen auf entsprechende Dokumente und Verfahren.

Tabelle 6: Inhalte der Risikomanagement-Akte gemäß EN ISO 14971 nach [16].

5.5 Der Risikomanagement-Plan, Risikopolitik und Risikoakzeptanzkriterien

Die EN ISO 14971 fordert die Erstellung eines Risikomanagement-Plans [10]. Dabei kann dieser Plan als getrenntes Dokument von der Risikomanagement-Akte erstellt werden. Der Plan soll beschreiben, wie das Risikomanagement über den Produktlebenszyklus anzuwenden ist. Dabei kann auch auf weitere Verfahren bzw. Prozesse (z.B. Entwicklungsprozess, Gebrauchstauglichkeitsprozess) verwiesen werden, es soll aber auch beschrieben werden, wie hierbei das Risikomanagement angewandt wird. Vorausgesetzt wird auch, dass für jedes spezifische Produkt ein eigener Plan definiert wird. Ebenso muss der Plan die Verantwortlichkeiten in Bezug auf das Risikomanagement definierten (RMB und Risikoteam). Wie schon beschrieben, dienen die Risikoakzeptanzkriterien als Basis zur Bewertung von Risiken, welche ebenso im Risikomanagement-Plan festgehalten sind. Um die einzuführenden Beherrschungsmaßnahmen zu verifizieren, sind die dafür vorgesehenen Tätigkeiten auch in diesen Plan festzuhalten. Schließlich muss auch noch dargestellt werden, wie die Informationen aus der nachgelagerten Phase gewonnen werden. Dazu kann auch ein Verweis auf das entsprechende Verfahren genügen.

Der Risikomanagement-Plan zur Software-Entwicklung von *ilvi* beinhaltet eine Beschreibung, um welches Produkt es sich im Zuge der RM-Anwendung handelt. Hier *ilvi* in der Version 1.1. In Folge verweist der Plan auf die Durchführung des Risikomanagements nach der entsprechenden Verfahrensanweisung, wie sie im QMS dokumentiert ist. Des Weiteren werden die Rollen von Personen in Bezug auf das Risikomanagement definiert. Hier findet sich auch die Beschreibung der Verantwortung der obersten Leitung, sowie die Verantwortlichkeiten der anderen beteiligten Personen. Die Tätigkeiten des Risikomanagements werden als Meilensteine tabellarisch dargestellt und spiegeln den Produktlebenszyklus wider. Als wichtiger Punkt für das Risikomanagement werden hier auch die Risikoakzeptanzkriterien definiert und festgehalten. Dazu wird eine Risikobewertungsmatrix verwendet, wie sie in Abbildung 14 dargestellt ist. Bei Anwendung dieser Matrix wird es möglich, die jeweiligen Risiken zu bewerten, indem man die Schadenshöhe und die Eintrittswahrscheinlichkeit des Schadens kombiniert. Wie es zu dieser Bewertung kommt, wird in dem entsprechenden Kapitel dieser Arbeit erläutert.

Die EN ISO 14971 fordert eine Einteilung der Risiken in akzeptable und inakzeptable Risiken. Sie gibt dabei jedoch keine Vorgaben, wie diese Einteilung zu erfolgen hat. Jedoch sind bei inakzeptablen Risiken zwingend Beherrschungsmaßnahmen einzuführen, um diese auf ein akzeptables Niveau bringen zu können. Für *ilvi* wurde eine dritte Klasse an Risiken definiert, bei der sich der Hersteller entschieden hat, Beherrschungsmaßnahmen einzuführen, wenn diese als sinnvoll erachtet werden. In einer früheren (nicht mehr gültigen) Version der EN ISO 14971 war dies auch so beschrieben, und wird auch in der nun gültigen Version so abgebildet [17].

Ebenfalls im Risikomanagement-Plan werden die Tätigkeiten der Verifizierung von Beherrschungsmaßnahmen definiert. Diese sind hier Ergebnisse von System- und Integrationstest aus dem Software-Entwicklungsprozess sowie Ergebnisse aus Validierungen aus dem Gebrauchstauglichkeitsprozess.

Abbildung 19: Risikobewertungsmatrix für ilvi

Die in Abbildung 19 dargestellte Risikobewertungsmatrix spiegelt auch die Akzeptanzkriterien wieder, wie sie zur Entwicklung der Software *ilvi* definiert wurden. Dabei muss jedoch der Nutzen des Produktes beachtet werden. Es soll auch der Vorteil und der Nutzen des Produktes im Vergleich mit Alternativen zum Produkt oder bei Nichtanwendung des Produktes mit einfließen. Dieser Nutzen wird in der Risikomanagement-Akte im Kapitel ‚Risikopolitik' festgehalten und wird für *ilvi* wie folgt definiert. Hierbei werden auch die Systemgrenzen definiert, innerhalb derer das Risikomanagement durchgeführt wird.

„Das Produkt ilvi dient der (manuellen und automatischen) Erfassung und Archivierung von Vital- und Gesundheitswerten von Patienten in Gesundheitseinrichtungen unter Verwendung eines mobilen Handheld-Geräts. Um den Nutzen des Produktes beschreiben zu können, müssen vorher die möglichen Alternativen und derzeitigen Anwendungen zur Gesundheitswerterfassung betrachtet werden:

- Eine 'manuelle' Dokumentation auf einer Papier-Fieberkurve
- Die erfassten Vital- und Gesundheitswerte werden im Idealfall ohne Zwischenschritt (evtl. Erfassung auf 'Klebenotiz') in eine Papier-Fieberkurve eingetragen. Aus Datenschutzgründen geschieht dies jedoch meist im Anschluss der Erfassung. Es wurde beobachtet, dass die erfassten Werte oft auf Notizzetteln oder gar im Kopf 'dokumentiert' und erst im Pflegestützpunkt in die entsprechende Fieberkurve eingetragen werden.
- Eine 'manuelle' Erfassung der Werte mit anschließender digitaler Verarbeitung an einem PC
- Die Erfassung geschieht auf dem selben Weg wie oben beschrieben, jedoch findet eine elektronische Dokumentation statt.

- Eine 'manuelle' Erfassung mit direkter digitaler Verarbeitung an einem mobilen PC
- Die Dokumentation der Werte findet direkt bei der Erfassung statt. Verwendet werden dazu meist Laptops auf einem Gerätewagen mit kabelloser Anbindung an das Krankenhausinformationssystem (KIS).

Die angeführten Methoden zur Erfassung und Archivierung der Vital- und Gesundheitswerte werden in einem Großteil der Krankenanstalten verwendet bzw. wie beschrieben durchgeführt.

Im Vergleich zu diesen Methoden zeigt das Produkt ilvi folgende Vorteile bzw. folgenden Nutzen:

- Vermeidung von Patientenverwechslungen
    - Die Patienten werden durch die Identifikation via Barcode am Patientenarmband eindeutig zugeordnet.
- Vermeidung von 'Schlampigkeitsfehlern'
    - Die Vital- und Gesundheitswerte werden direkt am Gerät eingegeben und müssen nicht 'zwischendokumentiert' werden.
- Erfassung von Anwendern
    - Die Anwender werden durch Anmeldung via NFC-, QR-/Barcode oder über eine Passworteingabe (Tastatur) eindeutig zugeordnet.
- Direkte Archivierung von Vital- und Gesundheitswerten
    - Die gesammelten Daten werden gesammelt ohne Zwischenschritte an das KIS übertragen. Es sind keinerlei Nachdokumentationen notwendig.
- Automatische Erfassung von Medizinprodukten
    - Von Medizinprodukten, welche über eine entsprechende Funktionalität verfügen, können Messwerte automatisch erfasst werden. Dadurch können Ablese- und Eingabefehler vermieden werden.
- Warnhinweise bei Über- oder Unterschreitung von Grenzwerten
    - Der Benutzer erhält Informationen über eine mögliche Verschlechterung des Gesundheitszustandes des betreffenden Patienten.
- Plausibilitätsprüfung bei manueller Eingabe
    - Fehler bei der manuellen Eingabe werden durch Prüfung auf Plausibilität minimiert.
- Einfache Bedienung (GUI)
    - Durch intuitive und selbsterklärende Menüführung.

Somit bringt die Anwendung des Produkts ilvi im Vergleich zu den anderen Methoden oder bei Nichtanwendung den oben beschriebenen Nutzen für Patienten und Anwender.

Systemabgrenzung:
Wir analysieren im Folgenden Risiken, welche durch die Anwendung von ilvi entstehen können.
Wir betrachten dabei das System von der Erfassung der Werte bis zur Archivierung der Vital- und Gesundheitswerte im KIS bzw. in der elektronischen Fieberkurve über eine kabellose Anbindung. Wir definieren diese Systemgrenze, da auch Alternativen (s.o.) im Idealfall die selben Werte liefern und die Weiterverarbeitung bzw. Nutzung der Daten nicht mehr in unserem Einfluss stehen. „

Die nun definierte Systemgrenze ist in Hinblick auf das Risikomanagement und der Zweckbestimmun wichtig. Die Zweckbestimmung besagt, dass die übertragenen Werte die Therapie und die Diagnose des betreffenden Patienten unterstützen können. Wie diese Unterstützung erfolgt obliegt den Anwendern. Die ausgegebenen Warnungen bei Über- oder Unterschreitung von Vitalwert-Grenzwerten dienen ebenfalls nur der Unterstützung. Eine direkte Diagnose kann anhand der mit *ilvi* erfassten Werte nicht erfolgen, sondern bedarf einer weiteren Untersuchung des Patienten.

Um nun die in Abbildung 14 dargestellte Risikobewertungsmatrix erstellen zu können, müssen die Stufen der Eintrittswahrscheinlichkeiten und die Stufen der Schadenshöhe definiert werden. Sind diese Stufen definiert, kann eine Definition der Risikoakzeptanzkriterien erfolgen.

Auf der horizontalen Achse der Matrix wird der Schweregrad des möglichen Schadens aufgetragen. Dabei muss man den größtmöglich vorstellbaren Schaden, der eintreten könnte als die größte Stufe annehmen. [16] empfiehlt für eine einfachere Zuordnung der einzelnen Risiken eine ‚binäre' Schadensbeschreibung, also z.B. Eintritt des Todes: Ja, oder Nein. Die EN ISO 14971 wiederum erlaubt es dem Hersteller frei zu wählen, wie die Schweregrade beschrieben und definiert werden, sieht es jedoch als erforderlich, bei einer nicht aussagekräftigen Einstufung dies argumentativ zu begründen. Damit diese Begründung nicht nötig ist, wurden zur Entwicklung von *ilvi* folgende Stufen der Schadenshöhe gewählt, wie sie in Tabelle 7 gezeigt werden:

Nr.	Beschreibung	Definition	Beispiel
1	Unwesentlich	Keine Verletzung oder Schädigung	Wiederholung / Verzögerung der Untersuchung
2	Geringfügig	Nur leichte und/oder reversible Schädigung ohne ärztliche Intervention	Verzögerung einer Therapie / Behandlung mit leichter Auswirkung auf Gesundheit des Patienten
3	Ernst	Reversible Schädigung, welche eine ärztliche Intervention bedarf	Ärztliche Intervention nötig
4	Kritisch	Nicht vollständig reversible Schädigung oder lebensbedrohliche Schädigung	Aufnahme in Intensivstation nötig
5	Katastrophal	Ein oder mehrere Todesfälle	Tod

Tabelle 7: Schweregrade des Schadens für ilvi

Es wurde wie dargestellt eine Abstufung in 5 Schweregraden definiert.

Als höchste Stufe des Schadensausmaßes (Katastrophal) wurde der Tod des Patienten angenommen, wobei dies bei Anwendung von *ilvi* zwar unvorstellbar ist, jedoch durch unvorhersehbare Ereignisse eintreten könnte.

Die nächst-geringere Stufe (Kritisch) definiert den Schaden als eine irreversible Schädigung von Personen, welche in Folge z.B. eine Aufnahme in eine Intensivstation bedarf.

Die Stufe 3 (Ernst) beschreibt Schäden, welche zwar reversibel sind, also keine bleibende Beeinträchtigung zur Folge hat, jedoch einer ärztlichen Intervention bedürfen.

Stufe 2 (Geringfügig) definiert Schäden, die zu einer Schädigung führen, welche ohne ärztliche Intervention reversibel sind. Dazu zählt aber beispielsweise auch eine Verzögerung der geplanten Therapie aufgrund der Anwendung von *ilvi*.

Als geringsten Schaden (Unwesentlich) werden Beeinträchtigungen definiert, die keine direkte Schädigung der Gesundheit zur Folge haben und etwa nur eine Wiederholung oder Verzögerung einer Untersuchung bedürfen.

Um die Risikobewertungsmatrix zu vervollständigen muss nun aber auch die vertikale Achse definiert werden, welche die Eintrittswahrscheinlichkeiten von Schäden beschreibt. Vor allem bei Software ist diese Definition nicht so einfach vorzunehmen, wie die Definition der Schweregrade. Als Basis für die Definition der Eintrittswahrscheinlichkeiten sollte man mehrere Faktoren beachten, wie es die EN ISO 14971 im Anhand D vorgibt:

- Wie oft wird das Produkt verwendet?
- Wie hoch ist die vorgesehene Produktlebensdauer?
- Was sind die Patientenpopulation und die Anwenderpopulation?
- Wie hoch ist die Anzahl der Patienten und Anwender?
- Wie lange erfolgt die Exposition der Patienten und Anwender? [10]

Dazu wurden folgende Annahmen für *ilvi* festgelegt:

- Mittlere Anzahl der im Markt befindlichen Produkte: 1000 Stück
- Mittlere zu erwartende Lebensdauer eines Produkts: 5 Jahre
- Mittlere Anzahl der Anwendungen des Produkts an Patienten: 20 Anwendungen pro Tag

Daraus ergeben sich folgende Daten:

Bei 20 vorgesehenen Anwendungen von *ilvi* pro Tag ergeben sich 7300 Anwendungen pro Jahr. Über die erwartete Lebensdauer ergeben sich also 36500 Anwendungen pro Produkt (pro *ilvi*).

Auf die vorgesehenen durchschnittlichen 1000 Stück *ilvi* im Markt ergeben sich in einer ‚Lebensdauerperiode' (5 Jahre) 36500000 Anwendungen von *ilvi*.

Aus diesen Daten der Anwendungshäufigkeit kann man nun quantitative Aussagen über Eintrittswahrscheinlichkeiten treffen, wie sie in Tabelle 8 festgehalten sind. Hierbei wird als die geringste Eintrittswahrscheinlichkeit jene angenommen, dass ein Schaden während der Lebensdauer aller Produkte nicht eintritt, also die Wahrscheinlichkeit geringer ist, als dass der Schaden innerhalb von 36500000 Anwendungen eintritt. Daher ergibt sich die Eintrittswahrscheinlichkeit eines Schadens, der ‚Unvorstellbar' ist von $p \leq 10^{-8}$.

‚Seltene Ereignisse' treten dementsprechend häufiger ein; nämlich ein- bis zweimal während der Lebensdauer des Produktes, also ein bis zweimal unter 36500000 Anwendungen.

‚Gelegentlich' wird definiert als der Eintritt eines Schadens, der unregelmäßig bis mehrfach pro Jahr stattfindet.

Als ‚Wahrscheinlich' gilt die Eintrittswahrscheinlichkeit eines Schadens, wenn er bei bestimmungsgemäßem Gebrauch öfters als einmal pro 1000 Anwendungen eintritt.

Und als ‚häufig' wird die Wahrscheinlichkeit beschrieben, wenn ein Risiko bzw. ein Schaden regelmäßig pro Anwendung eintreten kann.

Nr.	Beschreibung	Häufigkeit	Eintrittswahrscheinlichkeit
5	Häufig	Ein- oder mehrmals pro Anwendung	$p < 1$
4	Wahrscheinlich	Kann bei bestimmungsgemäßen Gebrauch auftreten	$10^{-3} < p \leq 1$
3	Gelegentlich	Unregelmäßig mehrfach pro Jahr	$10^{-6} < p \leq 10^{-3}$
2	Selten	Ein- bis mehrmals während Lebensdauer des Medizinprodukts	$10^{-8} < p \leq 10^{-6}$
1	Unvorstellbar	Nicht während Lebensdauer des Medizinprodukts	$p \leq 10^{-8}$

Tabelle 8: Eintrittswahrscheinlichkeiten von Schäden bei ilvi

Mit den nun definierten Stufen der Schweregrade und der Eintrittswahrscheinlichkeiten wird die Risikobewertungsmatrix wie in Abbildung 19 erstellt. Damit werden die in Folge identifizierten und bewerteten Risiken in akzeptable und inakzeptable Risiken eingeteilt. Die Risiken der Klasse I sind als akzeptabel anzusehen, die der Klasse III als prinzipiell inakzeptabel. Es wurde aber auch noch eine Klasse II an Risiken definiert, die nach dem ALARP-Prinzip zu behandeln sind (as low as reasonable possible). Dies sieht die EN ISO 14971 in der aktuellen Version nicht vor. Jedoch wurde im Zuge der Entwicklung von *ilvi* entschieden, diese Klasse einzuführen, um dabei gegebenenfalls Risiken durch geeignete Beherrschungsmaßnahmen trotzdem zu minimieren, obwohl sie als akzeptabel gelten würden. Das bedeutet, Risiken der Klasse I und der Klasse II sind als akzeptabel anzusehen, Risiken der Klasse III als inakzeptabel. Sollte es jedoch möglich sein, auch akzeptable Risiken durch Beherrschungsmaßnahmen zu reduzieren, wird dies bei Klasse I Risiken in Erwägung gezogen, bei Klasse II Risiken wird dies durchgeführt. Dies sind auch die Akzeptanzkriterien, wie sie in der Risikomanagement-Akte festgehalten sind. Zu beachten ist hierbei auch, dass auf die Wahl der Akzeptanzkriterien der Nutzen des Produktes berücksichtigt werden muss. Die Beschreibung dieses Nutzens im Vergleich zu alternativen Methoden wurde schon beschrieben.

6 Risiko- und Gefährdungsanalyse

Die Risiko- und Gefährdungsanalyse ist die erste ‚operative' Tätigkeit im Risikomanagement-Prozess. Hier werden mögliche Gefährdungen identifiziert, die durch das Produkt selbst bzw. durch dessen Anwendung entstehen können. Um erste Gefährdungen zu erkennen, bedient man sich der Zweckbestimmung des Produktes. Zusätzlich muss man hierbei auch den vorhersehbaren Missbrauch des Produkts beachten. Um Gefährdungen zu identifizieren, die ihre Ursache in der Verwendung des Produktes haben, muss man darauf achten, dass erst eine Gefährdung in Verbindung mit einer auslösenden Ursache zu einer Gefährdungssituation führt. „*Medizinprodukte verursachen einen Schaden nur dann, wenn eine Abfolge von Ereignissen eintritt, die eine Gefährdungssituation hervor ruft, und die dann einen Schaden bewirken oder zu diesen führen könnte. Eine Abfolge von Ereignissen schließt sowohl ein einzelnes Ereignis als auch eine Kombination von Ereignissen ein. Eine Gefährdungssituation tritt ein, wenn Personen, Güter oder die Umwelt einer Gefährdung ausgesetzt sind*. [10] Anhang D S.40." In Abbildung 20 wird diese Abfolge speziell für Software dargestellt.

Abbildung 20: Ereignisabfolge von Softwarefehler zum Schaden nach [16]

Die Gefährdungsanalyse dient in erster Linie, um die oben genannten Gefährdungen und Gefährdungssituationen zu erkennen. Eine Bewertung der Gefährdungen, damit es zu einem Risiko (Kombination aus Schaden und Eintrittswahrscheinlichkeit) kommt, erfolgt in einem weiteren Schritt, der Risikobewertung.

6.1 Methoden zur Identifizierung von Gefährdungen und Risiken

Um die Gefährdungen für ein Produkt zu erkennen, gibt es verschiedene Methoden. Am Beginn der Entwicklung steht sinnvollerweise die Zweckbestimmung des Produktes. Anhand dieser Informationen ist es nicht möglich eine beliebige Methode zur Risikoanalyse anzuwenden. Sinnvollerweise kann man in diesem Entwicklungsstadium Checklisten, geeignete und zielgerichtete Fragestellungen oder eine sogenannte ‚preliminary hazard analysis'(PHA) anwenden. Durch diese Methoden wird es möglich, Gefährdungen zu identifizieren, die aus der grundlegenden Funktion und der Anwendung des Produktes entstehen können.

6.2 Checklisten

Als einfache und ‚ressourcenschonende' Methode zur Findung erster Gefährdungen eignen sich Checklisten. In Anhang C der EN ISO 14971 werden für eine solche initiale Gefährdungsanalyse geeignete Fragen aufgelistet, anhand derer man auf Gefährdungen vom Produkt schließen kann. Für *ilvi* können diese Fragen wie in Tabelle 9 beschrieben beantwortet werden. Fragestellungen, die nicht auf *ilvi* zutreffen, werden hier nicht dargestellt.

Absatz in EN ISO 14971	Beantwortung bzw. Kommentar
C.2.1 Welches ist die Zweckbestimmung und wie soll das Medizinprodukt angewendet werden? Zu den Faktoren, die berücksichtigt werden sollten, zählen: Welches ist die Rolle des Medizinprodukts hinsichtlich: der Erkennung, Verhütung, Überwachung, Behandlung oder Linderung einer Krankheit; der Kompensierung von Verletzungen oder Behinderungen oder des Ersatzes oder der Veränderung des anatomischen Aufbaus oder der Empfängnisregelung? Welches sind die Indikationen für die Anwendung (z. B. die Patientenpopulation)? Ist das Medizinprodukt lebenserhaltend oder lebensunterstützend? Ist im Fall des Versagens des Medizinprodukts ein spezielles Eingreifen erforderlich?	Erfassung von Vital- und Gesundheitswerten von Patienten Unterstützung zur Diagnose Bei Versagen des MP müssen Daten manuell im Archiv abgelegt werden oder eine andere Alternativmethode angewandt werden.
C.2.3 Ist es vorgesehen, dass das Medizinprodukt mit dem Patienten oder anderen Personen in Berührung kommt? Zu den Faktoren, die berücksichtigt werden sollten, zählen der vorgesehene Kontakt, d. h. Oberflächenkontakt, invasiver Kontakt oder Implantation sowie für jeden Kontakt dessen Dauer und Häufigkeit.	Nein*, ilvi* dient nur zur Erfassung von Vitalparametern. Im bestimmungsgemäßen Gebrauch kommt *ilvi* nicht mit dem Patienten in Berührung. Die Messung der Parameter wird mit geeigneten Messgeräten durchgeführt. Auch
C.2.4 Welche Werkstoffe oder Bauteile werden mit dem Medizinprodukt verwendet werden zusammen mit dem Medizinprodukt gebraucht oder kommen in Berührung mit ihm? Zu den Faktoren, die berücksichtigt werden sollten, zählen: die Verträglichkeit mit Substanzen, die von Bedeutung sind; die Verträglichkeit mit Geweben oder Körperflüssigkeiten; und ob sicherheitsrelevante Eigenschaften bekannt sind; wird das Produkt unter Verwendung von Materialien tierischen Ursprungs hergestellt?	Die verwendete Hardware ist ein mobile Touch-Computer (Handheld). Ein bedenklicher Werkstoff kommt hier nicht zur Anwendung.
C.2.9 Soll das Medizinprodukt als Routinemaßnahme durch den Anwender gereinigt und desinfiziert werden? Zu den Faktoren, die berücksichtigt werden sollten, zählen die Arten der zu verwendenden Reinigungs-	Nein, bei ersichtlicher Verschmutzung kann eine Oberflächenreinigung des Handhelds nach den Herstellerangaben dessen erfolgen.

und Desinfektionsmittel und jegliche Begrenzung der Anzahl der Reinigungszyklen. Das Design des Medizinprodukts kann die Wirksamkeit der Routinereinigung und -desinfektion beeinflussen. Zusätzlich sollten die Auswirkungen von Reinigungs- und Desinfektionsmitteln auf die Sicherheit oder Leistung des Produkts berücksichtigt werden.	
C.2.11 Werden Messungen vorgenommen? Zu den Faktoren, die berücksichtigt werden sollten, zählen die gemessenen Variablen und die Genauigkeit und Präzision der Messergebnisse.	Nein! Es werden nur bereits von anderen Messgeräten gemessene Daten erfasst und an ein KIS weitergeleitet.
C.2.12 Liefert das Medizinprodukt interpretierende Aussagen? Zu den Faktoren, die berücksichtigt werden sollten, zählt, ob das Medizinprodukt Schlussfolgerungen aus Eingabedaten oder erfassten Daten darbietet, die hierfür verwendeten Algorithmen und die Vertrauensbereiche. Besonders beachtet werden sollten unbeabsichtigte Anwendungen von Daten oder Algorithmen.	Nein. Es werden Anzeigen ausgegeben, die Hinweise auf ein Unter- oder Überschreiten von Grenzwerten geben. Eine direkte Interpretation erfolgt nicht.
C.2.13 Ist das Medizinprodukt für die Verwendung mit anderen Medizinprodukten, Medikamenten oder sonstiger Medizintechnik vorgesehen? Zu den Faktoren, die berücksichtigt werden sollten, zählen die Identifizierung anderer Medizinprodukte, der Medikamente oder sonstigen Produkte, die beteiligt sein können, und die möglichen Probleme, die mit solchen Wechselwirkungen verbunden sein können, wie auch die Einhaltung der Therapie durch den Patienten.	Ja. Es werden Messdaten (Vitalparameter) von anderen Medizinprodukten an *ilvi* übergeben, um diese anzuzeigen und ins Archiv weiterzuleiten.
C.2.15 Ist das Medizinprodukt gegen Umwelteinflüsse empfindlich? Zu den Faktoren, die berücksichtigt werden sollten, zählen die Betriebs-, Transport- und Lagerbedingungen. Dazu gehören Licht, Temperatur, Schwingungen, Auslaufen, Empfindlichkeit gegenüber Schwankungen in der Stromversorgung und Kühlung sowie elektromagnetische Interferenzen.	Verwendung bei Raumtemperatur und standardmäßigen Umgebung innerhalb eines Krankenzimmers. Limitierender Faktor ist hier die Verwendung des Handheld-Computer.
C.2.16 Beeinflusst das Medizinprodukt die Umwelt? Zu den Faktoren, die berücksichtigt werden sollten, zählen: die Auswirkungen auf die Strom- und Kühlmittelversorgung; die Abgabe toxischer Substanzen; die Erzeugung elektromagnetischer Störungen.	Ja, es kommen kabellose Kommunikationsprotokolle zum Einsatz. Dabei ist auf die Einhaltung der geltenden EMV-Standards zu achten. (beim Handheld-Computer)

C.2.18 Ist Wartung oder Kalibrierung erforderlich? Zu den Faktoren, die berücksichtigt werden sollten, zählen: ob die Wartung oder Kalibrierung durch den Bediener, den Anwender oder einen Fachmann durchzuführen ist; sind für die richtige Wartung oder Kalibrierung besondere Substanzen oder Werkzeuge erforderlich?	Nein, da keine Messung stattfindet.
C.2.19 Enthält das Medizinprodukt Software? Zu den Faktoren, die berücksichtigt werden sollten, zählt, ob das Installieren, die Verifizierung, die Änderung oder der Austausch der Software durch den Bediener, den Anwender oder einen Fachmann vorgesehen ist.	Ja, ilvi ist eine Software, welche auf einem Handheldgerät läuft. (Softwaresystem)
C.2.23 Was bestimmt die Lebensdauer des Medizinprodukts? Zu den Faktoren, die berücksichtigt werden sollten, zählen die Alterung und die Entleerung von Batterien.	Der Akku/die Batterie des Handhelds.
C.2.25 Ist eine sichere Außerbetriebnahme oder Entsorgung des Medizinprodukts erforderlich? Zu den Faktoren, die berücksichtigt werden sollten, zählen die Abfallprodukte, die bei der Entsorgung des Medizinprodukts selbst entstehen. Enthält es zum Beispiel toxische oder gefährdende Substanzen oder sind die Werkstoffe recycelbar?	Ja, es sind die Angaben des Handheld-Herstellers zu beachten.
C.2.26 Erfordert die Installierung des Medizinprodukts eine Spezialausbildung oder spezielle Fertigkeiten? Zu den Faktoren, die berücksichtigt werden sollten, zählen die Neuheit des Medizinprodukts und die wahrscheinlichen Fertigkeiten und Ausbildungen der Person, die das Medizinprodukt installiert.	Ja, Installation der Software erfolgt ausschließlich durch den Hersteller oder durch den Hersteller autorisierte Personen.
C.2.27 Wie werden die Angaben über eine sichere Verwendung zur Verfügung gestellt? Zu den Faktoren, die berücksichtigt werden sollten, zählen: ob die Angaben dem Endanwender direkt geliefert werden oder ob dritte Seiten wie Installierer, Pflegepersonen, Fachkräfte des Gesundheitswesens oder Apotheker einbezogen werden und ob dies Auswirkungen auf die erforderliche Ausbildung hat; die Inbetriebnahme und Übergabe an den Endanwender und ob es wahrscheinlich bzw.	Ja, Einschulung des Personals Gebrauchsanweisung, geeignete Gebrauchstauglichkeit.

möglich ist, dass die Installation durch Personen ohne die erforderlichen Fertigkeiten durchgeführt werden kann; ob, auf der Grundlage der erwarteten Lebensdauer des Produkts, eine erneute Ausbildung oder erneute Zertifizierung von Bedienern oder Wartungspersonal erforderlich wäre.	Ja, Einschulung des Personals Gebrauchsanweisung, geeignete Gebrauchstauglichkeit.
C.2.29 Hängt die erfolgreiche Anwendung des Medizinprodukts entscheidend von menschlichen Faktoren wie der Schnittstelle für den Anwender ab? **C.2.29.1 Können die Gestaltungsmerkmale der Schnittstelle zum Anwender zu den Fehlern bei der Anwendung beitragen?** Zu den Faktoren, die berücksichtigt werden sollten, zählt die Gestaltung der Schnittstelle zum Anwender, die zu Fehlern bei der Anwendung beitragen kann. Zu Beispielen der Gestaltung der Schnittstelle gehören Stellteile und Anzeiger, verwendete Symbole, die ergonomische Gestaltung, die physische Gestaltung, die Hierarchie der Betriebsoperationen, die Menüs für softwaregesteuerte Geräte, die gute Sichtbarkeit von Warnvorrichtungen, die gute Hörbarkeit akustischer Warnsignale und eine genormte Farbkodierung. Siehe IEC 60601-1-6 [25] zu einer zusätzlichen Anleitung zur Gebrauchstauglichkeit und IEC 60601-1-8 [26] zu einer Anleitung zu Alarmeinrichtungen.	Ja. Eine einfache und leicht verständliche Bedienung grafische und farbliche Darstellung, große Bedienelemente sollen Bedienfehler verhindern.
C.2.29.4 Hat das Medizinprodukt eine Schnittstelle für die Steuerung? Zu den Faktoren, die berücksichtigt werden sollten, zählen die räumliche Gestaltung, die Kodierung, die Gruppierung der Bedienelemente, die Lageanordnung, die Modi der Rückmeldung, Fehlbedienungsmöglichkeiten, Versehen des Bedieners, die Differenzierbarkeit der Steuerung, gute Sichtbarkeit, die Richtungen von Einschaltung oder Umschaltung sowie ob die Steuerungen stufenlos oder schrittweise sind und die Umkehrbarkeit von Einstellungen oder Schaltungen.	Nein, es erfolgt keine Steuerung über ilvi.
C.2.29.5 Zeigt das Medizinprodukt Informationen an? Zu den Faktoren, die berücksichtigt werden sollten, zählen die gute Sichtbarkeit in unterschiedlichen Umgebungen, die räumliche Anordnung, die Sehfähigkeiten des Anwenders, die Anwenderpopulation sowie die Sichtperspektive, die Klarheit der dargebotenen Angaben, Angabe der Einheiten, Farbkodierung und die Zugänglichkeit zu entscheidenden Angaben	Ja. Dazu zählen Partienteninformationen, Anwenderinformationen, erfasste oder manuell eingegebenen Vitalparameter, Fotodokumentation.

C.2.29.6 Wird das Medizinprodukt durch ein Menü gesteuert? Zu den Faktoren, die berücksichtigt werden sollten, zählen die Komplexität und die Anzahl der Schichten, die Statusanzeige, die räumliche Anordnung der Einstellungen, das Navigationsverfahren, die Anzahl der Schritte je Bedienhandlung, die Klarheit der Sequenzen und Probleme der Speicherung sowie die Wichtigkeit der Steuerfunktion im Verhältnis zu ihrer Zugänglichkeit und die Auswirkungen von Abweichungen von festgelegten Bedienungsverfahren.	Ja. Es ist dabei auf eine einfache und gebrauchstaugliche Menüführung zu achten.
C.2.29.7 Wird das Medizinprodukt durch Personen mit besonderen Bedürfnissen angewendet? Zu den Faktoren, die berücksichtigt werden sollten, zählen die Anwender, deren geistige und körperliche Fähigkeiten, deren Fertigkeiten, ergonomische Gesichtspunkte, die Umgebung bei der Anwendung, Anforderungen an die Installation und die Fähigkeit des Patienten, die Anwendung des Medizinprodukts zu steuern oder zu beeinflussen. Besondere Beachtung sollten Anwender mit besonderen Bedürfnissen finden wie Behinderte. Zu ihren besonderen Bedürfnissen könnte die Unterstützung durch eine andere Person gehören, die die Anwendung eines Medizinprodukts ermöglicht. Ist das Medizinprodukt zur Anwendung durch Personen mit unterschiedlichen Graden der Fertigkeiten und unterschiedlichem kulturellem Hintergrund vorgesehen?	Nein, eine Anwendung erfolgt nur im professionellen Bereich durch Pflegepersonal oder Ärzte.
C.2.29.8 Kann die Schnittstelle zum Anwender verwendet werden, um Tätigkeiten des Anwenders einzuleiten? Zu den Faktoren, die berücksichtigt werden sollten, zählt die Möglichkeit der Einleitung einer geplanten Tätigkeit des Anwenders, um in einen gesteuerten Betriebsmodus zu gelangen, der die Risiken für den Patienten erhöht und bei dem der Anwender sich dieses Zustands bewusst sein muss.	Ja, gegebenfalls muss eine Messung an einem Medizinprodukt gestartet werden oder eine Kommunikation mit dem Patienten stattfinden. Ebenso muss der Anwender die Daten an das KIS ‚absenden'.
C.2.30 Wird beim Medizinprodukt ein Alarmsystem verwendet? Zu den Faktoren, die berücksichtigt werden sollten, zählen das Risiko von Fehlalarmen, ausfallenden Alarmen, nicht angeschlossenen Alarmsystemen, unzuverlässiger externer Alarmsysteme und die Verständnismöglichkeit für das medizinische Personal, wie das Alarmsystem funktioniert. Eine Anleitung zu Alarmsystemen findet sich in IEC 60601-1-8 [26].	Nein, duch ilvi erfolgt keine kontinuierliche Überwachung und keine Alarmierung. Die erfassten Parameter werden nur auf Über- oder Unterschreiten von Grenzwerten geprüft, und das Ergebnis ausgegeben.

C.2.31 Auf welche Weise(n) könnte das Medizinprodukt vorsätzlich falsch angewendet werden? Zu den Faktoren, die berücksichtigt werden sollten, zählen die falsche Verwendung von Anschlüssen, das Außerbetriebsetzen von sicherheitsbezogenen Merkmalen oder Alarmen und die Vernachlässigung der vom Hersteller empfohlenen Wartung.	Absichtlich Falsche Eingabe von Daten durch Benutzer, Absichtliche Patientenverwechslung Hacking über eine Schnittstelle.
C.2.32 Speichert das Medizinprodukt Daten, die für die Versorgung des Patienten entscheidend sind? Zu den Faktoren, die berücksichtigt werden sollten, zählen die Auswirkungen veränderter oder verfälschter Daten.	Nein, es erfolgt nur eine Zwischenspeicherung der Daten und anschließende Weiterleitung an ein KIS. Diese Daten sind in diesem Zusammenhang nicht entscheidend für die Versorgung des Patienten.
C.2.33 Ist das Medizinprodukt als ortsbeweglich oder tragbar vorgesehen? Zu den Faktoren, die berücksichtigt werden sollten, zählen die erforderlichen Griffe, Handgriffe, Räder und Bremsen, die mechanische Stabilität und Dauerhaftigkeit.	ilvi läuft auf einem tragbarem Handheldgerät

Tabelle 9: Checkliste aus der EN ISO 14971 [10] für ilvi

6.3 PHA – preliminary hazard analysis

Da diese Checkliste aber nicht konkret auf ein bestimmtes Produkt Fragestellungen vorgibt, ist es sinnvoll eine anschließende PHA gezielt auf die Funktionen des Produktes durchzuführen. Dieser Methode liegt die Zweckbestimmung und andere bis dahin bekannte Funktionen des Produktes zu Grunde. Ziel der PHA ist es die Gefährdungen ausgehend der Zweckbestimmung zu identifizieren, dabei ist es aber nicht möglich, eine Bewertung der Gefährdungen bzw. Risiken durchzuführen [18]. Die PHA ist eine einfache, induktive Methode, mit welcher man auch unter geringer Kenntnis von Details mögliche Gefährdungen erkennen kann. Hierzu betrachtet man folgende Merkmale:

- Verwendete Materialen (Biokompatibilität – trifft auf *ilvi* nicht zu)
- Eingesetzte Hardware
- Betriebsumgebung
- Auslegung / Zweckbestimmung
- Schnittstellen (für *ilvi* Schnittstellen zum Anwender und interne Systemschnittstellen)

Um nun auf Gefährdungen zu kommen, kann bzw. muss man wiederum weitere Tools verwenden, um diese Tätigkeiten vor allem im Risikoteam zu erleichtern.

Dazu zählt beispielsweise das Brainstorming oder eine strukturierte Befragung durch den Teamleiter. Beim Brainstorming unterscheidet man ein formales und ein informales Brainstorming, wobei sich diese zwei Methoden im Vorgehen unterscheiden. Formales Brainstorming ist eher strukturiert, und dient einer gezielten Ergebnisfindung,

informales Brainstorming ist eher unstrukturiert und hat meist einen ad-hoc Charakter [18]. Für eine gezielte Gefährdungsanalyse soll, wenn möglich ein formales Brainstorming durchgeführt werden, bei welchem die Teammitglieder über die Ziele informiert sind, und sich vorab über den Inhalt des Treffens einig sind.

Eine weitere unterstützende Methode, um ein Ergebnis im Sinne einer PHA zu erhalten ist eine ‚Strukturierte Befragung' durch den Moderator / Teamleiter. Diese Methode unterscheidet sich von der vorgenannten Methode darin, dass es zu einer Befragung durch den Teamleiter in Einzelgesprächen kommt. Dabei sind die gestellten Fragen sinnvollerweise gezielt auf einen entsprechenden Fokus, z.B.: Gefährdungen aus der verwendeten Hardware, über die verwendete Betriebsumgebung oder des verwendeten Betriebssystems. Dabei ist aber auch zu achten, dass der Befragte Wissen darüber mitbringt.

Die Ergebnisse dieser Methoden werden in einer Tabelle zusammengefasst und in der RM-Akte abgelegt. Für *ilvi* wurden mittels der PHA folgende Gefährdungen identifiziert, wie sie in Tabelle 11 aufgelistet sind. Dabei wurden die grundlegenden Funktionen und Informationen aus der Zweckbestimmung betrachtet.

Um das Risikomanagement zielführend weiter durchführen zu können, ist es naheliegend, die größtmöglichen Schäden zu finden, die durch das System hervorgerufen werden können. Es ist dabei zu beachten, dass *ilvi* aufgrund der Eigenschaft als Software, keinen direkten Schaden erzeugen kann. Es muss immer die Ursachenkette wie in Abbildung 15 beachtet werden. Somit wird für *ilvi* ‚nur' der direkte Schaden betrachtet, da der mögliche Folgeschaden außerhalb der Systemgrenzen stattfindet. Zu effektiveren Behandlung der Gefährdungen in Folge der Risikoanalyse und -bewertung wird dieser aber aufgezeigt.

In weiterer Folge müssen aber auch die Ursachen (z.B. Fehler in Software, vgl. Abb. 20) die zu den identifizierten Gefährdungen führen können bekannt sein. Um diese Ursachen zu erkennen ist es aber auch notwendig, detaillierte Kenntnisse über das zu entwickelnde Produkte zu haben. Diese Kenntnisse kommen wiederum aus Ergebnissen des Entwicklungsprozesses oder auch aus Ergebnissen des Gebrauchstauglichkeitsprozesses.

6.4 FTA – failure tree analysis

Eine Methode, um die Ursachen granularer zu erkennen, ist die Fehlerbaumanalyse (FTA – Fault Tree Analysis). Mittels dieser Methode wird es möglich, die ursächlichen Fehler zu identifizieren, welche eine Schadensfolge bewirken. Die FTA ist eine grafische ‚Top-Down' Methode. Es werden von einem Schadensereignis (z.B. fehlerhafte Daten im KIS) die Ursachen, welche zu diesem Schaden führen, dargestellt. Es ist dabei nicht nötig, den betrachteten Umfang, der analysiert werden soll, zu begrenzen. Das Ergebnis einer FTA kann somit zu Gefährdungsursachen führen, die mehrere Bereiche miteinschließen. Bei *ilvi* ist dies auch naheliegend, dass z.B.: ‚fehlerhaften Daten im KIS' Ursachen im Gebrauch (Gebrauchstauglichkeit) als auch in der Software selbst (Softwarekomponenten, Softwarearchitektur) haben.

Die Vorgehensweise bei einer FTA ist wie folgt:

- Festlegung des Hauptereignisses (z.B. fehlerhafte Daten im KIS), Untersuchung, durch welche Ereignisse es zum Hauptereignis kommen kann
- Weitere Untersuchung, wie es zu den ‚Zwischenereignissen' kommen kann
- Diese Untersuchungen werden so lange fortgesetzt, bis es als unproduktiv erachtet wird [18] oder die betrachtete Systemgrenze erreicht wird.

Führen mehrere Ereignisse unabhängig zu einem Folgeereignis, so werden diese mit einem ‚ODER' im Fehlerbaum verknüpft. Führen mehrere Ereignisse nur in deren Zusammenwirken zu einem Folgeereignis, werden die mit einem ‚UND' verknüpft.

Ein Vorteil dieser Methode ist es auch, dass die Eintrittswahrscheinlichkeiten des Hauptereignisses bestimmt werden können; wobei es Voraussetzung ist, dass die Eintrittswahrscheinlichkeiten der Einzelereignisse ebenfalls bekannt sein müssen. Bei einer initialen Untersuchung mittels FTA ist es aber schwierig, solche Einzelwahrscheinlichkeiten zu ermitteln bzw. zu kennen. Wie Risiken schließlich bewertet werden, wird im entsprechenden Kapitel betrachtet.

Wie ein solcher Fehlerbaum aussehen kann, ist in Abbildung 23 dargestellt. Dabei stellen ‚fehlerhafte Daten im KIS' das Hauptereignis dar, für welches die auslösenden Ereignisse (Fehler) gesucht werden. Diese auslösenden Ereignisse sind in Rot dargestellt. Es sind auch Ereignisse identifiziert worden, welche einer weiteren Ursachenanalyse unterzogen werden müssen. In diesem Fall sind dies Ereignisse, welche durch die Software selbst verursacht werden. Diese sind gelb dargestellt.

Durch die Betrachtung verschiedener Bereiche in der FTA ist es naheliegend, dass diese nicht durch eine einzelne Person durchgeführt werden kann. Um ein ausreichendes Wissen über diese Bereiche in die Analyse einzubringen, muss eine FTA im Risikoteam durchgeführt werden. Nun ist es aber auch eine Tatsache, dass die Teammitglieder über die Ziele der Analyse instruiert werden müssen, um zielgerichtete Ergebnisse schaffen zu können. Es ist dafür hilfreich, weitere grafische Tools anzuwenden.

6.5 Ishikawa-Diagramm

Ein solches Tool ist das Ishikawa-Diagramm, auch Fischgrätendiagramm genannt. Diese Methode ist sehr gut geeignet um eine FTA zu unterstützen. Bei Anwendung dieser Methode sollen auch die 5M (Mensch, Maschine, Methode, Material, Mitwelt) [19] betrachtet werden, welche einen möglichen Einfluss bzw. eine Ursache für ein Hauptereignis beinhalten. Wie ein solches Diagramm im Allgemeinen aussieht, ist in Abbildung 21 dargestellt.

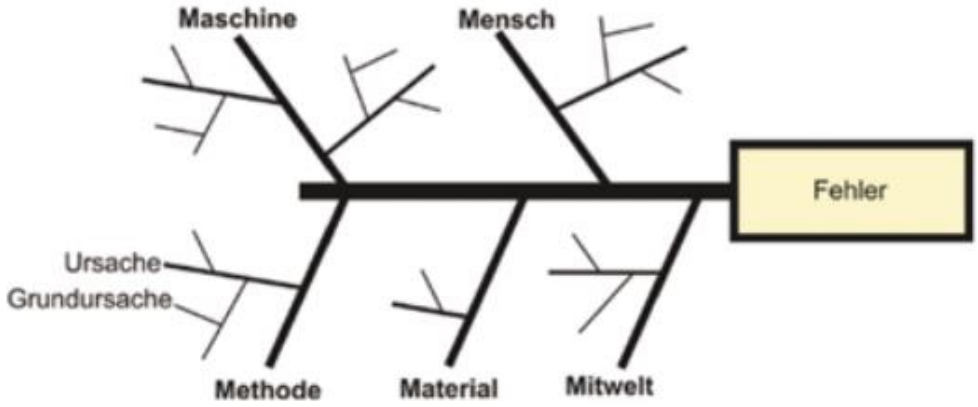


Abbildung 21: Ishikawa-Diagramm aus [18]

Die dabei genannten 5M's stellen aber lediglich Hinweise dar, welche im Zuge der Betrachtung beachtet werden sollen. Diese entsprechen der Anwendung bzw. der Gebrauchstauglichkeit (Mensch), der Gebrauchsumgebung (Mitwelt), der verwendeten Hardware (Material und Maschine) und der eigentlichen Funktion (Methode).

Um nun ein Fischgrätendiagramm für einen konkreten Fehler bzw. Hauptursache erstellen zu können, muss eben diese Hautursache bestimmt werden, welche untersucht werden soll. In weiterer Folge werden die dafür zugrundeliegenden Ursachen erörtert und als ‚Gräte' im Diagramm eingetragen. Hat diese Ursache wiederum eine ‚Nebenursache' wird auch diese als weitere Gräte im Diagramm dargestellt. Dies wird so lange fortgesetzt, bis alle möglichen Ursachen zu einem Hauptereignis gefunden wurden. In Abbildung 22 ist dies für *ilvi* dargestellt.

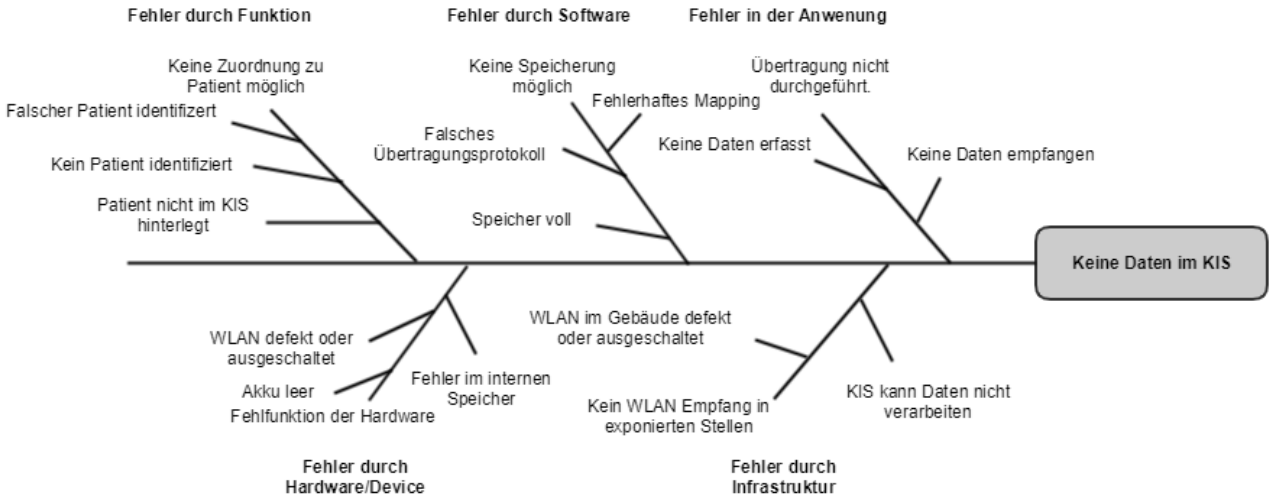


Abbildung 22: Ishikawa-Diagramm für ilvi mit dem Hauptereignis ‚Keine Daten im KIS'

Die Informationen, welche aus dieser grafischen Methode gewonnen werden, fließen in die Erstellung des Fehlerbaums während einer FTA mit ein.

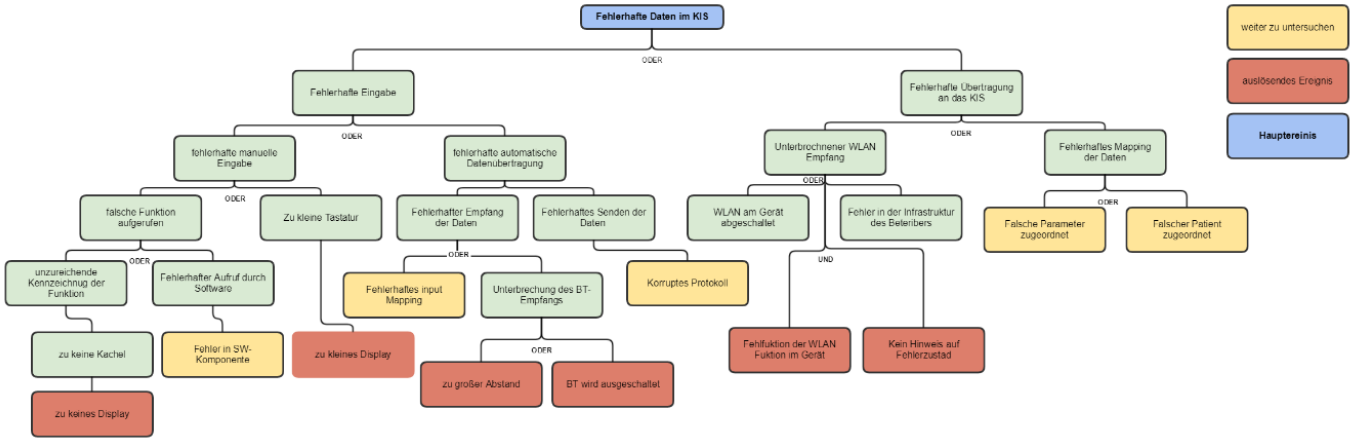


Abbildung 23: Fehlerbaum für ilvi mit dem Hauptereignis ‚Fehlerhafte Daten im KIS'

6.6 FMEA – failure mode effective analysis

Eine Methode, die den umgekehrten Weg zu einem Hauptereignis (Schaden) untersucht, ist die sogenannte FMEA (Failure mode effective analysis oder Fehlermögllichkeits und -einfluss Analyse). Diese Analyse geht nicht von einem ‚finalen' Schaden aus, sondern untersucht die Folgen eines einzelnen auslösenden Ereignisses (z.B. Softwarefehler) in der Schadenskette (vgl. Abbildung 15), es ist eine ‚Bottom-up Methode'. Um diese Methode jedoch anwenden zu können, ist für Software eine definierte Architektur notwendig, um für jede Komponente bei Fehlverhalten die daraus entstehende Gefährdung zu erkennen. Bei der Durchführung einer FMEA sollte nicht zu granular begonnen werden, um nicht unnötig und unüberschaubar viele Fehler zu untersuchen, die immer zur selben Gefährdung führen [16]. Die Dokumentation wird hier nicht grafisch dargestellt, sondern erfolgt in tabellarischer Form. Um einen Überblick bei der Untersuchung zu behalten, kann man die FMEA auch auf einzelne Bereiche durchführen. So ist es möglich, getrennte FMEAs z.B.: bei der Software-Architektur, für die Benutzungsumgebung oder die verwendete Hardware durchzuführen.
Mit dieser Methode ist es auch möglich, die einzelnen identifizierten Gefährdungen zu bewerten und damit Risiken zu erhalten. Ebenfalls können im Zuge einer FMEA geeignete Beherrschungsmaßnahmen zur Risikominderung gefunden bzw. definiert werden und in tabellarischer Form dokumentiert werden, die beispielhaft in Tabelle 10 dargestellt wird.

Unter-suchte Komponente	Fehler	Aus-wirkung direkt	Folge-wirkung	Schaden	Ein-tritts-wahr-schein-lichkeit	Risiko ID	Beher-rschungs-maß-nahme
Empfangen von BT-Daten	Falsches internes Mapping	Fehler-hafte Zu-ordnung der Werte	Falsche Daten im System	Falsche Daten im KIS	Gering	123	Validierung der Daten durch Anwender
Aufruf von Funktionen	Falsche Funktion wird auf-gerufen	Fehler-hafte Dar-stellung der Funktion	Keine Anwendung möglich	Keine Daten im KIS	Gering	124	Fehler-meldung vor Datenüber-tragung

Tabelle 10: Ergebnis einer FMEA als Beispiel

Damit diese Methode im Risikoteam angewandt werden kann, ist es wiederum sinnvoll, unterstützende Tools oder Hilfsmethoden anzuwenden, wie das schon beschriebene Ishikawa-Diagramm. Ebenfalls zu den unterstützenden Methoden zählt die sogenannte SWIFT-Methode (strukturiertes ‚Wass-Wenn' Verfahren).

6.7 SWIFT

Dieses Verfahren wird im Risikoteam durchgeführt, um ausgehend von Stichwörtern oder Aussagen des Moderators auf Risiken daraus zu schließen. Dabei soll sich immer die Frage "Was ist, wenn" zum Schlagwort gestellt, und diese im Team beantwortet werden. Zum Beispiel. „Was passiert, wenn der Abstand während der Bluetooth-Datenübertragung zu groß wird?", oder „Was ist, wenn die Softwarekomponente ‚KIS Controller' fehlerhaft funktioniert?".

Durch solch gezielte (strukturierte) Fragestellungen wird es möglich, in kurzer Zeit (z.B. im Rahmen eines Teammeetings) Gefährdungen und auch deren Ursachen zu finden, die wiederum Input für eine FMEA oder auch FTA darstellen.

Ihre Grenzen findet dieses Verfahren jedoch, wenn es um sehr detaillierte Systemebenen geht [18], z.B.: um zu untersuchen, warum eine Software-Komponente ausfällt.

Wenn man über die vorgegebene ‚strukturierte' Befragung der Teammitglieder hinaus geht, ist es auch möglich, Beherrschungsmaßnahmen im Zuge des Teammeetings zu finden.

6.8 Ergebnisse der PHA für *ilvi*

Wie beschrieben, wurde zu Beginn der Risikoanalyse von *ilvi* die Checkliste, wie sie die EN ISO 14971 vorgibt, [10] für *ilvi* beantwortet. Die Ergebnisse daraus sind in Tabelle 9 dargestellt.

In weiterer Folge wurde eine PHA unter Einbeziehung der Zweckbestimmung durchgeführt. Die im Zuge dieser PHA identifizierten Gefährdungen werden in Tabelle 11 aufgelistet.

Betrachteter Bereich	**Risiko-ID**	**Gefährdung**	**Schaden**
Funktion	RM-ZB-FUNKTION-1	Falsche Erfassung von Vitalparametern	Übertragung falscher Daten
	RM-ZB-FUNKTION-2	Falscher Patient identifiziert	Zuordnung der Daten zu falschem Patienten
	RM-ZB-FUNKTION-3	Inkorrekte Überprüfung der erfassten Werte	Falsche Ausgabe von Hinweisen Falsche Daten werden übertragen
	RM-ZB-FUNKTION-4	Falscher Benutzer authentifiziert	Erfasste Daten werden einem falschen Benutzer zugeordnet
	RM-ZB-FUNKTION-5	Falsche Anzeige der vom Benutzer eingegebenen Werte	Falsche Daten werden übertragen.
	RM-ZB-FUNKTION-6	Falsche Daten bei automatischer Datenübertragung von Messgeräte	Fehlende Daten Falsche / Korrupte Daten Werden übertragen.
	RM-ZB-FUNKTION-7	Fehlerhafte Datenübertragung zum KIS	Fehlende Daten Falsche / Korrupte Daten Werden übertragen

Gebrauchstauglichkeit	RM-ZB-USABILITY-1	Zu kleine Bedienelemente	Fehlerhafte Dateneingabe Unerwünschte Eingaben des Benutzers.
	RM-ZB-USABILITY-2	Zu kleine Schrift	Unleserlichkeit Fehlinterpretation der dargestellten Informationen
Hardware	RM-ZB-HARDWARE-1	Akku leer	Datenverlust Keine Erfassung / Benutzung möglich Zeitverlust
	RM-ZB-HARDWARE-2	Beeinflussung anderer Medizinprodukte oder Geräte	Durch EMV-Einfluss Fehlfunktion anderer MP Falsche Daten
	RM-ZB-HARDWARE-3	allgemeine Fehlfunktion der Hardware	Keine oder mangelhafte Erfassung/Benutzung möglich Verzögerte oder keine Diagnose
Benutzungsumgebung	RM-ZB-BENUTZUNG-1	Display zu unlesbar	Fehlerhafte Dateneingabe Unleserlichkeit Fehlinterpretation der dargestellten Informationen
	RM-ZB-BENUTZUNG-2	Zu laute Umgebungsgeräusche	Ablenkung des Benutzers Fehleingaben Fehlinterpretation der dargestellten Informationen Fehlerhafte Bedienung allgemein
	RM-ZB-BENUTZUNG-3	Unzureichend geschulte Anwender	Falsche Benutzung des Produktes Gefährdung für Patient

Tabelle 11: Ergebnisse der vorläufigen Gefährdungsanalyse (PHA) für ilvi

Zusammengefasst konnte damit geklärt werden, welche Schäden bzw. Gefährdungssituationen *ilvi* hervorrufen kann. Einerseits muss darauf geachtet werden, dass die verwendete Hardware inakzeptable Risiken beherbergt, andererseits wurden aber auch folgende Gefährdungssituationen erkannt, die durch die Software von *ilvi* hervorgerufen werden könnten. Diese sind in folgender Tabelle 12 aufgelistet.

Gefährdung	**‚direkter' Schaden**	**Schadensfolge**
Nutzung des Gesamtsystems nicht möglich	Keine Daten im KIS	Keine oder verzögerte Therapie oder Diagnose
Daten werden dem falschen Patienten zugeordnet	Falsche Daten im KIS	Keine oder verzögerte Therapie oder Diagnose
Daten können nicht übertragen werden	Keine Daten im KIS	Keine oder verzögerte Therapie oder Diagnose
Falsche Daten werden erfasst	Falsche Daten im KIS	Keine oder verzögerte Therapie oder Diagnose

Tabelle 12: Gefährdungen, die durch ilvi verursacht werden können

Somit kann zusammenfassend festgehalten werden, dass die ‚finale' Gefährdung folgende ist:

- Es befinden sich falsche Daten oder gar keine Daten durch eine Ursache von *ilvi* im KIS.

In Bezug auf die Hardware bzw. den Handheld-Computer müssen passende Anforderungen definiert werden, da die Hardware nicht im Zuge der Entwicklung selbst hergestellt wird.

Idealerweise sollen die relevanten Richtlinien betreffend EMV oder auch die MDD bei dem verwendeten Device beachtet werden. Aus diesen Anforderungen wurde das Gerät ‚TC51-HC' als Handheld-Computer gewählt. Dieses Device ist CE gekennzeichnet, womit bestätigt wird, dass die relevanten Richtlinien eingehalten werden. Hinzu kommt, dass dieses Device u.a. auch die Anforderungen der EN 60601-1 erfüllt und sich somit besonders für die Anwendung im Gesundheitswesen eignet.

Für *ilvi* wurde die Dokumentation der Risikoanalyse inkl. der Risikobewertung durchgeführt.

Aus diesem Grund muss vor Darstellung der Ergebnisse geklärt werden, wie eine Risikobewertung durchzuführen ist.

6.9 Risikobewertung

Wie in den vorherigen Kapiteln beschrieben, ist ein Risiko erst dann definiert, wenn zu einer gegebenen Gefährdung die Eintrittswahrscheinlichkeit und die Höhe des daraus resultierenden Schadens bekannt ist.

Dabei nutzt man die ebenfalls schon vorab beschriebenen Stufen von Schadenshöhen und Eintrittswahrscheinlichkeiten, um die Gefährdungen in eine Risikomatrix eintragen zu können. Erst durch diese Bewertung wird es möglich, über die Akzeptanz der Risiken (anhand der festgelegten Akzeptanzkriterien) zu entscheiden.

Zur Bestimmung des Schadensausmaßes bzw. der Schadenshöhe betrachtet man den Schaden, der durch eine Gefährdung entstehen kann. Diesen definierten Schaden vergleicht man folgend mit den Schadensstufen aus der Risikopolitik. Um dies auch nachvollziehbar zu machen, ist es oft notwendig Personen hierbei miteinzubeziehen, die über den medizinischen Sachverstand verfügen [16]. Aufgrund der konkreten Schäden, die in der Risikoanalyse identifiziert wurden, ist es möglich, diese mit den definierten Schadenshöhen zu vergleichen und somit einer Schadensstufe zuzuordnen.

Anders verhält es sich bei der Bestimmung der Eintrittswahrscheinlichkeit einer Gefährdung. So ist es explizit schwierig eine Aussage über die Ausfallswahrscheinlichkeit einer Softwarekomponente zu treffen. Die Wahrscheinlichkeit von Bedienfehlern kann möglicherweise im Zuge von Usability-Untersuchungen oder aus der Vorgeschichte eines Produktes bestimmt werden. Um nun, wie von der EN ISO 14971 gefordert, [10] Eintrittswahrscheinlichkeiten zu bestimmen, können drei Verfahren herangezogen werden:

- Verwendung von relevanten Daten aus der Vorgeschichte
- Vorhersage von Wahrscheinlichkeiten unter Anwendung von analytischen und Simulationstechniken
- Beurteilung von Experten [16], [10]

Es wird empfohlen, wenn möglich auf das erstgenannte Verfahren zurückzugreifen, um Eintrittswahrscheinlichkeiten zu bestimmen. [16] Bei komplexen Systemen kann auch die Vorhersage durch Simulationen oder Analysen von Komponenten durchgeführt werden. Bei Herstellern, die aber diese Methoden nicht anwenden können (aufgrund fehlender Vorgeschichte oder wenn eine Simulation unangebracht erscheint), mussen auf die Abschätzung der Wahrscheinlichkeiten durch Experten vertraut werden.

Durch das Bewerten von Schweregrad und Eintrittswahrscheinlichkeit wird also die Bestimmung der Risiken, wie es die EN ISO 14971 definiert erreicht. Diese Ergebnisse werden in der Risikobewertungsmatrix eingetragen. Aufgrund der Akzeptanzkriterien kann nun bestimmt werden, für welche Risiken Beherrschungsmaßnahmen notwendig sind.

Bei Anwendung der Norm EN 62304 ist es aber vorab nötig, der Software eine Sicherheitsklasse zuzuordnen. [11]

6.10 Klassifizierung in Software-Sicherheitsklassen

Die EN 62304 sieht folgende Klassen vor: [11]

- Klasse A: Keine Verletzung oder Gefährdung möglich
- Klasse B: Keine schwerwiegenden Verletzungen möglich
- Klasse C: Tod oder schwerwiegende Verletzungen möglich

Abhängig von der Sicherheitsklassifizierung von Software oder Softwarekomponenten sieht die EN 62304 verschiedene, mit der Klasse steigende Dokumentationsgrade vor.

Ohne eine dokumentierte Zuordnung zu einer dieser Klassen ist jede Software als Medizinprodukt der Klasse C zuzuordnen. Durch das Risikomanagement können aber die von der Software ausgehenden Gefährdungen erkannt werden, und somit ist eine Klassifizierung in eine niedrigere Klasse (je nach Gefährdung) möglich. Um diese Klassifizierung durchzuführen, kann man wie in Abbildung 24 vorgehen. Anhand der Erkenntnisse aus dem Risikomanagement ist zu entscheiden, ob eine Gefährdungssituation durch die Software entstehen kann. Für *ilvi* ist dies mit ‚Ja' zu beantworten. Nun können anhand von Risikobeherrschungsmaßnahmen diese Gefährdungssituationen verhindert werden; jedoch nur, wenn diese Maßnahmen nicht in der Software umgesetzt werden, sondern außerhalb davon. Bei *ilvi* sind diese Maßnahmen als Hinweise bezüglich der bestehenden Restrisiken in der Gebrauchsanweisung ausgeführt, als auch durch die Verwendung von Hardware, die konform der entsprechenden Richtlinien hergestellt wurde. Somit kommt man zum nächsten Schritt, der befragt, ob diese möglichen Gefährdungssituationen inakzeptabel sind, oder nicht. Bei *ilvi* kommt es auch ohne Software-Beherrschungsmaßnahmen zu keinen inakzeptablen Risiken bzw. Gefährdungssituationen, womit die Software der Sicherheitsklasse A zugeordnet werden kann.

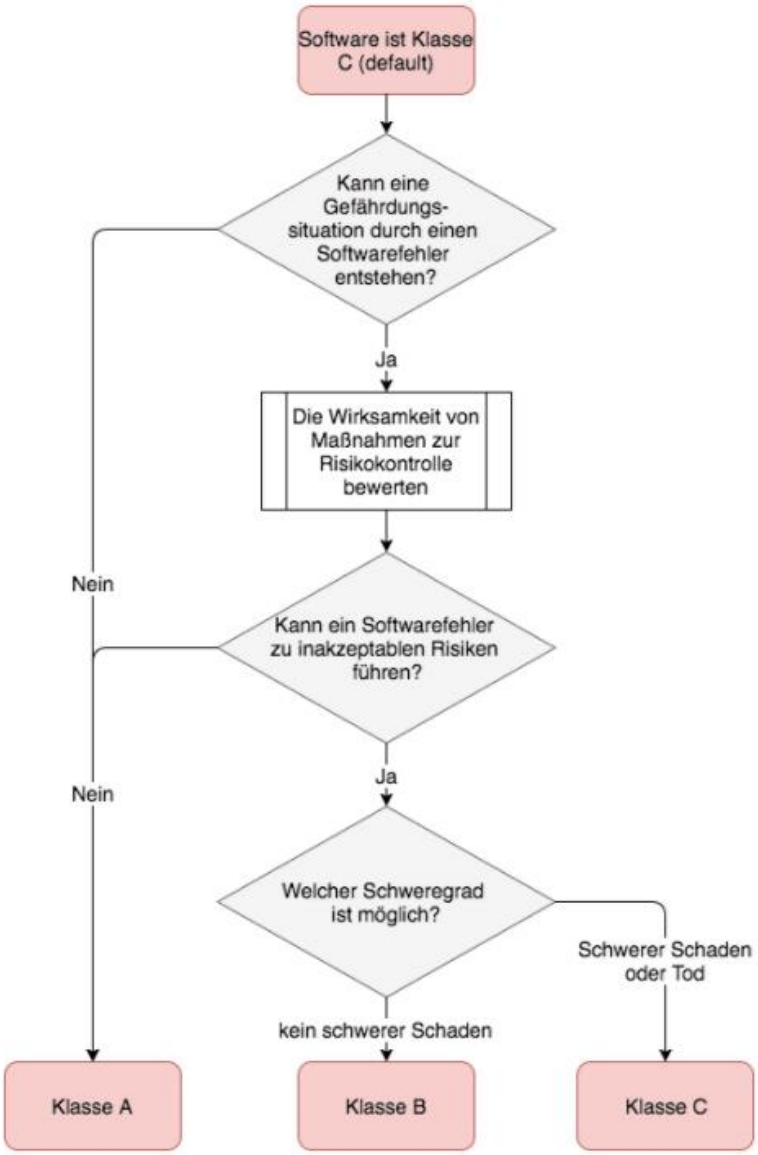


Abbildung 24: Vorgehensweise zur Software-Klassifizierung aus [16]

Bei dieser Klassifizierung ist zu beachten, dass die ISO 62304 eine Eintrittswahrscheinlichkeit für einen Softwarefehler von 100% vorsieht. Die Norm zielt dabei darauf ab, dass nur die möglichen Gefährdungen und nicht die Eintrittswahrscheinlichkeiten als Grundlage zur Bestimmung der Klasse heran gezogen werden [16]. Es ist auch möglich, verschiedenen Software-Komponenten verschiedenen Klassen zuzuweisen. Jedoch ist auch hierbei darauf zu achten, dass eine ‚Tochterkomponente' keine höhere Klasse haben darf, als die ‚Mutterkomponente'. Das bedeutet, dass eine Komponente, die von einer anderen Komponente abhängig ist, nicht höher klassifiziert werden darf, als diese.

Um diese Klassifizierung für *ilvi* durchführen zu können, muss also die SW-Architektur mit den einzelnen SW-Komponenten bekannt sein. Abbildung 25 zeigt diese SW-Architektur. Die entsprechende der Komponenten zu einer Sicherheitsklasse und deren Beschreibung ist in Tabelle 13 dargestellt.

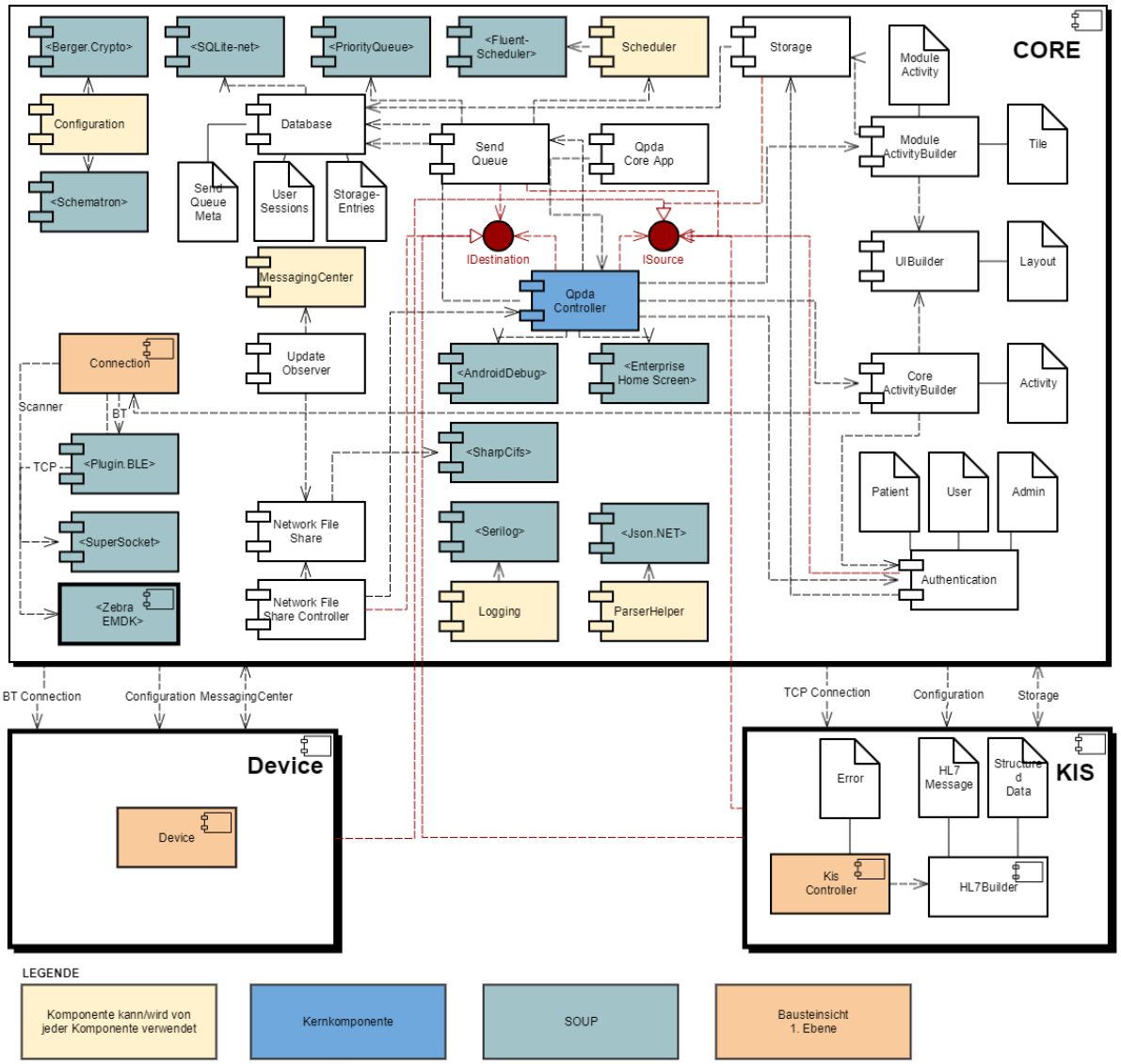


Abbildung 25: Softwarearchitektur von ilvi

Komponente	Beschreibung	Sicherheitsklasse
QpdaController	Zentrale Komponente zur Steuerung der Software	A
Qpda	Android-App	A
ModuleActivityBuilder	Erzeugt ModuleActivities laut Konfiguration und stellt diese bereit. Liefert ebenso Layouts und Events der HomeActivity aus. Liefert ebenso Layouts und Events für InfoActivity aus.	A

Komponente	Beschreibung	Sicherheitsklasse
UIBuilder	Erzeugt der Konfiguration Layouts, welche für das Endgerät angepasst sind.	A
CoreActivityBuilder	Erzeugt User-, Patientactivities und stellt diese bereit. Liefert ebenso komplette Dialoge (Warnungen, Entscheidungsdialoge).	A
Authentication	Verarbeitet Authentifizierungsinformationen und überprüft ob sie im jeweiligen Kontext (User, Patient) gültig sind.	A
UpdateObserver	Überwacht den vorkonfigurierten NetworkFileShare-Importordner und den lokalen Importordner (notwendig bei MDM-Update) auf vorhandene Dateien/Imports und meldet Updates an.	A
Connection	Stellt für TCP-Sockets, Bluetooth, Barcode/QR-Code Scanner, NFC-Reader, Audio Verbindungen bereit.	A
Database	Persistiert - wenn vorhanden - lokale Benutzerdaten dauerhaft. Der Benutzer der letzten Sitzung wird ebenso gespeichert. Dient ebenso zur Speicherung der Values-Storage (Patientendaten, Messdaten, Systemdaten)	A
Configuration	Liest die Konfiguration ein. Beinhaltet die Lizenzüberprüfung durch Signaturcheck und Entschlüsselung mit Device-ID. Eine veraltete Konfiguration wird ggf. gelöscht.	A
Storage	Container für internes Datenformat. Es werden hauptsächlich Vitalparameter/Gesundheitswerte gespeichert. Die Übertragung dieser Daten übernimmt die "Sending Queue". Zur Speicherung in den internen Datenstorage können InputTransformer verwendet werden. Zum Auslesen aus dem Datenstorage OutputTransformer.	A
NetworkFileShare	Kann Dateien von einem Windows Share lesen und ggf. schreiben.	A

Komponente	Beschreibung	Sicherheitsklasse
NetworkFileShareController	Steuert NetworkFileShare Verbindungen	A
SendQueue	Verwaltet alle zu übertragenen Messdaten in einer vollständigen HL7 Nachricht mit allen benötigten Patientendaten. Versucht im Hintergrund nach Vorgabe diese Daten zu übertragen. Nach erfolgreicher Übertragung werden diese aus der Queue entfernt.	A
Logging	Erzeugt nach Anforderung das Logfile und befüllt dieses mit Logeinträgen. Stellt allen Komponenten die Logging-Funktionalität zur Verfügung.	A
ParserHelper	Bietet anderen Komponenten allgemeine Funktionalität zum Verarbeiten von CSV-, Strings-, Json- und Xml-Daten an.	A
MessagingCenter	Ermöglicht das Senden und Empfangen von Objekten zwischen Komponenten mittels eines einfachen Nachrichtendienstes.	A
Scheduler	Ausführen von regelmäßigen zeitgesteuerten Jobs.	A
Device	Steuert die Kommunikation mit Medizingerät. Empfängt Daten vom Gerät bzw. schickt ggf. Daten ans Gerät.	A
KisController	Steuert die Kommunikation mit KIS	A
HL7Builder	Generiert mit vorgegebenen Daten eine HL7-Nachricht. Analysiert und zerlegt eine HL7-Nachricht in strukturierte Daten zur Weiterverarbeitung.	A

Tabelle 13: Sicherheitsklassen der SW-Komponenten von ilvi

6.11 Risikobewertung und Risikobeherrschungsmaßnahmen für ilvi

Zur Risikobewertung bei *ilvi* wurden verschiedene Bereiche während der Entwicklung analysiert, die Informationen zu möglichen Gefährdungen und Fehlern liefern können. Im Bereich der Gebrauchstauglichkeit waren dies die Benutzungsszenarien und die dabei anzuwendenden Hauptbedienfunktionen. Im Bereich der Software-Funktion wurde die SW-Architektur und deren Komponenten untersucht, sowie die Schnittstellen und die Laufzeitumgebung (SW-Umgebung, unter der *ilvi* ausgeführt wird). Als wichtiger Bereich der Entwicklung wurden auch die eingesetzten SOUPS auf etwaige Risiken analysiert. SOUPs (Software of unknown Provenance) sind Software-Komponenten von Drittherstellern, also Software, welche nicht selbst entwickelt wird. Dies hat den Vorteil, dass sich der Entwicklungsaufwand reduziert, aber auch den Nachteil, dass genau geprüft werden muss, welche Fehlerquellen diese Komponenten beinhalten oder hervorrufen können.

Für Risiken, die aufgrund ihrer Bewertung als inakzeptabel eingestuft werden, müssen entsprechende Beherrschungsmaßnahmen definiert werden, um das betroffene Risiko auf ein akzeptables Niveau zu bringen. Dahingehend besteht die Möglichkeit, einerseits die Schadenshöhe zu verringern, andererseits durch eine Maßnahme die Eintrittswahrscheinlichkeit zu verringern.

Die MDD sieht hierfür folgende Stufen für Beherrschungsmaßnahmen bzw. deren Umsetzung vor:

- Inhärentes Design
- Schutzmaßnahmen (ggf. Konstruktiv)
- Hinweise auf gegebene Restrisiken [3]

Dabei ist es immer vorzuziehen, dass Risiken aufgrund des Designs des betreffenden Produktes vermieden bzw. verringert werden. Dies hat zur Folge, dass das gegebene Risiko aufgrund der Design- oder Anforderungsanpassung nicht mehr in der Risikomatrix einzutragen ist.

Ist dies nicht möglich, sollen entsprechende konstruktive Schutzmaßnahmen implementiert werden. Für Software kann eine solche Schutzmaßnahme ein

entsprechender Warnhinweis sein. Kann ein Risiko auch durch solche Schutzmaßnahmen nicht verringert werden, muss auf dieses Restrisiko gesondert hingewiesen werden. Dabei ist zu beachten, dass ein solcher Hinweis nicht in der Gebrauchsanweisung zu lesen sein darf. Solche Hinweise müssen direkt am Produkt und bei der Anwendung einer Software zu erkennen ein. Man spricht hierbei auch von „integrierter Sicherheit“ [20]. In Abbildung 26 wird diese stufenweise Integration von Beherrschungsmaßnahmen dargestellt.

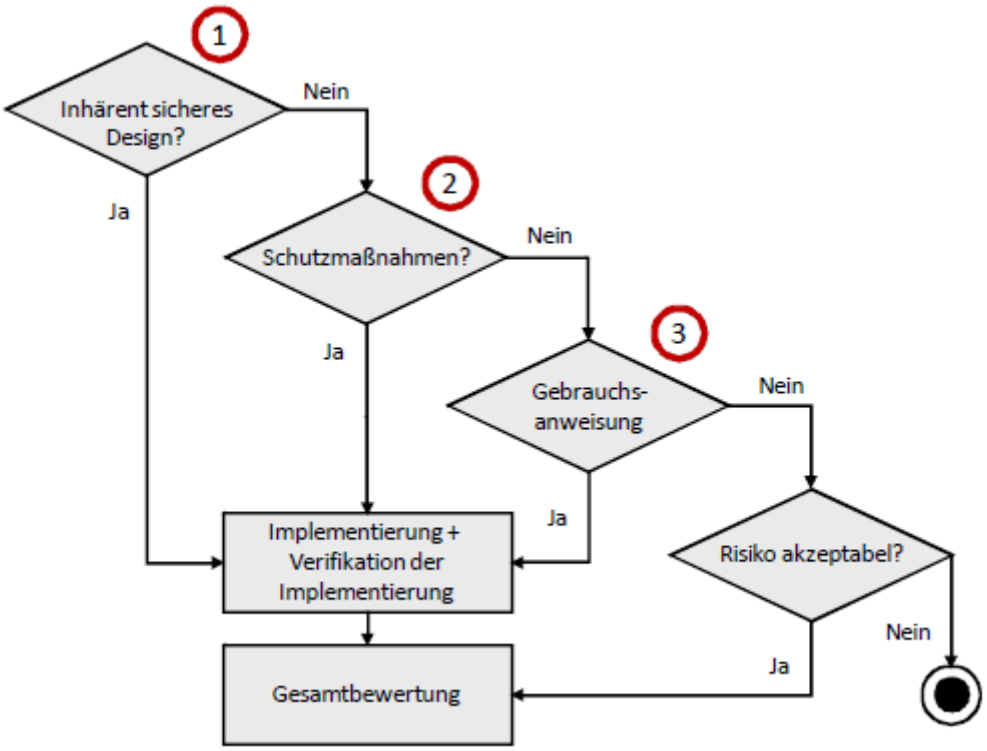


Abbildung 26: ‚integrierte Sicherheit‘ durch geeignete Risikobeherrschungsmaßnahmen aus [16].

Nach der Einführung von Beherrschungsmaßnahmen muss eine erneute Bewertung des betroffenen Risikos vorgenommen werden, um zu beurteilen, ob das Risiko tatsächlich verringert und akzeptabel ist.

Eine Folge der Einführung von Risikobeherrschungsmaßnahmen ist auch, dass diese selbst Risiken beherbergen können. So müssen die definierten Maßnahmen ebenfalls auf eine Rückwirkung zu einem Risiko untersucht werden (vgl. Risikomanagementprozess in Abb. 17.). So darf eine eingeführte Beherrschungsmaßnahme keinesfalls ein inakzeptables Risiko hervorrufen oder bedarf einer weiteren Maßnahme, um das neu entstandene Risiko zu verringern.

Wurden nun die geeigneten Beherrschungsmaßnahmen definiert, müssen diese auch implementiert und verifiziert werden.

6.12 Verifikation von Risikobeherrschungsmaßnahmen – Traceability

Die Dokumentation des QMS als auch die Ablage der technischen Dokumentation erfolgt bei der Entwicklung von *ilvi* elektronisch. Dafür wird das Programm ‚Confluence' des Herstellers ‚Atlassian' verwendet. Diese Anwendung eignet sich besonders gut, um die Anforderungen aus der EN ISO 13485 als auch die Anforderungen aus den weiteren relevanten Normen (Gebrauchstauglichkeit, SW-Lebenszyklus, Risikomanagement) umzusetzen. Sei es die ‚Lenkung der Dokumente', oder aber eben auch die Rückverfolgbarkeit von Systemanforderungen. Um diese Rückverfolgbarkeit zu gewährleisten, wird das Plug-In ‚Requirement-Yogi' angewandt. Dies erlaubt die Zuweisung von ID's zu einer Anforderung, welche eine Rückverfolgbarkeit über den gesamten Entwicklungsprozess inklusive des Risikomanagements erlaubt. Hintergrund dafür ist die geforderte Verifikation von Risikobeherrschungsmaßnahmen aus der EN ISO 14971. In Abschnitt 6.3 ‚Umsetzung von Maßnahmen zur Risikobeherrschung' fordert die Norm, dass die Umsetzung der Maßnahmen verifiziert werden müssen. Für *ilvi* werden diese Maßnahmen im Zuge von Integrations- und Systemtests verifiziert. Durch die Verwendung des ‚Requirement Yogi' ist dies nachvollziehbar dokumentiert. Voraussetzung dafür ist jedoch, dass Risikobeherrschungsmaßnahmen als Software-Anforderung (vgl. Software-Entwicklungsprozess) aufgenommen werden. In Abbildung 27 wird dieser Zusammenhang grafisch dargestellt.

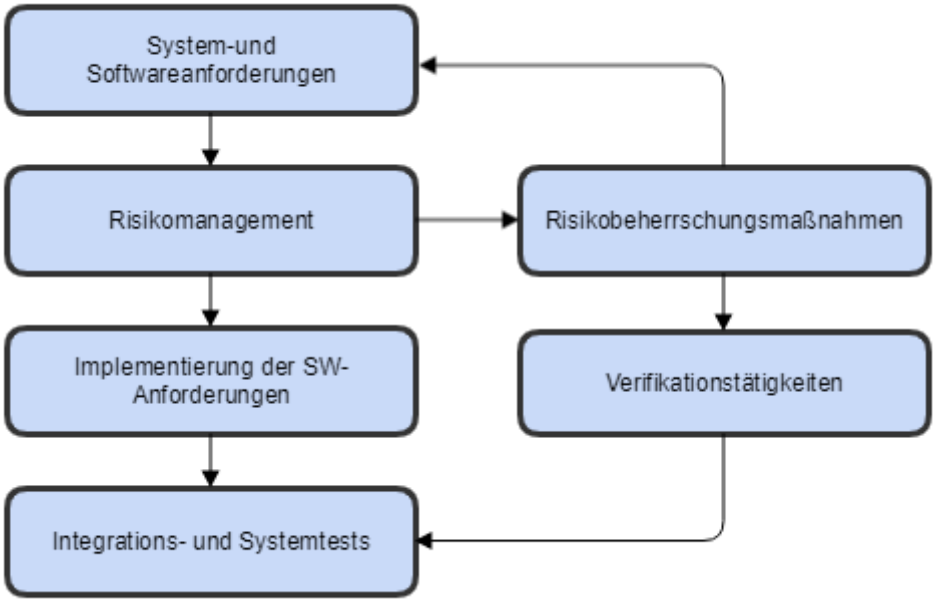


Abbildung 27: Verifikation der Risikobeherrschungsmaßnahmen im Zuge von SW-Tests.

7 Risikotabellen und Risikomatritzen für *ilvi*

Für *ilvi* wurden die Risiken in Tabellen zusammengefasst. Darin enthalten ist auch die Bewertung der Einzelrisiken sowie die gegebenenfalls notwendigen Risikobeherrschungsmaßnahmen. In weiterer Folge wird auch die neuerliche Bewertung nach Einführung der Beherrschungsmaßnahmen dargestellt. Bei der Risikoanalyse wurden hier folgende Bereiche betrachtet, die gewissermaßen auch den Zusammenhang zum Software-Lebenszyklus und zur Gebrauchstauglichkeit abbilden.

- Benutzungsszenarien
- Hauptbedienfunktionen
- Software-Architektur
- Verwendete SOUPS
- Systemschnittstellen und Laufzeitumgebung
- Rückwirkungen von Beherrschungsmaßnahmen

In den dargestellten Tabellen werden folgende Abkürzungen verwendet:

- ID: Risiko-ID
- S: Schadenshöhe
- E: Eintrittswahrscheinlichkeit
- RK: Risikoklasse
- BHM: Beherrschungsmaßnahme
- BHM ver?: Wurde die Beherrschungsmaßnahme implementiert und verifiziert?
- RW: Rückwirkung auf neue Risiken
- Sn: Schadenshöhe nach Einführung der Beherrschungsmaßnahme
- En: Eintrittswahrscheinlichkeit nach Einführung der Beherrschungsmaßnahme
- RKn: Risikoklasse nach Einführung der Beherrschungsmaßnahme

7.1 Risiken aus den Benutzungsszenarien

Es wurden hier Gefährdungen ausgehend der definierten Benutzungsszenarien identifiziert und bewertet. Dabei wurden keine inakzeptablen Risiken festgestellt, jedoch trotzdem Risikobeherrschungsmaßnahmen definiert, wenn diese als sinnvoll erachtet wurden oder Risiken der Klasse II vorhanden waren. Dieses Ergebnis entspricht auch der Klassifizierung der Software in die Klasse A. Folgende Risikomatritzen und Tabellen in Abbildung 28 bzw. Tabelle 14 geben einen Überblick der erkannten Risiken vor und nach Einführung von diesen Beherrschungsmaßnahmen.

Benutzungsszenario: Benutzeranmeldung und identifizieren des Patienten											
ID	**Gefährdung**	**Schaden**	**S**	**E**	**RK**	**BHM**	**RW?**	**BHM ver?**	**Sn**	**En**	**RKn**
BS-Ident-01	Inkorrekte Anmeldung am System	Falsche Zuordnung des Anwenders	1	2	I	-	-	-	-	-	-
		Anwendung des Systems nicht möglich	1	2	I			-	-	-	-
BS-Ident-02	Inkorrekte Identifizierung des Patienten	Zuordnung der erfassten Werte zu falschem Patienten	3	3	II	Anzeige des Patientennamen nach dessen Identifizierung Sprachausgabe des Patientennamens	-	Ja	3	2	I
		Anzeige falscher gesundheitsrelevanter Daten des Patienten	2	3	I				2	2	I
BS-Ident-03	Fehlerhafte Anzeige detaillierter Informationen	Fehlerhafte Behandlung des Patienten	3	2	I	-	-	-	-	-	-
BS-Ident-04	Anwender vergisst Patient abzumelden	Zuordnung der erfassten Werte zu falschem Patienten	3	3	II	Timeout, Durchgehende Anzeige des Patientennamens, Abmeldung des Patienten bei Beendigung der Anwendung	-	Ja	3	1	I
		Daten werden nicht übertragen	2	4	II				2	2	I

BS-Ident-05	Anwender vergisst sich abzumelden	Falsche Zuordnung des Anwenders	1	3	I	Timeout Abmeldung des Anwenders bei Beendigung der Anwendung	-	Ja	1	1	I
Benutzungsszenario: Erfassen von Vitalparametern											
ID	**Gefährdung**	**Schaden**	**S**	**E**	**RK**	**BHM**	**RW**	**BHM ver?**	**Sn**	**En**	**RKn**
BS-Vit-01	Fehlerhafte automatisierte Übertragung der gemessenen Werte auf das System	Falsche Daten im KIS / Archiv	3	2	I	Bestätigung der Werte durch Anwender	-	Ja	3	1	I
BS-Vit-02	Keine empfangene Werte	Keine Daten vorhanden	1	3	I	Warnhinweis für Anwender	-	Ja	1	2	I
BS-Vit-03	Fehlerhafte Eingabe des Benutzers	Falsche Daten im KIS / Archiv	3	3	II	Unterstützung für korrekte Eingabe Prüfung der Werte auf Plausibilität	Ja	Ja	3	2	I

BS-Vit-04	Falsche Auswahl des gewünschten Parameters	Falsche Zuordnung der Werte	3	2	I	Farbliche Kennzeichnung Ausreichender Abstand zwischen Buttons Eindeutige Symbole	-	Ja	3	2	I
BS-Vit-05	Fehlerhafte Plausibilitätsprüfung	Fehlerhafter Hinweis auf ggf. nicht plausible Werte	2	2	I	Validierung durch Anwender	-	ja	2	2	I
BS-Vit-06	Bearbeiten von Werten nicht möglich	Falsche Werte im System	2	2	I	nachträgliche Bearbeitung ermöglichen	-	Ja	2	1	I
BS-Vit-07	Unbeabsichtigtes Löschen eingegebener/empfangener Werte	Verlust von erfassten Daten	1	3	I	Validierung durch Anwender	-	Ja	1	2	I
BS-Vit-08	Fehlerhaftes Übertragen von Daten ins Informationssystem	Korrupte Daten im Informationssystem	3	3	II	Acknowledge bei Übertragung	-	Ja	2	2	I
BS-Vit-09	Keine Datenübertragung ins Informationssystem	Keine Daten im Informationssystem	2	4	II	Lokale Speicherung der Werte im System	Ja	Ja	2	2	I
BS-Vit-10	Unbeabsichtigtes Übertragen der Daten	Unvollständige Daten im Informationssystem	2	3	I	Validieren der Übertragung	-	Ja	2	2	I
		Fehlerhafte Daten im Informationssystem	3	3	II				2	2	I

Benutzungsszenario: Erfassen von gesundheitswerten											
ID	**Gefährdung**	**Schaden**	**S**	**E**	**RK**	**BHM**	**RW**	**BHM ver?**	**Sn**	**En**	**RKn**
BS-Ges-01	Fehlerhafte Eingabe des Benutzers	Falsche Daten im KIS / Archiv	2	3		Unterstützung für korrekte Eingabe Prüfung der Werte auf Plausibilität	Ja	Ja	2	2	I
BS-Ges-02	Falsche Auswahl des gewünschten Parameters	Falsche Zuordnung der Gesundheitswerte	2	3	II	Farbliche Kennzeichnung Ausreichender Abstand zwischen Buttons Eindeutige Symbole	-	Ja	2	2	I
BS-Ges-03	Fehlerhafte Plausibilitätsprüfung	Fehlerhafter Hinweis auf ggf. nicht plausible Werte	2	2	I	Validierung durch Anwender	-	Ja	2	1	I
BS-Ges-04	Benutzer vergisst Wert zu bestätigen	Keine Übernahme des Wertes ins System	2	2	I	Übersicht der gespeicherten Werte im Home-Bildschirm	-	Ja	2	1	I
BS-Ges-05	Unbeabsichtigtes Löschen eingegebener Werte	Verlust von erfassten Daten	2	3	I	Validierung durch Anwender	-	Ja	2	2	I

BS-Ges-06	Fehlerhaftes Übertragen von Daten ins Informationssystem	Korrupte Daten im Informationssystem	2	3	I	Acknowledge bei Übertragung	-	Ja	1	2	I
BS-Ges-07	Keine Datenübertragung ins Informationssystem	Keine Daten im Informationssystem	2	4	II	Lokale Speicherung der Werte im System	Ja	Ja	2	2	I
BS-Ges-08	Unbeabsichtigtes Übertragen der Daten	Unvollständige Daten im Informationssystem	2	3	I	Validieren der Übertragung	-	Ja	2	2	I
		Fehlerhafte Daten im Informationssystem	2	3	I				2	2	I
Benutzungsszenario: Fotodokumentation											
ID	**Gefährdung**	**Schaden**	**S**	**E**	**RK**	**BHM**	**RW**	**BHM ver?**	**Sn**	**En**	**RKn**
BS-Wund-01	Ungewolltes Starten der Wunddokumentation	Unerwünschte Anzeige am System	1	3	I	Klare und eindeutige Kennzeichnung des Buttons	-	Ja	1	2	I
BS-Wund-02	Fehlerhaftes Starten der Kamera	Keine Wunddokumentation möglich	2	2	I		-	-	-	-	-

BS-Wund-03	Fehlerhafte Aufnahme von Fotos	Keine verwendbaren Fotos	2	2	I	Validierung der Aufnahme durch Anwender Möglichkeit ein neues Foto aufzunehmen	-	Ja	1	2	I
BS-Wund-04	Fehlerhafte Anzeige des aufgenommenen Fotos	Kein verwendbares Foto	2	2	I	Möglichkeit ein neues Foto aufzunehmen	-	Ja	1	1	I
BS-Wund-05	ungewolltes Bestätigen einer Aufnahme	Fehlerhaftes Foto im System	2	3	I	nachträgliches Löschen ermöglichen	Ja	Ja	1	3	I
BS-Wund-06	Fehlerhaftes Übertragen von Daten ins Informationssystem	Korrupte Daten im Informationssystem	2	2	I	Acknowledge bei Übertragung	-	Ja	2	1	I
BS-Wund-07	Keine Datenübertragung ins Informationssystem möglich	Keine Daten im Informationssystem	2	2	I	Fehlermeldung anzeigen Lokale Speicherung der Daten	Ja	Ja	2	2	I
BS-Wund-08	Unbeabsichtigtes Übertragen der Daten	Unvollständige Daten im Informationssystem	2	2	I	Validierung der Übertragung durch Anwender	-	Ja	2	2	I
BS-Wund-09	Fehlerhafte Zuordnung zum Patienten (falsche interne Benamung)	Keine korrekte Zuordnung zum Patienten / falsche Zuordnung	3	2	I	Anzeige der Patientendaten bei Anwendung des Systems Identifikation des Patienten	-	Ja	2	2	I

Tabelle 14: Risikotabelle der Benutzungsszenarien von ilvi

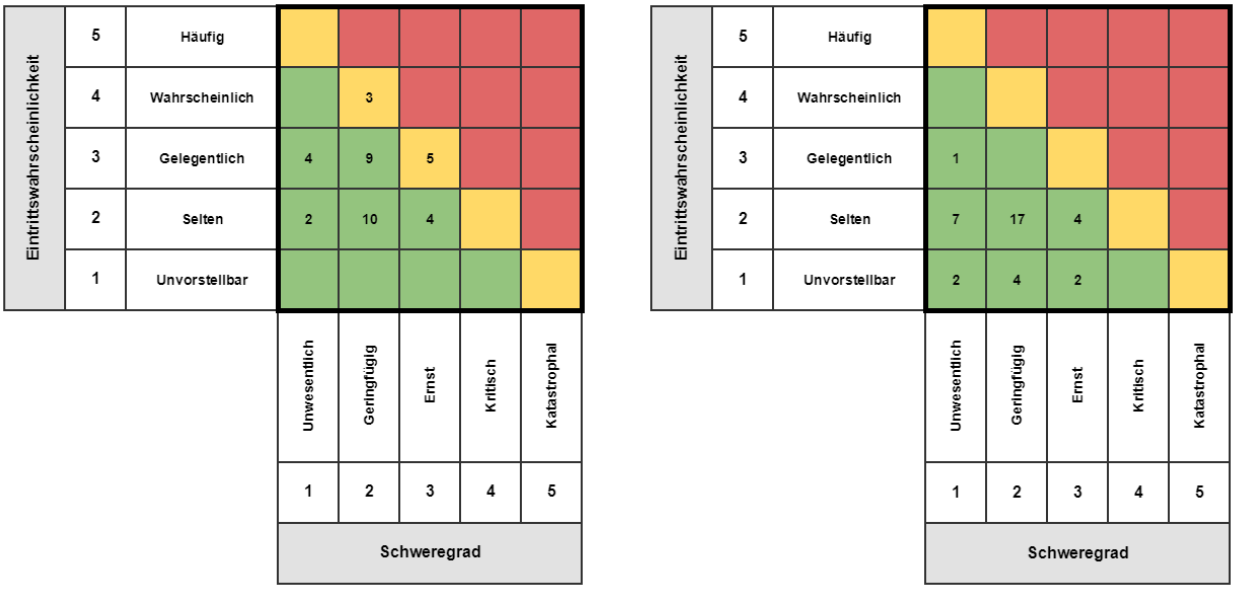


Abbildung 28: Risikomatritzen für Benutzungsszenarien – vor und nach Beherrschungsmaßnahmen

7.2 Risiken aus den Hauptbedienfunktionen

Folgend auf die Untersuchung der Benutzungsszenarien wurden die definierten Hauptbedienfunktionen auf Gefährdungen untersucht. Auch hier wurden keine inakzeptablen Risiken erkannt, und trotzdem (vgl. Risikopolitik) Risikobeherrschungmaßnahmen definiert, um Risiken der Klasse 2 zu minimieren. Wie schon erwähnt, bildet diese Klasse nicht die Vorgaben der Norm ab, wurde aber in der Risikopolitik zur Entwicklung von *ilvi* so definiert, um etwaige Risiken dabei trotzdem zu minimieren. Dabei ergeben sich folgende Risikomatritzen in Abbildung 29 bzw. Tabelle 15.

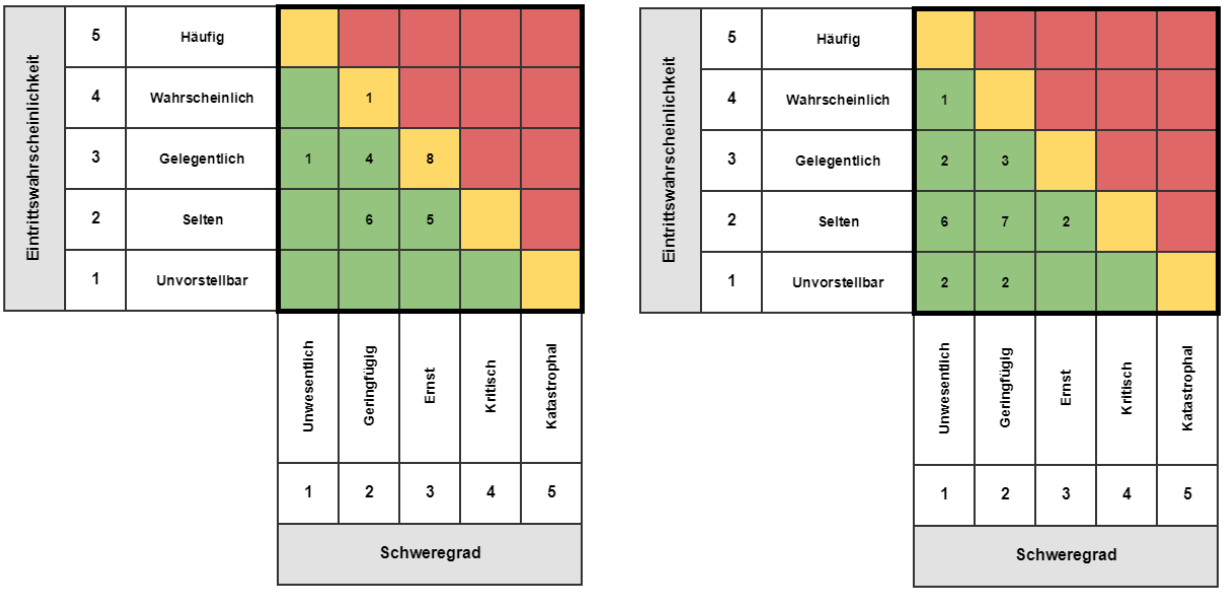


Abbildung 29: Risikomatritzen für Hauptbedienfunktionen - vor und nach Beherrschungsmaßnahmen

Hauptbedienfunktion: Benutzeranmeldung und identifizieren des Patienten											
ID	**Gefährdung**	**Schaden**	**S**	**E**	**RK**	**BHM**	**RW**	**BHM ver?**	**Sn**	**En**	**RKn**
HB-User-01	Falsche Interpretation der Information Scannen einer ungültigen ID	Keine Zuordnung der Werte zu Patienten möglich	2	2	I	Fehlermeldung bei falschem Barcode-Scan		Ja	1	1	I
HB-User-02	Falsche Interpretation der Information, Scannen eines falschen Barcodes	Keine Zuordnung der Werte zu Patienten möglich, Falscher Pat. identifiziert	3	3	II	Fehlermeldung bei falschem Barcode-Scan, siehe Anzeige des Pat. Namen		Ja	2	1	I
HB-User-03	Inkorrekte ID	unbefugtes Benutzen des Systems	3	2	I	Überprüfung der ID auf Berechtigung	Ja	Ja	1	2	I
HB-User-04	Inkorrekte ID	Falscher Patient angemeldet	3	3	II	Überprüfung der ID im KIS, Anzeige der Patientendaten	Ja	Ja	1	2	I
HB-User-05	Ungewolltes Abmelden	Datenverlust	2	3	I	Validierung der Abmeldung durch Anwender Abmeldung erst nach Datenübertragung		Ja	2	1	I
HB-User-06	Ungewolltes Abmelden	Datenverlust	2	3	I	Validierung der Abmeldung durch Anwender		Ja	1	1	I
Hauptbedienfunktion: Erfassen von Vitalparametern											

ID	Gefährdung	Schaden	S	E	RK	BHM	RW	BHM ver?	Sn	En	RKn
HB-Vit-01	Falsche Interpretation der angezeigten Werte	Falsche Behandlung des Patienten	3	3	II	eindeutige Zuordnung und Beschreibung der dargestellten Werte		Ja	2	3	I
HB-Vit-02	Falsche Interpretation der Darstellung	Aufruf einer falschen Funktion	2	3	II	eindeutige Beschreibung und Darstellung der Übersicht		Ja	1	2	I
HB-Vit-03	Falsche Eingabe von Daten	Falsche Daten im System	3	3	II	benutzerfreundliche Eingabefunktion, ausreichend große Tastatur Validierung der eingegebenen Werte durch Benutzer		Ja	3	2	I
HB-Vit-04	Keine BT-Kopplung möglich	Keine automatische Datenübertragung möglich	2	2	I	manuelle Eingabe ermöglichen		Ja	1	2	I
HB-Vit-05	Auswahl falscher Funktion	Falsche Zuordnung eines Wertes	3	3	II	eindeutige Beschreibung und Darstellung der Übersicht		Ja	2	3	I

HB-Vit-06	Fehleingabe von Werten	Flasche Werte zum Vitalparameter zugeordnet	3	2	I	genügend große Tastatur, Löschfunktion der Eingabe		Ja	2	2	I
HB-Vit-07	Ungewolltes Bestätigen der eingegebenen Werte	Inkorrekte Werte im System	3	2	I	nachträgliches Löschen/Bearbeiten ermöglichen	Ja	Ja	1	3	I
HB-Vit-08	Ungewolltes Löschen	Keine Werte im System	2	2	I	Validierung durch Anwender vor Löschen		Ja	2	2	I
HB-Vit-09	Ungewolltes Übertragen der erfassten Werte	Inkorrekte oder unvollständige Werte im System/KIS	3	2	I	Validieren der Übertragung durch Anwender		Ja	2	2	I

Hauptbedienfunktion: Erfassen von Gesundheitswerten											
ID	**Gefährdung**	**Schaden**	**S**	**E**	**RK**	**BHM**	**RW**	**BHM ver?**	**Sn**	**En**	**RKn**
HB-Ges-01	Falsche Interpretation der Darstellung	Aufruf einer falschen Funktion	3	3	II	eindeutige Beschreibung und Darstellung der Übersicht		Ja	2	3	I
HB-Ges-02	Fehleingabe von Werten	Flasche Werte zum Gesundheitswert zugeordnet	2	2	I	genügend große Tastatur, Löschfunktion der Eingabe		Ja	2	2	I
HB-Ges-03	Auswahl falscher Funktion	Falsche Zuordnung eines Wertes	3	3	II	eindeutige Beschreibung und Darstellung der Übersicht		Ja	3	2	I
HB-Ges-04	Fehleingabe von Werten	Flasche Werte zum Gesundheitswert zugeordnet	2	2	I	genügend große Tastatur, Löschfunktion der Eingabe		Ja	1	2	I
HB-Ges-05	Ungewolltes Bestätigen der eingegebenen Werte	Inkorrekte Werte im System	3	3	II	Validierung der Bestätigung, nachträgliches Löschen ermöglichen	Ja	Ja	1	3	I
HB-Ges-06	Ungewolltes Löschen	Keine Werte im System	2	2	I	Validierung durch Anwender vor Löschen		Ja	2	2	I

HB-Ges-07	Ungewolltes Übertragen der erfassten Werte	Inkorrekte oder unvollständige Werte im System/KIS	3	2	I	Validieren der Übertragung durch Anwender		Ja	2	2	I
Hauptbedienfunktion: Fotodokumentation											
ID	**Gefährdung**	**Schaden**	**S**	**E**	**RK**	**BHM**	**RW**	**BHM ver?**	**Sn**	**En**	**RKn**
HB-Wund-01	Fehlinterpretation der Darstellung	Aufruf einer falschen Funktion	1	3	I	eindeutige Beschreibung und Darstellung der Übersicht		Ja	1	2	I
HB-Wund-02	Fehlerhafter Aufruf der Funktion	Aufruf einer falschen Funktion	-	-	-	-	-	-	-	-	-
HB-Wund-03	Aufnahme eines ungewollten Fotos	Inkorrekte Darstellung einer Wunde	2	4	II	Löschen einer Aufnahme ermöglichen	Ja	Ja	1	4	I
HB-Wund-04	Ungewolltes Übertragen von Aufnahmen	Fehlerhafte oder unnötig viele Aufnahmen im System	2	3	I	Validierung des Anwenders vor Übertragung		Ja	2	2	I

Tabelle 15: Risikotabelle der Hauptbedienfunktionen von ilvi

7.3 Risiken durch die Software-Architektur

Hier wurden die Komponenten und Schnittstellen der SW-Architektur auf Risiken untersucht. Die untersuchten Komponenten verursachen Risiken der Klasse I oder keine Risiken, dahingehend ist auch die Klassifizierung der Einzelkomponenten als auch der gesamten Software in Klasse A korrekt.

Folgende Risikomatritzen (Abbildung 30) und Tabelle 16 geben einen Überblick über die Risiken aus der SW-Architektur.

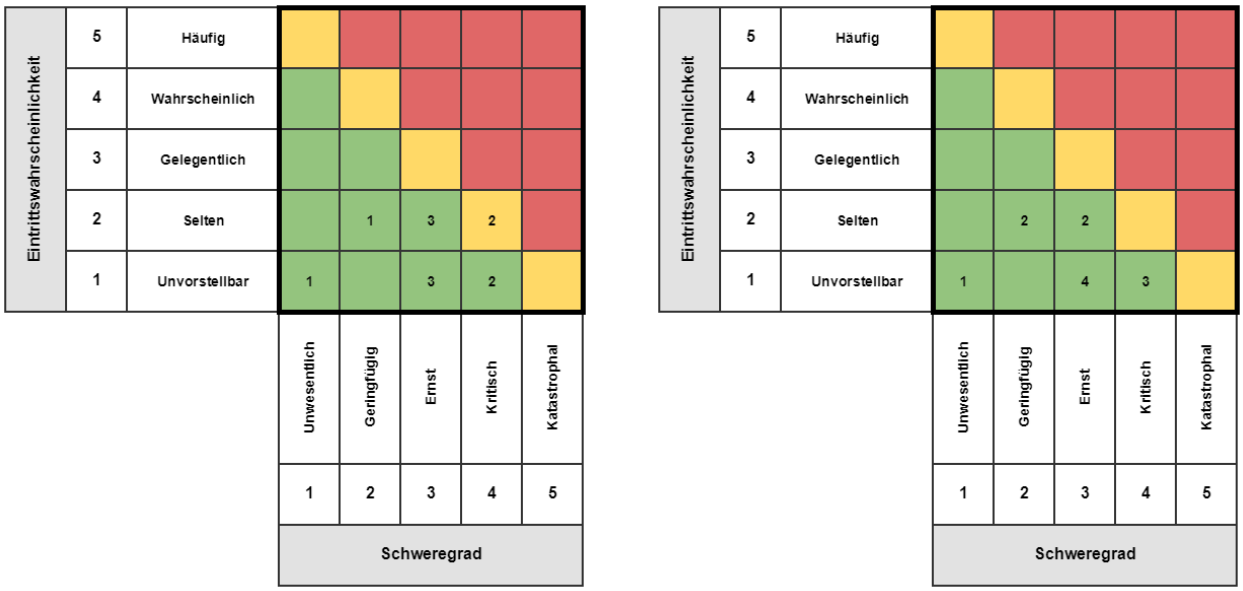


Abbildung 30: Risikomatritzen für die SW-Architektur von ilvi
- von und nach Beherrschungsmaßnahmen

Komponente	ID	Gefährdung	Schaden	E	S	RK	BHM	RW	BHM ver?	En	Sn	RKn
Konfiguration	SWA-01	Fehlerhaftes Mapping der Konfig-Datei	Unvollständige Konfiguration - Anwendung des Produktes nicht möglich	2	4	II	Konfigurationsfile validieren	-	Ja	1	4	I
	SWA-02	Fehlerhaftes Mapping von Daten	Daten werden nicht angezeigt. Daten können nicht versendet werden.	2	4	II	Konfigurationsfile validieren	-	Ja	1	4	I
MessagingCenter	SWA-03	Messages werden nicht weitergeleitet	Startscreen bleibt. Anwendung nicht möglich	2	3	I		-	-	-	-	-
ModuleActivityBuilder	SWA-04	Keine Module-Activities erzeugbar	Module können nicht angezeigt werden.	2	3	I	Eingegebene/Empfangene Werte müssen validiert werden	-	Ja	2	2	I
CoreActivityBuilder	SWA-05	Patientenidentifizierung fehlerhaft	Patienten können nicht mit KIS identifiziert werden	2	3	I		-	-	-	-	-
	SWA-06	Benutzeranmeldung fehlerhaft	Keine Benutzeranmeldung möglich, daher kann Software nicht verwendet werden.	2	2	I		-	-	-	-	-
SendQueue	SWA-07	Fehlerhafte Konfiguration.	Daten werden an falsches KIS übertragen oder gar nicht.	1	4	I	• Korrekte Konfiguration entsprechend des vorhandenen KIS	-	Ja	1	3	I
UpdateObserver	SWA-08	Fehlerhafte Konfiguration oder Networkfileshare	Updates werden nicht erkannt.	1	3	I		-	-	-	-	-

UpdateObserver	SWA-09	Keine Schreibrechte am Networkfileshare	Updates werden nie im Networkfileshare gelöscht. Daher erhöhter Netzwerkverkehr, weil immer wieder eine Übertragung notwendig ist.	1	1	I		-	-	-	-	-
QpdaController	SWA-10	Fehlerhafte Konfiguration	Startscreen bleibt. Einzelne Funktionen lassen sich nicht nutzen. Software wird unbenutzbar.	1	3	I		-	-	-	-	-
DeviceController	SWA-11	Fehlerhafte Konfiguration	Daten werden von einem falschen Medizinprodukt eingelesen. Daten werden falsch gespeichert und daher nicht mehr angezeigt.	1	3	I		-	-	-	-	-
KisController	SWA-12	Fehlerhafte Konfiguration	Patient kann nicht identifiziert werden. KIS-Server erhält keine Messungsdaten. KIS-Server erhält vertauschte Daten.	1	4	I		-	-	-	-	-

Tabelle 16: Risikotabelle der SW-Architektur von ilvi

Gefährdungen aus SOUPS

Da bei der Erstellung der Software auch SOUPS verwendet werden, müssen auch diese auf Risiken untersucht werden. Dabei ist jedoch eine Bewertung der Gefährdungen sehr schwierig, da eine Abschätzung der Eintrittswahrscheinlichkeit bzw. der Ausfallswahrscheinlichkeit nicht möglich ist. Deshalb wurden hier zwar die möglichen Gefährdungen identifiziert, jedoch nicht bewertet. Zur Gewährleistung der Zuverlässigkeit der SOUPS wurden die sog. Bugfixlisten herangezogen, welche Auskunft über behobene Fehler geben. Ebenso wurde die Anzahl der Anwender (wenn möglich) betrachtet. Man kann davon ausgehen, dass eine hohe Anwenderzahl eine hohe Zuverlässigkeit der SOUP bedeuten kann. Um die Funktion der SOUPs aber auch in Verwendung bei ilvi zu gewährleisten, wird diese in Systemtests geprüft und dokumentiert (Tabelle 17).

Name	Hersteller (ggf. URL)	Version	Funktion der SOUP	Bekannte und erkannte Gefährdungen / Einfluss der SOUP auf Software
Serilog, inkl.: - Serilog.Enrichers.Thread - Serilog.Exceptions - Serilog.Sinks.Console - Serilog.Sinks.Debug - Serilog.Sinks.File - Serilog.Sinks.TestCorrelator	https://serilog.net/	2.6.0	Stellt Logging-Funktionalität für Debugging-Zwecke bereit.	Keine Gefährdungen
Zebra Enterprise Home Screen	Zebra	2.8	Stellt KIOSK-Mode für Qpda zur Verfügung. Kann über Software ein- und ausgeschaltet werden.	Einschränkung der Funktionalität des Betriebssystems Bei einem Problem kann ein Zugriff auf die App unmöglich werden.
Name	**Hersteller (ggf. URL)**	**Version**	**Funktion der SOUP**	**Bekannte und erkannte Gefährdungen /**

				Einfluss der SOUP auf Software
EMDK for Xamarin	Zebra	2.7	Stellt Funktionalität zum Scannen, Laden des Geräteprofils, Bereitstellen des verschlüsselten Datenspeicher, zur Verfügung.	Scanner - Zuverlässigkeit Starten der Anwendung Speicherung von Daten (Verschlüsselt/Datenschutz) Daten können über das Endgerät selbst ausgelesen werden
SuperSocket, inkl.: - SuperSocket.ProtoBase - SuperSocket.ClientEngine	http://www.supersocket.net/	1.7.0.17	Erweiterbares Framework für Socketbasierte Kommunikation. Stellt TLS/SSL zur Verfügung.	gesicherte /verschlüsselte Datenübertragung an KIS
Json.NET	Newtonsoft	10.0.3	Bietet Umwandlung von und zu JSON-Objekten	Wandelt JSON Files in Objekte und umgekehrt um. Verwendung im ParserHelper
Plugin.BLE	Adrian Seceleanu	1.3.0	Bietet Vereinfachung der Bluetooth-Kommunikation	Automatische Datenübertragung / BT-Kopplung Bietet fertige Events zur BT-Kommunikation an
SQLite-net	Github	1.5.166	Abstraktionsfunktionalitäten für SQLite Datenbanken	Datenspeicherung in Datenbank
SQLitePCLRaw	Eric Sink	1.1.11	SQL-Bibliothek	Ermöglicht Datenbankzugriff

Name	Hersteller (ggf. URL)	Version	Funktion der SOUP	Bekannte und erkannte Gefährdungen / Einfluss der SOUP auf Software
NeoLua	Neolithos	1.2.25	Lua Implementierung für die Dynamic Language Runtime (DLR)	Datentransformation mit scripts
SharpCifs.Std	Github	0.2.12	Xamarin & .NET Bibliothek	Windows Freigaben lesen und schreiben im .NET
Android-Debug-Database	Github	1.0.3	Library zum Debugggen von Xamarin.Android	Administratoren können damit ein Webservice öffnen, und auf das Storage am Device zugreifen, um Debugging durchzuführen Wird im bestimmungsgemäßen Gebrauch nicht benötigt
Schematron	Daniel Cazzulino	0.6.18	Eine C# high-performance Implementierung von Schematron.	Prüft Config mittels Schemadateien (Schemavaidierung)
FluentScheduler	Jim Geurts	5.3.0	Automatisierter Job-Scheduler inkl. Schnittstelle	Scheduler (Timing für bestimmte Funktionen/Aufgaben)
OptimizedPriorityQueue	BlueRaja	4.1.1	Eine optimierte Priority Queue zur Datenübertragung.	Verwendung in SendQueue
RestSharp	Alexey Zimarev, Michael Hallett	106.5.0	Implementierung zum Verbinden mit einem REST Server.	Datenaustausch mit Backend/KIS

Tabelle 17: Gefährdungen aus SOUPs

7.4 Risiken aus Systemschnittstellen und der Laufzeitumgebung

Dabei wurden Schnittstellen des Systems zur Datenübertragung, aber auch physikalische Schnittstellen, wie die Bedienelemente der Hardware auf Gefährdungen und daraus resultierende Schäden untersucht.

Die Risiken aus Tabelle 18 werden wiederum in Risikomatritzen eingetragen – für die Systemschnittstellen und die Laufzeitumgebung ergeben sich diese wie in Abbildung 31 bzw. Tabelle 18 dargestellt.

Abbildung 31: Risikomatritzen für Systemschnittstellen und die Laufzeitumgebung - vor und nach Beherrschungsmaßnahmen

Komponente	ID	Gefährdung	Schaden	E	S	RK	BHM	RW?	BHM ver?	En	Sn	RKn
Touchscreen, Hardbuttons	LZ-HW-01	Touchscreen fällt aus.	Anwendung des Systems nicht möglich, verzögerte Behandlung, Datenverlust	2	4	II	Gerät mit hoher Zuverlässigkeit verwenden entsprechende Anforderungen an HW		Ja	1	4	I
	LZ-HW-02	Bildschirm fällt aus, Touchscreen funktioniert	Fehlerhafte Datenerfassung, unbeabsichtigte Datenübertragung	1	4	I			-	-	-	-
	LZ-HW-03	Hardbuttons (einzelne, alle) funktionieren nicht	Scanner kann nicht aktiviert werden	2	3	I	Gerät mit hoher Zuverlässigkeit verwenden entsprechende Anforderungen an HW		Ja	1	3	I
	LZ-HW-04	Verwechslung der Hardbuttons mit Akkuauswurf	Ungewollter Auswurf des Akkus	2	2	I		-	-	-	-	-

Komponente	ID	Gefährdung	Schaden	E	S	RK	BHM	RW?	BHM ver?	En	Sn	RKn
Elektrische Schnittstellen	LZ-HW-05	Akku fällt aus oder wird unerwartet leer	Unvollständige Datenübertragung Datenverlust	2	4	II	• Warnhinweis vor Ausfall des Akkus • Hochwertigen Akku verwenden		Ja	2	2	I
Datenschnittstelle - WLAN	LZ-Dat-01	Device-WLAN fällt aus.	Keine Datenübertragung ans KIS	2	3	I	Lokale Speicherung der Daten		Ja	2	2	I
Datenschnittstelle - Bluetooth	LZ-Dat-02	Bluetooth fällt aus.	Keine automatische Datenerfassung möglich	2	2	I	manuelle Erfassung ermöglichen		Ja	2	2	I
Datenschnittstelle - NFC	LZ-Dat-03	NFC funktioniert nicht	Anmeldung des Benutzers nicht möglich.	2	2	I	Gerät mit hoher Zuverlässigkeit verwenden entsprechende Anforderungen an HW Anmeldung über Barcode ermöglichen		Ja	1	4	I

Komponente	ID	Gefährdung	Schaden	E	S	RK	BHM	RW?	BHM ver?	En	Sn	RKn
Datenschnittstelle - Barcodescanner	LZ-Dat-04	Barcodescanner funktioniert nicht	Benutzer/Patient kann nicht angemeldet werden, Admin-Anmeldung nicht möglich.	2	3	I	Gerät mit hoher Zuverlässigkeit verwenden entsprechende Anforderungen an HW		Ja	1	2	I
Datenschnittstelle - Kamera	LZ-Dat-05	Kamera funktioniert nicht.	Keine Wunddokumentation möglich.	2	2	I	Gerät mit hoher Zuverlässigkeit verwenden entsprechende Anforderungen an HW		Ja	1	3	I
Datenschnittstelle - Filesystem (Share)	LZ-Dat-06	Filesystem funktioniert nicht, Daten werden fehlerhaft gespeichert	Arbeiten mit System nicht möglich, korrupte oder keine Daten	1	3	I		-	-	-	-	-

Komponente	ID	Gefährdung	Schaden	E	S	RK	BHM	RW?	BHM ver?	En	Sn	RKn
Benutzer- und Patienten-anmeldung	LZ-User-01	Barcode wird falsch interpretiert.	Falscher Anwender oder Pat. identifiziert. Keine Identifizierung möglich,	2	4	II	Nur definierte Barcodes zulassen Anzeige des Patientennamen		Ja	1	3	I
	LZ-User-02	fehlerhaftes Mapping der ID	Falscher Anwender oder Pat. identifiziert. Keine Identifizierung möglich	2	3	I	Anzeige des Pat.-Namen Anzeige des Anwenders Meldung bei Fehler		Ja	2	2	I
	LZ-User-03	Keine Antwort des Servers	Keine Anmeldung möglich	3	2	I	Fehlermeldung		Ja	3	1	I
	LZ-User-04	Fehlerhaftes Mapping	Fehlerhafte Anzeige von Anwender oder Patientendaten.	2	3	I	Fehlermeldung für Anwender		Ja	2	2	I
Komponente	**ID**	**Gefährdung**	**Schaden**	**E**	**S**	**RK**	**BHM**	**RW?**	**BHM ver?**	**En**	**Sn**	**RKn**

Laufzeitsicht - Empfangen von Vital-parametern (Bluetooth)	LZ-Data-01	Kopplung zu falschem Gerät	Falsche Daten werden empfangen	3	3	II	Korrekte Kopplung über NFC-Trigger auslösen	Ja	Ja	2	3	I
	LZ-Data-02	Verbindungsabbruch	Keine Daten	2	2	I	Warnhinweis manuelle Eingabe ermöglichen		Ja	2	1	I
	LZ-Data-03	Beeinflussung von anderen Medizinprodukten	Fehlfunktion anderer MP	3	3	II	Einhaltung der vorgegebenen EMV-Richtlinien		Ja	1	3	I
Laufzeitsicht (NFC-Trigger)	LZ-Data-04	Fehlerhaftes Mapping	Korrupte Daten im System, Datenübertragung nicht möglich, Fehlerhafte BT-Kopplung	2	2	I	Validierung der Datenübertragung durch Anwender Warnhinweise bei Fehler		Ja	2	1	I
Komponente	**ID**	**Gefährdung**	**Schaden**	**E**	**S**	**RK**	**BHM**	**RW?**	**BHM ver?**	**En**	**Sn**	**RKn**
	LZ-Data-05	Kein WLAN-Empfang	Keine Datenübertragung möglich	3	2	I	Lokale Speicherung am Gerät	Ja	Ja	3	1	I

Laufzeitsicht - Übertragen von Daten an ein KIS	LZ-Data-06	Falsches Mapping-Format,	Korrupte Daten im KIS, Daten können nicht interpretiert werden	2	3	I	Fehlermeldung bei korrupter Datenübertragung (via ACK)		Ja	2	2	I
	LZ-Data-07	Verbindungsabbruch	Keine Datenübertragung, keine Daten im KIS	2	3	I	Acknowledge bei Datenübertragung		Ja	2	2	I
Laufzeitsicht - Einspielen eines Konfig-Files	LZ-Konfig-01	Keine Verbindung zu Konfig-Ordner	Kein Konfig-File vorhanden	2	3	I	Übertragung erfolgt über Filesystem (Share)	Ja	Ja	1	1	I
	LZ-Konfig-02	Korruptes Konfig-File am Share-Ordner	Korruptes Konfig-File am System	2	3	I	Validierung des Konfig-Files bei Erstellung Schema-Check bei Einlesen des Files		Ja	1	1	I
	LZ-Konfig-03	Feherhaftes Konfig-File wird als korrektes interpretiert	Fehlerhaftes Konfig-File am System	2	3	I	Sofern vorhanden, wird ein altes, funktionierendes File verwendet, Schema-check		Ja	1	1	I
Laufzeitsicht - Update		Update bei nicht übertragenen Daten	Lokal gespeicherte Daten werden gelöscht.	2	3	I	Kein Zugriff auf das encrypted Filesystem bei		Ja	2	2	I

	LZ-Update-01						Update. Lokal gespeicherte Daten bleiben erhalten.						
	LZ-Update-02	Betrieb mit veralteter, möglicherweise fehlerhafter SW-Version.	Ggf. keine Benutzung des Systems möglich	2	2	I	Installation gemäß Handbuch		Nein	2	2	I

Tabelle 18: Risikotabelle der Systemschnittstellen und der Laufzeitumgebung von ilvi

7.5 Rückwirkungen und Risiken aus Risikobeherrschungsmaßnahmen

Es ist möglich, dass die definierten Risikobeherrschungsmaßnahmen ebenfalls eine Gefährdung bzw. ein Risiko hervorrufen können. Dahingehend wurden die Risikobeherrschungsmaßnahmen aus den vorherigen Risikoanalysen auf eine Rückwirkung dazu untersucht (Tabelle 19 und Abbildung 32).

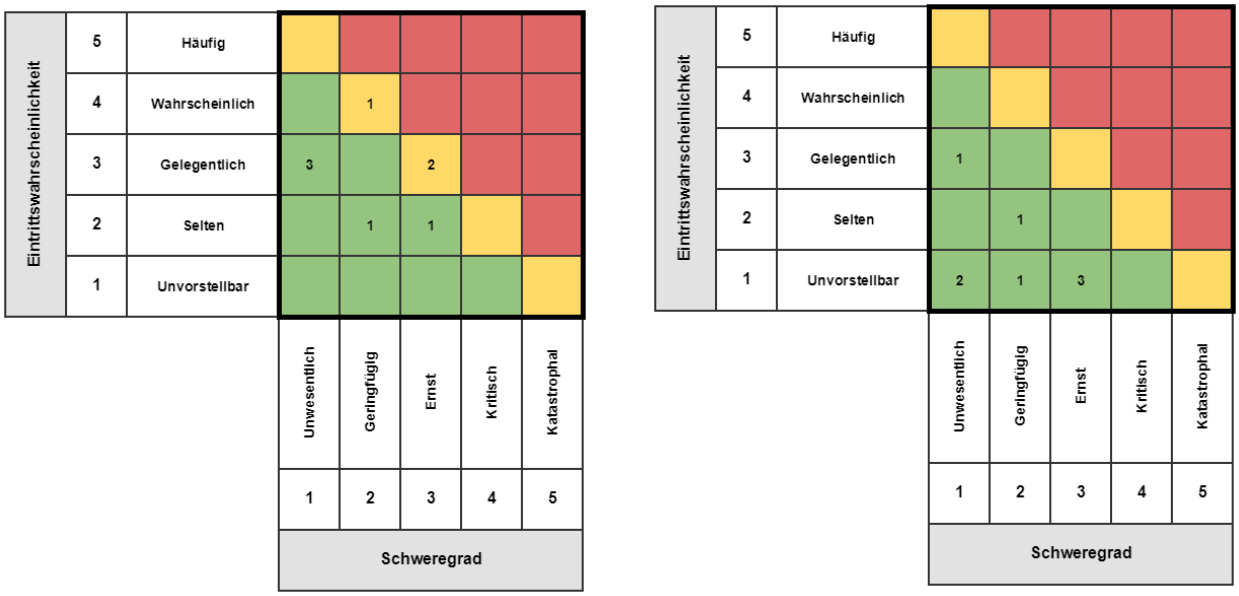


Abbildung 32: Risikomatritzen für Rückwirkungen aus Beherrschungsmaßnahmen

Benutzungsszenarien												
ID des ursprünglichen Risikos	**Risiko-ID**	**Gefährdung**	**Schaden**	**S**	**E**	**RK**	**BHM**	**RW**	**BHM Ver?]**	**Sn**	**En**	**RKn**
BS-Vit-03	RW-01	Es können nicht alle Vitalwerte erfasst werden	Unvollständige Daten	1	3	I	Ermöglichen, dass per 'Longpress' auch Werte außerhalb der definierten Grenzen eingegeben werden können		Ja	1	1	I
BS-Vit-09 BS-Ges-07 BS-Wund-07	RW-02	Gefahr von Missbrauch von Patientendaten	Eingriff in die Privatsphäre des Patienten	3	3	II	Verschlüsselung der lokal gespeicherten Daten Daten werden in einem 'encrypted filesystem' abgelegt		Ja	3	1	I
BS-Wund-05	RW-03	Unbeabsichtigtes Löschen einer Aufnahme	Datenverlust	2	4	II	Abfrage an Benutzer, ob die Aufnahme tatsächlich gelöscht werden soll		Ja	2	2	I

Hauptbedienfunktionen												
ID des ursprünglichen Risikos	**Risiko-ID**	**Gefährdung**	**Schaden**	**S**	**E**	**RK**	**BHM**	**RW**	**BHM ver?]**	**Sn**	**En**	**RKn**
HB-User-03 HB-User-04	RW-04	Das System kann nicht benutzt werden, wenn die Abfrage der ID fehlerhaft ist.	Verzögerung der Behandlung	1	3	I		-	-	-	-	-
HB-Vit-07 HB-Ges-05 HB-Wund-03	RW-05	Ungewolltes Löschen von Vital- und Gesundheitswerten oder Bildaufnahmen	Erneute Erfassung der Werte	1	3	I	Abfrage an Benutzer, ob die Aufnahme tatsächlich gelöscht werden soll		ja	1	1	I
Systemschnittstellen und Laufzeitumgebung												
ID des ursprünglichen Risikos	**Risiko-ID**	**Gefährdung**	**Schaden**	**S**	**E**	**RK**	**BHM**	**RW**	**BHM ver?**	**Sn**	**En**	**RKn**
LZ-Data-05	RW-06	Gefahr von Missbrauch von Patientendaten	Eingriff in die Privatsphäre des Patienten	3	3	II	Verschlüsselung der lokal gespeicherten Daten Daten werden in einem 'encrypted filesystem' abgelegt		Ja	3	1	I

Systemschnittstellen und Laufzeitumgebung												
ID des ursprünglichen Risikos	**Risiko-ID**	**Gefährdung**	**Schaden**	**S**	**E**	**RK**	**BHM**	**RW**	**BHM ver?**	**Sn**	**En**	**RKn**
LZ-Data-01	RW-07	Möglichkeit der Manipulation des NFC-Tags	Erfassen falscher Daten	3	2	I	Read-only NFC-Tags verwenden Base-64-Codierung beim Auslesen der Tag-Daten		Nein	3	1	I
LZ-Konfig-01	RW-08	Möglicher Zugriff auf ein falsches Filesystem	Kein Zugriff auf das Kofigurationsfile	2	2	I	Sofern vorhanden, wird ein altes, funktionierendes File verwendet, Schema-check		Ja	2	1	I

Tabelle 19: Risikotabelle der Rückwirkungen aus Risikobeherrschungsmaßnahmen von ilvi

7.6 Bewertung des Gesamt-Restrisiko

Wurden sämtliche Risiken bewertet und geeignete Beherrschungsmaßnahmen für inakzeptable Risiken eingeführt, muss der Hersteller das danach bestehende Gesamt-Restrisiko bewerten. Hierfür soll der Hersteller ‚*aus einer umfassenden Perspektive das Restrisiko betrachten*' [10]. Es sollen also die verbleibenden Risiken in ihrer Kombination auf Akzeptanz (oder Nichtakzeptanz) beurteilt werden.

Um diese Bewertung durchführen zu können, kann wieder eine Risikomatrix herangezogen werden, in welcher sämtliche Restrisiken (nach Beherrschungsmaßnahmen) eingetragen sind. Anhand der Akzeptanzkriterien wird untersucht, ob sich sämtliche Einzelrisiken auf einem akzeptablen Niveau befinden. Es muss aber auch die Kombination aus den Einzelrisiken und die Kombination von Beherrschungsmaßnahmen untersucht werden. Beispielswese kann ein Warnhinweis in einer Software ein Einzelrisiko minimieren – treten diese Warnhinweise jedoch gehäuft auf, kann die Wirkung eines einzelnen Hinweises verringert werden (Überforderung des Anwenders durch zu viele Warnungen).

Es ist daher notwendig, das Gesamtrestrisiko mit dem Nutzen des Produktes zu vergleichen. Überwiegt der Nutzen dem Restrisiko, kann das Produkt freigegeben werden.

Für ilvi stellt sich die Gesamt-Risikomatrix nach Einführung von Beherrschungsmaßnahmen wie in Abbildung 33 dar.

Anhand des schon beschriebenen Nutzens überwiegt dieser den Restrisiken. Dabei bleibt es auch zu erwähnen, dass *ilvi* mit dessen Anwendung eine Risikominderung im Vergleich zu Alternativmethoden hervorbringt (Vermeidung von Eingabefehlern, sichere und

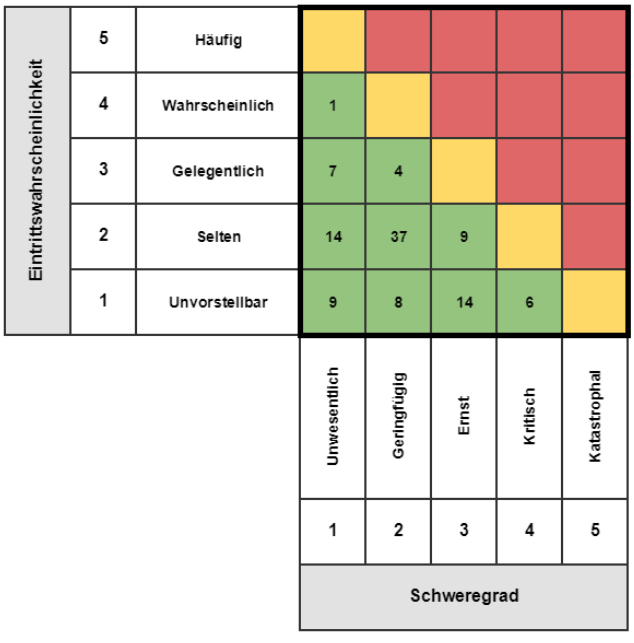


Abbildung 33: Gesamtrestrisikomatrix für ilvi

schnellere Datenübertragung), und es somit auch unter Betrachtung der Restrisiken und des Gesamtrestrisikos zu einer Überwiegung des Nutzens zu den Risiken kommt.

7.7 Marktüberwachung aus nachgelagerten Phasen

Wie schon im Kapitel ‚Risikomanagementprozess' beschrieben, endet dieser nicht mit der Freigabe bzw. In-Verkehr-Bringung des Produktes. Die EN ISO 14971 sieht vor bzw. fordert, dass Informationen aus der nachgelagerten Phase (der In-Verkehrbringung nachgelagert) in das Risikomanagement einfließen müssen. Dafür muss der Hersteller einen geeigneten Prozess oder Methoden bestehend haben, um diese Informationen auch zu erhalten. Idealerweise wird dafür eine Verfahrensanweisung in das QMS integriert. Darin werden spezifische Aufzeichnungen der Behörden, Informationen aus Kundenreklamationen, Informationen der verwendeten SOUPS, neue Normen und Richtlinien als auch Daten durch aktives Kundenfeedback berücksichtigt.

Diese neuen Informationen dienen zum einen der Anpassung der Risikobewertung – möglicherweise wurden Schadenshöhen oder Eintrittswahrscheinlichkeiten falsch abgeschätzt, zum anderen werden eventuell neue Funktionen oder Komponenten in das Produkt integriert – welche ebenfalls auf Risiken untersucht werden müssen.

Somit muss das Risikomanagement über den gesamten Produktlebenszyklus angewandt werden. Risikoanalyse, -bewertung und ggf. –beherrschungsmaßnahmen müssen immer aktuell gehalten und angepasst werden.

Für neue Funktionen bzw. Produktiterationen ist dies selbstverständlich, aber eben auch durch oben genannte Informationen aus im Markt befindlichen Produkten muss die Risikomanagement-Akte aktuell gehalten werden.

8 Diskussion und Schlussfolgerung

Die Anwendung von Software ist heute in der Medizin nicht mehr wegzudenken. Dabei spielt Software für mobile Anwendungen eine immer tragendere Rolle. Hierbei ist es wichtig, diese Software auf einem konformen Weg zur Marktzulassung zu bringen.

Ein Teil dieser Marktzulassung ist ein adäquates Risikomanagement – wie es in dieser Arbeit durchgeführt wurde.

So wurden im Zuge dieser Arbeit aber nicht nur die Aspekte des Risikomanagements dargelegt, sondern auch der Weg der Risiko-Klassifizierung, des Qualitätsmanagements und weiterer relevanter Normen sowie deren Zusammenhänge bei der Entwicklung medizinischer Software. Der Fokus wurde aber auf das Risikomanagement gemäß den regulatorischen Anforderungen gelegt.

Im Zuge dieser Arbeit wurde unter anderem nach den Methoden der FMEA, FTA, SWIFT als auch des Ishiwaka-Diagramms gearbeitet.

Hieraus zeigte sich, dass es im Risikoteam am effizientesten war, die SWIFT-Methode anzuwenden, da hierbei auch Personen Input liefern konnten, die kein regulatorisches oder methodisches Hintergrundwissen besitzen.

Mittels den durchgeführten Risikoanalysen, konnten 109 Einzelrisiken identifiziert und bewertet werden. Zur Bewertung wurde aufgrund der fehlenden Erfahrung aus vorangegangen Entwicklungen meist auf Expertenmeinungen zurückgegriffen. Es wird sich im Laufe der Marktüberwachung zeigen, ob diese Bewertungen gegebenenfalls aktualisiert werden müssen.

Durch die in dieser Arbeit durchgeführten Risikoanalysen, -bewertungen und die eingeführten Risikobeherrschungsmaßnahmen konnte das System *‚ilvi‘* von Seiten des Risikomanagements zur Freigabe vorbereitet werden. Durch geeignete Wahl von Beherrschungsmaßnahmen konnten 27 inakzeptable Risiken auf ein akzeptables Niveau gebracht werden.

Die definierten Beherrschungsmaßnahmen wurden als Software-Anforderungen aufgenommen – welche in weiterer Folge über Systemtests verifiziert wurden. Die dabei notwendige Rückverfolgbarkeit war durch die Verwendung einer eindeutigen ID im Dokumentationssystem klar strukturiert.

Nach der erfolgten Markteinführung muss eine aktive Marktbeobachtung von Seiten des Herstellers durchgeführt und dokumentiert werden, um das Risikomanagement weiterhin konform zu betreiben.

9 Literaturverzeichnis

[1] C. Bräutigam, P. Enste, M. Evans, J. Hilbert, S. Merkel, and F. Öz, *Digitalisierung im Krankenhaus. Mehr Technik – bessere Arbeit?* 2017.

[2] "Richtlinie 2006/42/EG des europäischen Parlaments und des Rates vom 17.05.2006 über Maschinen und zu Änderung der Richtlinie 95/16/EG."

[3] European Commission, "Richlinie 93/42/EWG über Medizinprodukte," 2007.

[4] "Richtlinie 98/79/EG des europäischen Parlaments und des Rates über In-vitro-Diagnostika."

[5] "Richtlinie 90/385/EWG des europäischen Parlaments über implantierbare aktive Medizinprodukte."

[6] D. C. Johner, "Software als Medizinprodukt: Definitionen und Klassifizierungshilfen," 2018.

[7] A. Gärtner, "MEDDEV-Leitfaden 2.1/6 für Software als Medizinproduktam Beispiel PDMS," 2012.

[8] European Commission, *MEDICAL DEVICES : Guidance document 2.1/6 GUIDELINES ON THE QUALIFICATION AND CLASSIFICATION OF STAND ALONE SOFTWARE USED IN HEALTHCARE WITHIN THE REGULATORY FRAMEWORK OF MEDICAL DEVICES*. EU-Kommision, 2016.

[9] "EN ISO 13485: Medizinprodukte - Qualitätsmanagementsysteme - Anforderungen für regulatorische Zwecke, europäische, harmonisierte Fassung der Norm ISO 13485." 2016.

[10] ISO, "ISO 14971 - Medizinprodukte -Anwendung des Risikomanagements auf Medizinprodukte." .

[11] "EN 62304: Medizingeräte-Software - Lebenszyklusprozesse, europäische, harmonisierte Fassung der Norm IEC 62304."

[12] "EN 62366: Anwendung der Gebrauchstauglichkeit auf Medizinprodukte, europäische, harmonisierte Fassung der Norm IEC 62366."

[13] "EN 60601-1: Medizinische elektrische Geräte; Teil 1: Allgemeine Festlegungen für die Sicherheit einschließlich der wesentlichen Leistungsmerkmale."

[14] European Commission, "MEDICAL DEVICES: 2.4/1 Rev.9 Guidance document-Classification of medical devices.," vol. MEDDEV 2.4, 2010.

[15] "ISO 9001: Qualitätsmanagementsysteme - Anforderungen."

[16] C. Johner, M. Hölzer-Klüpfel, and S. Wittorf, *Basiswissen Medizinische Software*. dpunkt.verlag, 2015.

[17] J. Harer, *Anforderungen an Medizinprodukte : Praxisleitfaden für Hersteller und Zulieferer*. Hanser, 2014.

[18] "EN 31010 Risikomanagement - Verfahren zur Risikobeurteilung." 2010.

[19] M. Werdich, *FMEA - Einführung und Moderation*. 2011.

[20] N. Leitgeb, *Sicherheit von Medizingeräten. Recht-Risiken-Chancen*. 2010.