

INSTITUT FÜR INFORMATIK  
DER TECHNISCHEN UNIVERSITÄT MÜNCHEN

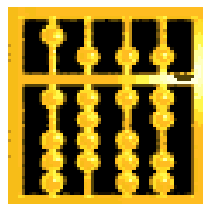
Diplomarbeit

**Richtlinienkonforme Softwareentwicklung von  
Medizinprodukten am Beispiel eines  
internetbasierten CTG Monitors mit LabVIEW**

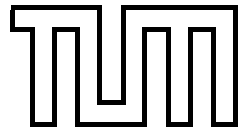
Bearbeiter: Christian Harböck

Aufgabensteller: Prof. Dr. Manfred Broy

Betreuer: Dr. Martin Daumer  
Dr. Bernhard Schätz







INSTITUT FÜR INFORMATIK  
DER TECHNISCHEN UNIVERSITÄT MÜNCHEN

**Diplomarbeit**

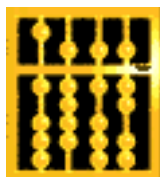
Richtlinienkonforme Softwareentwicklung von  
Medizinprodukten am Beispiel eines  
internetbasierten CTG Monitors mit LabVIEW

Bearbeiter: Christian Harböck

Aufgabensteller: Prof. Dr. Manfred Broy

Betreuer: Dr. Martin Daumer  
Dr. Bernhard Schätz

Abgabetermin: 15. März 2001



Hiermit versichere ich, daß ich die vorliegende Diplomarbeit selbständig verfaßt und keine anderen als die angegebenen Quellen und Hilfsmittel verwendet habe.

München, den 15. März 2001

.....  
*(Unterschrift des Kandidaten)*



# Danksagung

Herrn Dr. Martin Daumer danke ich für die intensive Betreuung und die Einführung in den für mich äußerst interessanten Bereich der anwendungs- und industrienahen Forschung. Ohne seinen Einsatz und die Anbindung an die von ihm zusammen mit Herrn Dipl.-Stat. Scholz gegründete Firma Trium - Analysis Online wäre die Arbeit in dieser Form nicht möglich gewesen. Trium danke ich für die Möglichkeit der Teilnahme an Schulungen und der Finanzierung der Beratungsfirma. Herrn Scholz danke ich für zahlreiche hilfreiche Kommentare hinsichtlich JavaScript Programmierung.

Herrn Dipl. Ing. Michael Justen von der Firma EUROCAT danke ich für zahlreiche nützliche Kommentare.

Herrn Prof. Dr. Albrecht Neiß und dem Institut für Medizinische Statistik und Epidemiologie der Technischen Universität München danke ich für eine wissenschaftlich anregende Forschungsatmosphäre sowie die Möglichkeit der Teilnahme und Finanzierung an der Fachtagung MEDICA während meiner Zeit als Diplomand.

Herrn Prof. Dr. Manfred Broy vom Lehrstuhl für Informatik IV „Software and Systems Engineering“ danke ich für die Bereitschaft, diese interdisziplinäre Arbeit von Seiten der Informatik aus zu begleiten.

Herr Dr. Bernhard Schätz vom Lehrstuhl für Informatik IV „Software and Systems Engineering“ danke ich für seinen Einsatz und Unterstützungsbereitschaft.

Meiner Freundin danke ich für die entgegengebrachte Geduld und die Ausdauer diese Zeit durchzustehen.



# Inhaltsverzeichnis

<b>1</b>	<b>Einleitung und Motivation</b>	<b>1</b>
<b>2</b>	<b>Das Medizinproduktegesetz</b>	<b>5</b>
2.1	Anforderungen . . . . .	5
2.2	Problematik durch das MPG . . . . .	10
<b>3</b>	<b>Der Zertifizierungsprozeß</b>	<b>13</b>
3.1	Zertifizierung nach CE . . . . .	13
3.1.1	Zweckbestimmung . . . . .	13
3.1.2	Klassifizierung . . . . .	15
3.1.3	Konformitätsbewertungsverfahren . . . . .	17
3.1.4	Risikomanagement . . . . .	22
3.1.5	Risikoanalyse . . . . .	27
3.1.6	Technische Dokumentation . . . . .	30
3.2	Anforderungen der FDA . . . . .	31
3.2.1	Anforderungen an die Dokumentation . . . . .	32
3.2.2	Off the Shelf Software . . . . .	36
<b>4</b>	<b>V-Modell</b>	<b>39</b>
4.1	Systemerstellung . . . . .	41
4.2	Projektmanagement . . . . .	43
4.3	Qualitätssicherung . . . . .	44
4.4	Konfigurationsmanagement . . . . .	45
4.5	Tailoring . . . . .	46
4.6	Handbuchsammlung . . . . .	46
<b>5</b>	<b>Umsetzung</b>	<b>51</b>
5.1	Zielsetzung . . . . .	51

5.2	Das Beispielprojekt . . . . .	51
5.2.1	Das Unternehmen . . . . .	51
5.2.2	Projektbeschreibung . . . . .	52
5.2.3	Ausgangssituation . . . . .	53
5.2.4	Vorgehensweise . . . . .	54
5.2.5	Projektdurchführung . . . . .	56
5.3	Anforderungszuordnung . . . . .	67
5.3.1	Tailoring . . . . .	68
5.3.2	Projektmanagement . . . . .	69
5.3.3	Konfigurationsmanagement . . . . .	71
5.3.4	Systemerstellung . . . . .	74
5.3.5	Qualitätssicherung . . . . .	78
5.3.6	Risikomanagement . . . . .	81
5.4	Bewertung . . . . .	83
<b>6</b>	<b>Konforme Entwicklung mit LabVIEW</b>	<b>87</b>
6.1	Was ist LabVIEW . . . . .	87
6.2	Das VI Metrik Tool . . . . .	88
6.3	Source Code Control . . . . .	89
6.4	Documentation Tool . . . . .	90
6.5	Entwicklungsstrategie . . . . .	91
6.6	Zusammenfassung . . . . .	91
<b>7</b>	<b>Zusammenfassung</b>	<b>93</b>
<b>A</b>	<b>Risikoanalyse Plan</b>	<b>95</b>
A.1	Zweck und Geltungsbereich . . . . .	95
A.2	Kriterien für die Risikoeinstufung . . . . .	95
A.2.1	Schadensausmaß . . . . .	95
A.2.2	Schadenshäufigkeit . . . . .	96
A.2.3	Risikograph und Akzeptanzbereiche . . . . .	96
A.2.4	Akzeptanzkriterien und Zielsetzungen für die Risikominderung . . .	97
A.3	Risiken . . . . .	98
A.3.1	Hauptgefährdungen . . . . .	99
A.3.2	Risiken die sich aus peripheren Einflüssen ergeben . . . . .	99
A.3.3	Risiken die sich aus Internen Einflüssen ergeben: . . . . .	105

A.4	Änderungen . . . . .	107
<b>B</b>	<b>Risikoanalyse Report</b>	<b>109</b>
B.1	Zweck und Geltungsbereich . . . . .	109
B.2	Kriterien für die Risikoeinstufung . . . . .	109
B.2.1	Risikograph und Akzeptanzbereiche . . . . .	109
B.2.2	Akzeptanzkriterien und Zielsetzungen für die Risikominderung . . .	110
B.3	Rest - Risiken . . . . .	112
B.3.1	Risiken die sich aus peripheren Einflüssen ergeben . . . . .	113
B.3.2	Risiken die sich aus Internen Einflüssen ergeben: . . . . .	119
B.4	Änderungen . . . . .	120

# Kapitel 1

## Einleitung und Motivation

Seit einigen Jahren findet man in Krankenhäusern und Kliniken vermehrt elektronische Geräte, die für den Einsatz am Patienten konzipiert sind. Im medizinischen Umfeld wird hierbei die Bezeichnung **P**rogrammierbare **E**lektronisch **M**edizinische **S**ysteme - kurz PEMS - benutzt. Waren es früher noch häufig reine Hardwaregeräte, findet man heute immer öfter Software in PEMS an. Die Palette reicht hierbei vom Embedded System bis hin zur Standalone Softwarelösung.

Bedingt durch ihr Anwendungsfeld birgt ein Teil dieser Geräte ein hohes Gefährdungspotential gegenüber Patienten und Anwender in sich, weshalb der Gesetzgeber sich verpflichtet sah, regulatorische Maßnahmen zu ergreifen. So wurde 1998 der zweite Entwurf des Medizinproduktegesetzes (MPG) verabschiedet und ist seither auf alle Medizinprodukte zwingend anzuwenden.

Für die Hersteller von Medizinprodukten bedeutet dies, daß ihre Produkte zertifiziert werden müssen. Das Ziel der Zertifizierung ist, zu belegen, daß das Produkt konform den gängigen Normen und Richtlinien entwickelt und produziert wurde. Die Zertifizierung erfolgt hierbei in einem europaweit anerkannten Verfahren und wird mit der CE-Kennzeichnung abgeschlossen.

Der Zertifizierungsprozeß sollte von den Herstellern allerdings nicht nur als zusätzliche Pflicht gesehen werden, da bei konsequenter Anwendung der geforderten Prozesse, folgende Vorteile entstehen<sup>1</sup>:

- Verringerung der Fehleranfälligkeit
- Erhöhte Akzeptanz beim Kunden
- Verringertes Risiko für Anwender und Patienten
- Erhöhung der Zuverlässigkeit des Systems
- Geringeres Haftungsrisiko für den Hersteller
- Schnelleren Anpassungen an veränderte Marktanforderungen

---

<sup>1</sup>aus <http://www.eurocat.de/de/test/vorteile.html>

- Leichtere Revalidierung nach Änderungen an der Software

Als zusätzlicher Faktor sollte noch bedacht werden, daß gerade in einer kleinen Branche wie dem Medizinproduktemarkt, ein Imageverlust des Produktes oder gar des Herstellers, eine weitaus stärkere Belastung bedeuten kann.

Im Rahmen dieser Diplomarbeit soll erörtert werden, welche Anforderungen und Maßnahmen für die Erfüllung der gesetzlichen Vorschriften durchzuführen sind. Die Umsetzung soll an einem internetbasierten Programm zur automatisierten Befundung und Visualisierung von Cardiotokogrammen (CTG) durchgeführt werden, das in einer vorangegangenen Diplomarbeit<sup>2</sup> erstellt wurde. Die Umsetzung wird von einer Zertifizierungsstelle (man spricht in diesem Zusammenhang auch von einer Benannten Stelle) geprüft und soll die Konformität mit den Richtlinien bestätigen. Darüber hinaus wird untersucht, ob die Anwendung des „Entwicklungsstandard für IT Systeme des Bundes, Vorgehensmodell“, kurz V-Modell, für die Anforderungen einer Zertifizierung medizinischer Geräte ausreicht und welche zusätzlichen Aktivitäten und Produkte zu erstellen sind.

### **Medizinischer Hintergrund**

Die Kardiotokographie (CTG) ist das am häufigsten eingesetzte Verfahren zur Überwachung von Schwangerschaften und Geburten. Als Meßwerte gehen zum einen die fetale Herzfrequenz und zum anderen die Wehentätigkeit der Frau ein. Je nach Gerätetyp können zusätzliche Werte wie die Kindsbewegung oder die Sauerstoffsättigung erfaßt werden. Standard CTG-Monitore beschränken sich meist auf die Visualisierung der Meßwerte, die Beurteilung bleibt dem klinischen Fachpersonal überlassen. Der Arzt bzw. die Geburtshelferin bestimmen aus aufgezeichneten Meßwerten die sogenannte Baseline - eine Art Mittelwertslinie, die als Basis aller weiteren Klassifikatoren benutzt wird. Im weiteren werden die Anzahl, Dauer und Stärke von „Abweichungen“ von der Baseline bestimmt, anhand deren letztendlich die Klassifizierung des CTGs vorgenommen wird. Die Klassifizierung selbst erfolgt über ein definiertes Regelwerk sogenannte „Scores“.

Das Programm geht analog dem hier skizzierten Verfahren vor. Es bestimmt die Baseline und berechnet hieraus die Klassifikatoren. Als Grundlage der Klassifizierung dient die Empfehlung der FIGO(International Federation of Gynecology and Obstetrics).

### **Aufbau dieser Arbeit**

Das folgende Kapitel erläutert die gesetzlichen Anforderungen durch das Medizinproduktegesetz im Detail. Neben den erforderlichen Definitionen werden die Unterschiede von Medizinproduktegesetz, Medizinprodukteverordnung und Richtlinien erklärt.

Kapitel drei erörtert die Anforderungen der Medizinprodukteverordnung und der Europäischen Richtlinie 93/42/EWG. Darüber hinaus soll ein Einblick in die Anforderungen des amerikanischen Marktes gegeben werden, die von der Food and Drug Administration (FDA) - die amerikanische Gesundheitsbehörde - überprüft wird.

Kapitel vier stellt das V-Modell 97 vor.

Das fünfte Kapitel beschreibt die Umsetzung der Anforderungen der Norm EN60601-1-4 in Produkte. Als Ziel soll hierbei eine Zertifizierung für den europäischen Markt erreicht

---

<sup>2</sup>siehe [Gol00]

werden. Weiterhin wird untersucht, ob das V-Modell als Entwicklungslebenszyklus für diesen Einsatz geeignet ist und anhand einer Zuordnungstabelle gezeigt, welche Produkte für die Zertifizierung medizinischer Software mindestens benötigt werden.

In Kapitel sechs soll das Entwicklungswerkzeug LabVIEW - eine graphische Programmiersprache der Firma National Instruments - auf ihre Tauglichkeit und Unterstützung bezüglich der Entwicklung medizinischer Software untersucht werden, insbesondere hinsichtlich der Anforderungen, die aus Sicht des Qualitätsmanagements gestellt werden.

Die Arbeit wird durch eine Zusammenfassung und einen Ausblick abgeschlossen.



# Kapitel 2

## Das Medizinproduktegesetz

Das 1998 aus der europäischen Richtlinie 93/42/EWG (MDD) in deutsches Recht überführte Medizinproduktegesetz (MPG) ist seit dem 14. Juni 1998 zwingend anzuwenden. Das Medizinproduktegesetz regelt nach §1 den Verkehr von Medizinprodukten und somit die Sicherheit, Eignung und Leistung der Medizinprodukte. Weiterhin wird die Gesundheit und der erforderliche Schutz der Patienten, Anwender und Dritter geregelt. Für die Erfüllung von §1 wird eine Reihe von Maßnahmen und Regeln definiert, die während der Herstellung, Auslieferung und Wartung von Medizinprodukten beachtet werden müssen.

### 2.1 Anforderungen durch das Medizinproduktegesetz

Das Medizinproduktegesetz stellt einen allgemeinen Rahmen für die Herstellung, die Produktion, den Vertrieb das Betreiben und Anwenden von Medizinprodukten dar. Das MPG regelt folgende Punkte (im Gesetzesentwurf werden diese in sogenannten Abschnitten behandelt):

- Zweck
- Anwendungsbereich des Gesetzes und Begriffsbestimmung
- Anforderungen an Medizinprodukte
- klinische Prüfung
- Benannte Stellen, Sachverständige
- Vorschriften für das Errichten, Betreiben und Anwenden von Medizinprodukten
- Überwachung und Schutz vor Risiken
- Zuständige Behörden, Ausschüsse, sonstige Bestimmungen
- Sondervorschriften für die Bundeswehr

- Straf- und Bußgeldvorschriften
- Regelungen für den Übergang.

Die Medizinprodukteverordnung (MPV) regelt die im MPG allgemein gehaltenen Anforderungen an Medizinprodukte<sup>1</sup> (siehe §1 MPV), insbesondere werden hier die grundlegenden Anforderungen, die Klassifizierung, das Konformitätsbewertungsverfahren, Anforderungen an die klinische Bewertung und Anforderungen an Benannte Stellen geregelt.

Zur Angleichung des Binnenmarktes der europäischen Union werden vom Rat der EG Richtlinien erlassen, die von den Mitgliedsstaaten in nationales Recht umzusetzen sind. In diesen Zusammenhang ist auch von Harmonisierung die Rede. Ziel der Harmonisierung ist der Abbau von Hemmnissen innerhalb der Mitgliedsstaaten zur Verbesserung des innergemeinschaftlichen Handels. Für Medizinprodukte wurde die Richtlinie 93/42/EWG bzw. 98/79/EG für Produkte über In-vitro-Diagnostica erlassen. Alle Richtlinien erhalten durch die Umsetzung in nationales Recht Gesetzesstatus und sind verpflichtend anzuwenden.

Im Unterschied zu den oben genannten Dokumenten werden Normen nicht von Regierungen sondern von unabhängigen Gremien erstellt. In Europa sind das u.a. das Komitee für Normierung (CEN) und das Komitee für elektrotechnische Normung (CENELEC). Um den unverbindlichen Charakter zu erhalten werden Normen von privatrechtlichen Einrichtungen erstellt. Sie dienen dazu die immer noch allgemein gehaltenen Regeln auf den jeweiligen Anwendungsbereich hin zuzuschneiden. Die privatrechtlichen Einrichtungen werden deshalb mit Interessensvertretern aus den jeweiligen Fachgebieten besetzt, die Ihr Anwendungswissen zum Zwecke der Verbesserung und Erleichterung der Arbeit zur Verfügung stellen. Der Anwender hat so zum einen die Möglichkeit sich an eine Vorgabe zu halten zum anderen werden Normen für die Kontrolle auf Übereinstimmung mit gesetzlichen Anforderungen herangezogen. Innerhalb der EWG sind Normen als harmonisiert zu entwickeln. Anerkannte Gremien hierfür sind das bereits erwähnte CEN und CENELEC. Die Umsetzung der europäischen Norm in eine deutsche Norm wird durch DIN und VDE vorgenommen. Die Bekanntgabe von harmonisierten Normen erfolgt im Amtsblatt der Europäischen Gemeinschaft, die der deutschen Norm im Bundesanzeiger . Für die Umsetzung dieser Diplomarbeit wurden speziell die Normen EN60601-1-4 „Medizinische elektrische Geräte - Teil 4: Programmierbare elektrische medizinische Systeme“ und EN1441 „Medizinprodukte - Risikoanalyse“ verwendet.

Neben den Normen gibt es noch sogenannte MEDDEV Dokumente (Leitlinien). Diese werden von Kommissionen, zuständigen Behörden, Interessensverbänden und Vertretern der Industrie erarbeitet. Auch diese Dokumente haben einen unverbindlichen Charakter, sind jedoch in vielen Bereichen „State of the Art“, was insbesondere durch die Vielzahl qualifizierter Mitarbeiter herrührt, die zur Erstellung beitragen. MEDDEV Dokumente werden häufig als Teilprojekte in Richtlinien eingearbeitet. Als Beispiel sei hier MEDDEV 2.4/1 rev. 6 erwähnt. Dieses Dokument stellt die Grundlage für die Regeln zur Klassifizierung von Medizinprodukten dar und wurde in die Richtlinie 93/42/EWG als Anhang IX eingearbeitet.

---

<sup>1</sup>Nach §1(2) mit Ausnahme der Produkte der In-Vitro-Diagnostica (IVD)

Neben der Harmonisierung innerhalb der europäischen Gemeinschaft ist man auch daran interessiert, international geltende Regelungen zu treffen. Für Richtlinien bedeutet dies meist, daß eine zusätzliche Regelung zwischen zwei Vertragspartnern erarbeitet wird, die zusätzliche Regelungen enthält

Bei Normen ist man dazu übergegangen ein internationales Konsortium zu bilden unter dessen Dach man international geltende Normen entwickelt. Beispielsweise wurde die Norm EN60601-1-4 als IEC601-1-4 auf internationaler Ebene herausgegeben. Die Einhaltung einer internationalen Norm stellt einen Meilenstein für die Entwicklung eines Produktes dar, allerdings wäre es ein Trugschluß zu glauben, daß die Erfüllung dieser Norm nun international gesehen für die Einführung des Medizinproduktes in allen Ländern ausreichen würde. Hierfür sind schließlich die Gesetze und Richtlinien der einzelnen Länder einzuhalten.

Nachdem die verschiedenen Dokumenttypen erläutert wurden soll eine Übersicht über diese gegeben werden. Als Diskussionsgrundlage wird zuerst die Definition des Begriffs „Medizinprodukt“ (aus MPG §3 Abs 1) angeführt werden:

*Medizinprodukte sind alle einzeln oder miteinander verbunden verwendeten Instrumente, Apparate, Vorrichtungen, Stoffe und Zubereitungen aus Stoffen oder andere Gegenstände einschließlich der für ein einwandfreies Funktionieren des Medizinproduktes eingesetzten Software, die vom Hersteller zur Anwendung für Menschen mittels ihrer Funktionen zum Zwecke*

- a) der Erkennung, Verhütung, Überwachung, Behandlung oder Linderung von Krankheiten,*
- b) der Erkennung, Überwachung, Behandlung, Linderung oder Kompensierung von Verletzungen oder Behinderungen,*
- c) der Untersuchung, der Ersetzung oder der Veränderung des anatomischen Aufbaus oder eines physiologischen Vorgangs oder*
- d) der Empfängnisregelung*

*zu dienen bestimmt sind und deren bestimmungsgemäße Hauptwirkung im oder am menschlichen Körper weder durch pharmakologisch oder immunologisch wirkende Mittel noch durch Metabolismus erreicht wird, deren Wirkungsweise aber durch solche Mittel unterstützt werden kann.*

### **Beispiele**

Chirurgisches Messer ↔ Brotmesser

Der Unterschied zwischen beiden Messern ist, daß das chirurgische Messer zur Anwendung am Menschen bestimmt ist. Es soll nach Definition zum Zweck der Behandlung von Verletzungen oder Krankheiten eingesetzt werden.

Ergometer ↔ Hometrainer

Obwohl moderne Hometrainer durchaus ähnliche Funktionalität wie ein Ergometer bieten, sind diese Geräte in der Regel keine Medizinprodukte. Grund hierfür ist, daß der Zweck der Anwendung nicht zur Erkennung, Überwachung oder Behandlung von Krankheiten ausgewiesen ist.

Spritze gefüllt ↔ ungefüllt (einweg=Arzneimittel, mehrweg=MP) Hier muß zusätzlich eine Unterscheidung gemacht werden, ob die Spritze als Einweg- oder Mehrwegprodukt entwickelt wurde. Eine gefüllte Einwegspritze würde dann als Verpackung des Arzneimittels angesehen werden und wäre somit kein Medizinprodukt, wohingegen Mehrwegspritzen als Medizinprodukt gehandhabt werden.

Aus der Definition folgt auch, daß Software - sowohl standalone als auch zur Steuer- bzw. Regelung von medizinischen Geräten - ein Medizinprodukt darstellt und dieses im Sinne des MPG entwickelt, ausgeliefert und gewartet werden muß. Im weiteren soll erarbeitet werden, was es heißt, eine Software im Sinne des MPG in Verkehr zu bringen:

Die Voraussetzungen hierfür regelt §8 des MPG (bzw. Artikel 4 93/42/EWG) . Dieser schreibt vor, daß ein Medizinprodukt nur dann auf den Markt gebracht werden darf, wenn dieses mit einem CE Kennzeichen versehen ist. Das CE Kennzeichen soll hierbei zeigen, daß die „grundlegenden Anforderungen“ erfüllt wurden. Als grundlegende Anforderungen gelten:

- allgemeine Anforderungen
  - klinischer Zustand des Patienten
  - Sicherheit für Patient, Anwender, Dritter
  - Prinzip der integrierten Sicherheit
  - Erbringung der vorgegebenen Leistungen
- Anforderungen an die Auslegung und die Konstruktion
  - Chemische, physikalische und biologische Eigenschaften
  - Infektion und mikrobielle Kontamination
  - Eigenschaften im Hinblick auf die Konstruktion und die Umgebungsbedingungen
  - Produkte mit Meßfunktion
  - Schutz vor Strahlung
  - Anforderungen an Produkte mit externer oder interner Energiequelle
  - Bereitstellung von Informationen durch den Hersteller

Hierfür muß nach §14 MPG ein Konformitätsbewertungsverfahren durchgeführt werden, das notwendige Voraussetzung für die CE Kennzeichnung eines Medizinproduktes ist. Das CE Zeichen bestätigt, daß das Medizinprodukt konform der Richtlinie 93/42/EWG entwickelt wurde und die Voraussetzungen für die Inverkehrbringung erfüllt. Der Begriff Inverkehrbringen wurde hierfür in der Richtlinie bzw. dem MPG folgendermaßen definiert: „Erste entgeltliche oder unentgeltliche Überlassung eines Produktes, das nicht für klinische Prüfungen bestimmt ist, im Hinblick auf seinen Vertrieb und/oder seine Verwendung

innerhalb der Gemeinschaft, ungeachtet dessen, ob es sich um ein neues oder ein als neu aufbereitetes Produkt handelt.“

Für die Durchführung des Konformitätsbewertungsverfahrens müssen Medizinprodukte nach §13 MPG Klassen zugeordnet werden. Dieser Prozeß wird als Klassifizierung bezeichnet und im Regelfall vom Hersteller durchgeführt. Die Richtlinie 93/42/EWG gibt im Anhang IX das Schema vor, nachdem eine Klassifizierung zu erfolgen hat. Medizinprodukte werden in 4 Klassen eingeteilt. Die Einleitung der Richtlinie 93/42/EWG beschreibt dieses Vorgehen folgendermaßen: *„Die Klassifizierung erfolgt anhand der Verletzbarkeit des menschlichen Körpers und berücksichtigt die potentiellen Risiken im Zusammenhang mit der technischen Auslegung der Produkte und mit ihrer Herstellung. Die Konformitätsbewertungsverfahren für Produkte der Klasse I können generell unter der alleinigen Verantwortung des Herstellers erfolgen, da der Grad der Verletzbarkeit durch diese Produkte gering ist. Für die Produkte der Klasse IIa ist die Beteiligung einer benannten Stelle für das Herstellungsstadium verbindlich. Für die Produkte der Klassen IIb und III, die ein hohes Gefahrenpotential darstellen, ist eine Kontrolle durch eine benannte Stelle in bezug auf die Auslegung der Produkte sowie ihre Herstellung erforderlich. Die Klasse III ist den kritischsten Produkten vorbehalten, deren Inverkehrbringen eine ausdrückliche vorherige Zulassung im Hinblick auf die Konformität erfordert.“*

Sind sich Hersteller und Benannte Stelle nicht über die während der Klassifizierung ermittelte Klasse einig, kann ein zuständige Stelle angerufen werden. Diese kann ihrerseits im Zweifelsfall die zuständige Bundesbehörde befragen. Entscheidungen der Benannten Stelle bezüglich des Konformitätsbewertungsverfahrens können einer beschränkten Lebensdauer unterliegen. Diese muß nach Ablauf verlängert werden, ansonsten verliert das Produkt seine Zulassung. Benannte Stellen prüfen die Produkte auf ihre Konformität bzgl. der vom Gesetzgeber gestellten Anforderungen (Richtlinien). Die Benannte Stelle muß ihrerseits für die Durchführung von Maßnahmen in diesem Gesetzesbereich in einem Akkreditierungsverfahren nach §20 Abs. 1 MPG nachweisen, daß Sie in der Lage ist, alle in einem der Anhänge II bis VI und im Abschnitt 5 des Anhangs VII der Richtlinie 93/42/EWG genannten Aufgaben wahrzunehmen. Jeder benannten Stelle wird eine Kennziffer zugeteilt, die als Erweiterung an das CE Zeichen angehängt wird (z.B. CE 0123  $\hat{=}$  TÜV).

Die CE-Kennzeichnung stellt als Anforderung, daß der Hersteller eindeutig gekennzeichnet und zusätzliche Angaben unverwechselbar sein müssen. Werden beispielsweise Vertrieb und Service von einer separaten Firma abgewickelt, lautet der Aufdruck:

Hersteller: CE

Fa. Mayer + Co

Musterstr. 34

D-PLZ Musterort

Vertrieb und Service

Electron AG

Das CE Kennzeichen muß am Medizinprodukt, in der Gebrauchsanweisung und der Verpackung angebracht sein.

Nach §25 „Allgemeine Anzeigepflicht“ ist jeder Hersteller dazu verpflichtet, sein Medizinprodukt vor der erstmaligen Inverkehrbringung bei der zuständigen Behörde (diese leitet die Anzeige zu DIMDI weiter) oder direkt beim deutschen Institut für Medizinische Doku-

mentation und Information (DIMDI) anzuzeigen<sup>2</sup>. Nach Inverkehrbringung verpflichtet sich der Hersteller jedes „Vorkommnis“ (durch Einsatz des Medizinproduktes ist ein Mensch zu Schaden gekommen) bzw. Beinahevorkommnis (bei Einsatz des Medizinproduktes entsteht eine Gefährdung für Patienten, Anwender oder Dritte, eine Schädigung liegt nicht vor) dem Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) zu melden. Analog dazu verpflichtet sich der Betreiber nach der Medizinprodukte Betreiber-Verordnung (MPBtreibV) Vorkommnisse zu melden. Als Meldepflicht gelten folgende Vorkommnisse:

- jede Funktionsstörung
- jede Änderung der Merkmale und / oder Leistung
- jede Unsachgemäßheit der Kennzeichnung oder der Gebrauchsanweisung eines Medizinproduktes, die zum Tode oder zur schwerwiegenden Verschlechterung des Gesundheitszustandes eines Patienten oder Anwenders führen kann oder geführt hat.

Vorkommnisse sind innerhalb einer Frist von 10 Tagen und Beinahevorkommnisse in einer Frist von 30 Tagen zu melden. Die Frist beginnt an dem Tag, an dem der Hersteller zuerst über das Vorkommnis informiert wurde und endet mit dem Eingang der entsprechenden Mitteilung des Herstellers bei der zuständigen Behörde. Eine Meldung bedeutet immer, daß ein Mangel im Rahmen des Konformitätsbewertungsverfahrens aufgetreten ist, durch den eine Gefahr für Patienten, Anwender und Dritte besteht bzw. bereits eingetreten ist. Das Bundesinstitut für Arzneimittel und Medizinprodukte kann in diesem Fall eine Sperrung des Medizinproduktes veranlassen. Nach Behebung der Gefährdung ein Abschlußbericht erstellt und zur Information an das BfArM geschickt.

## 2.2 Problematik durch das MPG

Als besonderes Problem zeigt sich die Definition des Begriffs „Inverkehrbringen“. Bei strenger Auslegung, könnte bereits das Testen von Prototypen ein Verstoß gegen das MPG bedeuten. Prototypen sind jedoch als Akzeptanztest, zum Einholen von Expertenwissen und Testen im Einsatzumfeld (z.B. Anschluß an medizinische Geräte) unumgänglich. Darüber hinaus erweist es sich berufsbedingt sehr schwierig, im klinischen Alltag mit klinischen Personal einen festen Termin einzuhalten. Als optimale Kommunikationsform hat sich hier die asynchrone Kommunikation erwiesen, indem eine Probeinstallation durchgeführt und anschließend auf Feedback von Seiten der Ärzte gewartet wird.

Einzige anwendbare Ausnahme wäre eine klinische Studie, welche typischerweise nach Abschluß der Entwicklung durchgeführt wird. Abschnitt drei des MPG regelt die Durchführung von klinischen Studien<sup>3</sup>. Wichtige Eckpunkte hieraus sind:

- Die Anwendung darf Anwendung nur erfolgen, falls der Patient damit gerettet bzw. der gesundheitliche Zustand verbessert werden könnte

---

<sup>2</sup>Formblätter zur Anzeigepflicht usw. stehen unter <http://www.dimdi.de/germ/mpg/fr-mpg.htm> bereit

<sup>3</sup>vgl. auch 93/42/EWG Artikel 15

- Klinische Studien müssen bei der zuständigen Behörde - in Deutschland beim Deutschen Institut für Medizinische Dokumentation und Information (DIMDI) - angemeldet werden
- Es bedarf der schriftlichen Zustimmung jedes Patienten (dieser muß geschäftsfähig sein)
- Es muß die sicherheitstechnische Unbedenklichkeit für die Anwendung nachgewiesen werden
- es muß ein dem Stand der wissenschaftlichen Erkenntnissen entsprechender Prüfplan geschrieben werden
- Für jeden Patienten muß eine spezielle Versicherung abgeschlossen werden
- Die Studie muß von einem entsprechend qualifizierten Arzt bzw. Personal durchgeführt werden
- Es bedarf der Zustimmung einer Ethikkommission zu dem Prüfplan<sup>4</sup>

Gerade im Bereich Forschung und Lehre stellt diese Regelung einen erheblichen Hemmschuh dar. Für die Datenverarbeitung ist es zum einen schwierig Originaldaten für Tests zu erhalten, da diese häufig dem Datenschutz unterliegen, zum anderen dürfen neue Verfahren nur nach Anmeldung von klinischen Studien geprüft werden. Für klinische Studien muß allerdings bereits ein Großteil der Anforderungen des Konformitätsbewertungsverfahrens durchgeführt werden, was für die Erprobung neuartiger Algorithmen teilweise sehr schwierig ist, da es zu beweisen gilt, daß das Verfahren kein Risiko sondern insbesondere eine Verbesserung für den Patienten bedeutet. Dieses Verfahren grenzt gerade kleinere Firmen die Produkte mit Risikoklasse IIb oder III entwickeln aus, da ein Konformitätsbewertungsverfahren sehr kostspielig ist. Eine Verzögerung der Markteinführung bedeutet zusätzlich Einnahmeausfälle, die nur durch einen großen Kapitalstock überbrückt werden können.

---

<sup>4</sup>falls innerhalb einer Frist von 60 Tagen keine Stellungnahme der Ethikkommission vorliegt, kann mit der Studie begonnen werden. Für Ausnahmeregelungen sei auf 93/42/EWG Artikel 15.3 verwiesen.



# Kapitel 3

## Anforderungen an medizinische Software durch den Zertifizierungsprozeß

Dieses Kapitel stellt die Anforderungen dar, die durch die Richtlinie 93/42/EWG an medizinische Software gestellt wird. Der folgende Unterpunkt (Kapitel 3.1) motiviert die Anforderungen der europäischen Norm, während der zweite Unterpunkt (Kapitel 3.2) die Erweiterungen der Zulassung für den amerikanischen Markt beschreibt. Die Umsetzung der Anforderungen wird im nächsten Kapitel vorgestellt.

### 3.1 Zertifizierung nach CE

Die Zertifizierung für den europäischen Markt ist dank der europäischen Richtlinie „92/43/EWG – Medical Devices Directive, MDD<sup>1</sup>“ einheitlich geregelt. Im folgenden werden die für die Entwicklung von Medizinprodukten geforderten Dokumente beschrieben.

#### 3.1.1 Zweckbestimmung

Ein besonderer Augenmerk bei der Entwicklung medizinischer Software liegt in der Erstellung der Zweckbestimmung. Anhand der Formulierung wird entschieden, ob es sich um ein Medizinprodukt handelt oder nicht. Die Hauptaufgabe liegt darin, den Verwendungszweck des Produktes zu definieren nach dem Anwender oder Betreiber das Medizinprodukt benutzen können. Wird das Produkt nicht gemäß der Zweckbestimmung eingesetzt wird der Betreiber aus juristischer Sicht zum Hersteller und kann somit strafrechtlich belangt werden. Ein solcher Verstoß kann beispielsweise durch das Verbinden mehrerer Geräte erfolgen, die vom Hersteller nicht explizit dafür aufgeführt sind.

---

<sup>1</sup>In der Literatur wird häufig nur die Abkürzung MDD verwendet

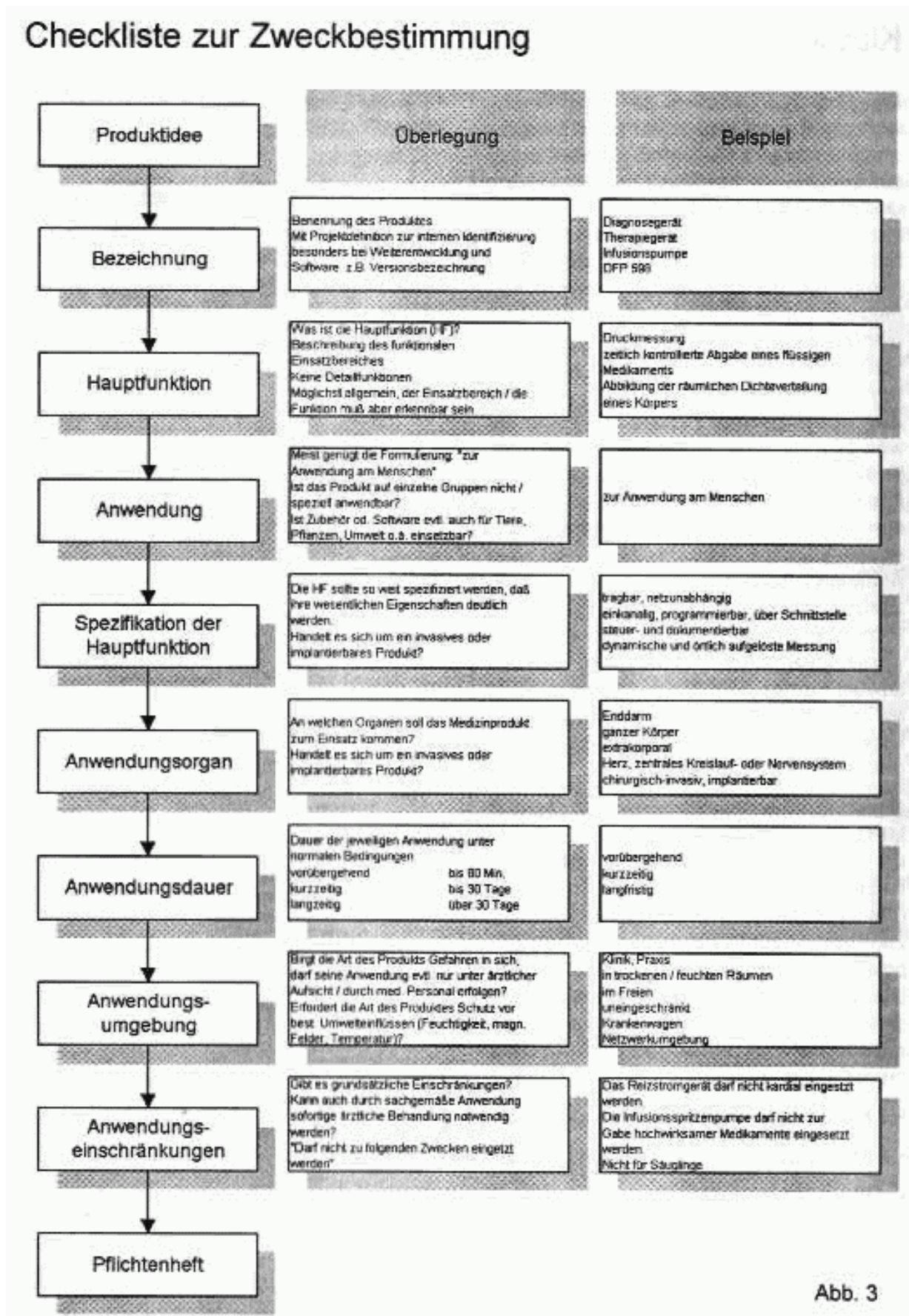


Abb. 3

Abbildung 3.1: Checkliste zur Zweckbestimmung

Im späteren Entwicklungsverlauf wird eine Risikoanalyse durchgeführt, die den in diesen Dokument definierten Einsatzbereich auf mögliche Gefährdungen untersuchen muß und auch bei der Klassifizierung spielt dieses Dokument eine zentrale Rolle, da hier insbesondere die Kriterien für die Klassifizierung spezifiziert werden. Die Formulierung der Zweckbestimmung soll grundsätzlich kurz und prägnant sein. Es soll neben den Eigenschaften die das Produkt leistet auch angegeben sein, was das Produkt nicht leisten kann.

Die Zweckbestimmung legt zusammen mit der Gebrauchsanweisung den bestimmungsgemäßen Gebrauch des Medizinproduktes fest. Eine mögliche Gliederung stellt [CH99] vor (siehe Abbildung 3.1).

### 3.1.2 Klassifizierung

Medizinprodukte werden nach dem MPG in Klassen eingeteilt. Die MDD gibt folgende vier Klassen vor: I, IIa, IIb und III.

Klasse I:	geringes Risikopotential
Klasse IIa:	erhöhtes Risikopotential
Klasse IIb:	hohes Risikopotential
Klasse III:	höchstes Risikopotential

Hintergrund der Klassifizierung ist es, Medizinprodukte entsprechend der von ihnen ausgehenden Gefährdung für Patienten, Anwender und Umgebung in Risikoklassen einzuordnen. Auf diese Weise wird ein stufiges Risikoanalyseverfahren ermöglicht, d.h. anstatt einer einzigen „high level“ Risikoklasse definiert man vier Kategorien, die unterschiedliche Anforderung bezüglich des Risikomanagements zu erfüllen haben.

Die Zuordnung eines Medizinproduktes zu seiner Risikoklasse erfolgt anhand Anhang IX der Medizinproduktedirektive. Anhang IX enthält 18 Regeln, die entsprechend ihrer Nummerierung durchlaufen werden. Vorab muß das Produkt entsprechend den in der Zweckbestimmung definierten Anwendungseigenschaften kategorisiert werden. Folgende Kriterien werden definiert:

- Dauer der Anwendung
- Ort der Anwendung
- Art der Anwendung
- Kreislaufsystem oder Nervensystem betreffend

Als Dauer werden „vorübergehend“, „kurzzeitig“ und „langzeitig“ definiert, wobei „vorübergehend“ bis zu 60 min., „kurzzeitig“ bis zu 30 Tagen und „langzeitig“ mehr als 30 Tage bedeutet. Das Kriterium „Ort“ bezieht sich auf invasive (Körperöffnung, chirurgisch, implantierbar) oder nicht invasive Anwendungen. Als „Art“ definiert man therapeutische bzw. diagnostische Medizinprodukte. Darüber hinaus wird nach „aktiv“ (Das Gerät wirkt durch Umwandlung von Energie die einer Energieversorgung entstammt, außer: Muskelkraft oder Schwerkraft) und „inaktiven“ Medizinprodukten unterschieden. Software wird

somit als aktives Medizinprodukt betrachtet, da insbesondere die Hardware eine Energiequelle benötigt und zudem eine Umwandlung von elektrischer Energie stattfindet.

Wie bereits erwähnt richtet sich die Klassifizierung nach den in der Zweckbestimmung definierten Anwendungseigenschaften. Soll das Produkt zusammen mit anderen Produkten klassifiziert werden, kann dies gesondert erfolgen, was gerade im Zusammenhang mit Zubehör von Fremdherstellern sinnvoll ist. Für Produkte mit verschiedenen Komponenten kann es vorkommen, daß einzelne Komponenten unterschiedlichen Risikoklassen angehören können. Produkte werden immer nach dem ihrer Anwendung zufolge größtem Gefährdungspotential klassifiziert. Sind mehrere der 18 Regeln anwendbar, erfolgt die Klassifizierung nach derjenigen Regel mit der höchsten Klasse. Software ist wie das Medizinprodukt zu behandeln, dessen Leistung sie direkt steuert bzw. beeinflusst<sup>2</sup>.

Es sollen hier nicht alle Regeln im Detail angesprochen werden, vielmehr ist der Aufbau der Regeln zu beachten. Hieraus ergibt sich, daß alle nicht invasiven Produkte minimal Klasse 1 zuzuordnen sind (Regel 1). Regel 2 - 11 erweitern die Risikoklassen entsprechend der von dem Einsatzgebiet ausgehenden Gefährdung. Regel 12 dient als Rückfallregel und besagt, daß alle aktiven Geräte minimal der Klasse 1 zuzuordnen sind. Alle folgenden Regeln stellen die Risikoklassen für Geräte, die das Kreislaufsystem bzw. das Nervensystem betreffen. Die Klassifizierungsregeln können MDD Anhang IX, Abs. III entnommen werden.

Im weiteren sollen einige Beispiele das Verfahren erläutern. Hierfür werden die benötigten Regeln angeführt.

---

<sup>2</sup>aus MDD Anhang IX, II

### 3.1.3 Konformitätsbewertungsverfahren

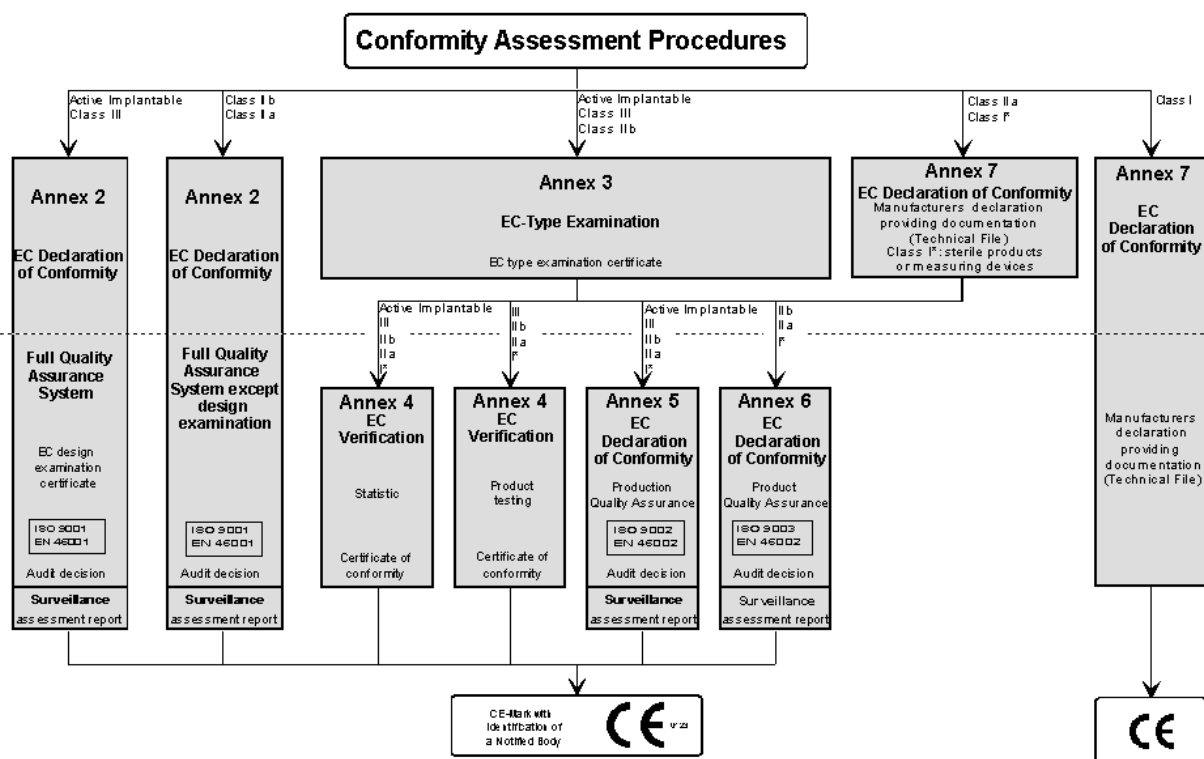


Abbildung 3.2: Schematische Darstellung des Konformitätsbewertungsverfahrens (Quelle: Kursunterlagen „CE-Zertifizierung medizinisch genutzter Software“ TÜV Akademie)

Ausgehend von der Klassifizierung wird mittels der Konformitätsbewertung ein Verfahren festgelegt, um die unterschiedlichen Anforderungen zu bearbeiten, die sich aus der Risikoklasse ergeben. Abbildung 3.2 zeigt den Baum aller möglichen Vorgehensweisen. Das Konformitätsbewertungsverfahren wird in MDD Art. 11 festgesetzt und durch die Anhänge 2 - 7 geregelt. Die Risikoklasse (Beschriftung der Verbindungslinien) entscheidet, welcher Anhang für welches Produkt angewendet werden kann.

Das Konformitätsbewertungsverfahren unterscheidet zwischen Entwicklung und Produktion (in Abbildung 3.2 angedeutet durch die horizontale Linie). Die Unterteilung wird bei einer Baumusterprüfung nach Anhang 3 bzw. einer Konformitätserklärung nach Anhang 7 für Produkte der Klasse I\* und IIa klar, diese beiden Anhänge stellen die Entwicklung dar. Analog dazu regeln die Anhänge IV, V und VI die Produktionsseite.

Der Hersteller kann alternativ entweder ein Qualitätssicherungssystem nach ISO 9001 und EN 46001 installieren und so selbst die Konformität überwachen oder eine Baumusterprüfung zusammen mit einer EG-Prüfung von einer Benannten Stelle für jedes Produkt durchführen lassen. Die Entscheidung hängt von der konkreten Situation des Herstellers ab. Entscheidungsfaktoren sind nach [CHKT99]:

- Organisation des Herstellers

- Flexibilität des Unternehmens
- Kosten
- Anzahl und Losgröße der Medizinprodukte
- Produktvielfalt

Der wesentliche Unterschied zwischen den beiden Verfahren ist, daß bei einem Qualitätssicherungssystem die Benannte Stelle prüft ob das System ausreichende Tests durchführen kann, so daß eine Konformität mit der Richtlinie eingehalten wird, wohingegen bei der Baumusterprüfung von der Benannten Stelle das Baumuster auf Konformität mit der Richtlinie geprüft wird (dies beinhaltet auch die Dokumentation).

Produkte der Klasse I müssen konform Anhang 7 produziert werden. Im Kern heißt dies, daß die Teile der technischen Dokumentation beim Hersteller hinterlegt werden müssen. Es ist dabei unerheblich, ob der Hersteller das Produkt selbst entwirft bzw. produziert oder nur als solcher auftritt. Alternativ kann auch eine vertragliche Regelung getroffen werden, die Zulieferfirmen dazu verpflichtet, die Teile der technischen Dokumentation bereitzuhalten. Auf diesen Wege ist es möglich spezielle Entwicklungen innerhalb einer Firma zu belassen und somit keine Firmengeheimnisse weiterzugeben (z.B. in Designspezifikation). In diesem Fall reicht es aus, daß der Hersteller (bzw. der Inverkehrbringer, falls der Hersteller nicht innerhalb der europäischen Union niedergelassen ist) die technische Dokumentation für das Produkt bereithält.

Produkte der Klasse I<sup>3</sup> bzw. IIa haben während der Entwicklung ebenfalls Anhang 7, während der Produktion einen der Anhänge IV, V oder VI zu erfüllen.

Produkten der Klassen IIb und III kann und muß ein CE-Kennzeichen angebracht werden, falls der Hersteller das Produkt gemäß eines eigenen Qualitätssicherungssystems nach Anhang II oder eine Baumusterprüfung nach Anhang III in Verbindung mit Anhang IV oder V entwickelt hat. Für die Risikoklasse IIb kann die Baumusterprüfung auch zusammen mit Anhang VI durchgeführt werden.

Wurde die Konformität des Produktes bestätigt, kann das Produkt mit dem CE-Kennzeichen versehen werden. Wurde für die Konformitätsbewertung eine Benannte Stelle hinzugezogen bzw. hatte das Unternehmen ein eigenes Qualitätssicherungssystem darf dem CE-Kennzeichen die Identifikation der Benannten Stelle angefügt werden. Produkte der Risikoklasse I, die nach Anhang 7 entwickelt und produziert werden tragen ein CE-Kennzeichen ohne Identifikation.

---

<sup>3</sup>sterile Produkte oder Produkte mit Meßfunktion

Anhang II:	Vollständiges Qualitätssicherungssystem
Anhang III:	Baumusterprüfung
Anhang IV:	EG Prüfung
Anhang V:	Qualitätssicherung Produktion
Anhang VI:	Qualitätssicherung Produkt
Anhang VII:	EG Konformitätserklärung

Tabelle 3.1: Übersicht über die Anhänge

Für die Umsetzung des Konformitätsbewertungsverfahrens nach Anhang II muß ein vollständiges Qualitätssicherungssystem implementiert werden. Das bedeutet, daß der Hersteller die Auslegung, die Fertigung und die Endkontrolle der betreffenden Produkte vornimmt. Das Qualitätssicherungssystem stellt die erforderlichen Abläufe und Maßnahmen dar, die der Hersteller anwendet um zu prüfen, ob das Produkt mit den Richtlinien konform ist. Als Grundlage dient ISO 9001 bzw. EN 46001. Das QS-System wird von einer Benannten Stelle auditiert um festzustellen, ob der Hersteller in der Lage ist, die Konformität seiner Produkte zu überwachen. Dabei soll das Produkt von der Auslegung bis hin zur Endkontrolle durch das System geprüft werden. Alle durchgeführten Arbeiten sind zu dokumentieren, wobei folgende Punkte minimal zu erfüllen sind:

- Qualitätsziele des Herstellers
- Organisation des Unternehmens
- Verfahren zur Steuerung und Kontrolle der Produktauslegung
- Qualitätssicherungs- und -kontrolltechniken auf der Ebene der Herstellung
- geeignete Untersuchung und Prüfung vor, während und nach der Herstellung; Häufigkeit, verwendete Prüfgeräte ..

Änderungen am geprüften System müssen der Benannten Stelle gemeldet werden und ggf. von dieser überprüft werden. Die Benannte Stelle hat weiterhin die Aufgabe, Inspektionen durchzuführen um sicherzustellen, daß der Hersteller seinen Verpflichtungen nachkommt.

Bei Produkten der Risikoklasse III muß der Hersteller zusätzlich eine Benannte Stelle für die Prüfung der Auslegungsdokumentation hinzuziehen.

Als weitere Alternative bietet sich die Baumusterprüfung (Anhang III) an. Im Gegensatz zur vorhergehenden Variante auditiert die Benannte Stelle nicht das QS System des Herstellers, sondern ein Baumuster des Produkts. Diese Aufgabe ist eng verzahnt mit einem funktionierendem Konfigurationsmanagement, da die Prüfung einer Versionsnummer zugeordnet wird. Die Benannte Stelle bescheinigt im Erfolgsfall die Konformität mit den Richtlinien und stellt eine EG Baumusterprüfbescheinigung aus. Zusätzlich zur Baumusterprüfung muß eine Prüfung der Produktion nach einem der Anhänge IV - VI vollzogen werden, da die Baumusterprüfung rein zur Kontrolle des entwickelten Produktes dient. Die Anhänge IV - VI werden im folgenden erläutert.

Zur Gewährleistung der Konformität vor, während und nach der Produktion wurden die Anhänge IV, V und VI definiert. Bei allen verwendeten Verfahren steht die Übereinstimmung des Produktes mit dem Baumuster im Vordergrund, allerdings unterscheiden sich die Verfahren wesentlich. Ein Unterscheidungsmerkmal ist das Vorhandensein eines QS Systems für die Herstellung. Hat ein Hersteller kein QS System, muß er das Produkt nach Anhang IV herstellen. Für Hersteller, die ein QS System implementiert haben, unterscheidet man, ob die Produktion (Anhang V) oder das Produkt (Anhang VI) durch das QS System erfaßt wird.

Anhang IV: Der Hersteller dokumentiert das Herstellungsverfahren vor Beginn der Herstellung. Der Hersteller muß gewährleisten, daß das Produkt mit dem Baumuster für das er die EG-Baumusterprüfbescheinigung erworben hat übereinstimmt. Die benannte Stelle hat dies zu kontrollieren, wobei die Überprüfung von der Losgröße der erzeugten Produkte abhängt. Der Anhang definiert zum einen die Einzelstückprüfung, bei der jedes einzelne Produkt überprüft wird, zum anderen wird ein statistisches Verfahren vorgeschlagen. Bei letzterem geht man davon aus, daß die Herstellung für alle Produkte gleich ist. Aus einer repräsentativen Menge (homogenen Partien) werden zufällige Stichproben gewählt, die die Benannte Stelle überprüft.

Für die Produktion von Software gemäß Anhang IV würde dies bedeuten, daß man das Installationsmedium mit dem des Baumusters vergleicht, was beispielsweise durch einen bitweisen Vergleich oder durch Berechnung von Prüfsummen über die installierten Dateien durchgeführt werden kann. Wichtig ist letztendlich, daß eine Übereinstimmung mit dem Baumuster festgestellt wird. Für den Fall, daß die Software vorkonfiguriert auf einem Rechner ausgeliefert wird und dies als Voraussetzung zur Umsetzung risikomindernder Maßnahmen (siehe Risikoanalyse) vorgesehen ist, müßte die benannte Stelle das Gesamtsystem auf Konformität prüfen. Sieht die Risikoanalyse zusätzlich eine Schulung bzw. Einweisung von Anwendern vor, muß die benannte Stelle vor Ort die Umsetzung überprüfen.

Wird ein Produkt als konform geprüft, stellt die benannte Stelle die Konformitätserklärung aus. Bei der Einzelstückprüfung bringt die benannte Stelle ihre Kennnummer an jedem genehmigten Produkt an und stellt eine Konformitätserklärung aus. Bei der statistischen Überprüfung kann der Hersteller während des Herstellungsprozesses das CE-Kennzeichen anbringen. Wird eine Partie zurückgewiesen, verhindert die benannte Stelle das Inverkehrbringen dieser Partie.

Sowohl für Anhang V als auch für Anhang VI gilt, daß das QS-System von einer benannten Stelle geprüft werden muß. Der Hersteller stellt hierfür einen Antrag auf Bewertung des QS-Systems, der folgendes enthält<sup>4</sup>:

- Name und Anschrift des Herstellers
- alle einschlägigen Angaben über die Produkte oder die Produktkategorie, die Gegenstand des Verfahrens sind/ist
- eine schriftliche Erklärung dahingehend, daß bei keiner anderen benannten Stelle ein Antrag zu denselben Produkten eingereicht worden ist

---

<sup>4</sup>aus 93/42/EWG Anhang V Abschnitt 3

- die Dokumentation über das Qualitätssicherungssystem
- eine Zusicherung, die Verpflichtungen, die sich aus dem genehmigten Qualitätssicherungssystem ergeben, zu erfüllen
- eine Zusicherung, das genehmigte Qualitätssicherungssystem so zu unterhalten, daß dessen Eignung und Wirksamkeit gewährleistet bleiben
- gegebenenfalls die technische Dokumentation über die genehmigten Baumuster und eine Kopie der EG-Baumusterprüfbescheinigungen
- eine Zusicherung des Herstellers, ein systematisches Verfahren einzurichten und auf dem neuesten Stand zu halten, mit dem Erfahrungen mit Produkten in den der Herstellung nachgelagerten Phasen ausgewertet werden, und Vorkehrungen zu treffen, um erforderliche Korrekturen durchzuführen. Diese Zusicherung schließt die Verpflichtung des Herstellers ein, die zuständigen Behörden unverzüglich über folgende Vorkommnisse zu unterrichten, sobald er selbst davon Kenntnis erlangt hat

Werden wesentliche Änderungen am QS System vorgenommen, muß die benannte Stelle informiert werden. Diese hat zu überprüfen, ob das geänderte QS System noch den Anforderungen entspricht. Das QS System unterliegt der Kontrolle durch die benannte Stelle um sicher zu stellen, daß der Hersteller seinen Verpflichtungen nachkommt. Die benannte Stelle führt hierzu regelmäßige Inspektionen durch und übermittelt dem Hersteller einen Bewertungsbericht. Darüber hinaus kann die benannte Stelle unangemeldete Besichtigungen beim Hersteller durchführen.

Weiterhin muß der Hersteller folgende Unterlagen für mindestens fünf Jahre nach der Herstellung aufbewahren:

- die Konformitätserklärung
- die Dokumentation des QS Systems (nur für Anhang V)
- Unterlagen über ggf. vorgenommene Änderungen am QS System (diese müssen von der Benannten Stelle genehmigt werden)
- die technische Dokumentation über die genehmigten Baumuster und EG-Baumusterprüfbescheinigungen
- Die im Rahmen der Überwachung erstellten Entscheidungen und Berichte der benannten Stelle
- ggf. die EG-Baumusterprüfbescheinigung gemäß Anhang III

Der Hersteller stellt für alle erzeugten Produkte eine schriftliche Konformitätserklärung aus und bringt das CE-Kennzeichen nach Artikel 17 (93/42/EWG) an.

Für Produkte der Risikoklasse IIa reicht es aus, wenn der Hersteller erklärt und bescheinigt, daß die Produkte im Einklang mit der technischen Dokumentation hergestellt werden und den Anforderungen der Richtlinie 93/42/EWG genügen.

Für die Konformitätsbewertung der Produktion nach Anhang V hat der Hersteller ein QS-System für die Produktion (ISO 9002) zu installieren. Die Benannte Stelle überprüft das QS-System des Herstellers um festzustellen, ob geeignete Verfahren implementiert sind, um eine Übereinstimmung von Baumuster und hergestelltem Produkt festzustellen. Nach Anhang V muß hierfür das Herstellungsverfahren untersucht werden, wobei insbesondere die Kontrollmechanismen bei der Herstellung im Vordergrund stehen. Als Abschluß ist eine Endkontrolle des Produktes vorgeschrieben.

Für die Konformitätsbewertung der Produktion nach Anhang VI hat der Hersteller ein QS-System für das Produkt (ISO 9003) zu installieren. Das QS-System wird dabei so ausgelegt, daß entsprechende Prüfberichte aller Tests entweder für jedes Produkt oder für eine repräsentative Stichprobe aus einem Los erstellt werden. Vorgeschriebene Wartungen Kalibrierungen o.ä. der Herstellungsmaschinen müssen durchgeführt werden und sind zu dokumentieren. Desweiteren ist die Qualifikation des Personals zu bewerten und zu dokumentieren.

### 3.1.4 Risikomanagement

Der zentrale Baustein bei der Entwicklung medizinischer Software ist das Risikomanagement, dessen Ziel der Schutz der Gesundheit und des Lebens ist. Mögliche Risiken müssen verglichen mit der nützlichen Wirkung so weit wie möglich minimiert werden. Aus den in den Richtlinien definierten Grundlegenden Anforderungen folgt, daß jeder Hersteller von Medizinprodukten in Europa verpflichtet ist, eine Risikoanalyse durchzuführen und Maßnahmen zur Risikobeherrschung umzusetzen.

DIN EN 60601 „Medizinische elektrische Geräte; Ergänzungsnorm: Programmierbare elektrische medizinische Systeme“ legt die Anforderungen fest die für eine Umsetzung zu erfüllen sind. Es ist Aufgabe der Qualitätssicherung bzw. der Benannten Stelle die Konformität des Produktes mit der Norm zu überprüfen. Ausgangspunkt des Risikomanagement-Prozesses ist der Risikomanagement-Plan, der die Zuständigkeiten, die nötigen Verfahren und die konzeptionelle Vorgehensweise festlegt. Das eigentliche Verfahren ist der sogenannte Risikomanagement Prozeß. Dieser teilt sich in Risikoanalyse und Risikobeherrschung. Alle gefundenen Gefährdungen werden in der Risikomanagement-Zusammenfassung dokumentiert. Abbildung 3.3 zeigt den schematischen Aufbau der Risikomanagement-Dokumentation.

Der Risikomanagement-Plan muß nach DIN EN 60601-1-4 mindestens folgende Punkte enthalten:

- Geltungsbereich
- Entwicklungslebenszyklus einschließlich Verifizierungs- und Validierungs-Plan
- Verantwortung des Managements entsprechend 4.1 der ISO 9001
- Risikomanagement-Prozeß
- Anforderungen für Reviews

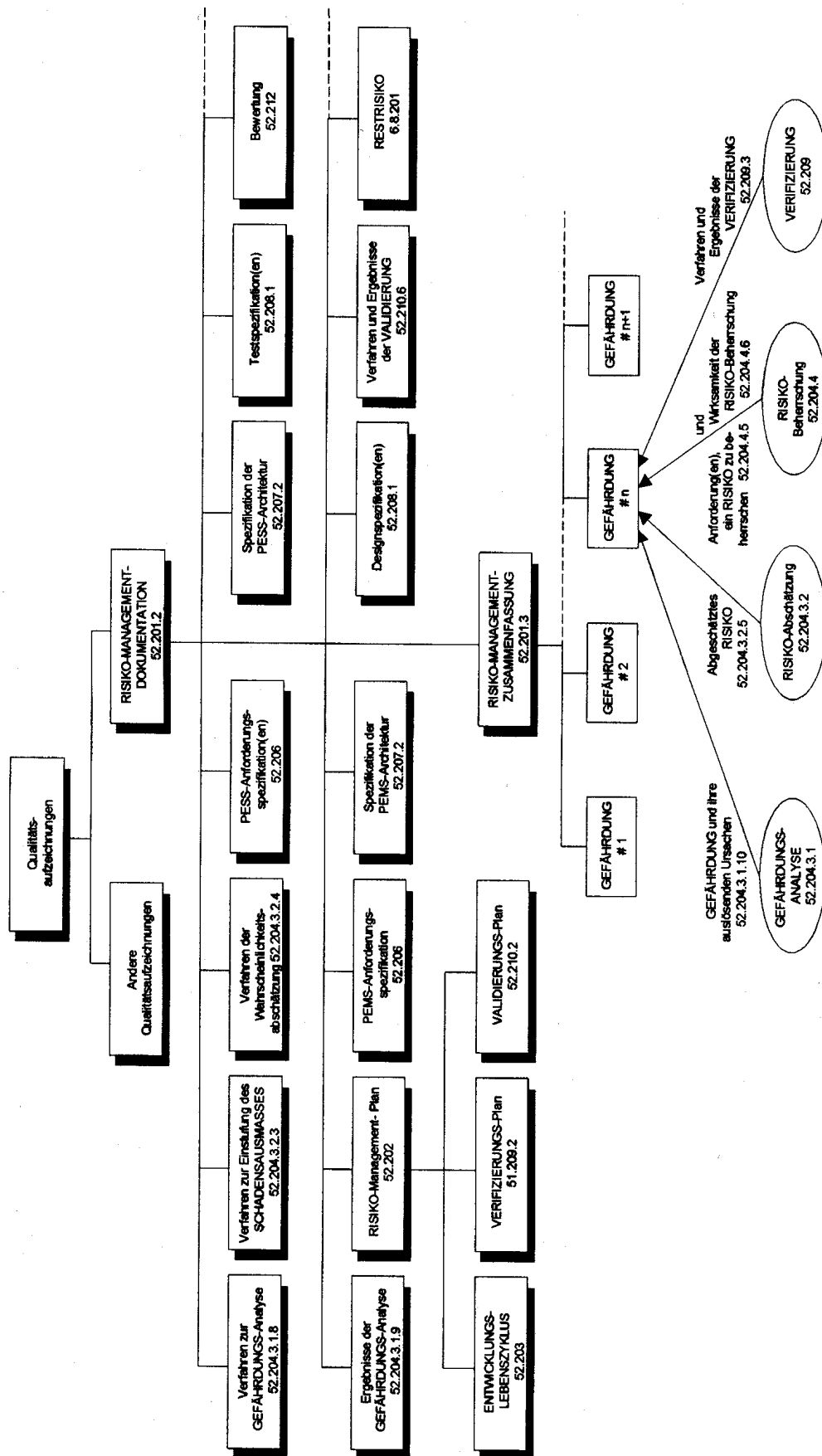


Abbildung 3.3: Schematischer Aufbau der Risikomanagement-Dokumentation nach EN60601-1-4

Der *Geltungsbereich* legt den Anwendungsbereich des Risikomanagement-Plans auf das Projekt bzw. Produkt fest. Es empfiehlt sich diesen Punkt mit einer kurzen Einleitung an den Dokumentanfang zu legen. Die Norm 60601-1-4 schreibt keinen bestimmten *Entwicklungslebenszyklus* vor, stellt jedoch Anforderungen, die der gewählte Entwicklungslebenszyklus erfüllen muß. Hierzu gehören eine Einteilung in Phasen und Aufgaben mit festen Eingängen, Ausgängen und Tätigkeiten. Es müssen Prozesse für das Risikomanagement vorgesehen und Anforderungen bezüglich der Dokumentation beschrieben sein. Desweiteren muß sich das Risikomanagement auf den gesamten Entwicklungslebenszyklus erstrecken. Abbildung 3.4 zeigt den in Anhang DDD der Norm EN 60601-1-4 vorgeschlagenen Lebenszyklus. Dieser zeigt am linken Ast einen Dekompositionsprozeß und einen Integrationsprozeß am rechten Ast. Bei der Dekomposition wird ausgehend von den Anforderungen ein Design für das medizinische Gerät abgeleitet (Grobdesign). Dieses wird in Subsysteme und weiter in Komponenten zerlegt. Der Dekompositionsprozeß endet dann, wenn es möglich ist, die gefundenen Komponenten zu erstellen. Während der Integration wird der Aufbau und das Zusammenspiel der Komponenten verifiziert. Der Integrationsprozeß wird durch die Validierung abgeschlossen. Diese soll zeigen ob das erstellte Produkt, die anfangs gestellten Anforderungen erfüllt und somit bestimmungsgemäß arbeitet. Tabelle DDD.1 der Norm EN 60601-1-4 schlägt eine mögliche Zuordnung zwischen den einzelnen Phasen des Entwicklungslebenszyklus und den Dokumentationsanforderungen vor. Zusätzlich werden aber auch Anforderungen an die Anforderungsspezifikation, Architektur, Design und Implementierung gestellt. Die wichtigsten Eckpunkte hieraus sind: jedes Subsystem eines Medizinischen Systems muß in der Anforderungsspezifikation enthalten sein, wobei minimal nur die risikobezogenen Funktionen detailliert aufgeführt werden müssen. Die Architektur muß der Anforderungsspezifikation genügen und für alle Subsysteme festgelegt sein. EN60601-1-4 Punkt 52.207.3 enthält eine Liste von Anforderungen die in die Spezifikation eingearbeitet werden müssen. Für die Design und Implementierungsdokumente ist zu beachten, daß das System in Subsysteme zerlegt werden muß (falls anwendbar) von denen jedes eigene Design- und Prüfspezifikationen hat. Die Norm gibt hier eine Liste von Anforderungen<sup>5</sup> vor, die es umzusetzen gilt.

Als Teil des Entwicklungslebenszyklus ist ebenfalls der Verifizierungsplan und der Validierungsplan zu erstellen. Der Verifizierungsplan legt fest, wie die Anforderungen an das Produkt am Ende jeder Phase überprüft werden müssen. Der Validierungsplan legt fest, wie man die Anforderungen, die zu Beginn der Entwicklung festgesetzt wurden, am Ende der Entwicklung prüft. Die Anforderungen sowohl für Verifizierung als auch Validierung beschränken sich auf die Sicherheit.

Aus personeller Sicht ergibt sich die Forderung, daß kein Entwickler sein eigenes Design validieren darf. Die Leitung der Validierungsgruppe muß unabhängig von der Entwicklungsgruppe sein. Im Punkt *Verantwortung des Managements entsprechend 4.1 der ISO 9001* sind unter Beachtung dieser Anforderungen, die Tätigkeiten der ausführenden und freigebenden Rolle<sup>6</sup> zuzuordnen. Die Umsetzung erfolgt häufig tabellarisch.

---

<sup>5</sup>Punkt 52.208.2

<sup>6</sup>Eine Rolle steht stellvertretend für die eigentliche Person, die die Aufgabe oder Tätigkeit ausführt, so daß diese - eine geeignete Qualifikation vorausgesetzt - in mehreren Rollen auftreten kann.

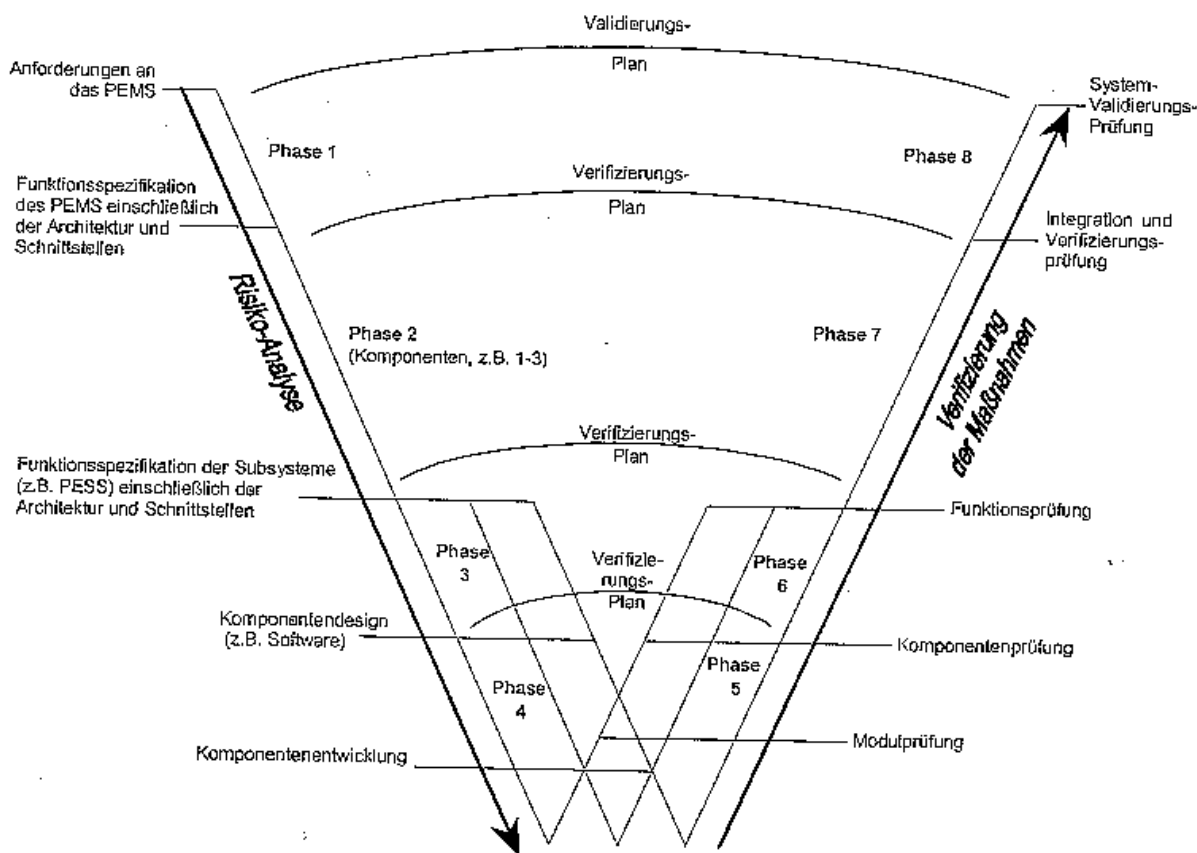


Abbildung 3.4: Vorschlag eines Entwicklungs-Lebenszyklus nach EN 60601-1-4 Anhang DDD

Tätigkeit	Ersteller	Freigabe
Erstellen der Anforderungsspezifikation	Entwicklung	Projektleiter
...	..	..

Tabelle 3.2: Tabelle Verantwortung des Managements

Als Beispiel die in Tabelle 3.1.4 definierte Tätigkeit des Schreibens der Anforderungsspezifikation gewählt. Diese wird von der Entwicklung durchgeführt und von der Projektleitung freigegeben. Die Dokumentation des *Risikomanagement-Prozesses* beinhaltet die Dokumentation der Verfahren zur Umsetzung der Risikoanalyse und der Risikobeherrschung, wobei es sich als sinnvoll erweisen kann, die unterschiedlichen Verfahren zur Bestimmung von Gefährdungen, in Abhängigkeit der Phasen des Entwicklungszyklus festzulegen. Der letzte Punkt des RM-Plans „Anforderungen für Reviews“ legt fest, welche Dokumente einem Review unterzogen werden.

Der Prozeß zur Analyse, der Abschätzung und Umsetzung von Maßnahmen zur Beherrschung der Risiken wird Risikomanagement-Prozeß genannt. Als interdisziplinäres Instrument sollte Risikomanagement in jedem Fall von einem Projektteam aus Mitgliedern ver-

schiedener Fachabteilungen durchgeführt werden. Die Quantifizierung der Risiken erfolgt mit Hilfe der Portfolio-Technik, wobei die Bewertungsmatrix durch die Achsen Schadensausmaß und Auftretenswahrscheinlichkeit aufgespannt wird<sup>7</sup>. Für den Bereich der Medizintechnik entziehen sich diese beiden Parameter einer mathematisch exakten Beschreibung. Es ist deshalb sinnvoll, mit quantitativen Skalen zu arbeiten und die entsprechenden Kategorien durch Kriterien und Beispiele zu konkretisieren. Die Bewertungsmatrix wird entsprechend der Risikoakzeptanz in drei unterschiedliche Regionen unterteilt<sup>8</sup>:

- der weitgehend akzeptable Bereich - Risiken in diesem Bereich können verglichen mit der nützlichen Wirkung des Medizinprodukts ohne weitere Maßnahmen akzeptiert werden.
- der sogenannte ALARP-Bereich (As Low As Reasonable Practicable) - befinden sich Risiken in diesem Bereich, muß geprüft werden, ob das Risiko bereits so weit wie vernünftigerweise möglich minimiert ist; andernfalls müssen geeignete Maßnahmen ergriffen werden.
- der nicht akzeptable Bereich - hier sind auf jeden Fall weitere Maßnahmen zur Risikominimierung erforderlich.

Abbildung 3.5 zeigt eine solche Bewertungsmatrix. Dunkelgrau markierte Felder stellen den nicht akzeptierten Bereich, graue Felder den ALARP und hellgraue Felder den akzeptierten Bereich dar.

Häuf.				
Wahr				
Gel				
Entf				
Unwahr				
Unvor				
	Unwes	Gering	Krit.	Katastr.

Abbildung 3.5: Risikograph

Die eigentliche Risikoanalyse untersucht die Gefährdungen und Ursachen und bewertet diese an Hand der festgelegten Parameter. Anschließend werden die als nicht akzeptabel erkannte Risiken durch geeignete Maßnahmen soweit als sinnvoll möglich reduziert. Bevor im weiteren der Prozeß der Risikoanalyse und Risikobeherrschung detaillierter dargestellt wird, soll zuerst der Begriff „Gefährdung“ erklärt werden. Abbildung 3.6 stellt eine Kausalkette von Abläufen dar, die ausgehend vom Ausfall eines Transistors einen möglichen Verlauf bis hin zum Tod des Patienten aufzeigt. Die Frage ist nun, ab welchem Punkt eine Gefährdung vorliegt?

<sup>7</sup>Die Aufteilung in Schadensausmaß und Auftretenswahrscheinlichkeit resultiert aus der Definition des Begriffs „Risiko“, das als „Auftrittswahrscheinlichkeit einer Gefährdung, die einen Schaden hervorruft und der Grad ihres Schadens“ definiert wird (aus EN 60601-1-4).

<sup>8</sup>aus [Hof98]

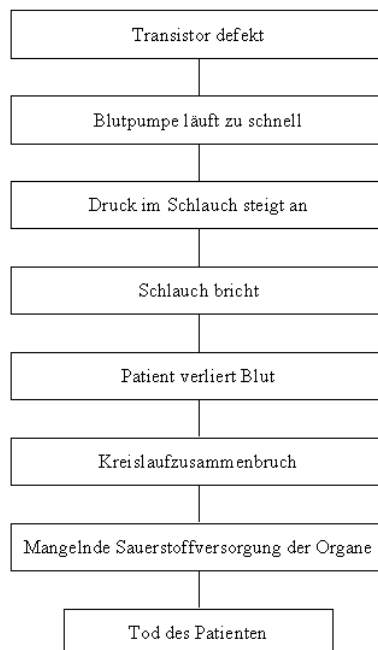


Abbildung 3.6: Beispiel Gefährdung (Quelle: Kursunterlagen „CE Zertifizierung medizinisch genutzter Software“ TÜV Akademie)

Eine Gefährdung liegt dann vor, wenn der erste Punkt der Kausalkette erreicht wird, an dem der Patient betroffen ist. Im Beispiel ist das der „Patient verliert Blut“.

### 3.1.5 Risikoanalyse

Zur Bestimmung der Gebrauchstauglichkeit von Medizinprodukten wird als Verfahren die Risikoanalyse eingesetzt. Ziel ist es, alle vernünftigerweise vorhersehbare Gefährdungen, die durch das PEMS entstehen können, zu erkennen und einzudämmen. Als vernünftigerweise vorhersehbar sind hier sowohl Gefährdungen zu erkennen, die sich aus bestimmungsgemäßen Gebrauchs ergeben als auch solche die sich aus unsachgemäßen Gebrauch ergeben. Es werden dabei alle Risiken betrachtet, die einen Schaden am Patienten, den Anwendern, Servicepersonal, Unbeteiligte oder für die Umgebung und Umwelt verursachen können. Da es sich hierbei für Medizinprodukte um ein elementares Verfahren handelt, wurde von der europäischen Komitee für Normung die Norm EN1441 erstellt, die 1997 in eine deutsche Fassung umgesetzt wurde<sup>9</sup>.

Die Risikoanalyse ist ein iteratives Verfahren das während des gesamten Entwicklungslebenszyklus des Medizinprodukts durchgeführt wird. Ziel ist es, die Gefährdungen festzustellen und ihre Risiken abzuschätzen.

Die Vorgehensweise beschreibt das Flußdiagramm in Abbildung 3.7.

<sup>9</sup>vgl. auch ISO 14971-1 Medical Devices - Risk Management, Part 1: Application of risk analysis

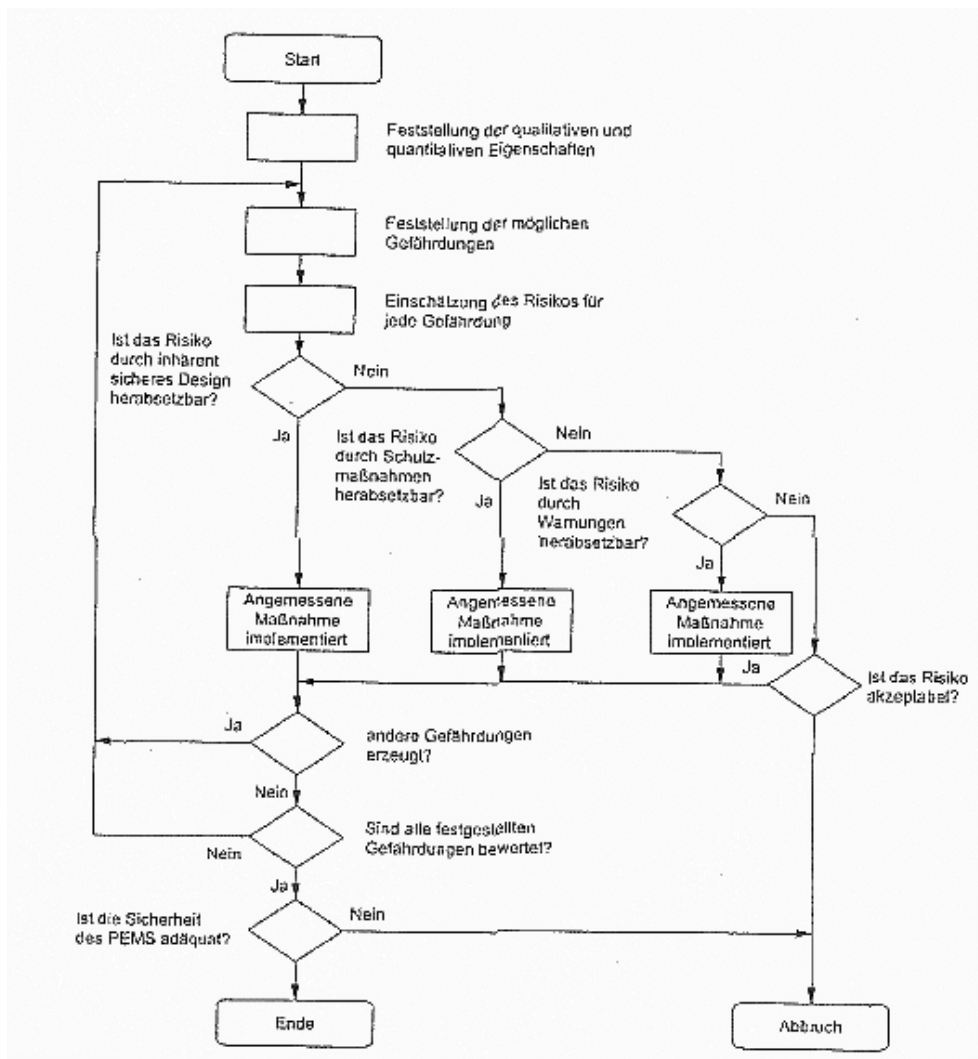


Abbildung 3.7: Flußdiagramm des Risikoanalyse Verfahrens (Quelle: Bild CCC.2 EN60601-1-4)

**Feststellung der qualitativen und quantitativen Eigenschaften von Medizinprodukten** In diesem Schritt werden alle Eigenschaften eines Produktes oder Zubehörs aufgeführt, von denen im weiteren alle mit einer sicherheitsgefährdenden Funktion für Menschen bzw. Umwelt betrachtet werden. Zur Feststellung der qualitativen und quantitativen Eigenschaften bietet die Norm verschiedene Fragestellungen, die Anregungen geben sollen, die sicherheitsgefährdenden Eigenschaften des Produkts zu finden.

**Feststellung der möglichen Gefährdungen** Hierfür gibt die Norm ebenfalls eine Liste möglicher Gefährdungen vor. Diese soll als Gedächtnisstütze dienen, um Gefährdungen zu erkennen, die man nicht in Betracht gezogen hat.

**Risikoeinschätzung für jede Gefährdung** In diesem Schritt werden die Risiken eingeschätzt. Für diesen Schritt muß vorab eine „Skala“ definiert werden, die das Schadensausmaß und die Eintrittswahrscheinlichkeit festlegen<sup>10</sup>. Die Norm empfiehlt das Auftreten von Gefährdungen zusätzlich danach zu untersuchen, wenn kein Fehlerfall vorliegt, wenn ein Fehlerfall vorliegt oder nur falls mehrere Fehler auftreten. Als Analysemethode wird die Fehler-Möglichkeiten- und Einflußmöglichkeit (FMEA) oder die Fehlerbaumanalyse (FTA) vorgeschlagen. Diese Methoden sind allerdings nicht verpflichtend.

Die FMEA Methode stellt den klassischen „bottom up“ Ansatz dar. Man betrachtet die Auswirkungen eines Fehlers auf die darüberliegenden Schichten. Betrachtet man zusätzlich den Schweregrad der Auswirkung eines Fehlers, spricht man von einer „Failure Mode Effect and Criticality Analysis“ (FMECA).

Die FTA Methode stellt die umgekehrte Vorgehensweise vor (top down). Ausgehend von einer unerwünschten Konsequenz werden hier alle aufgerufenen Module soweit „nach unten“ verfolgt, bis man die auslösende Komponente/Modul/Funktion findet. Bedingt dadurch, daß diese Methode den möglichen Ablaufstrang aufzeigt, hat sich diese Methode für gerichtliche Zwecke bewährt.

**Risikoakzeptanz** Die Beurteilung der Risiken bezüglich des Schadensausmaßes und der Schadenshäufigkeit ermöglicht die Zuordnung in akzeptierte und nicht akzeptierte Bereiche. Der Grenzbereich wird als ALARP (As Low As Reasonable Possible) Bereich bezeichnet. Liegt eine Funktion im akzeptierten Bereich, kann mit der Analyse neu erzeugter Gefährdungen weitergemacht werden, ansonsten muß eine Risikominderung durchgeführt werden.

**Risikominderung** Falls das Risiko nicht akzeptierbar ist müssen risikomindernde Maßnahmen eingeleitet werden. Man verwendet hierfür ein abgestuftes Verfahren. Begonnen wird mit inhärenter Risikominderung. Kann keine inhärente Lösung gefunden werden, versucht man das Risiko durch indirekte Maßnahmen herabzusetzen. Hierzu zählen beispielsweise bauliche Maßnahmen oder bei Software die Überprüfung des Eingabeformates. Eine weitere Abschwächung bedeuten hinweisende Schutzmaßnahmen (z.B. Hinweis in der Gebrauchsanweisung).

**Erzeugung anderer Gefährdungen** Die Umsetzung gefährdungsmindernder Maßnahmen kann selbst wieder neue Risiken erzeugen. Diese gilt es in diesem Schritt zu erkennen und einzuordnen.

**Bewertung aller festgestellten Gefährdungen** Der Prozeß der Risikoeinschätzung für jede Gefährdung, Risikoakzeptanz, Risikominderung und Überprüfung, ob neue Gefährdungen erzeugt wurden, wird solange fortgesetzt, bis alle festgestellten Risiken bewertet wurden. Anschließend wird ein Risikoanalysebericht erstellt.

---

<sup>10</sup>vgl. Abbildung 3.5

**Risikoanalysebericht** Anhand des Risikoanalyseberichts wird die Entscheidung getroffen, ob das verbleibende Restrisiko akzeptiert werden kann. Es gilt der Grundsatz: so wenig Risiko wie möglich.

**Überprüfung der Risikoanalyse** Änderungen am Source Code oder neuer Daten werden erneut auf ihr Risiko überprüft.

**Der Risikoanalyse Plan** legt vor Erstellung der Risikoanalyse folgendes fest:

1. Geltungsbereich auf den der RA Plan anzuwenden ist
2. Definition Schadensausmaß
3. Definition Schadenshäufigkeit
4. Hauptgefährdungen

Des Weiteren werden alle erkannten Risiken vor der Umsetzung gefährdungsmindernder Maßnahmen aufgeführt, insbesondere die Gefährdung für den Patienten, die Ursache, eine Bewertung der Gefährdung (aufgeschlüsselt nach Ausmaß, Häufigkeit und Einstufung) sowie eventueller Maßnahmen zur Verringerung der Risiken.

Analog zu diesem Dokument wird der Risikoanalyse Report erstellt. Anders als im RA Plan wird hier die Wirksamkeit der Maßnahmen beurteilt.

Das Risikomanagement wird durch Verfassen eines Reports (Zusammenfassung) abgeschlossen. Diese stellt alle gefundenen Gefährdungen zusammen mit den ermittelten Ursachen, dem abgeschätztem Risiko, einer Bewertung der Risikobeherrschung plus den Verfahren und Ergebnissen der Verifizierung dar (siehe Abbildung 3.3). Die Gesamtheit aller Dokumente, die als Teil der Qualitätsaufzeichnung für die Umsetzung der Norm EN 60601-1-4 verlangt werden nennt man Risiko-Management-Dokumentation.

### 3.1.6 Technische Dokumentation

Die Technische Dokumentation ist für das Anbringen einer CE - Kennzeichnung eine zwingende Voraussetzung, die von der Klassifizierung des Medizinproduktes unabhängig ist.

Die Technische Dokumentation läßt sich in zwei Bereiche gliedern<sup>11</sup>:

- Dokumente die beim Hersteller bzw. Inverkehrbringer bleiben
  - Definition der Zweckbestimmung
  - Klassifikation nach MDD
  - Hardwaredokumentation
  - Prüfprotokolle

---

<sup>11</sup>aus <http://www.eurocat.de/de/text/technisc.html>; siehe auch MDD Anhang I

- Risikoanalyse
- Dokumentation über den Nachweis zur Erfüllung der „Grundlegenden Anforderungen“
- Klinische Bewertung nach Anhang X, MDD
- Softwaredokumentation
- Dokumente die der Endbenutzer bzw. Betreiber erhält
  - Betriebsanleitung oder Gebrauchsanleitung
  - Technische Beschreibung
  - Ersatzteilkatalog
  - Konformitäts-Erklärungen

## 3.2 Anforderungen der FDA

Für die Inverkehrbringung von Medizinprodukten auf dem amerikanischen Markt müssen die Anforderungen der amerikanischen Gesundheitsbehörde FDA (Food and Drug Administration) erfüllt werden. Analog zum CE Kennzeichen wird hierfür ein Zertifizierungsprozeß durchlaufen. Dieses Kapitel stellt die Anforderungen dar. Der Schwerpunkt liegt darauf die Unterschiede heraus zu arbeiten, die als zusätzliches „add-on“ erstellt werden müssen um eine Zulassung für beide Märkte zu erhalten. Die Auswahl des amerikanischen Marktes resultiert zum einen aus der wirtschaftlichen Größe der USA, aus der sich ein großer Markt für Medizinprodukte ableiten läßt, zum anderen an der sehr fortschrittlichen Art, sich Informationsquellen zu besorgen - die FDA stellt auf ihrer Homepage sogenannte „Guidance“ Dokumente zur Verfügung. Im Vergleich dazu stehen im europäischen Raum nur die Normtexte bereit. Diese können in Deutschland ausschließlich über den Beuth Verlag bestellt werden. Medizinprodukte, die Software enthalten oder reine Softwareprodukte sind, sollten nach den Guidance Dokumenten *General Principles of Software Validation*, *Guidance for the Content of Premarket Submission for Software Contained in Medical Devices* und *Guidance for Off-the-shelf Software Use in Medical Devices* erstellt werden.

Die Vorgehensweise wird in einem 3 stufigen Plan festgelegt. Zuerst muß bestimmt werden, ob das Produkt ein Medizinprodukt gemäß der Definition ist. Die Definition für den US amerikanischen Markt unterscheidet sich leicht von der europäischen Definition:

*„an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including a component part, or accessory which is:*

- *recognized in the official National Formulary, or the United States Pharmacopoeia, or any supplement to them,*
- *intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man or other animals, or*

- *intended to affect the structure or any function of the body of man or other animals, and which does not achieve any of its primary intended purposes through chemical action within or on the body of man or other animals and which is not dependent upon being metabolized for the achievement of any of its primary intended purposes.*“

Als zweiter Schritt wird dem Medizinprodukt die Risikoklasse zugeordnet. Analog des europäischen Ansatzes werden hierfür drei Stufen definiert die die Gefährdung durch das Produkt im Fehlerfall darstellen:

- Major - falls Menschenleben direkt oder indirekt (z.B. Verzögerung durch Information) schwere Verletzungen oder sogar den Tod bedeuten könnten
- Moderate - falls Fehler zu nicht schwerwiegenden Verletzungen führen können
- Minor - falls keine Verletzungen von Menschenleben zu erwarten ist.

Diese werden nicht weiter unterteilt. Die Klassifizierung wird anhand eines Fragenkatalogs durchgeführt, die der Hersteller zur Klassifizierung des Produktes durchgehen muß. Abbildung 3.8 zeigt die schematische Vorgehensweise. Die Fragen zur Einstufung findet man z.B. unter [FDA98]. Als weitere Möglichkeit der Klassifizierung bietet die FDA sogenannte *device panels* an. Das sind bereits vorklassifizierte Gerätetypen, deren Zuordnung einer Datenbank (siehe <http://www.fda.gov/cdrh/devadvice/3131.html>) entnommen werden kann. Es ist hierbei hervorzuheben, daß es nicht möglich ist, eine direkte Abbildung der „europäischen“ auf die „amerikanischen“ Risikoklassen vorzunehmen. Eine Klassifizierung ist deshalb separat für jeden Markt vorzunehmen.

Der dritte Schritt besteht in der Methode, wie die Markteinführung vorgenommen werden soll. Im wesentlichen stellen sich hier zwei Methoden zur Auswahl: die „*Premarket Notification (510 k)*“ und das „*Premarket Approval (PMA)*“.

### 3.2.1 Anforderungen an die Dokumentation

Als wesentliche Komponenten der Entwicklung Medizinischer Geräte stellt die FDA die in der folgenden Liste zusammengefaßten Anforderungen an den Umfang der Dokumentation. Alle Dokumente müssen in englischer Sprache verfaßt sein. Für den europäischen Markt reicht es aus, wenn die Gebrauchsanweisung in der jeweiligen Landessprache verfaßt ist.

1. Klassifizierung
2. Softwarebeschreibung
3. Risikoanalyse
4. Anforderungsspezifikation
5. Architektur Überblick
6. Designspezifikation

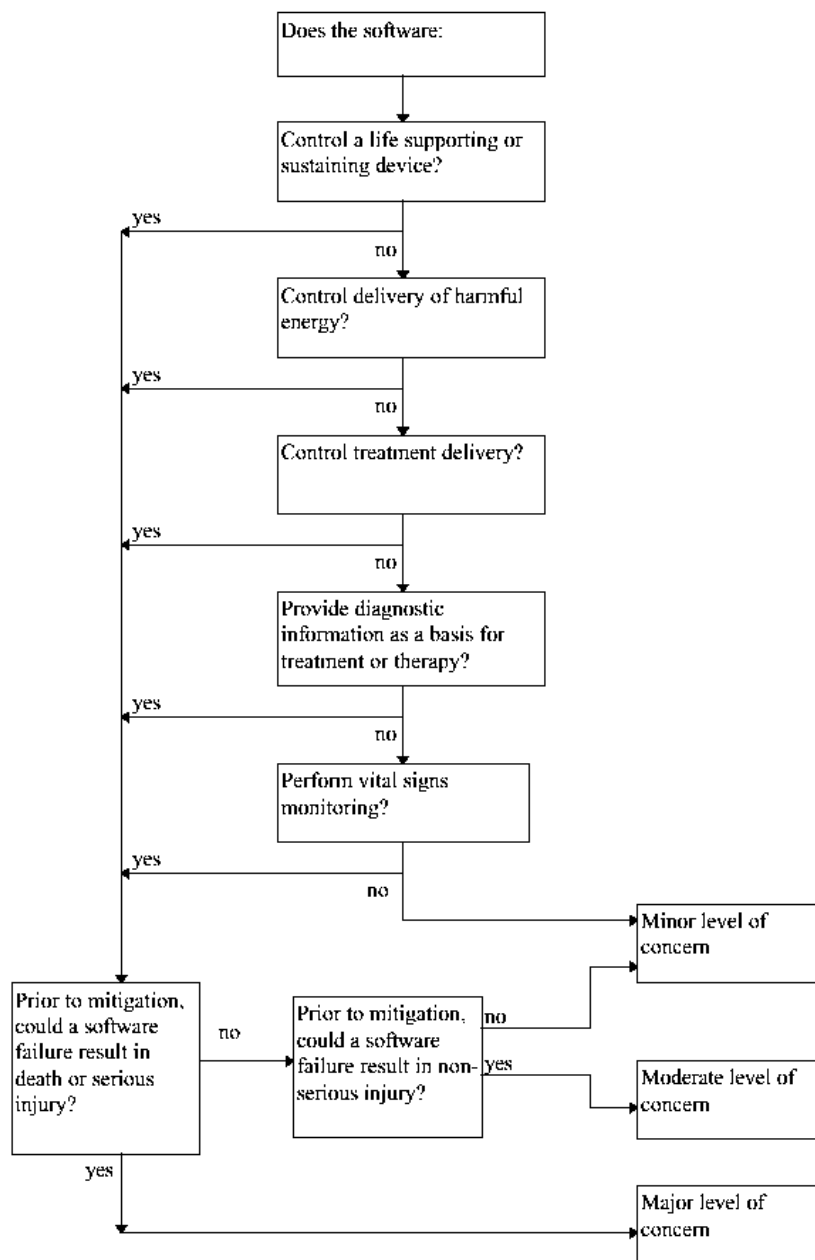


Abbildung 3.8: Determining Level of Concern (aus Guidance FDA)

7. Rückverfolgungsanalyse
8. Entwicklung
9. Validierung, Verifizierung, Tests
10. Revision History
11. Softwareanomalien (BUGS)

## 12. Release Versionsnummer

ad 1) Es soll dokumentiert werden, wie man auf das Ergebnis der Klassifizierung gekommen ist.

ad 2) Die Softwarebeschreibung stellt eine Zusammenfassung der Geräteeigenschaften dar. Sie enthält zum einen die von der Software ausgeführten Funktionalitäten und zum anderen Angaben zur betrieblichen Umgebung. [FDA98] stellt für die Umsetzung eine Reihe von Punkten bereit.

ad 3) Enthält eine Zusammenfassung aller vorhersehbarer Risiken, die durch den Einsatz des Gerätes entstehen können. Die Anforderungen entsprechen denen des Risikomanagements nach EN 60601-1-4:

- die Risiken
- das Schadensausmaß
- Auslösende Ursache
- Methode zur Kontrolle des Risikos (typischerweise Prinzip der integrierten Sicherheit)
- Maßnahmen zur Risikobeherrschung
- Beschreibung über durchgeführte Tests, die belegen, daß die Maßnahmen zur Risikobeherrschung wirksam sind

ad 4) Die Anforderungsspezifikation sollte unter anderem Angaben zur Funktionalität, Leistung, Schnittstellen, Design- und Entwicklungsanforderungen enthalten. Die Anforderungen decken sich weitestgehend mit denen der Europäer, mit der Ausnahme der Behandlung von „*Off the Shelf Software*“ (siehe Kapitel weiter unten).

ad 5) Die Architektur-Übersicht stellt die Zusammenhänge der Module auf funktionaler Ebene graphisch dar. Weiterhin sollte eine Liste der funktionalen Module und eine Beschreibung deren Aufgabe enthalten sein.

ad 6) Die Designspezifikation stellt einen Rahmen für den Designentwurf dar. Von Seiten der FDA wird eine Einteilung in Grob- und Feindesign durchgeführt wird, wobei das Feindesign detailliert genug sein sollte, um keine ad-hoc Entscheidungen des Programmierers zu erfordern. Gegenüber einer Zulassung auf dem europäischen Markt erfordert die Zulassung durch die FDA zusätzlich eine Beschreibung der Akzeptanzkriterien, die in das Design eingeflossen sind. Außerdem müssen Variablendefinitionen und der jeweilige Kontext, in dem diese benutzt werden, angegeben werden.

ad 7) Die Traceability Analyse stellt die Verknüpfung der Anforderungen mit den Designspezifikationen, den Risiken und der Validierung dar. Das Dokument kann als Inhaltsverzeichnis für die Bestimmung der Ablageorte der Anforderungen in den unterschiedlichen Dokumenten angesehen werden. Die Darstellung erfolgt üblicherweise tabellarisch. Falls sich die Zusammenhänge nicht eindeutig aus der Zuordnung ergeben, sollte eine Beschreibung beigefügt werden.

ad 8) Dieser Punkt umfaßt eine Kurzzusammenfassung des verwendeten Software-Entwicklungszyklus. Für Geräte der Risikoklasse „moderate“ und „major“ sollten zusätzlich Qualitätssicherungs- Konfigurationsmanagement- und Wartungsdokumente erstellt werden.

ad 9) Die Anforderungen an die Dokumentation von Verifizierung, Validierung und Test sind im wesentlichen dieselben wie die der EN 60601-1-4. Der Umfang wird durch ein abgestuftes Verfahren an die Risikoklassen gebunden. Das Guidance Dokument gibt in einer Liste den minimal zu testenden Umfang vor.

ad 10) Das „Revision History Log“ soll beigelegt werden, um den Änderungsverlauf insbesondere in Bezug auf die Umsetzung gefährdungsmindernder Maßnahmen nachvollziehen zu können.

ad 11) Für Geräte der Risikoklasse „moderate“ und „major“ muß eine Liste der Softwareanomalien (BUGS) beigelegt werden. Zu jeder Anomalie muß eine Problembeschreibung, der Einfluß auf die Geräteleistung und falls möglich ein zeitlicher Rahmen bis zur Behebung des Problems angegeben werden.

ad 12) Bei Auslieferung des Produkts sollte Release Nummer und Datum angegeben werden.

Der Umfang der Dokumentation ist abhängig von der Risikostufe des Geräts. Abbildung 3.9 stellt die Anforderungen an die Dokumentation bezüglich der Risikostufe dar.

SECTION NUMBER	SOFTWARE DOCUMENTATION	MINOR CONCERN	MODERATE CONCERN	MAJOR CONCERN
2, 3.1	Level of Concern	All levels of concern		
3.2	Software Description	All levels of concern		
3.3, 4.3	Device Hazard Analysis	All levels of concern		
3.4, 4.2	Software Requirements Specification (SRS)	Software functional requirements from SRS	SRS	
3.5	Architecture Design Chart	A chart depicting the partitioning of the software system into functional subsystems	A chart depicting the partitioning of the software system into functional subsystems, listing of the functional modules and a description of how each fulfills the requirements.	
3.6	Design Specification	No documentation is necessary in the submission.	Software design specification document	
3.7	Traceability Analysis	No documentation is necessary in the submission.	Traceability among requirements, identified hazards, and Verification and Validation testing.	
3.8, 4.1	Development	No documentation is necessary in the submission.	Summary of software life cycle development plan, including a summary of the configuration management and maintenance activities.	Summary of software life cycle development plan. Annotated list of control documents generated during development process. Include the configuration management and maintenance plan documents.
3.9	Validation, Verification and Testing (VV&T)	Software functional test plan, pass / fail criteria, and results	Description of VV&T activities at the unit, integration and system level. System level test protocol including pass/fail criteria, and tests results.	Description of VV&T activities at the unit, integration and system level. Unit, integration and system level test protocols including pass/fail criteria, test report, summary, and tests results.
3.10	Revision Level History	No documentation is necessary in the submission.	Revision history log	
3.11	Unresolved anomalies (bugs)	No documentation is necessary in the submission.	List of errors and bugs which remain in the device and an explanation how they were determined to not impact safety or effectiveness, including operator usage and human factors.	
3.12	Release Version Number	Version number and date for all levels of concern.		

Abbildung 3.9: Dokumentation in a Premarket Submission (Quelle: [FDA99] Abb. 1-1)

### 3.2.2 Off the Shelf Software

Häufig werden in Medizinprodukten neben der eigentlichen Software, die als Teil des Medizinproduktes erstellt wurde, noch zusätzliche eingebunden. Wird die Software beispielsweise für einen PC erstellt, wird häufig auf Standardbetriebssysteme zurückgegriffen. Bei „off the shelf“ Software handelt es sich um allgemein erhältliche Softwarekomponenten, die vom Hersteller eines Medizinproduktes verwendet werden, über die er aber keine vollständige Kontrolle über den Entwicklungslebenszyklus besitzt (z.B. Betriebssysteme, Compiler..).

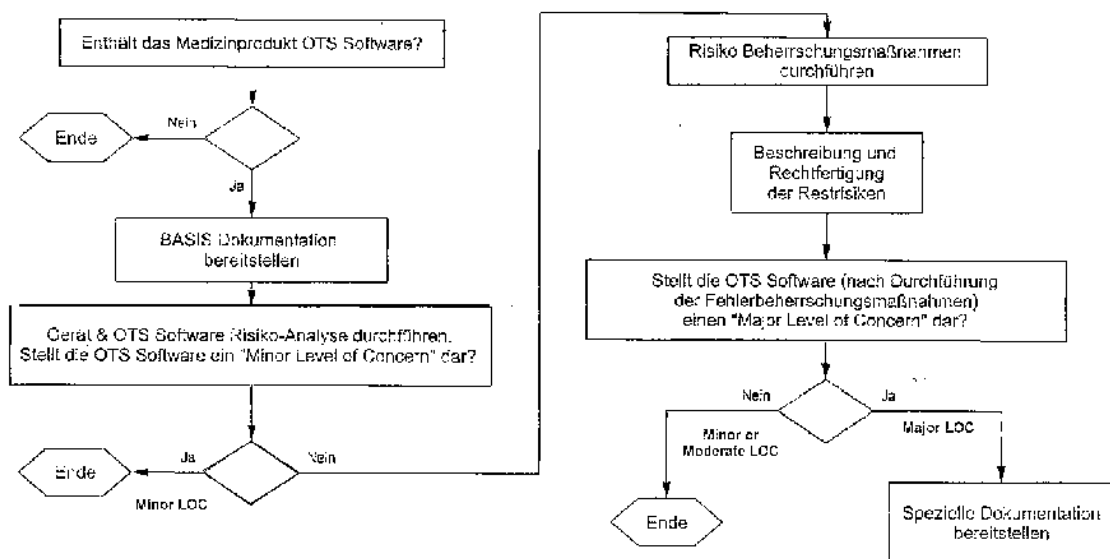


Abbildung 3.10: Off the Shelf Software

Das Flußdiagramm in Abbildung 3.10 zeigt den konzeptuellen Ablauf bei der Ermittlung des Aufwands der durch die zusätzliche Software entsteht. Wird off the shelf Software eingesetzt, muß eine Basis-Dokumentation bereitgestellt werden. Diese umfaßt folgende Punkte:

- Titel, Hersteller, Versionsstand, Datum, Patchversion, Dokumentation für den Endanwender
- Systemanforderungen (Hardware und Software)
- Anforderungen an den Anwender
  - Installation
  - Konfiguration
  - normale und akzeptierte Datenbereiche
  - Voreinstellungen
  - Erforderliche Ausbildung und Kenntnisse/Training
- Maßnahmen die den Betrieb nicht spezifizierter Software (z.B. Spiele ..) verhindern
- Verwendungszweck
- Schnittstellen zu anderer Software (z.B. Netzwerk)
- Hinweis auf die Funktionsfähigkeit der Software (Tests, Verifizierung, Validierung)

- Testergebnisse müssen bereitgestellt werden
- „Wie erhält man Updates“ / Bug Liste
- Kontrolle der OTS Software (Erkennung der korrekten Version, Einbindung in Konfigurationsmanagement, Sicherstellung der korrekten Installation, Wartung und Support)

Stellt die Off the Shelf Software keinen „minor Level of Concern“ dar, müssen Risikobeherrschungsmaßnahmen durchgeführt und anschließend die Restrisiken beschrieben werden. Es muß eine komplette Betrachtung aller Restrisiken bereitgestellt werden, wobei auch Alternativen (z.B. Eigenentwicklung) in Betracht gezogen werden sollten. Die Akzeptanz des Restrisikos ist vom Nutzen der Anwendung abhängig. Sollte das Restrisiko als „major level of concern“ eingestuft werden, muß zusätzlich noch eine spezielle Dokumentation verfaßt werden, die aufzeigt, daß die Verfahren und Ergebnisse der Verifizierungs- und Validierungsaktivitäten für die OTS Software angemessen und hinreichend sind um die Sicherheits- und Performanceanforderungen zu erfüllen. Zudem müssen angemessene Maßnahmen zur kontinuierlichen Wartung und Pflege der OTS Software getroffen werden, falls der ursprüngliche Hersteller die OTS Software nicht mehr unterstützt. Es muß außerdem dargelegt werden, daß die Methodik, die der Entwickler der OTS Software für die Erstellung verwendet hat, angemessen und hinreichend für den beabsichtigten Einsatz ist. Diese Forderung sollte zusätzlich durch ein Audit gezeigt werden.

# Kapitel 4

## V-Modell

Das V-Modell ist ein internationaler anerkannter Entwicklungsstandard für IT-Systeme. Der Standard wurde 1992 im Auftrag des Bundesverteidigungsministeriums für Verteidigung (BMVg) und dem Bundesamt für Wehrtechnik und Beschaffung von der Industrieanlagen-Betriebsgesellschaft mbH (IABG) entwickelt. 1996 wurde das V-Modell vom Bundesinnenministerium des Inneren (BMI) übernommen und ist dort seither verbindlich einzusetzen. Die Weiterentwicklung wird durch das BMVg und BMI betrieben und finanziert.

Der Standard legt einheitlich und verbindlich fest, was zu tun ist, wie die Aufgaben durchzuführen sind und womit das zu geschehen hat. Das V-Modell umfaßt

- das Vorgehensmodell („Was ist zu tun“)
- die Methodenzuordnung („Wie ist etwas zu tun“)
- die Funktionalen Werkzeuganforderungen („Womit ist etwas zu tun“).

Das Vorgehensmodell gliedert sich in den Regelungsteil, die behördenspezifische Ergänzungen und die Handbuchsammlung. Der Regelungsteil enthält verbindliche Regelungen für durchzuführende Arbeitsschritte und Ergebnisse wohingegen die Handbuchsammlung eine Reihe von Handbüchern zu speziellen Themen wie „IT Sicherheit“ oder „Reverse Engineering“ enthält.

Das V-Modell wurde für verschiedene Anwendungsaspekte entwickelt, wobei die Einsatzschwerpunkte die *Vertragsgrundlage*, *Arbeitsanleitung* und *Kommunikationsbasis* sind. Als Vertragsgrundlage definiert das V-Modell eindeutig den Erstellungsprozeß, den Lieferumfang der Hard- und Software und legt den Umfang der Dokumentation fest. Detaillierte Beschreibungen der Aktivitäten und Entwicklungsdokumente stellen die Arbeitsanleitung und die Beschreibung der Vorgehensweise in Verbindung mit einem bereitgestelltem Glossar stellen die Kommunikationsbasis zwischen Auftraggeber und Auftragnehmer sowie zwischen interdisziplinär arbeitenden Nutzern.

Die anfallenden Tätigkeiten werden in vier funktionale Abschnitte (Submodelle) eingeteilt. Diese sind eng miteinander verzahnt, d.h. daß Produkte und Aktivitäten des einen

Abschnitts neue Eingabedaten für Produkte anderer Abschnitte liefern können. Das bekannteste Submodell dürfte wohl die *Systemerstellung (SE)* sein, das aufgrund des V-förmigen Aufbaus dem Modell seinem Namen gegeben hat. Die begleitenden Tätigkeiten werden durch die Submodelle *Projektmanagement (PM)*, *Qualitätssicherung (QS)* und *Konfigurationsmanagement (KM)* abgedeckt. Im folgenden wird jedes dieser Submodelle kurz vorgestellt - für eine detaillierte Einführung sei auf das Buch von W. Dröschel und M. Wiemers [DW00] verwiesen. Alternativ kann der V-Modell Standard als Word Dokument von der URL „www.v-modell.iabg.de“ heruntergeladen bzw. auf einer CD-ROM bestellt werden. Bevor im weiteren die Submodelle erklärt werden, folgen einige Anmerkungen zur Notation

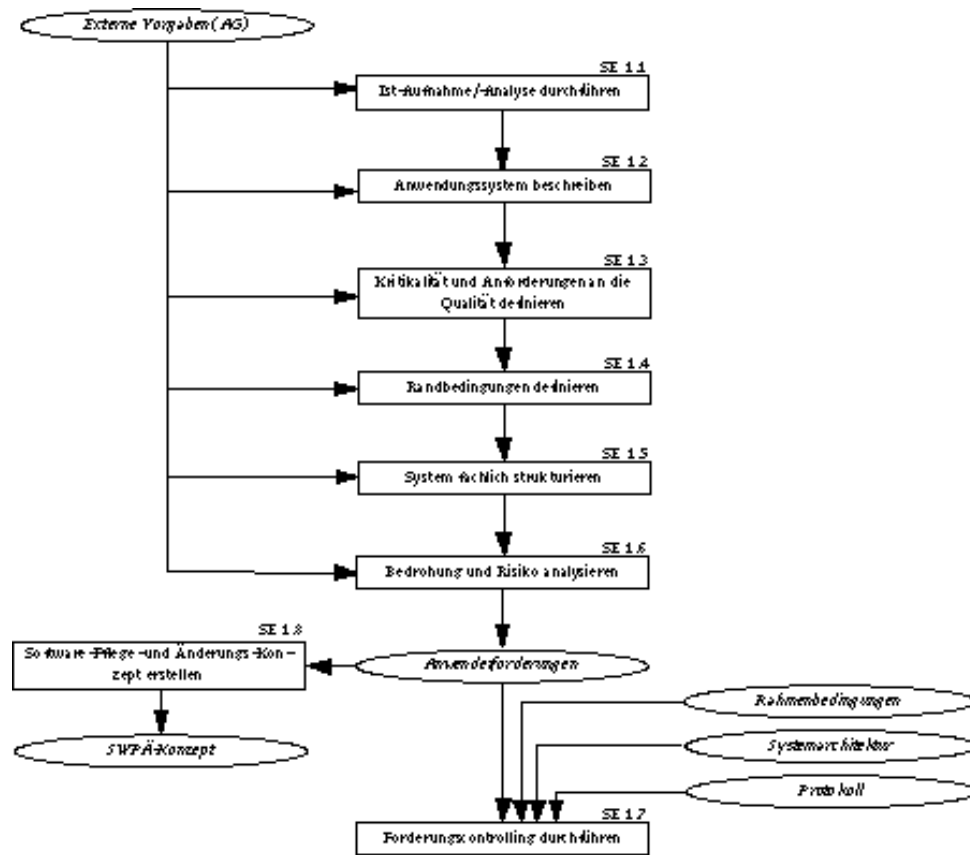


Abbildung 4.1: Abwicklung der Teilaktivität SE 1

und den verwendeten Begriffen: Das V-Modell unterscheidet zwischen Produkten und Aktivitäten, wobei Aktivitäten die durchzuführenden Maßnahmen sind, die für die Erstellung der Produkte durchgeführt werden müssen. Aktivitäten werden durch eine Kombination aus Buchstaben und Zahlen einem Submodell und den jeweiligen Teilaktivitäten zugeordnet. Beispielsweise ist die Aktivität SE 1.2 die 2. Teilaktivität der Anforderungsanalyse (SE 1) im Submodell Systementwicklung (SE). Die hierarchischen Zerlegung von Aktivitäten (im oberen Beispiel die Anforderungsanalyse SE 1 in ihre Teilaktivitäten SE 1.1 .. SE 1.8) wird in Diagrammen dargestellt. Abbildung 4.1 zeigt das Diagramm für die Teilaktivität SE 1.

## 4.1 Systemerstellung

<sup>1</sup> Der produktive Anteil des IT Projekts wird im Submodell SE beschrieben. Dieses beschreibt alle notwendigen Aktivitäten um ausgehend von der Anforderungsanalyse bis hin zur Abnahme des installierten Systems durchgeführt werden sollen. Das Submodell SE unterteilt sich in zwei Ebenen, die durch bestimmte Aktivitäten geprägt sind:

1. System- bzw. Segment-Ebene
2. Ebene der Software- und Hardwareeinheiten

Innerhalb dieser Ebenen wird zunächst die Anforderungsanalyse erstellt und darauffolgend der Entwurf des Systems bzw. der Einheiten spezifiziert. Sie dienen dazu in zeitlich frühen Phasen von abstrakten Beschreibungen zu Software- oder Hardwareeinheiten zu gelangen und in späteren Phasen zum Gesamtsystem zu kommen.

Die Aktivität System-Anforderungsanalyse (SE 1) setzt sich aus den Teilaktivitäten SE 1.1 bis SE 1.8 zusammen. Sie erhält als Eingangsprodukte die externen Vorgaben, die Rahmenbedingungen, die Systemarchitektur und Protokolle. Auf Basis dieser Produkte erzeugt bzw. bearbeitet SE 1 die Anwenderanforderungen, die eine grobe Systembeschreibung darstellen und auf der in weiteren Entwicklungszyklen aufgebaut wird und dort weiter verfeinert werden. Die Anwenderanforderungen fließen dann in den System-Entwurf (SE 2) ein, aus denen aufgrund der Eingangsprodukte eine möglichst technische Systemarchitektur erarbeitet wird. Hierbei wird bereits auf den geeigneten Einsatz von Fertigprodukten geachtet. Der Lösungsvorschlag wird nachfolgend bewertet und ist bei einer Ablehnung zu überarbeiten. Wurde er akzeptiert, wird die Systemarchitektur verfeinert und endet mit der Identifikation der Schnittstellen, die in der Schnittstellenübersicht angeführt werden und in der Schnittstellenbeschreibung näher erläutert werden. Die SW-Architektur und die Schnittstellenbeschreibungen stellen im folgenden die Informationsquellen für den SW-Feinentwurf (SE 5-SW) dar. Hier werden die Details für die Realisierung jedes Moduls, jeder Komponente und jeder Datenbank festgelegt und der Betriebsmittel- und Zeitbedarf der einzelnen Elemente ermittelt. Niedergeschrieben werden die Ergebnisse im Datenkatalog und SW-Entwurf. Im Rahmen der SW-Implementierung (SE 6-SW) sind nun die Module und Datenbanken zu verwirklichen bevor sie während der SW-Integration (SE 7-SW) unter Einhaltung des Integrationsplans und unter Hinzunahme - falls vorhanden - der HW-Einheiten und Nicht-IT-Anteile zu einem System zusammengeführt (System-Integration, SE 8). Ist das System fertiggestellt, sorgt die Aktivität Überleitung in die Nutzung (SE 9) für die Installation und Inbetriebnahme an der vorgesehenen Einsatzstelle. Abbildung 4.2 zeigt den Funktionsüberblick zum Submodell SE.

---

<sup>1</sup>aus: [IP98]

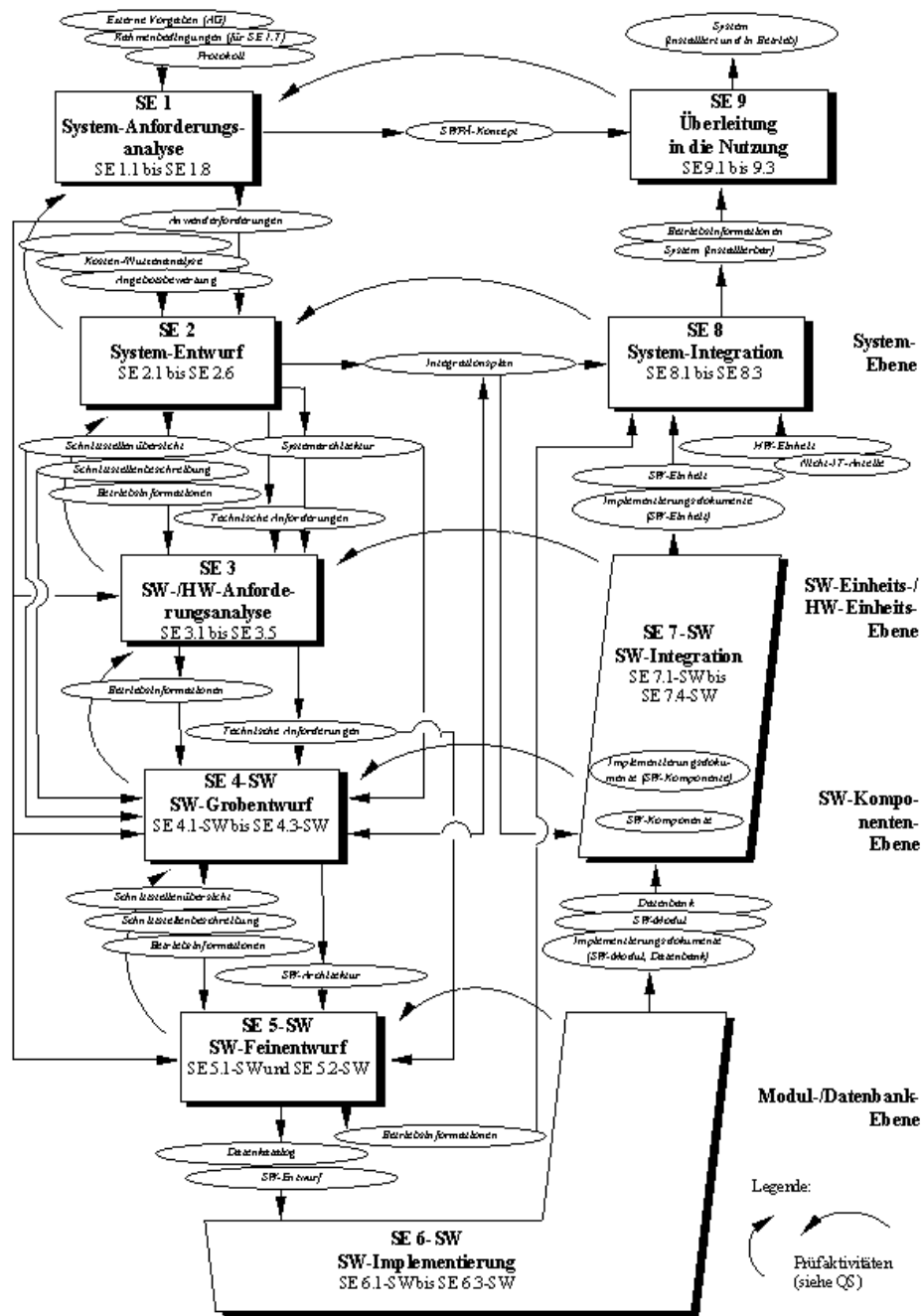


Abbildung 4.2: Funktionsüberblick Subsystem SE

## 4.2 Projektmanagement

<sup>2</sup> Die Aktivitäten des Projektmanagements beziehen sich auf die Bezugspunkte „Projekt“, „Vergabe/Beschaffung“, „Planungsabschnitt“, „Periodisch durchzuführende Aktivitäten“ und „Arbeitsabschnitt“. Projektbezogene Tätigkeiten sind beispielsweise das Erstellen des Projekthandbuchs. Vergabebezogene Aktivitäten regeln die Vorbereitung und Durchführung einer Vergabe. Im Planungsabschnitt erfolgt die Feinplanung (z.B. Kosten/Nutzenanalyse). Periodisch durchzuführende Aktivitäten umfassen u.a. das Risikomanagement, wohingegen der Bezugspunkt „Arbeitsschritte“ z.B. die Definition von Arbeitsaufträgen beinhaltet. Das V-Modell legt nicht fest, wie die Aktivitäten im Projektmanagement durchzuführen bzw. welchen Organisationseinheiten (Personen) sie zugeordnet sind. In der Regel nimmt die zentrale Rolle im PM ein Projektleiter ein. Dieser initialisiert das Projekt mit der ersten gleichnamigen Aktivität, in der die projektinterne Zusammenarbeit und ggf. die Schnittstellen zu externen Beteiligungen im ersten Produkt, dem Projekthandbuch, festgehalten werden. Hierfür werden die Projektkriterien und -randbedingungen zusammengetragen, wodurch das Tailoring am V-Modell erfolgen kann. Das so entstehende projektspezifische V-Modell (PM 1.3) ist ebenfalls Inhalt des Projekthandbuchs. Darauf aufbauend wird der grobe Projektplan erstellt (PM 1.4), wobei die Historie ähnlich gearteter Projekte einfließen kann. Der Grobplan legt die Aufwands-, Termin- und Personalplanung zunächst näherungsweise bis zum Projektende dar. Ferner erfolgt die Auswahl einer für das Projekt geeigneten bzw. zugeschnittenen Entwicklungsumgebung, die den Projektmitarbeitern verfügbar gemacht werden muß. Falls das System oder Teile davon durch externe Leistungen realisiert werden sollen, bilden die Aktivitäten Vergabe/Beschaffung (PM 2) und Auftragnehmer-Management (PM 3) das Gerüst zum Vertragsabschluß bzw. zur Beschaffung und zur Überwachung der Arbeitsfortschritte innerhalb der vereinbarten Termine. Werden keine externen Leistungen in Anspruch genommen, entfallen diese zwei Aktivitäten. In der Feinplanung (PM 4) werden auf Basis der bestehenden Grobplanung und unter Hinzunahme des Projekthandbuchs in verschiedenen Teilschritten Verfeinerungen am Projektplan durchgeführt. Hinter den Teilschritten verbergen sich unter anderem das technische Tailoring und die Aufwands- und Terminplanung. Um die Rentabilität von geplanten Lösungen feststellen zu können, werden in der Kosten-/Nutzenanalyse (PM 5) für die verschiedenen Lösungsvorschläge die Kosten abgeschätzt und dem Nutzen gegenübergestellt. Dabei werden die Kosten und der Nutzen des gesamten Lebenszyklus - und nicht nur der Entwicklung - der Lösung betrachtet. Entscheidungen, die im Projektverlauf den Zwecken des Abschlusses von Verträgen oder der Bestätigung der im Projektplan definierten Baselines dienen, sind in der Durchführungsentscheidung (PM 6) zu treffen und werden in ein Protokoll verfaßt. Die Erkennung möglicher Risiken im Projekt, die Einleitung geeigneter, vorbeugender Maßnahmen und die Überwachung der Maßnahmen sind Aufgaben des Risikomanagements (PM 7). Im PM wird natürlich auch der Projektfortschritt verfolgt und kontrolliert und bei Abweichungen wird steuernd eingegriffen. Diese Aktivität trägt den Namen Projektkontrolle und -steuerung (PM 8). Für die notwendige Kommunikation zwischen der Projektleitung, den Mitarbeitern, externen Auftragnehmern und Anwendern sorgt die Aktivität Informationsdienst/Berichtswesen (PM 9). Sie infor-

---

<sup>2</sup>aus [IP98]

miert über den aktuellen Stand des Vorhabens und ist periodisch durchzuführen. Aus ihr abfallende Dokumente ist bspw. der Sachstandsbericht und der Sachbericht. Werden vom Projektmanagement Defizite im Ausbildungsstand des Personals bemerkt, so sind im Rahmen der Schulung/Einarbeitung (PM10) entsprechende Aus- und Fortbildungsmaßnahmen zu veranlassen. Für die Durchführung der Arbeitsschritte muß das Management die dafür vorausgesetzten Mittel wie Arbeits- und Betriebsmittel, Rechenanlagen und die festgelegte Software-Entwicklungsumgebung (SEU) bereitstellen. Die dafür definierte Aktivität im PM trägt den Namen Bereitstellung der Ressourcen (PM 11). Soll ein Arbeitsschritt durch externe Leistungen verwirklicht werden, so wird durch die Vergabe von Arbeitsaufträgen (PM 12) beschrieben, welche Angaben im Arbeitsauftrag gemacht werden müssen. Dazu zählen die Arbeitsanleitung sowie Soll-Werte und Erläuterungen und der gleichen mehr. Das PM sieht schließlich die Einweisung der Mitarbeiter vor. Hier werden die Mitarbeiter mit dem Arbeitsabschnitt vertraut gemacht und die Aufgabenstellung wird ihnen erläutert.

### 4.3 Qualitätssicherung

Die Regelungen des Submodell QS berühren analog zum Projektmanagement in keiner Weise organisatorische oder personelle Festlegungen. Bevor die Arbeit der QS erfolgen kann, muß eine Abbildung auf die konkret vorhandene Ablauforganisation stattfinden.

Wie bereits erläutert wurde, werden die aufgestellten Anforderungen an das zu entwickelnde System im Laufe eines Projekts durch die Aktivitäten in den Submodellen PM und SE verfeinert und in den Produkten „Anwenderforderungen“ und „Technische Anforderungen“ festgehalten. Die in der QS zusammengefaßten Aktivitäten dienen nun dem Nachweis der Erfüllung der gegebenen Anforderungen, der Vermeidung von Mängeln und der Sicherstellung einer Prozeßqualität.

Die erste eigenständige QS-Aktivität ist die QS-Initialisierung (QS 1), in der der organisatorische Rahmen niedergeschrieben wird. Hier werden die für das gesamte Projekt gültigen Festlegungen bzgl. der Erreichung der Qualitätsziele, die Vermeidung von Qualitätsrisiken und der Nachweisführung der tatsächlichen Erreichung der Qualitätsforderungen festgelegt. Im Prüfplan werden unter Abstimmung mit der Projektleitung und dem zugrundeliegendem QS-Plan die zu prüfenden Produkte und Aktivitäten mit den jeweiligen Qualifikationserfordernissen der Prüfer bestimmt und die zeitliche Synchronisation mit dem Projektfortschritt dargestellt. Befinden sich die Produkte „QS-Plan“ und „Prüfplan“ im Akzeptiert-Zustand, extrahiert die Aktivität Prüfungsvorbereitung (QS 2) aus ihnen die Prüfspezifikation und -prozedur, die der „QS-Verantwortliche“ nach erfolgreicher Kontrolle freigibt. Die Prozeßprüfung von Aktivitäten (QS 3) stellt fest, ob gewählte Vorgehensweisen und Produktstandards bei der Durchführung von Aktivitäten in allen vier Submodellen eingehalten wurden. Produkt dieser Aktivität ist das Prüfprotokoll. Auch die Produktprüfung (QS 4) erzeugt bzw. bearbeitet ein Prüfprotokoll. Dieses beinhaltet, ob die formalen Vorgaben eingehalten worden sind und ob das Produkt inhaltlich prüfbar ist. Ist dies der Fall wird es gemäß der Prüfspezifikation untersucht. Wenn nicht, geht es in das zugehörige Submodell (Aktivität) zur Überarbeitung zurück. In beiden Fällen findet ein Zustandswechsel gemäß des Zustandsdiagramms statt. Die Prüfprotokolle der Aktivitäten Prozeß-

und Produktprüfung gehen in das QS-Berichtswesen (QS 5) ein, in dessen Rahmen sie auf die Anzahl, die Schwere, die Klassifikation und die Ursache der Probleme hin ausgewertet werden. Die hieraus entstehenden Produkte sind die sogenannten Berichtsdokumente.

## 4.4 Konfigurationsmanagement

Das Ziel des Konfigurationsmanagements ist, Produkte bezüglich ihrer funktionellen Merkmale sowie ihrer zugehörigen Bestandteile (bspw. Dokumentation) jederzeit eindeutig identifizierbar zu machen, um sie systematisch und kontrolliert ändern bzw. erweitern zu können und die Integrität zu gewährleisten. Das KM überwacht und dokumentiert hierfür die Konfigurationen, so daß die Zusammenhänge und Unterschiede zwischen früheren und aktuellen Konfigurationen nachvollziehbar und überprüfbar sind. Jedes Produkt erhält auf diesem Weg eine Historie, auf dessen Grund die bis dato entwickelten Konfigurationen selektierbar sind.

Die erste KM-bezogene Aktivität legt den organisatorischen Rahmen im KM-Plan fest und stellt Einsatzmittel wie die Produktbibliothek und ihr zugehörige Werkzeuge bereit. Die nächste Aktivität stellt sicher, daß die Produkte und Konfigurationen eindeutig identifiziert, zugriffsgesichert und rekonstruierbar abgelegt sind. Das Änderungsmanagement - die dritte Hauptaktivität des KM - ist für die Abwicklung des Änderungsprozesses, vom Änderungsantrag bis zum Änderungsabschluß und der Rückmeldung zuständig. Die letzte Aktivität - der KM-Dienste (KM 4) - enthält alle diejenigen Aktivitäten, die nach Bedarf, in Intervallen oder auf Veranlassung durchzuführen sind. Dazu gehört die Datenadministration, die Ergebnissicherung, die KM Dokumentation sowie die Schnittstellenkoordination und das Releasemanagement.

von		Produkt	nach	
Aktivität	Zustand		Aktivität	Zustand
Extern SE 1.1-SE 1.3	— in Bearb.	Externe Vorgaben (AG) Anwenderforderungen	— —	— —
—	—	Anwenderforderungen. Randbedingungen	SE 1.5-SE 1.6	in Bearb.

Abbildung 4.3: Produktfluß für Aktivität SE 1.4 „Randbedingungen definieren“

Das V-Modell definiert die Erstellung von Systemen als Folge von Aktivitäten, bei denen Produkte<sup>3</sup> erzeugt werden. Mithilfe einer Produktflußmatrix (siehe Abbildung 4.3) wird für jede Aktivität dargestellt, welche Eingangsprodukte für die Ausführung ausgeführt werden müssen und welche Ausgangsprodukte erzeugt werden. Den Produkten wird dabei einer der Zustände *geplant*, *in Bearb.*, *vorgelegt* oder *akzeptiert* zugewiesen, dabei bedeutet „geplant“, daß das Produkt in der Planung vorgesehen ist (siehe Abschnitt Tailoring weiter unten), „in Bearb.“ deutet an, daß das Produkt gerade bearbeitet wird. Ist ein Produkt

<sup>3</sup>Die Bezeichnung „Produkt“ beschränkt sich hierbei nicht auf die erstellten Dokumente sondern meint auch alle anderen erzeugten Ergebnisse insbesondere der Software selbst.

aus Sicht des Entwicklers fertig, wird es unter Konfigurationsverwaltung genommen und der QS-Prüfung „vorgelegt“. Der Zustand „akzeptiert“ deutet an, daß das Produkt von der QS freigegeben wurde. Die Produktflußmatrix zeigt außerdem in welcher Aktivität die eingehenden Produkte vorher bearbeitet wurden und in welcher Aktivität diese weiter bearbeitet werden.

## 4.5 Tailoring

Das Vorgehensmodell zeichnet sich durch Allgemeingültigkeit aus. Für den Einsatz in konkreten Projekten ist eine Anpassung nötig um einerseits nicht zuviel unnötige Dokumente zu erzeugen, andererseits aber keine wichtigen Dokumente zu vergessen. Diese projektspezifische Anpassung wird *Tailoring* genannt. Das V-Modell regelt die Vorgehensweise hierfür im Handbuch *Tailoring und projektspezifisches V-Modell*. Es sind zwei Stufen vorgesehen:

1. *Ausschreibungsrelevantes Tailoring*

wird zu Beginn des Projekts durchgeführt. Man wählt die benötigten Aktivitäten und Produkte für das Produkt und streicht diejenigen, die nicht benötigt werden. Die festgelegte Teilmenge des Vorgehensmodells wird im Projekthandbuch dokumentiert. Streichbedingungen sind im Kapitel „Übersicht“ des Projekthandbuchs aufzunehmen (mit AT markiert)

2. *Technisches Tailoring*

während des Projektverlaufs wird innerhalb der Aktivität PM4 „Feinplanung“ anhand definierter Ausführungsbedingungen kontinuierlich entschieden, welche der Aktivitäten durchzuführen sind. Um Abweichungen des Projektverlaufs gegenüber den Projektvorstellungen auszuschließen müssen die Gründe für das Weglassen bereits vorab im Kapitel „Übersicht“ eingetragen werden.

## 4.6 Handbuchsammlung

Die Dokumente der Handbuchsammlung erweitern das Vorgehensmodell für spezielle Anwendungsbereiche. Ob das jeweilige Handbuch angewendet werden muß, ist individuell vom Projekt abhängig. Folgende Themen werden aktuell behandelt:

- Erfüllung der IT-Mindestanforderungen des Bundesrechnungshofes durch das V-Modell (BRH)
- Zusammenhang zwischen Geschäftsprozessoptimierung und dem V-Modell (GPO)
- Hardwareerstellung (HW)
- Das V-Modell in einer ISO- und AQAP-Umgebung (ISO)
- Berücksichtigung objektorientierter Sprachen (OOS)

- Rollenkonzept im V-Modell (R)
- Reverse Engineering (RE)
- Anwendung des V-Modells und der ITSEC (SEC)
- Sicherheit und Kritikalität (SI)
- Szenarien (SZ)
- Tailoring und projektspezifisches V-Modell (T)
- Einordnung des V-Modells in sein Umfeld (UMF)

Im weiteren wird kurz auf das Handbuch *Kritikalität und Sicherheit (SI)* eingegangen. Für die Umsetzung der Datenschutzbestimmungen sollten zusätzlich noch die Anforderungen des Handbuchs *Anwendung des V-Modells und der ITSEC* beachtet werden.

Das Handbuch SI stellt keine zusätzlichen Anforderungen an den Entwicklungsprozeß, da dieser durch die Regelungen des V-Modells abgedeckt wird. Vielmehr werden Vorschläge für die Zuordnung der Kritikalität zu den physischen oder logischen Betrachtungseinheit vorgeschlagen. Eine konkrete Zuordnung ist immer vom Projekt abhängig. Das Handbuch SI gibt vor, daß die Kritikalität einer Betrachtungseinheit immer in Stufen ausgedrückt werden muß, deren Einstufung umso höher ist, je kritischer die Auswirkungen bei einem Fehlverhalten sind. Als Beispiel für technische Systeme wird die Einstufung in Tabelle 4.1 vorgeschlagen. Falls das System eine kritische Komponente enthält, d.h. für technische Sy-

Kritikalität	Art des Fehlverhaltens
hoch	Fehlverhalten kann zum Verlust von Menschenleben führen
mittel	Fehlverhalten kann die Gesundheit von Menschen gefährden oder zur Zerstörung von Sachgütern führen.
niedrig	Fehlverhalten kann zur Beschädigung von Sachgütern führen, ohne jedoch Menschen zu gefährden
keine	Fehlverhalten gefährdet weder die Gesundheit von Menschen noch Sachgüter

Tabelle 4.1: SSI.1: Festlegung von Kritikalität für technische Systeme (aus Handbuch SI)

steme, daß eine Gefährdung der Gesundheit für Personen oder Umwelt besteht, leiten sich zusätzliche Qualitätsanforderungen ab. Diese sind den jeweiligen Funktionen zuzuordnen. Die Festlegung wird in der *Kritikalitäten/Funktionen-Matrix* dargestellt, die jeder Funktion eine Kritikalität zuordnet. Im Verlauf der Entwicklung werden die Betrachtungseinheiten zunehmend verfeinert. Die Kritikalität vererbt sich hierbei von der höheren auf die tiefere Ebene. Würde man generell alle Funktionen der tieferen Ebene die Kritikalität der übergeordneten Ebene zuweisen, würde dies die Entwicklungskosten negativ beeinflussen. Das Ziel ist eine Minimierung der kritischen Funktionen bei unverändertem Systemverhalten. Hohe Kritikalität darf also nur dort vergeben werden, wo diese notwendig ist. Das Handbuch SI

definiert hierfür die Vererbungsregeln R 1a und R 1b. Die in Regel R 1a verwendete Formulierung „oben angeführtem Verfeinerungsprozeß“ bezieht sich auf die Funktionalitäten die sich aus der stufenweisen Zerlegung der Betrachtungseinheiten ergeben:

R 1a Produkt  $\Leftarrow$  Funktion

Mindestens eine der bei oben angeführtem Verfeinerungsprozeß aus einem Produkt erzeugten Funktionen muß eine gleich hohe Kritikalitätsstufe wie das Produkt selbst besitzen.

R 1b Funktion  $\Leftarrow$  Produkt

Bei der Zuordnung der Funktionen zu den Produkten muß mindestens ein einer Funktion zugeordnetes Produkt eine gleich hohe Kritikalitätsstufe haben wie die Funktion.

Funktionen, die voneinander abhängig sind, müssen den folgenden Regeln genügen:

R 2a Beeinflussen sich zwei Funktionen einseitig, d.h. eine Funktion nutzt Leistungen der anderen, so muß die Kritikalitätsstufe der beeinflussenden (benutzten) Funktion mindestens ebenso hoch sein wie die der nutzenden Funktion.

R 2b Beeinflussen sich zwei Funktionen gegenseitig, z. B. durch gegenseitiges Senden von Signalen, müssen beide die gleiche Kritikalitätseinstufung haben.

Regel R1 bewirkt, daß mindestens eine Funktion die Kritikalität der darüberliegenden Ebene behält, um so die Kritikalität möglichst genau zuzuordnen. Regel R2 soll die Abhängigkeiten zwischen den Funktionen minimieren um so die Sicherheit, Zuverlässigkeit und Wartbarkeit zu erhöhen.

Im Handbuch SI werden Maßnahmen zur Senkung des Risikos grob in *konstruktiv* und *analytisch* eingeteilt. Um sowohl auf Hardware als auch auf Software anwendbar zu sein, werden keine genaueren Angaben gemacht.

Abbildung 4.4 zeigt das Zusammenspiel der Submodelle SE und QS. Beim Durchlaufen der Aktivitäten SE 1 bis SE 4 werden unter Beachtung der Regeln R1 und R2 die Funktionseinheiten bestimmt, verfeinert und als Kritikalitäten/Funktionen-Matrix dargestellt. In Aktivität QS 1 werden anhand der Kritikalitätsstufen Maßnahmen (Methoden und Werkzeuge) festgeschrieben, die anzuwenden sind um möglichem Fehlverhalten entgegen zu wirken. Die Darstellung erfolgt als *Kritikalitäten/Methoden-Matrix*. Unter Verwendung der Kritikalitäten/Methoden-Matrix im QS-Plan werden

- die Konstruktionsvorgaben in eine Aufgabenplanung umgesetzt (Aktivitäten PM 1, PM 4),
- die Konstruktionsschritte durchgeführt (Aktivitäten SE 1-SE 6-SW),
- Prüfvorgaben festgeschrieben (Aktivität QS 2),
- Prüfungen durchgeführt (Aktivität QS 4),
- geprüfte Produkte integriert (Aktivitäten SE 7-SW-SE 8),
- integrierte SE-Produkte geprüft (Aktivität QS 4).





# Kapitel 5

## Umsetzung

### 5.1 Zielsetzung

Das Ziel der Arbeit war, zu untersuchen welche Produkte und Aktivitäten im Rahmen eines Zertifizierungsprozesses auszuführen bzw. zu erstellen sind, um medizinische Software in Verkehr zu bringen. Aus Sicht der Zertifizierung wird hierfür der in Kapitel 3 vorgestellt Risikomanagementprozeß definiert. Dieser wird als phasenübergreifender Prozeß während des gesamten Software-Entwicklungslebenszyklus angewandt. Weiterhin wird in [CH99] in einem Vergleich<sup>1</sup> von Wasserfall-Modell, Prototypen-Modell, Spiralmodell, Evolutions-Modell und des V-Modells, das V-Modell (Submodell SE) aufgrund seiner stark risikoorientierten Weise, als der beste Entwicklungslebenszyklus für Medizinprodukte bezeichnet. Neben der Untersuchung des Zertifizierungsprozesses soll deshalb zusätzlich untersucht werden, welche Produkte des Zertifizierungsprozesses, bei einem Vorgehen nach V-Modell (vgl. Kapitel 4) automatisch erstellt werden und welche noch zusätzlich zu erstellen sind.

Zur Durchführung des Zertifizierungsprozesses wurde ein Programm zur automatischen CTG Befundung verwendet, welches im Rahmen einer vorangegangenen Diplomarbeit (siehe [Gol00]) erstellt wurde. Kapitel 5.2 stellt den Zertifizierungsprozeß dar. In Kapitel 5.3 wird die Zuordnung der Produkte erarbeitet.

### 5.2 Das Beispielprojekt

#### 5.2.1 Das Unternehmen

Die Firma „Trium Analysis Online“ wurde 1999 von Dr. M. Daumer und Dipl. Stat. M. Scholz als Spin-Off des Instituts für Medizinische Statistik und Epidemiologie (IMSE) gegründet. Zur Zeit beschäftigt Trium 4 feste und ca. 10 freie Mitarbeiter und hat seit November 2000 die Rechtsform einer GmbH. Trium tritt neben Beratungen, insbesondere im Bereich der biometrischen Betreuung klinischer Studien und internetbasierter Schulungen eine Reihe von ASP-Produkten, die sich im Schnittbereich Medizin/IT und Statistik

---

<sup>1</sup>siehe auch <http://www.eurocat.de/de/text/entwicl.html>

befinden.

## 5.2.2 Projektbeschreibung

Projektgegenstand ist ein Programm zur automatischen CTG Befundung. CTG steht für **C**ardio **T**oko **G**ramm und stellt heute das am häufigsten eingesetzte Verfahren zur Überwachung der Schwangerschaft und der Geburt dar. Die drei zentralen Module „Datenaufnahme“, „Datenverarbeitung“ und „Visualisierung“ bilden das sogenannte „Monitoring System“. Abbildung 5.1 zeigt den schematischen Aufbau inklusive der Schnittstellen. Das

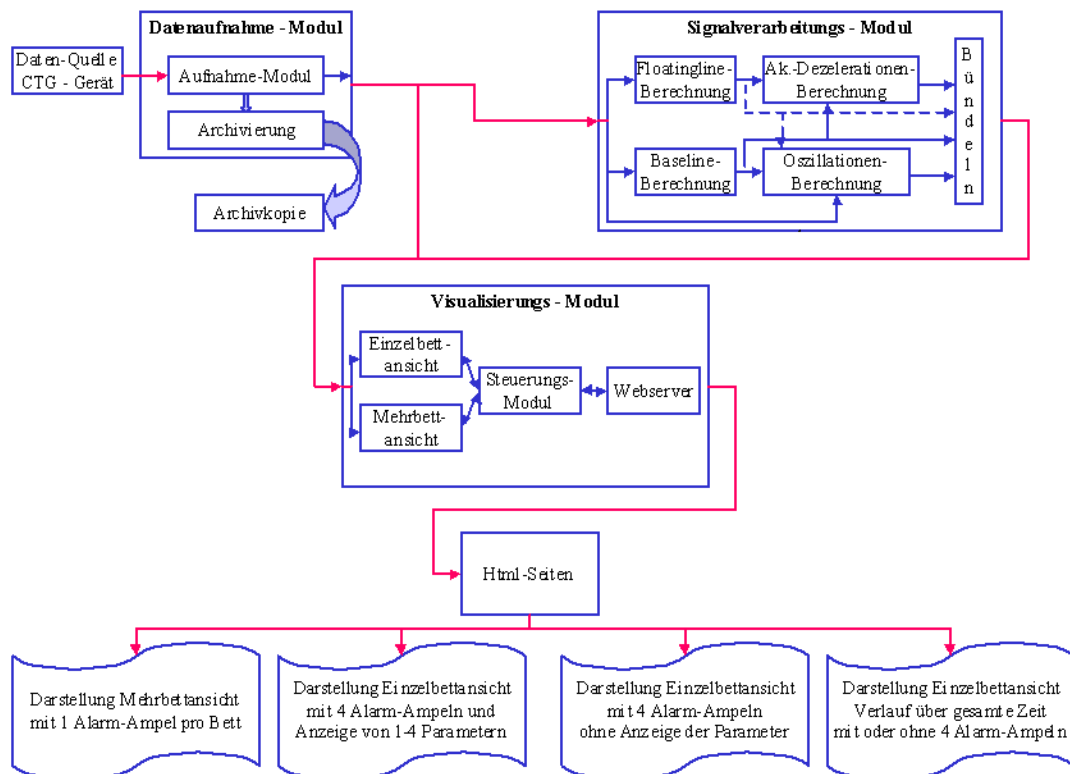


Abbildung 5.1: Schematische Architekturübersicht

„Datenaufnahmemodul“ legt den aktuellen Status fest (z.B. Bett X belegt) und übergibt die neu erfassten Daten an die nachgeschalteten Module. Das „Datenverarbeitungsmodul“ berechnet die zentralen Werte und erstellt aus diesen eine Klassifizierung des Zustandes („normal“, „suspekt“, „pathologisch“) der Patientin. Erfasste und berechnete Werte können im „Visualisierungsmodul“ angezeigt werden. Über eine Schnittstelle zum Inter/Intranet können entweder ein einzelnes oder alle Betten gemeinsam, von verschiedenen Rechnern eingesehen werden.

### 5.2.3 Ausgangssituation

Den Start der Arbeit stellte eine CD mit der aktuellsten Version des Programms und eine Kopie der Diplomarbeit dar. Das Programm wurde auf einem Rechner installiert und zum Kennenlernen durchprobiert. Hierfür konnte ein spezieller Demomodus aufgerufen werden, der bereits durchgeführte Aufzeichnungen kontinuierlich in das CTG System einspeist. In diesem Modus führt das System alle Berechnungen für die Klassifizierung durch. Das Datenaufnahmemodul wird damit allerdings nicht benutzt. Eine Analyse der Virtuellen Instrumente (VI)<sup>2</sup> zeigt, dass von den ca. 350 Funktionen nur die „top level“ VIs über die vorgesehenen Dokumentationsschnittstelle „VI Info“ dokumentiert waren.

Als weiteres Problem stellte sich heraus, daß drei der Kernberechnungsfunktionen paßwortgeschützt waren und das Paßwort mit dem Ausscheiden des Diplomanden ebenfalls ausschied. Während ich versuchte mich in das Thema mittels der Diplomarbeit einzuarbeiten, konnte ein Kontakt zu dem ehemaligen Diplomanden hergestellt werden, mit dessen Hilfe es gelang, verschiedene Versionen der Funktionen ohne Paßwortschutz zu finden.

Als Konsequenz hieraus wurde ein Versionsverwaltungstool installiert, das es ermöglicht, mehrere Versionen eines Programms zu verwalten. Das Programm ermöglicht zusätzlich Zugriffskontrollen, so daß beispielsweise Benutzer der Qualitätssicherung lesend auf das Repository zugreifen können, während Benutzer der Entwicklungsabteilung sowohl schreibend als auch lesend darauf zugreifen können. Darüber hinaus hilft das Tool, falls mehrere Entwickler parallel an derselben Funktion arbeiten und diese nach getaner Arbeit in das Repository einspielen möchten, indem es das Überschreiben neuerer Versionen, die zwischenzeitlich eingefügt wurden, durch ältere verhindert.

Um einen Überblick über alle anfallenden Prozesse und Anforderungen für die Zertifizierung medizinischer Software zu bekommen, wurde mir vorab eine eintägige Schulung beim TÜV Süddeutschland zum Thema „CE Zertifizierung medizinisch genutzter Software“ ermöglicht. Der überwiegende Teil der Teilnehmer arbeitete in kleinen oder mittelständischen Betrieben und hatte eine akademische Ausbildung. Interessant war, daß keiner der Teilnehmer Informatiker war oder eine vergleichbare Ausbildung hatte. Der Kursleiter selbst ist promovierter Elektrotechniker und führte neben den Schulungen auch Audits bei Kunden durch. Der Schwerpunkt liegt hier allerdings in der Abnahme eines QS-Systems nach ISO 9000.

Für die Zertifizierung wurden von verschiedenen benannten Stellen Angebote eingeholt. Nach einer Beurteilung wurde die Firma EUROCAT beauftragt. Da es aus gesetzlichen Gründen benannten Stellen nicht erlaubt ist, Zertifizierungen und Beratungen desselben Projektes zugleich durchzuführen, stand mir begleitend zur Arbeit ein Berater der Tochterfirma zur Seite. Dieser kontrollierte die von mir erstellten Produkte auf Konformität mit den Anforderungen der Norm EN60601-1-4 und stellte die Ergebnisse in Checklisten dar, die die Anforderungen widerspiegeln. Der Berater konnte zudem zusätzliche Aspekte in das Projekt einbringen. Zu Projektbeginn lagen die Checklisten allerdings nicht vor, so daß versucht wurde, konsequent das V-Modell anzuwenden. Das V-Modell erfüllt formal die Anforderungen der Norm EN60601-1-4. Das heißt, der Entwicklungszyklus (Submodell SE) ist in Phasen und Aufgaben eingeteilt. Der im Anhang der Norm (Abbildung 3.4) in-

---

<sup>2</sup>Der Funktionsbegriff in LabVIEW (siehe nächstes Kapitel)

formativ vorgeschlagene Entwicklungslebenszyklus gleicht im wesentlichen dem Submodell Systemerstellung.

#### 5.2.4 Vorgehensweise

Die Vorgehensweise bei der Umsetzung der Anforderungen, die letztendlich zu einer CE Kennzeichnung des Systems führt, wurde mit der Einarbeitung in die Thematik der Zertifizierung medizinischer Software und des Submodells SE des V-Modells begonnen. Mit dieser Grundlage wurde versucht, die technische und fachliche Sicht der zugrundeliegenden Software wieder zu gewinnen. Begleitend zu dieser Tätigkeit wurden die einzelnen Funktionen (VIs) dokumentiert und Anforderungen an das Programm abgeleitet und soweit ersichtlich gefährdungsmindernde Maßnahmen implementiert. Ziel war es, eine vollständige konsistente Dokumentation des Submodells SE zu erstellen, welches als Entwicklungslebenszyklus eingesetzt wurde.

Obwohl es sich hier um eine Reverse Engineering Aufgabe handelt, wurden die Produkte wie bei einer normalen Systemerstellung erstellt. Dies resultierte zum einen daraus, daß mir das Handbuch „Reverse Engineering“ zu diesem Zeitpunkt nicht bekannt war und zum anderen, daß die Systementwicklung parallel zum Zertifizierungsprozeß ablaufen sollte und nicht nachträglich.

Der im folgenden verwendete Begriff „Produkt“ bezieht sich, falls nicht anders vermerkt, auf die erstellten Dokumente und das Programm. Der Begriff „Dokumente“ steht allgemein für die Zertifizierung zu erstellenden Dokumente. Falls ein spezielles Produkt des V-Modells gemeint ist, wird dieses durch die Abkürzung des Standards verdeutlicht. Diese sind immer aus einer abkürzenden Produktbezeichnung, gefolgt von einem „-“ Zeichen und falls auf eine Untergliederung eingegangen wird, entsprechenden Unterpunkten gekennzeichnet (z.B. „Afo\_2“ für das Produkt Anwenderforderung „Ist-Aufnahme und Ist-Analyse“). Analog werden spezielle Aktivitäten des „V-Modell“ Standards durch deren Bezeichnung (z.B. SE 1.1 für „Ist-Aufnahme/Analyse durchführen“) verwendet.

In einem Kick-Off Meeting wurde gemeinsam mit dem Projektbetreuer der Beratungsfirma der Projektverlauf festgelegt. Insbesondere wurde festgelegt, welche Aktivitäten für die Zertifizierung durchgeführt werden müssen und welche Dokumente hierfür zu erstellen sind.

Von Seiten des Beraters wurde vorgeschlagen, das V-Modell in einer mittels Tailoring an Anhang DDD (siehe Abbildung 3.4) angelehnte Form zu verwenden und die Produkte der Phasen 1 zur Anforderungsspezifikation und die der Phasen 2, 3 und 4 zur Designspezifikation zusammenzufassen. Die Beschreibung des Modells wurde im Software-Qualitätsmanagementplan festgeschrieben. Abbildung 5.2 gibt einen Überblick über die zu erstellenden Dokumente und den Produktfluß. Die Abbildung zeigt auf der linken Seite die Dokumente der Systemerstellung, während auf der rechten Seite (in geschweifter Darstellung) die phasenübergreifenden Dokumente aufgezeigt sind. Der Produktfluß wird durch die hellgrauen Linien dargestellt, schwarze Linien und mit einem „R“ beschrifteten Rauten stehen für Reviews. Das folgende Kapitel stellt die Dokumente im einzelnen vor. Der Inhalt der Dokumente ergibt sich aus den Anforderungen der Norm EN60601-1-4, welche von der Zer-



Der Datenaustausch wurde über eine Kommunikationsplattform (BSCW<sup>3</sup>) durchgeführt. Die Ergebnisse wurden in Checklisten eingetragen und bei Bedarf mit Kommentaren zur Überarbeitung zurückgeschickt. Es ist hierbei hervorzuheben, daß die Aktivitäten, deren Durchführung letztendlich die Dokumente und das zertifizierungsreife System erzeugen, nicht durch die Norm festgelegt werden (diese stellt nur Anforderungen an Prozeß und Dokumente). Für den Systemerstellungsprozeß wurden die Aktivitäten des Submodells SE (V-Modell) verwendet, für den parallel dazu laufenden Risikomanagementprozeß wurde zusammen mit der Beraterfirma das methodische Vorgehen festgelegt.

### 5.2.5 Projektdurchführung

Dieser Abschnitt stellt die während der Umsetzung erarbeiteten Produkte des Zertifizierungsprozesses dar.

Für die im weiteren vorgestellten Dokumente gilt, daß deren Untergliederung nicht immer strikt bindend der Zuordnung zu einem Dokument sein muß. Zitat des Beraters: „Entscheidend ist, ob die abgeprüften Inhalte erfüllt werden, nicht ob diese im richtigen Dokument stehen“. Als weiteres Vorgehen werden die einzelnen Punkte der Checkliste (diese werden entweder der Reihenfolge ihres Auftretens durchgesprochen oder in Klammern („..“) angefügt) soweit erklärt, daß eine Zuordnung zu den (Teil-) Produkten des V-Modells im nächsten Kapitel möglich ist. Es soll dann auch gezeigt werden, welche Anforderungen der Checkliste automatisch erfüllt und welche für die Zertifizierung zusätzlich zu erstellen sind – bei Anwendung des V-Modells als Vorgehensmodell.

Für alle Dokumente ist ein Deckblatt, ein Inhaltsverzeichnis und ein Änderungsübersicht zu erstellen. Das Deckblatt enthält mindestens folgende Angaben<sup>4</sup>:

- Produktbezeichnung und -identifikation
- Projektidentifikation
- Version
- Ort und Datum der Erstellung und letzte Änderung
- Ersteller
- Datum und verantwortliche Person der Prüfung und Freigabe

Im folgenden werden die aus dem Zertifizierungsprozeß resultierenden Dokumente erläutert.

1. Software-Qualitätsmanagement-Plan
2. Zweckbestimmung, Klassifizierung
3. Konfigurationsmanagement

---

<sup>3</sup>Basic Support for Cooperative Work - siehe <http://bscw.gmd.de/>

<sup>4</sup>vgl. V-Modell Regelungsteil Produktmuster, Gliederungspunkt Allgemeines

4. Anforderungsspezifikation
5. Designspezifikation
6. Testpläne und Testreports
7. Risikomanagement-Plan
8. Risikoanalyse-Plan
9. Risikoanalyse-Report
10. Risikomanagement Report

#### 5.2.5.1 Software-Qualitätsmanagement-Plan

Wie bereits erwähnt wurde zu Beginn des Projekts ein Kick-Off Meeting abgehalten. Ziel dieses Meetings war, die konzeptuelle Vorgehensweise zu planen. Der Software-Qualitätsmanagement-Plan - im weiteren SQMP genannt - stellt den Großteil dieser Ergebnis dar, wodurch dieses Dokument als Projekthandbuch (nach V-Modell) zu sehen ist. Der SQMP enthält folgende Festlegung:

- einen Projektüberblick
- Festlegungen zur Kennzeichnung des Produktes
- Angaben über Entwicklungsvorgaben
- Festlegungen bzgl. Verantwortlichkeiten und projektspezifischem Entwicklungslebenszyklus
- eine Liste der zu erstellenden Dokumente.

Der Projektüberblick besteht aus der Angabe von

- Hersteller und Vertrieb,
- Zweckbestimmung und
- Entwicklungsvorgaben bzw. Anwendungsbereiche der Software.

Der Punkt „Hersteller und Vertrieb“ resultiert aus der Kennzeichnungspflicht (siehe Kapitel 2.1 auf Seite 9) für Medizinprodukte. Die Zweckbestimmung stellt eine Allgemeine Produktbeschreibung dar (vgl. Kapitel 3.1.1 bzw. 5.2.5.2), deren Gliederungspunkte den genauen Verwendungszweck des Systems festlegen. Aus Sicht der Softwareentwicklung müssen zusätzliche Entwicklungsvorgaben und Anwendungsbereiche beschrieben werden (z.B. Das System x soll auf Windows NT laufen)

Die weiteren Punkte entsprechen organisatorischen Festlegungen. Vorab werden die Hauptverantwortlichkeiten getroffen, d.h. daß allen Funktionen (z.B. Projektleiter, Entwickler ..)

im Projekt die entsprechenden Personen zugeordnet werden, wobei auf die Unabhängigkeit von Qualitätssicherung und Entwicklung zu achten ist. Die Personalqualifikationen und ein Verfahren zur Nachweisregelung sind zu beschreiben („Personalqualifikation Schulungsnachweise ..“).

Als weiterer Schritt ist der Entwicklungslebenszyklus zu definieren. In unserem Fall wurde der Entwicklungslebenszyklus aus EN60601-1-4 Anhang DDD angewendet. Bei der Festlegung und Beschreibung der Phasen wird nach Einzelphasen und phasenübergreifenden Maßnahmen unterschieden. Als Einzelphase wurde die Anforderungs- Design- Verifikations- und Validierungsphase festgelegt und phasenübergreifend die Risikoanalyse, das Konfigurationsmanagement, die Validierung der risikomindernden Maßnahmen und Reviews während der Phasenübergänge. Die Gliederungstiefe ist von der Komplexität des Projektes abhängig. Zusätzlich muß festgelegt werden, wie die einzelnen Phasen ineinander greifen (z.B. ob die Anforderungsspezifikation „freigegeben“ sein muß bevor mit der Designphase begonnen werden kann). Die durchgeführten Tailoringmaßnahmen sind zu beschreiben. Anschließend werden die zu entwickelnden Dokumente definiert und festgelegt, wer deren Erstellung und Freigabe vornimmt.

Die Dokumente „traceability of requirements“ und „traceability of safety requirements“ stellen die Bezüge zwischen den Anforderungen, deren Design und den Verifizierungs- und Validierungsmaßnahmen her. Das Dokument „traceability of safety requirements“ enthält hierbei nur die risikobezogenen Funktionen, die sich aus der Risikoanalyse ergeben. Zusätzlich werden noch die Bewertungen vor und nach der Umsetzung gefährdungsmindernder Maßnahmen angegeben. Die traceability Dokumente stellen eine Anforderung von Seiten der FDA dar.

Für die „Liste der Dokumente“ sind sowohl projektinterne als auch produktbegleitende (z.B. eine Gebrauchsanweisung, Verpackung, Werbung ..) Dokumente zu betrachten („Erstellung und Prüfung produktbegleitender Dokumente“).

### 5.2.5.2 Zweckbestimmung und Klassifizierung

Für die Zertifizierung müssen entsprechend der Anforderungen des MPG eine Zweckbestimmung verfaßt und eine Klassifizierung durchgeführt werden. Sowohl Zweckbestimmung als auch Klassifizierung werden in Kapitel 3 besprochen. Die Gliederung der Zweckbestimmung wurde direkt Abbildung 3.1 entnommen, umgesetzt und in den Software-Qualitätsmanagement-Plan eingebunden<sup>5</sup>.

Die Klassifizierung des Medizinproduktes erfolgte anhand MDD<sup>6</sup> Anhang IX. Die Definitionen der Klassifizierungsregeln (Anwendungsdauer, aktiv/passiv, ..) wurden bereits in der Zweckbestimmung festgelegt und konnten hier direkt übernommen werden. Da es sich um ein aktives nicht-invasives Medizinprodukt handelt, können die Regeln für invasive Produkte (5-8) ebenso wie die für besondere Produkte (13-18) außer Betracht gelassen werden. Tabelle 5.1 zeigt die aus Anhang IX Abschnitt III angewandten Regeln. Das Me-

---

<sup>5</sup>Anmerkung: Für die Klassifizierung gibt es keine Checkliste. Klassifizierung und Zweckbestimmung werden dem technischen File beigelegt

<sup>6</sup>93/42/EWG – Medical Device Directive, MDD. Siehe Kapitel 3

dizinprodukt entspricht Risikoklasse IIb, da immer die Regel mit der höchsten Risikoklasse klassifiziert wird.

Regel	anwendbar?	Risikoklasse
Regel 1	trifft zu	I
Regel 2	trifft nicht zu	
Regel 3	trifft nicht zu	
Regel 4	trifft nicht zu	
Regel 9	trifft nicht zu	
Regel 10	trifft zu	IIb
Regel 11	trifft nicht zu	
Regel 12 (Rückfallregel)	trifft zu	I

Tabelle 5.1: Klassifizierung

Wie in Kapitel 3.1.3 beschrieben, bieten sich für Medizinprodukte der Risikoklasse IIb zwei alternative Wege der Konformitätsbewertung: zum einen kann der Hersteller ein eigenes Qualitätssicherungssystem nach ISO 9001 implementieren (nach MDD Anhang II) und zum anderen kann eine Baumusterprüfung (nach MDD Anhang III) zur Überwachung der Entwicklung in Kombination mit einem der Anhänge IV, V oder VI zur Überwachung der Produktion durchgeführt werden.

Im Rahmen der Angebotsbewertung der Beraterfirmen wurden beide Wege (von unterschiedlichen Firmen) vorgeschlagen. Letztendlich wurde das Konformitätsbewertungsverfahren nach Anhang III und IV - also die Baumusterprüfung in Kombination mit einer EG Prüfung („Produkt Tests“) ausgewählt. Die Umsetzung bezieht sich auf die Produkterstellung, für die Produktion (EG Prüfung) gilt das in Kapitel 3.1.3 gesagte.

### 5.2.5.3 Konfigurationsmanagement

Das Konfigurationsmanagement verwaltet die projektbezogenen Versionen und regelt die Fehler- und Änderungsverwaltung. Der Konfigurationsmanagement-Plan - im weiteren KM-Plan genannt - legt die Rahmenbedingungen für das Konfigurationsmanagement fest. Im folgenden werden die Festlegungen beschrieben, die im Rahmen des KM-Plans zu treffen sind. Für die Umsetzung des Konfigurationsmanagements wurde eine toolgestützte Lösung auf Basis des Open Source Werkzeugs CVS implementiert. Der KM-Plan entspricht dem gleichnamigen Dokument im V-Modell.

Der KM-Plan legt als phasenübergreifendes Dokument zuerst die Verantwortlichkeiten für die Tätigkeiten fest, die im Rahmen des Konfigurationsmanagements durchzuführen sind (z.B. Versionsverwaltung der Konfigurationselemente, Archivierung, Datensicherung oder Zugriffskontrollen). Weiterhin sind alle Elemente, die dem Konfigurationsmanagement unterliegen und der Zeitpunkt, ab wann mit dem Konfigurationsmanagement begonnen wird (z.B. nach Freigabe der Anforderungsspezifikation) festzulegen.

Den Konfigurationselementen werden Identifikatoren zugeordnet („Identifizierbarkeit jedes

SW-Elements“) um diese eindeutig identifizieren zu können. Es muß festgelegt werden, wie dieser Identifikator bzgl. Struktur und Informationen aufgebaut ist, welche Methodik („Angabe der Versionsfolge“) bei Durchführung einer Änderung angewandt wird und welche Entwicklungsumgebung („Angaben zur versionsbezogenen Entwicklungsumgebung“) hierfür verwendet wurde (z.B. Werkzeuge, Hilfsmittel). Der Status (z.B. freigegeben, in Bearbeitung ..) jedes Konfigurationselements muß eindeutig erkennbar sein. Hierfür müssen die möglichen Statuszustände definiert werden und zusätzlich beschrieben werden, wer in welchen Zuständen auf Konfigurationselemente zugreifen darf.

Zudem müssen Regelungen zur Durchführung von Änderungen getroffen werden. Es muß geregelt werden, wie Änderungsanträgen bzw. Fehlermeldungen zu erfassen und verfolgen sind, wobei insbesondere geregelt werden muß, wer nach erfolgter Zertifizierung welche Änderungen machen darf. Wie in Kapitel 3.1.3 beschrieben, gilt prinzipiell, daß keine Änderungen am Funktionsumfang ohne erneutes Konformitätsbewertungsverfahren vorgenommen werden dürfen. Darüber hinaus muß berücksichtigt werden, daß eine Fehlermeldung bezüglich Funktionen, die Einfluß auf die Gefährdungsanalyse haben, eine Sperre des Produktes nach sich ziehen kann, falls die Fehlermeldung im Rahmen eines Vorkommnisses oder Beinahevorkommnisses aufgetreten ist. Zusätzlich muß eine Meldung an die zuständige Behörde gemacht werden (siehe Abschnitt „Anzeigepflicht“ in Kapitel 2.1).

Hierfür ist ein Auswahlverfahren (z.B. falls der Fehler keine Gefährdung auslöst, dann ..) und der Weg der Änderungen vom Änderungsantrag bis zur Änderungsmitteilung und anschließender Freigabe zu definieren. Weiterhin muß festgelegt werden, wer über die Art und Umsetzung von Korrekturen entscheidet, ebenso wie ein Verfahren zur Dokumentation („Verfahren zur Verwaltung von Änderungen und Fehlermeldungen nach dem Designfreeze“ und „Änderungs-Spezifikation“). Es ist ein Analyseverfahren zur Untersuchung der Auswirkungen der Änderungen auf das Gesamtprojekt zu beschreiben. Weiterhin muß eine Liste gepflegt werden, die ungelöste Fehler und deren Risikobewertung und falls möglich einen Bearbeitungszeitraum angibt.

Die Vorgehensweise zur Sicherung und Archivierung älterer Versionen wird festgelegt („Datensicherung / Datenverwaltung / Katalogisierung“). Die Identifikation und Rekonstruktion muß festgelegt sein, daß es auch über Versionswechsel hinweg möglich ist, Versionen inkl. Umgebungsbedingungen wiederherzustellen („Ältere Versionen archivieren bzw. reproduzieren“).

Unter dem Punkt „KMP - Review durchgeführt“ werden Reviewmaßnahmen für das Konfigurationsmanagement festgelegt.

#### **5.2.5.4 Testkonzept**

Dieses Dokument legt ein projektweit gültiges Konzept für die Durchführung qualitätssichernder Maßnahmen fest. Das Testkonzept beschreibt rein analytische Maßnahmen. Konstruktive Maßnahmen zur Vermeidung von Mängeln und der Sicherstellung einer Prozeßqualität werden im Software-Qualitätsmanagement-Plan definiert. Das Testkonzept basiert in seinen Festlegungen auf den im SQMP festgelegten Phasen. Hier soll nun definiert werden, in welcher Phase welche Tests von wem und mit welchen Mitteln durchgeführt werden. Das Testkonzept stellt weiter die Grundlage für die im Projektverlauf zu erstellenden

Testpläne. Die Testpläne wiederum werden nach Erstellung auf Konsistenz mit dem Testkonzept reviewed (vgl. Abbildung 5.2). Aus Sicht des V-Modells stellt dieses Dokument eine Mischung aus QS-Plan und Prüfspezifikation dar.

Im folgenden werden die Elemente dieses Dokumentes erklärt: vorab werden die Verantwortlichkeiten für das Testkonzept festgelegt. Im Beispielprojekt wurden hierfür die Verantwortlichkeiten für die Tätigkeiten „Erstellung der Testpläne“, „Durchführung Unit-, Integrations- und Systemtests“, „Durchführung Akzeptanztests“, „Durchführung Belastungstests“ und „Schreiben eines Prüfreports“ definiert.

Für die spezifizierten Tests sind Ziele zu beschreiben (siehe Spalte „Ziel“ in Tabelle 5.2.5.4).

Es sind detaillierte Testmethoden (z.B. Modultests, white-box, grey-box, black-box Tests) in Abhängigkeit der Phasen des Entwicklungslebenszyklus und Implementierungstiefe festzulegen (vgl. Kritikalitäten/Methoden-Matrix in Kapitel 4.6).

Test	Ziel	Testumgebung	Testmethode	Durchführung
Unittests	Überprüfung, ob Komponente die gewünschte Funktionalität erfüllt	Entwicklungsumgebung	Walkthrough	Entwickler
..	..	..	..	..

Tabelle 5.2: Definition von Tests, Testumgebung, Testmethode und Durchführung

Für die jeweiligen Testkriterien sind erwartete Ergebnisse (Testabbruch, Testwiederholung, Akzeptanzbereich) zu definieren (z.B. „Treten während der Tests Fehler bei Funktionen mit Kritischer Einstufung auf, führt dies zu einem Testabbruch. Die Tests werden nach Behebung wiederholt“).

Die Testumgebung ist zu definieren (siehe Spalte „Testumgebung“ in Tabelle 5.2.5.4). Es muß festgelegt werden, ob das Testkonzept einem Review zu unterziehen ist (nachdem ein Testplan erstellt wurde, muß reviewed werden, ob die Festlegungen der Testspezifikation eingehalten werden). Es kann außerdem festgelegt werden, was im Falle von unerwarteten Ergebnissen bzw. wie bei Auftreten neuer Risiken vorzugehen ist.

### 5.2.5.5 Anforderungsspezifikation

Die Norm EN60601-1-4 legt als Anforderungen fest, daß für jedes Teilsystem eines Medizinproduktes eine Anforderungsspezifikation zu erstellen ist. Diese muß minimal die risikobezogenen Funktionen detailliert beschreiben. Die Norm weist insbesondere auf Funktionen zur Beherrschung von Risiken hin, die durch<sup>7</sup>:

- Umgebungsbedingungen

---

<sup>7</sup>aus EN60601-1-4 Punkt 52.206.2

- sonstige Ursachen innerhalb des Systems
- mögliche Fehlfunktionen

hervorgerufen werden. Für diese Anforderungen müssen Angaben bzgl. der Zuverlässigkeit der Risikobeherrschung gemacht werden.

Von Seiten der Zertifizierungsstelle werden hierfür die im weiteren beschriebenen Kriterien geprüft, deren Umsetzung zugleich den Inhalt der Anforderungsspezifikation stellt. Die formulierten Anforderungen haben den formalen Anforderungen auf „Eindeutigkeit“, „Prüfbarkeit“ und „Realisierungsfreiheit“ zu genügen.

„Ersteller, Ausgabedatum, (Version) und Freigabe“: Dieser Punkt bezieht sich auf das zu erstellende Deckblatt, welches bereits in der Einleitung dieses Kapitels beschrieben.

„Allgemeine Beschreibung/Programmvorgaben“: In diesem Abschnitt soll kurz die Ausgangssituation und die Zielsetzung beschrieben werden. Es ist hervorzuheben, daß sich aus der Aktivität, die diesen Teilaspekt erzeugt, insbesondere Gefährdungen ableiten lassen sollten, die sich aus dem System „Soll“-Zustand gegenüber dem „Ist“-Zustand ergeben. Beispielsweise mußte im Beispielprojekt die örtliche Trennung, die sich durch den Einsatz der Internet-Technologie ergibt, berücksichtigt werden.

„Beschreibung DV-Systemumgebung“: Als Systemumgebungen werden Hardwareanforderungen und Randbedingungen angegeben (z.B. Das Gerät xy muß unterstützt werden).

„Ein-/Beschränkungen der HW/SW“: Unterliegt das Produkt vorab irgendwelchen Einschränkungen, sind diese in diesem Punkt zu beschreiben (z.B. wurde im Beispielprojekt eine „WAP<sup>8</sup> Unterstützung“ ausgeschlossen, obwohl ein Einsatz durchaus denkbar wäre). Im Fokus steht hier die Minimierung der zu Untersuchenden Gefährdungen in der Risikoanalyse.

„Betriebssysteme, Programmiersprachen, Entwicklungsumgebung (z.B. CASE - Tools)“: Diese Punkte legen die Forderung nach den Umgebungsbedingungen der Norm fest. Es ist festzulegen, auf welchem Betriebssystem die Anwendung laufen soll und welche Programmiersprachen bzw. Entwicklungsumgebungen für die Erstellung eingesetzt werden.

„Vernetzung“: Bei der Umsetzung dieses Punktes, werden Angaben bezüglich der verwendeten Protokolle, der Datensicherheit (Safty und Security) und der minimalen Anforderungen beschrieben (z.B. es muß mindestens eine Bandbreite von 9600bps gewährleistet sein)

Die „Liste der gewünschten/ungewünschten Funktionen und Eigenschaften“ beschreibt die Funktionalitäten des Systems.

„Benutzerschnittstellen Sprache, (Bildschirm-) Ein- Ausgabemasken, Kommandos, Tastaturbefehle, Druckerausgaben, E/A Geräte“: hier werden Eingabemasken, Fenster und Dialogabläufe für Softwareschnittstellen und Bedienelemente und die Parametrisierung der Werteeingabe bei Hardwareschnittstellen beschrieben.

„Sonstige Schnittstellen (zu anderen Systemen)“: spezifiziert die technischen Anforderungen für die Schnittstellen zu anderen Systemen.

---

<sup>8</sup>Wireless Application Protocoll

„Validierung von Fremdsoftware (OTS, etc.)“: Für die Umsetzung dieses Punktes wird eine Liste der verwendeten Software von Drittherstellern „Off-The-Shelf (OTS)“ zusammengestellt<sup>9</sup>. Für den Einsatz sollte vorab eine Prüfung auf Tauglichkeit erfolgen. Diese Maßnahmen sind im Rahmen qualitätssichernder Maßnahmen durchzuführen (z.B. ist Dokumentation ausreichend, Zuverlässigkeit gewährleistet ..).

„Gefährdungsmindernde Anforderungen (aus der Risikoanalyse)“: Wie bereits in Kapitel 3.1.5 erläutert, wird während des gesamten Entwicklungslebenszyklus eine Risikoanalyse durchgeführt. Dieser Punkt ist als Ergebnis dieser Analyse zu verstehen, d.h. falls während der Analyse Risiken entdeckt werden, deren Risikobeherrschungsmaßnahmen neue Anforderungen erzeugen, sind diese hier einzupflegen<sup>10</sup>. Beispielsweise wurde im Beispielprojekt eine Gefährdung aufgrund der Übertragung über Netzwerk erkannt, wobei zum einen die Daten im Klartext übertragen wurden und zum anderen der Benutzer die Authentizität des Servers nicht überprüfen konnte. Als gefährdungsmindernde Maßnahme wird die Datenübertragungstrecke durch eine Verschlüsselung und eine Serverauthentifizierung gesichert. Als Anforderung wurde „Verschlüsselung“ und „Serverauthentifizierung“ mit aufgenommen.

„Fehlermeldungen“: Dieser Punkt stellt die Umsetzung der Anforderung der EN60601-1-4 „mögliche Fehlfunktionen“ zur Beherrschung von Risiken zu beinhalten. Es muß eine Liste der Fehlermeldungen bereitgestellt werden, die darüber hinaus in die Gebrauchsanweisung mit einfließt.

„Qualifikationsvorgaben für den Anwender“: Weiterhin muß beschrieben werden, welche Qualifikationsvorgaben die Benutzer haben müssen. Aus dieser Anforderung entscheidet sich unter anderem, ob bei Systemauslieferung eine Schulung des Personals durchgeführt werden muß oder nicht.

„Datenmodelle, Datenschutz, Datensicherheit“: In diesem Punkt werden die globalen Datenmodelle<sup>11</sup> vorgestellt und Anforderungen bezüglich des Datenschutzes (z.B. es werden nur Initialen gespeichert .. ) und der Datensicherheit definiert (z.B. Restartsituation).

„Vorschriften (spezielle Normen oder Anforderungen)“: Werden neben der EN60601-1-4 noch weitere Normen oder Vorschriften angewendet, sind diese hier aufzuführen. Im Beispielprojekt mußte eine Richtlinie zur Klassifizierung von CTGs angegeben werden.

Der Punkt „Review - Plan / Report“ meint, daß die Anforderungsspezifikation gegebenenfalls einem Review unterzogen werden muß (Rückkopplung zum Auftraggeber (AG)), um festzustellen, daß alle Anforderungen seitens des Kunden, der normativen Gegebenheiten etc. enthalten sind, bevor die Anforderungsspezifikation freigegeben und daraus eine Designspezifikation abgeleitet wird.

Durch die Umsetzung des Unterpunktes „SW-Strukturvorgabe/Ablaufdiagramm“ wird die technische Struktur des Systems vorgestellt. Neben dem Aufbau des Systems werden auch die Schnittstellen zwischen den Elementen und nach außen definiert.

---

<sup>9</sup>vgl. Kapitel 3.2.2

<sup>10</sup>Anmerkung: In Abbildung 5.2 wird dieser Punkt als separates Dokument gezeigt.

<sup>11</sup>Für eine FDA-Zulassung muß zusätzlich der Kontext der Datenmodelle angegeben werden (vgl. Kapitel 3.2.1)

Aus Sicht des V-Modells fließen Teile der Produkte „Anwenderforderung“, „System-Architektur“, „technische Anforderungen“ und „Schnittstellenübersicht“ in dieses Dokument ein. Die Zuordnung wird im Kapitel 5.3.4 vorgestellt.

#### 5.2.5.6 Designspezifikation

Die Designspezifikation ist das Produkt, der Aktivitäten der Design- und Implementierungsphase (nach SQMP). In der Designphase werden die SW-Architektur und Strukturvorgaben der Anforderungsspezifikation verfeinert und in ein Design (SW-Entwurf nach V-Modell) umgesetzt und implementiert. Das Design sollte soweit in Komponenten zerlegt werden, daß der Programmierer keine „ad-hoc“ Entscheidungen zu treffen hat (vgl. Kapitel 3.2.1). Der Schwerpunkt der Designspezifikation liegt – unter Beachtung der regulatorischen Anforderungen seitens der Normen und Guidelines – in der Dokumentation der Funktionen, von denen eine Gefährdung ausgeht („Umsetzung der SW-Architektur/Struktur aus der Anforderungsanalyse“).

Sollte von Seiten des Unternehmens Strukturvorgaben für die Codierung („Style Guides“) existieren, werden in dieser Phase auch Anforderungen an die „Art“ wie programmiert wird festgelegt<sup>12</sup> („Einhaltung gegebener Strukturvorgaben bei der Codierung“). Die Einhaltung von Strukturvorgaben wird im Rahmen der Zertifizierung geprüft.

#### 5.2.5.7 Testpläne und Testreports

Während der Verfeinerung werden für die neu gefundenen Einheiten die Testgegenstände festgelegt und in den Testplan eingetragen. Deshalb werden in der Checkliste „Design - Phase“ auch die Punkte „Testvorgaben, erwartete Ergebnisse, Testziele“, „Angaben zur Testumgebung“ und Punkte für den „Unit- Integrations- und Systemtest- Plan bzw. Report“ angeführt. Die Testpläne legen Verantwortlichkeiten, Testgegenstände, Umfang und zeitliches Vorgehen der Testaktivitäten fest. Zur Umsetzung des Testplans auf einen speziellen Testfall wird eine Testspezifikation erstellt. Diese enthält Angaben über die Testumgebung, Testvorgaben und erwartete Ergebnisse und Testziele. Es ist hervorzuheben, daß die Freigabe der Testpläne und -spezifikationen vor der eigentlichen Durchführung erfolgen muß.

Die Durchführung der Tests sind Teil der Verifizierungsphase. Treten bei der Durchführung von Tests Fehler auf, sind diese in einem Fehlerbericht zu dokumentieren<sup>13</sup>. Das Ergebnis wird in einem Testbericht (Report) festgehalten. Werden die Testkriterien des Testkonzeptes nicht eingehalten sind zusätzliche Maßnahmen durchzuführen. Das Vorgehen entspricht den QS-Aktivitäten des V-Modells.

---

<sup>12</sup>aus [CH99] Seite 15

<sup>13</sup>vgl. [CH99] Seite 17

### 5.2.5.8 Risikomanagement-Plan

Der Risikomanagement-Plan ist das zentrale Dokument bei der Entwicklung medizinischer Software. Es werden sowohl die geplanten Methoden und Verfahren als auch der Zeitplan bzw. die Reihenfolge der geplanten Verifizierungen und Reviews festgelegt.

Nach Kapitel 3.1.4 enthält der Risikomanagement-Plan folgende Inhalte:

- Geltungsbereich
- anzuwendender Entwicklungslebenszyklus
- Verifizierungs-Plan
- Validierungs-Plan
- Verantwortung des Managements (nach 4.1 der ISO 9001)
- Risikomanagement-Prozeß
- Anforderungen für Reviews

Im Punkt „Geltungsbereich“ wird der Anwendungsbereich des Risiko-Management-Plans auf das Projekt festgelegt. Der Punkte „anzuwendender Entwicklungslebenszyklus“ wurde im SQMP festgelegt. Der Verifizierungs-Plan enthält eine Beschreibung aller durchzuführenden Tests aufgeschlüsselt nach den Entwicklungsphasen und wurde im Beispielprojekt als Dokument „Testkonzept“ erstellt. Der Validierungs-Plan beschreibt die geplanten Tests und Hilfsmittel für die Überprüfung des fertigen Produktes gegen die Anforderungsspezifikation und wurde ebenfalls in das Dokument „Testkonzept“ mit einbezogen. Beide Dokumente werden aus diesem Grund nicht in der Checkliste „Risikoanalyse“ geführt. Unter „Verantwortung des Managements (nach 4.1 der ISO 9001)“ werden die Verantwortlichkeiten des Managements in Bezug auf die Tätigkeiten und Dokumente der einzelnen Entwicklungsphasen festgelegt.

Der weitaus größte Teil des Risikomanagement-Plans definiert die Umsetzung des Risikomanagement-Prozesses. Die Anforderungen und das konzeptuelle Vorgehen wurden bereits in Kapitel 3.1.4 beschrieben. Die wichtigsten Festlegungen sind zum einen, daß der Risikomanagementprozeß auf den gesamten Entwicklungslebenszyklus angewendet wird und zum anderen, daß nach dem Prinzip der integrierten Sicherheit (vgl. Abbildung 3.7) immer zuerst versucht wird, das Risiko durch inhärent sicheres Design zu beherrschen. Falls das nicht möglich ist, werden Schutzmaßnahmen (z.B. Plausibilitätsprüfungen bei der Eingabe) eingeführt und erst wenn keine Schutzmaßnahmen (und damit auch keine inhärenten Lösungen) mehr implementiert werden können, dürfen Warnungen als Maßnahme zur Risikobeherrschung eingesetzt werden.

Im Beispielprojekt wurde in diesem Abschnitt zuerst eine Struktur festgelegt, die die verschiedenen Einflüsse, also die kausalen Zusammenhänge, die zu einer Gefährdung führen können, entsprechend ihrer Ursache einordnet. Anschließend wurde die Dokumentation der Risikoanalyse festgelegt, wobei für die eigentliche Durchführung ein Risikoanalyse-Plan erstellt und die Bewertung der Wirksamkeit der Maßnahmen in den Risikoanalyse-Report

eingetragen wurden. Als sehr wichtiger Punkt wurde das konzeptionelle Vorgehen bei der Risikoanalyse festgelegt. Es wurde keine formale Methode (z.B. Fehlerbaumanalyse oder FMEA) verwendet, statt dessen wurde ein eigenes Konzept definiert („Gefährdungsanalyse“).

Darüber hinaus wurden die Hauptgefährdungen, die durch den Einsatz der Software, für den Patienten, Anwender und Dritte entstehen, graphisch (als Kausalkette siehe Abbildung 3.6) aufgezeigt und Anforderungen an risikomindernde Maßnahmen und zur Risikobeherrschung festgelegt. Außerdem wurde beschrieben, wie die geplanten Kontrollen in die Phasen des Entwicklungslebenszyklus greifen (z.B. „Die Gefährdungen, die durch externe Einflüsse auf das Programm entstehen können, sollen parallel zur Anforderungsspezifikation ermittelt werden“) („Methoden zur RA je nach Fortschritt des Entwicklungszyklus“).

Einige dieser Regelungen werden im V-Modell im QS-Plan auf Grundlage des Handbuchs SI festgelegt.

#### 5.2.5.9 Risikoanalyse-Plan

Der Risikoanalyse Plan beschreibt die eigentliche Durchführung der Risikoanalyse. Vorab werden die Auftretenswahrscheinlichkeit und das Schadensausmaß wie in Kapitel 3.1.4 beschrieben eingeteilt und der daraus resultierende Risikograph definiert („Kriterien für die Risikoeinstufung“). Desweiteren wurden Akzeptanzkriterien festgelegt, die Grenzen für die akzeptierten Risiken darstellen (z.B. von den 30 ermittelten Risiken dürfen max. 5 im ALARP<sup>14</sup> Bereich liegen, ansonsten müssen weitere Risikobeherrschungsmaßnahmen durchgeführt werden). Es werden alle Risiken aufgezeigt („Gefährdungen/Ursachen“) und bewertet („Risikoabschätzung“), so wie die risikomindernden Maßnahmen („Risikobeherrschung“) festgelegt. Die Dokumentation hierzu erfolgt tabellarisch, wobei die Gliederungspunkte „Gefährdung“, „Ursache“, „Risikoabschätzung“ und „Risikobeherrschung“ die Spalten bilden. Diese werden einer Funktion zugeordnet, weshalb noch eine Spalte „Funktion“ hinzugefügt werden muß (Anmerkung: Funktion kann z.B. auch Stromausfall oder ein Eingabefehler sein).

Einige dieser Regelungen werden im V-Modell im QS-Plan auf Grundlage des Handbuchs SI festgelegt. Die Ergebnisse der Risikoanalyse würde man im V-Modell anhand der Kritikalitäten/Funktionen-Matrix dokumentieren.

#### 5.2.5.10 Risikoanalyse-Report

Im Report wird die Wirksamkeit der umgesetzten Maßnahmen aus dem Risikoanalyse-Plan bewertet („Beurteilung der Wirksamkeit des Risikobeherrschung“) und freigegeben, so wie das Restrisiko ermittelt („Dokumentation der Restrisiken“).

---

<sup>14</sup>As Low As Reasonable Possible

#### 5.2.5.11 Risikomanagement-Zusammenfassung

Die Risikomanagement-Zusammenfassung beinhaltet die Zusammenfassung des gesamten Projektablaufes, bewertet die Umsetzung des SQMP, des Testkonzeptes, der System und Integrationstests („Review d. Einhaltung des Entwicklungslebenszyklus“). Die abschließende Bewertung der Risikoanalyse anhand der Akzeptanzkriterien, so wie die Einstufung des Restrisikos gibt letztlich die Entscheidung zur Freigabe des Softwareprojektes.

#### 5.2.5.12 Abschließende Bemerkung

Nachdem alle oben angeführten Produkte erstellt sind, wird das Produkt dem Prüflabor der Zertifizierungsstelle vorgelegt. Dieses überprüft die Vollständigkeit der Dokumente in Bezug auf die Anforderungen der EN60601-1-4 (bzw. weiterer Normen, falls solche angewandt wurden). Neben der Vollständigkeit wird auch die Korrektheit der Umsetzung geprüft. Hiermit ist zum einen gemeint, daß die Dokumentation mit dem erstellten Produkt übereinstimmt und zum anderen die durchgeführten Tests ein reproduzierbares Ergebnis liefern. Von Seiten des Konfigurationsmanagements wird überprüft, ob die aus der Risikoanalyse resultierenden Risikobeherrschungsmaßnahmen nachvollziehbar eingearbeitet wurden. Außerdem wird nachvollzogen, ob die Entwicklungsergebnisse mittels eines Konfigurationsmanagements gehandhabt und entsprechend des geplanten Entwicklungslebenszyklus eingehalten werden.

Die Zertifizierungsstelle bewertet ob die Ergebnisse des Prüflabors der Einhaltung der normativen Forderungen entsprechen und alle Grundlegenden Anforderungen erfüllt sind.

Wie bereits in Kapitel 3.1.6 erwähnt, müssen zusätzlich zu den oben genannten Dokumenten, noch eine Softwaredokumentation, eine Gebrauchsanleitung und „Technische Beschreibung“ erstellt werden, um die Anforderungen der Technischen Dokumentation zu erfüllen. Eine „Klinische Bewertung nach Anhang X, MDD“ kann ebenfalls erforderlich sein.

### 5.3 Anforderungszuordnung Zertifizierungsstelle zu V-Modell

In diesem Abschnitt werden den Anforderungen der Zertifizierungsstelle die entsprechenden Produkte des V-Modells zugeordnet. Die Ausgangsbasis hierfür bildet die von mir im Rahmen der Zertifizierung erstellte Dokumente und deren Zuordnung der Prüfpunkte der Checklisten durch den Berater. Diesen Prüfpunkten werden nun die entsprechenden (Teil-) Produkte des V-Modells zugeordnet. Es bleibt zu beachten, daß der Umfang der Teilprodukte des V-Modells häufig zu umfangreich ist. Für die Zertifizierungsstelle sind schwerpunktmäßig diejenigen Funktionen interessant, die eine Gefährdung für Patienten, Anwender, Dritte oder die Umwelt bedeuten, wobei natürlich die Mindestanforderungen von Seiten der angewendeten Normen bzw. FDA Guidance-Dokumente einzuhalten sind.

Erläuterungen zur Konvention:

Für die im weiteren verwendeten Bezeichnungen werden die Aktivitäten des V-Modells

analog deren Definition als SE x.x, PM x.x, KM x.x und QS x.x bezeichnet (siehe Kapitel 4), wobei die beiden einleitenden Buchstaben jeweils dem Submodell entsprechen. Analog dazu werden die Produkte des V-Modells entsprechend deren Definition bezeichnet (z.B. AFo.2 für Anwenderforderungen „Ist-Aufnahme und Ist-Analyse“).

Die Zuordnungstabellen enthalten in der ersten Spalte den jeweiligen Punkt der Checkliste der Zertifizierungsstelle. Angaben in Klammern sind immer als optional zu verstehen. Die zweite Spalte gibt die Anforderungen der Norm EN60601-1-4 an und die dritte Spalte das (Teil-) Produkt des „V-Modell 97“.

Das folgende Kapitel „Tailoring“ legt die Vorhabenklasse des Beispielprojektes fest. Für die weiteren Betrachtungen ist entscheidend, ob die „Basis Anforderung“ dieser Vorhabenklasse ausreicht, d.h. ob alle Produkte für die zugrundeliegende Zertifizierung erstellt werden oder ob zusätzliche Produkte des V-Modells erstellt werden müssen.

### 5.3.1 Tailoring

Das Tailoring wird entsprechend dem Handbuch „Tailoring und projektspezifisches V-Modell“ durchgeführt. Das Vorgehen erfolgt nach Gliederungspunkt T.2.1.5 des Handbuchs „Tailoring und Projektspezifisches V-Modell“.

Als Vorhabenklasse wird das Projekt als technisch-wissenschaftliches IT Vorhaben eingestuft. Tabelle 5.3.1 zeigt den von mir nachträglich abgeschätzten Aufwand des Projektes: Für die Projektgröße wurden hierfür 2 Person mit einer Projektdauer von 1/2 Jahr angesetzt - das Risikomanagement läuft ja parallel und ist bei Abschluß der Abnahme ebenfalls fertig. Zur Abschätzung der Komplexität wurden folgende Annahmen gemacht: Anzahl Subfunktionen < 30, Anzahl der Schnittstellen < 10. Eine Einordnung nach Programmzeilen (LOC) konnte nicht durchgeführt werden, da es sich hier um eine graphische Programmiersprache handelt. Zur Messung der Komplexität wurde die Metrik „Number of nodes“ verwendet (siehe Kapitel 6.2). Diese liegt maximal bei 396. Dieser Wert stellt allerdings einen Ausreißer dar, da die komplexeren Funktionen einen Wert um 150 aufweisen. Die Zuordnung erfolgte willkürlich in die Kategorie „mittel“ was einer Obergrenze von 300 LOC bedeuten würde. Die Datenkomplexität wurde „gering“ eingestuft.

Kriterium	Projekt	Einstufung
Projektgröße	2 Person 1/2 PJ	klein
Komplexität Funktionen	30/10/300	mittel
Komplexität Daten	<< 10/10/20	gering
Wartbarkeitsanforderungen	nur minimale Anpassungen werden erwartet	gering

Das Projekt wurde dem IT Vorhabentyp „kleine/mittlere technisch-wissenschaftliche IT Vorhaben“ zugeordnet. Die erhöhten Kritikalitätsanforderungen des Systems werden durch die Durchführungsbedingung „Kritikalität“ abgefangen. PM-Plan und KM-Plan konnten aus einem vorangegangenen Projekt genommen und an die projektspezifischen Gegeben-

heiten angepaßt werden.

Medizinprodukte stellen im allgemeinen immer ein technisch-wissenschaftliches IT Vorhaben dar. Da das Beispielprojekt in die Kategorie „kleine/mittlere technisch-wissenschaftliche IT Vorhaben“ eingeordnet ist, läßt sich hieraus schließen, daß die im weiteren getroffenen Aussagen auch für „große technisch-wissenschaftlichen IT Vorhaben“ gültig sind, da von Seiten des V-Modells nur neue Aktivitäten und Produkte hinzukommen aber keine gestrichen werden.

### 5.3.2 Projektmanagement

Das phasenübergreifende Dokument *Software-Qualitätsmanagement-Plan (SQMP)* stellt aus Sicht des V-Modells weitestgehend das Projekthandbuch (PHb) dar. Im SQMP wird eine Projektbeschreibung erstellt, die Ergebnisse des Tailoring abgelegt, die Produkte des projektspezifischen V-Modell beschrieben und die Projektorganisation festgelegt. Die in PHb\_3 geforderten vertragsrelevanten Festlegungen werden im wesentlichen durch den Umfang der Technischen Dokumentation (siehe Kapitel 3.1.6) festgelegt. PHb\_6 „Auswahl von Methoden und Werkzeugen“ und PHb\_8 „Standards und Richtlinien“ wurden entsprechend der Checklisten in der Anforderungsspezifikation dokumentiert. Der von Seiten des V-Modells geforderte Projektplan wurde nicht erstellt, da dieser zum einen keine Anforderung für die Zertifizierung ist und zum anderen das System zu „Projektbeginn“ ja bereits fertig implementiert vorlag. Tabelle 5.3 stellt die Ergebnisse der Zuordnung dar.

Inhalt	EN60601-1-4	Produkt V-Modell
Projektüberblick, Entwicklungsvorgaben	52.202.2	PHb_2
Zweckbestimmung des PEMS Entwicklungsvorgaben für Anwendungsbereich des PEMS siehe auch Zweckbest. in GA, (Beschreibungen, Werbematerialien)	52.206.1	PHb_2
(Organisation des Projektes)	52.202.2	PHb_7
Hauptverantwortlichkeiten	52.210.5	PHb_7.1, PHb_7.2
Phasenübergreifende Meilensteine bei der PEMS - Entstehung (Entwicklungslebenszyklus)	52.203.1 52.203.2 52.204.2 52.202.2	PHb_5
Festlegung der Reviews (in Abhängigkeit von der Komplexität der Anforderungen)	52.211.2	PHb_5
Überblick über grobe Dach - Architektur des PEMS	52.202.2 52.203.2	Wurde als Teil der endgültigen Realisierung von SwArc.2 (SysArc.3.1) genommen
Dokumentenstruktur zum PEMS (Liste der Dokumente)	52.201.1 52.203.4	PHb_5

Inhalt	EN60601-1-4	Produkt V-Modell
Verantwortlichkeiten für: SQMP	–	PHb_7.2
Verantwortlichkeiten für: KMP	52.201.2	PHb_7.2
Verantwortlichkeiten für: Gefährdungsanalyse	52.202.2 c) 52.203.3	kein Teil des V-Modells
Verantwortlichkeiten für die Archivierung der nachweißpflichtigen Dokumente	52.201.1	PHb_7.2
(Plan für die traceability of PEMS requirements)	–	PHb_5
(Plan für die traceability of safety – requirements)	–	PHb_5
Tailoring - Maßnahmen Beschreibung welche Punkte der norm. Anforderungen bzw. des Entwicklungs-Lebenszyklus an das Projekt angepasst wurden	52.202.2 b) 52.203.5	PHb_3
Erstellung und Prüfung Produktbegleitender Dokumente z.B.: GA, Verpackung, Werbung, (Programmbeschreibung)	6.8.201 52.204.3.1.6	PHb_3, PHb_7.1
Kennzeichnung und Verpackung Herstellerangaben, CE- Kennzeichnung	52.204.3.1.6	PHb_3
Personalqualifikation Schulungsnachweise bzw. Arbeitsplatzbeschreibungen und Verfahren zur Regelung der Qualifikation	52.205	Folgt aus Aktivität PM10

Tabelle 5.3: Zuordnungstabelle Submodell Projektmanagement

Der im SQMP erstellte Projektüberblick entspricht dem Produkt PHb.2. Die in Aktivität PM 1.2 zu erstellende Projektbeschreibung wird in Form der Zweckbestimmung eingearbeitet. Allerdings ist zu beachten, daß die Angaben in der Zweckbestimmung fachlich detaillierter am Klassifizierungsprozeß orientiert sind.

Die Organisation des Projektes wird im V-Modell in PHb\_7 geregelt. Die „Hauptverantwortlichkeiten“ können von PHb\_7.2 übernommen werden. Die Organisation des Projektes besteht weiterhin in der Definition der Phasen der Systemerstellung („Phasenübergreifende Meilensteine bei der PEMS-Entstehung (Entwicklungslebenszyklus)“) - eingeteilt in Einzel- und übergreifende Phasen. Diese Produkte werden im Projekthandbuch unter PHb\_5 be-

schrieben. Die Definition der Phasen erfolgte im Beispielprojekt informell auf Grundlage von EN60601-1-4 Anhang DDD. Der Punkt „Festlegung der Reviews (in Abhängigkeit der Komplexität der Maßnahme)“ wird ebenfalls im Projekthandbuchabschnitt „Projektspezifisches V-Modell“ (PHb\_5) festgelegt. Die hier getroffene Regelung umfaßt neben dem Einbezug von Aktivität QS 1.2 auch den vom V-Modell vorgegebenen Produktfluß.

Als „Überblick über die grobe Dach - Architektur“ wird aus SwArc\_2 der gewählte Lösungsvorschlag entnommen (bei größeren Systemen kann hier SysArc\_3.1 die bessere Wahl sein). Die „Dokumentenstruktur des PEMS“ stellt der Produktteil der Aktivitäten/-Produktübersicht aus PHb\_5 bereit.

Die Verantwortlichkeiten für SQMP, KMP und „die Archivierung der nachweißpflichtigen Dokumente“ werden bei Anwendung des V-Modells in PHb\_7.2 eingetragen. Eine Gefährdungsanalyse wird bei Anwendung des V-Modells typischerweise nicht durchgeführt, weswegen diese Verantwortlichkeit zusätzlich festgelegt werden muß. Die Festlegung, ob die optionalen Dokumente „traceability of PEMS<sup>15</sup> requirements“ und „traceability of safety requirements“ erstellt werden sollen, wird von PHb\_5 übernommen<sup>16</sup>.

Die „Tailoring Maßnahmen“ werden aus PHb\_3 übernommen. Der Punkt „Erstellung und Prüfung produktbegleitender Dokumente“ legt fest, welche zusätzlichen Produkte von wem (PHb\_7.1) erstellt und freigegeben werden. Im V-Modell werden zusätzliche Produkte als vertragsrelevante Festlegung (PHb\_3) spezifiziert. Die „Kennzeichnung und Verpackung Herstellerangaben, CE-Kennzeichnung“<sup>17</sup> wird als solche nicht direkt geregelt. Allerdings wäre bei einer Auftragsentwicklung durchaus denkbar, daß diese Angaben vertragliche Gegenstände und somit in PHb\_3 geregelt werden. Der letzte Punkt der Checkliste „Personalqualifikation Schulungsnachweise bzw. Arbeitsplatzbeschreibungen und Verfahren zur Regelung der Qualifikation“ wird im V-Modell indirekt in PHb\_7.1 bzw. direkt durch die im Handbuch „Rollenkonzept im V-Modell“ geforderten Kenntnisse und Fähigkeiten definiert, die einer Rolle zugeordnet sind.

Der im getailorten V-Modell als Basis-Anforderung geforderte Projektabschlußbericht stellt keine Anforderung von Seiten der Zertifizierung dar<sup>18</sup>.

### 5.3.3 Konfigurationsmanagement

Tabelle 5.4 zeigt die Zuordnung der Anforderungen von Seiten der Zertifizierungsstelle zu den Teilprodukten des V-Modells. Das Konfigurations-Identifikationsdokument wurde nicht durch die Checkliste erfaßt. Festlegungen wie „Projektbezeichnung“, „KM Verantwortlicher“ werden im V-Modell im Projekthandbuch festgelegt. Tabelle 5.4 stellt die Zuordnung der Anforderungen der Zertifizierungsstelle an das V-Modell dar. Im Anschluß werden die einzelnen Teilpunkte kurz diskutiert. Die Checkliste basiert nach Auskunft der Beraterfirma auf dem V-Modell.

---

<sup>15</sup>Programmierbares Elektronisches Medizinisches System

<sup>16</sup>Die „traceability“ Dokumente stellen eine Anforderung von Seiten der FDA dar

<sup>17</sup>wird in MDD Art. 17 und Anhang XII gefordert (vgl. „Kennzeichnungspflicht“ Kapitel 2.1)

<sup>18</sup>Die Risikomanagement-Zusammenfassung stellt eine besondere Form des Projektabschlußberichts dar, wobei nicht die Projektplanungsdaten im Vordergrund stehen sondern die ermittelten Gefährdungen (siehe Abbildung 3.3).

Inhalt	EN 60601-1-4	V-Modell
Verantwortlichkeiten des KM	52.201.2	PHb_7.2
Verantwortlichkeiten des Zugriffs-Fehler- und Änderungs-Managements	52.202.2 c)	PHb_7.2
Festlegung <b>aller</b> Elemente, die dem KM unterliegen	52.211.2	KPl_2.2
Festlegung ab wann in der Spezifikationsphase das KM begonnen wird	52.211.2	KPl_2.2
Verfahren und projektbezogene Einteilung der Versionsverwaltung (z.B. "Check in Check out Verfahren")	52.208.2 a) 52.204.3.1.6 d)	KPl_2.2
Identifizierbarkeit jedes SW - Elementes (z.B. Release und Level Nr.)	52.211.2	KPl_2.3
Statusangabe jedes SW - Elementes	52.208.2 a), j), k)	KPl_2.2
Angaben der versionsbezogenen Entwicklungsumgebung (Compiler, Compileroptionen)	52.208.2 c)	KPl_2.3
Definition der Versionsfolge (Änderungsverfolgbarkeit – Revision History Log)	52.211.1	KPl_2.3
Ältere Versionen archivieren bzw. reproduzieren	52.208.2	KPl_3.3, KPl_4
Festlegung der Zugriffskontrolle auf SW- Elemente je nach Status	52.211.1	KPl_2.2
Verfahren zur Verwaltung von Änderungen und Fehlermeldungen (auch SW-Varianten) nach dem Designfreeze a) Änderungsanträge / Meldeverfahren b) Genehmigungsverfahren / Auswahlverfahren c) Freigabe und Info über die Änderung	52.211.1	KPl_3 KPl_3.1
Änderungs- Spezifikation (Begründung)	52.211.1	KPl_3.1.4

Inhalt	EN 60601-1-4	V-Modell
Analyse der Auswirkungen der Änderung auf das Gesamtprojekt des PEMS inklusive Gefährdungsanalyse (Revalidierung)	52.211.1	KPl.3.1.2
Liste der ungelösten Fehler und deren Risikobewertung (zu berücksichtigen operator usage and human factors)	52.211.1	KPl.3.1.4
Datensicherung / Datenverwaltung / Katalogisierung	52.211.2	KPl.4, Produktbibliothek
Versionsverwaltung der Dokumentation Lenkung der Dokumente	52.211.2	KPl.3.3, KPl.3.4
KMP - Review durchgeführt ?	52.212.1	PrPl.2

Tabelle 5.4: Zuordnungstabelle Submodell Konfigurationsmanagement

Die ersten beiden Punkte der Checkliste „Verantwortlichkeiten des KM“ und „Verantwortlichkeiten des Zugriffs- Fehler- und Änderungs- Managements“, werden bei Umsetzung des V-Modells im Projekthandbuch (PHb\_7.2) festgeschrieben.

Bei Erstellung eines Konfigurationsmanagement-Plans (KPl.) nach V-Modell werden im Abschnitt „Projektspezifische Festlegungen“ (KPl.2.2), Festlegungen getroffen, die die Checklistenpunkte „Festlegung **aller** Elemente, die dem KM unterliegen“, „Festlegung ab wann in der Spezifikationsphase das KM begonnen wird“, „Verfahren und projektbezogene Einteilung der Versionsverwaltung“, „Statusangabe jedes SW-Elementes“ und „Festlegung der Zugriffskontrolle auf SW-Elemente je nach Status“ umsetzen.

Die im Konfigurationsmanagement-Plan definierten „Konventionen zur Identifizierung“ (KPl.2.3) werden durch die Checklistenpunkte „Identifizierbarkeit jedes SW-Elementes (z.B. Release und Level Nr.)“, „Angaben der versionsbezogenen Entwicklungsumgebung (Compiler, Compileroptionen)“ und „Definition der Versionsfolge (Änderungsverfolgbarkeit – Revision History Log)“ überprüft.

Festlegung zur Archivierung und Reproduktion werden in KPl.4 getroffen (Ältere Versionen archivieren bzw. reproduzieren“ und „Datensicherung / Datenverwaltung / Katalogisierung“). Für den erstgenannten Punkt müssen zusätzlich die Regelungen zur Versionskontrolle (KPl.3.3), daß alle geänderten Produkte mitgeführt werden müssen, beachtet werden (z.B.: HW, OS, Compiler, ..).

Im Abschnitt „Änderungsmanagement“ (KPl.3) des Konfigurationsmanagement-Plans werden die Regelungen zur Durchführung von Änderungen getroffen. Die Änderungsprozedur selbst - also das Verfahren vom Änderungsantrag bis zur Änderungsmitteilung wird im Unterabschnitt KPl.3.1 definiert. Von Seiten der Zertifizierungsstelle werden diese Regelungen durch die Checklistenpunkte „Verfahren zur Verwaltung von Änderungen und Fehlermeldungen (auch SW-Varianten) nach dem Designfreeze a) Änderungsanträge / Mel-

Verfahren b) Genehmigungsverfahren / Auswahlverfahren c) Freigabe und Info über die Änderung“, „Änderungs- Spezifikation“, „Analyse der Auswirkungen der Änderung auf das Gesamtprojekt des PEMS inklusive Gefährdungsanalyse (Revalidierung)“ und „Liste der ungelösten Fehler und deren Risikobewertung (zu berücksichtigen operator usage and human factors“ überprüft. Eine explizite Sperrung des Produktes nach Auslieferung, wie es die Regelung der Meldepflicht (vgl. Kapitel 2.1) vorsieht, wird im V-Modell nicht geregelt. Der Punkt „Versionsverwaltung der Dokumentation/Lenkung der Dokumente“ wird in Unterpunkt KPl.3.3 bzw. KPl.3.4 erstellt.

Die Anforderungen an die Einhaltung des Konfigurationsmanagements durch Reviews („KMP Review durchgeführt“) werden im V-Modell in PrPl.2 (Submodell QS) geregelt, indem das Konfigurationsmanagement als Prüfgegenstand festgelegt wird.

### 5.3.4 Systemerstellung

Das für die Zertifizierung erstellte V-Modell sieht für die Dokumentation des Submodells SE die Produkte Anforderungsspezifikation und Designspezifikation vor. Hierbei werden die Produkte *Anwenderforderungen*, *Systemarchitektur*, *Technische Anforderungen* und *Schnittstellenübersicht* als Anforderungsspezifikation in einem Dokument zusammengefaßt. Analog werden die Phasen *SW-Grobentwurf*, *SW-Feinentwurf* und *SW-*

Phasen im Beispielprojekt	Produkt im Beispielprojekt	Phasen V-Modell	Produkte V-Modell
Anforderungsphase	Anforderungsspezifikation	System-Anforderungsanalyse System-Entwurf SW-/HW-Anforderungsanalyse	Anwenderforderungen  Schnittstellenübersicht, Systemarchitektur, Technische Anforderungen, Betriebsinformationen
Designphase	Designspezifikation Testplan System / Integration / Modul	SW-Grobentwurf SW-Feinentwurf SW-Implementierung	Schnittstellenübersicht, SW-Architektur, SW-Entwurf, Datenkatalog, Betriebsinformationen
Validierungsphase	Testreport System / Integration / Modul	System-Integration	Segment, System

Tabelle 5.5: Produkt-Phasenzuordnung

*Implementierung* zusammengelegt und deren Produkte *Schnittstellenübersicht*<sup>19</sup>, *SW-*

<sup>19</sup>Das Produkt Schnittstellenübersicht wird hier zweimal aufgeführt. Die Schnittstellen der Anforderungsspezifikation beschreiben die Anforderungen (z.B. Definition einer Schnittstelle zur Umwelt) an die

Architektur, SW-Entwurf und Datenkatalog als Designspezifikation zusammengefaßt. Betriebsinformationen fließen in die Gebrauchsanweisung mit ein. In der Designphase werden die Anforderungen der Anforderungsphase in einen Softwareentwurf umgesetzt. Die Abbildung der Anforderungen auf die „Softwarekonzepte“ erfolgt im Dokument *traceability of requirements*. Dieses ist analog den *Anforderungszuordnungen* im V-Modell zu sehen. Die Checkliste zur Design-Phase (Tabelle 5.7) enthält ferner Punkte, die die Verifizierungsphasen betreffen und typischerweise als Output der Integration zu sehen sind (vgl. Aktivitäten SE 7.1, SE 7.2, SE 7.3, SE 7.4, SE 8.1, SE 8.2). Die Umsetzung dieser Aktivitäten werden in Prüfereports zusammengefaßt. Für die Festlegung der Prüfgegenstände werden während der Entwurf und Implementierungsphasen, Prüfpläne und Prüfspezifikationen erstellt. Tabelle 5.5 faßt die Ergebnisse nochmals zusammen.

Von Seiten der Zertifizierungsstelle macht es keinen Unterschied, ob die Produkte entsprechend der festgelegten Zustände der Aktivitäten erstellt wurden. Die Prüfung erfolgt generell bevor das System in die Nutzung übergeleitet wird, wodurch die Zusammenführung der Produkte möglich ist<sup>20</sup>. Tabelle 5.6 zeigt welche Teilprodukte die Punkte der Checkliste zur Anforderungsspezifikation erarbeiten. Für die Aktivität SE 2 ist zu beachten, daß die Entscheidungsfindung durch alternative Lösungsvorschläge nicht aufgeführt werden muß. Liegen der Auswahl der Architektur sicherheitsrelevante Gesichtspunkte zugrunde, sollten diese jedoch im Rahmen der Risikoanalyse dokumentiert werden (Aktivität SE 2.2). Die Auswahl der Lösungsvorschläge selbst stellt ein „Soll-Kriterium“ für den europäischen Markt und ein „Muß-Kriterium“ für eine Zulassung durch die FDA<sup>21</sup> dar, wobei diese Angaben als „Design History“ in das Technische File<sup>22</sup> mit einfließen.

Die Anforderungsspezifikation enthält die in Tabelle 5.6 aufgelisteten Zuordnungen. Mehrfachnennungen bei der Zuordnung von (Teil-) Produkten des V-Modells resultieren zum einen aus der Zusammenlegung der V-Modell Produkte und zum anderen an den Vorgaben der Checkliste.

Anforderung	Numerierung EN60601-1-4	Anforderung V-Modell
Ersteller, Ausgabedatum, (Version), und Freigabe	–	Allgemein
Allgemeine Beschreibung / Programmvorgaben (z.B. Marketing Vorgaben)	–	AFo_6.1, AFo_6.2, AFo_6.3

Schnittstelle, wohingegen sich das Produkt Schnittstellenübersicht der „Designphase“ auf die im Abschnitt 4 „Schnittstellen“ des V-Modell Produktes SW-Architektur bezieht (SwArc\_4).

<sup>20</sup>Anmerkung: Werden im Projekthandbuch Festlegungen bzgl. der Statuszustände der Produkte bzw. Phasen getroffen (z.B. Anforderungsspezifikation muß im Zustand „akzeptiert“ sein, bevor Phase SW-Architektur begonnen werden kann), stellt diese Regelung ebenfalls einen Prüfgegenstand dar.

<sup>21</sup>vgl. [FDA97a]

<sup>22</sup>vgl. Kapitel 3.1.6

Beschreibung DV- Systemumgebung,	52.206.2	Tanf_x.5, Afo_6.2
Ein-/ Beschränkungen der HW / SW	52.206.2 52.204.3.1.6 a)	AFo_6.1, TAnf_5
Betriebssysteme	52.206.2	PHb_6
Programmiersprachen	52.206.2	PHb_6
Entwicklungsumgebung (z.B. CASE - Tools)	52.208.2	PHb_6
Vernetzung	–	SSÜb_2
Liste der gewünschten / ungewünschten Funktionen und Eigenschaften	52.206.1	AFo_6, AFo_7
Benutzerschnittstellen Sprache, (Bildschirm-) Ein- Ausgabemas- ken, Kommandos, Tastaturbefehle, Druckerausgaben, E/A Geräte	52.206.2 52.204.3.1.6 b)	SSÜb_2
Sonstige Schnittstellen (zu anderen Systemen)	52.206.2	SSÜb_2
Validierung von Fremdsoftware (OTS, etc.)	52.208.2 k) 52.204.3.1.6 f)	SysArc_3.1, SysArc_3.2
Gefährdungsmindernde Anforderun- gen (aus der Risikoanalyse)	52.206.2 52.207.3 52.204.4.4	AFo_6, TAnf_3,4,5
Fehlermeldungen und Alarme	52.206.2	AHb_2.f.3
Qualifikationsvorgaben für den An- wender,	–	AFo_6.2
Datenmodelle, Datenschutz, Datensi- cherheit	52.207.1 52.204.3.1.6 d)	TAnf_5
Vorschriften (spezielle Normen oder Anforderungen)	–	AFo_7.1
Review - Plan / Report	–	PrPl_2
SW - Strukturvorgabe / Ablaufdia- gramm	52.207.1	SwArc_2

Tabelle 5.6: Zuordnungstabelle Anforderungsspezifikation

Die „allgemeine Beschreibung/Programmvorgaben“ werden in Aktivität SE 1.1 und SE 1.2 erörtert und fließen in die Produkte Afo\_6.1 - Afo\_6.3 ein. Die „DV-Systemumgebung“ stellt die „Organisatorische Einbettung“ dar. „Einschränkungen der HW/SW“ treten zum einen als „grobe Systembeschreibung“ und zum anderen als „Technische Anforderungen an SW-Einheiten/HW-Einheiten“ auf. Die verwendeten Programmiersprachen, Entwicklungsumgebungen und die Vorabauswahl der Zielrechnerausstattung („Betriebssysteme“) sind als Ergebnisse der Aktivität PM 1.4 „Toolset-Management durchführen“ in PHb\_6 zu benennen. Angaben bezüglich Vernetzung können der Schnittstellenübersicht (SSÜb.2 bzw. TAnf\_x.3.2) entnommen werden. Die „Liste der gewünschten/ungewünschten Funktionen und Eigenschaften“ werden aus AFo\_6 und AFo\_7 übernommen.

Aus der Schnittstellenübersicht (SSÜb.2) werden die Punkte „Benutzerschnittstellen Sprache, (Bildschirm-) Ein- Ausgabemasken, Kommandos, Tastaturbefehle, Druckerausgaben, E/A Geräteüind „Sonstige Schnittstellen (zu anderen Systemen)“ ermittelt, wobei diese Punkte die Schnittstellen der Phasen 1 bis 3 berücksichtigen.

Die „Validierung von Fremdsoftware“ erfolgt im Rahmen der Aktivität SE 2.1 und fließt in die Lösungsvorschläge der Systemarchitektur (SysArc\_3.1 bzw. SysArc\_3.2) mit ein. Die „Gefährdungsmindernde Anforderungen“ werden mit Hilfe einer Risikoanalyse ermittelt. Die Ergebnisse werden im V-Modell als neue Anforderungen (fachlich oder technisch) eingebracht. Die Zuordnung gibt deshalb AFo\_6, TAnf\_3, TAnf\_4 oder TAnf\_5 an. Die hier gefundenen Anforderungen werden zudem in der „traceability of safty requirements“ Matrix eingetragen.

Es sind weiterhin alle „Fehlermeldungen und Alarme“ anzugeben. Im V-Modell werden diese Informationen im Anwendungshandbuch (AHb\_2.f.3) dokumentiert. Die „Qualifikationsvorgaben des Benutzers“ können Abschnitt AFo\_6.2 entnommen werden. Die Angaben zu „Datenmodelle, Datenschutz, Datensicherheit“ werden TAnf\_5 entnommen. „Vorschriften (spezielle Normen oder Anforderungen)“ werden in AFo\_7.1 festgelegt, wohingegen „SW - Strukturvorgabe / Ablaufdiagramm“ aus SwArc\_2 übernommen werden. Der Punkt „Review - Plan / Report“ entspricht im V-Modell einem Eintrag der Anforderungsspezifikation in den Prüfplan (PrPl\_2).

Anforderung	Anforderung EN60601-1-4	Anforderung V-Modell
Reports und Dokumente der Code - Reviews (gem. SQMP)		Wurden nicht durchgeführt
Dokument Design Spezifikation (FDA)	–	
Akzeptanzkriterien für das Design (FDA)	–	

Umsetzung der SW- Architektur / Struktur aus der Anforderungsspezifikation (Chart – Funktionale Modulbeschreibung – Logische Struktur)	52.207.1 52.207.2	SwArc, SwEnt
Variablen Definition und in welchem Kontext sie verwendet werden(FDA)	–	DatK_2
Einhaltung gegebener Strukturvorgaben bei der Codierung (Programmier – Richtlinien, Entwicklungsstandards)	52.208.2	PHb_8, PrPl_2

Tabelle 5.7: Zuordnungstabelle Designspezifikation

In der Designphase wird die „SW-Architektur“ aus der Anforderungsspezifikation in ein Softwaredesign umgesetzt („Umsetzung der SW-Architektur/Struktur aus der Anforderungsspezifikation (Chart – Funktionale Modulbeschreibung - Logische Struktur)“). Dies entspricht den Produkten „SW-Architektur“ und „SW-Entwurf“. In Aktivität SE 5.1 „SW-Komponente/-Modul/Datenbank beschreiben“ werden Variablendefinitionen ermittelt und anschließend in den Datenkatalog (DatK.2) eingetragen („Variablen Definition und in welchem Kontext sie verwendet werden(FDA)“). Die Einhaltung von Strukturvorgaben („Style Guides“) stellt eine konstruktiv Qualitätssichernde Maßnahme dar, deren Festlegung nach V-Modell im Projekthandbuch (PHb\_8) erfolgt. Die Vorgaben sind durch die Programmierer während der „SW-Implementierung“ (SE 6) einzuhalten. Die eigentliche Überprüfung der Einhaltung, erfolgt durch Aufnahme dieses Punktes in den Prüfplan (PrPl).

Die weiteren Punkte der Checkliste Design-Phase stellen aus Sicht des V-Modells Anforderungen des Submodells QS dar. Aus diesem Grunde wurde die Checkliste getrennt und in das folgende Kapitel als Tabelle 5.8 eingefügt.

### 5.3.5 Qualitätssicherung

Ein wesentlicher Bestandteil der Zertifizierung ist die Überprüfung der Qualitätssichernden Maßnahmen. Zur Sicherung der Qualität werden konstruktive (präventive) und analytische Maßnahmen festgelegt, wobei die konstruktiven Maßnahmen im Submodell SE umgesetzt werden. Da das Programm schon bei Projektbeginn fertig implementiert vorlag, wurden keine konstruktiven Maßnahmen festgelegt. Die Regelungen des QS-Plans wurden im SQMP (Projekthandbuch) eingetragen. Diese Regelung entspricht der Erläuterung in Aktivität QS 1.1.

Die Qualitätssichernden Maßnahmen bestanden in der Durchführung von Reviews, Verifizierungs- und Validierungsmaßnahmen nach Maßgabe des Testkonzeptes und des Risikomanagement-Prozesses. Im Rahmen der Qualitätssicherung wird eine Zuordnung für das „Testkonzept“ vorgenommen. Die Umsetzung des Testkonzeptes auf die Prüffe-

genstände erfolgt in den Prüfplänen (festlegen der Prüfgegenstände und Verantwortlichkeiten) und den dazugehörigen Prüfspezifikationen. Prüfpläne und Prüfspezifikationen sind für Test auf Modul- Segment- und Systemebene zu spezifizieren. Die Überprüfung dieser Produkte wird nicht weiter untergliedert. Die „Testpläne“ entsprechen inhaltlich einer Prüfspezifikation im V-Modell und die Test-Reports den Prüfprotokollen. In die Rückverfolgbarkeitsmatrix werden die Testfälle aus PrSpez\_5 eingetragen und den Anforderungen zugeordnet. Als weitere Testgegenstände sind die „Umsetzung des KMP“ und die „Bewertung des Testkonzeptes (Erfüllung aller Testkriterien, vollständige Umsetzung)“ festgelegt. Tabelle 5.8 zeigt die in der Checkliste Design-Phase eingetragenen Prüfpunkte.

<b>Anforderung</b>	<b>Anforderung EN60601-1-4</b>	<b>Anforderung V-Modell</b>
Testvorgaben, erwartete Ergebnisse, Testziele	52.208.1 52.209.1 52.210.5	PrSpez
Angaben der versionsbezogenen Testumgebung (Compiler, Compileroptionen etc.)	52.208.2	PrPl_5.1
Modul - Testpläne	52.209.2	PrSpez
Integrations- Testpläne	52.209.2	Int_Pl, PrSpez
System - Testpläne	52.209.2	PrSpez
Modul - Test - Reports	52.209.2	PrProt
Integrations- Test - Reports	52.209.2	PrProt
System - Test - Reports	52.209.2	PrProt
(traceability of requirements vollständig) (Rückverfolgbarkeit der Anforderungen und Risiken)	–	PrSpez_5
Umsetzung des KMP	52.201.2	PrProt
Bewertung des Testkonzeptes (Erfüllung aller Testkriterien, vollständige Umsetzung)	52.210.6	PrProt

Tabelle 5.8: Zuordnungstabelle Testpläne

Im folgenden wird die Zuordnung für das Dokument „Testkonzept“ diskutiert (siehe Tabelle 5.9). Dieses stellt eine Mischung aus QS-Plan, Prüfplan und Prüfspezifikation dar (vgl. auch Kapitel 5.2.5.4). Es sollen hierbei allgemeine Vorgaben an die Tests definiert werden (vgl. Kapitel 5.2.5.4).

<b>Inhalt</b>	<b>EN60601-1-4</b>	<b>(Teil-) Produkt V-Modell</b>
Verantwortlichkeiten für das Testkonzept	52.210.5	PHb_7.2
Ziele der jeweiligen Tests	52.209.2	QPl_2.1

Detaillierte Festlegung d. Testmethoden je nach Phase des Entwicklungslebenszyklus und Implementierungstiefe (z.B. Modultests, white - box, grey - box, black - box - Tests)	52.209.2	QPL3, PrSpez_3
Festlegung der jeweiligen Testkriterien, erwartete Ergebnisse (Testabbruch, Testwiederholung, Akzeptanzbereiche)	52.209.2	PrSpez_4
Definition der Testumgebung (Definition der geplanten Testwerkzeuge)	–	PrPl_5.1
Review des Testkonzeptes	–	PrPl_2
(Unerwartete Ergebnisse / Neue Risiken)	–	
Zu berücksichtigen ist: 1.Fehler, Alarme und Risiken 2. Grenzwerte. Fehlerwerte 3. Zeitliche Grenzen 4. Tests spezieller Algorithmen 5. Belastungstests 6. Umgebungstests in Abhängigkeit von der Konfiguration 7.Schnittstellentests 8. Speichertests 9. Test von Fremdsoftware 10. Feldversuche	–	PrSpez_3

Tabelle 5.9: Zuordnungstabelle Testkonzept

Die „Verantwortlichkeiten für das Testkonzept“ werden nach V-Modell im Projekthandbuch (PHb\_7.2) eingetragen. Die Festlegung betrachtet hierbei verschiedene Rollen, es erfolgt keine personelle Zuordnung.

Die „Ziele der jeweiligen Tests“ werden in QPL2.1 festgelegt. Ein Festlegung der Testmethoden entsprechend der Phasen des Entwicklungszyklus erfolgt in PrSpez\_3. Hier wurde zusätzlich noch eine Einstufung nach der Kritikalität entsprechend QPL3.2 (dem analytischen Teil der Kritikalitäten/Methoden Matrix des Handbuch SI) eingefügt. Die „Festlegung der jeweiligen Testkriterien, erwartete Ergebnisse“ werden PrSpez\_4 entnommen. Es wird weiterhin die Testumgebung (PrPl\_4) festgelegt und Anforderungen an den Review des Testkonzeptes gestellt (PrPl\_2). Weiterhin werden Maßnahmen definiert, falls die

Testkriterien nicht erfüllt werden („Unerwartete Ergebnisse/Neue Risiken“).

### 5.3.6 Risikomanagement

Wie in Kapitel 3.1.4 beschrieben, wird im Rahmen der Qualitätssicherung ein phasenübergreifender Prozeß – der Risikomanagement-Prozeß – durch die Norm EN60601-1-4 definiert.

Die aus Sicht der Qualitätssicherung definierten Tests haben das Ziel, die Zuverlässigkeit des Produktes zu erhöhen. Im Gegensatz dazu versucht das Risikomanagement alle vernünftigerweise vorhersehbaren Risiken zu beherrschen. Hintergrund hierfür ist die Annahme, daß es prinzipiell nicht möglich ist, ein vollständig sicheres System zu erstellen.

Im V-Modell wird die Behandlung kritischer Funktionen im Handbuch SI (siehe Kapitel 4.6) geregelt. Für die Risikoanalyse, wird eine Kritikalitäten/Funktionen-Matrix vorgeschlagen, die den Funktionseinheiten, unter Beachtung der Vererbungsregeln R1 und R2, in den Aktivitäten SE 1 bis SE 4-SW Kritikalitäten zuordnet<sup>23</sup>

Die Festlegung der Kritikalität nach EN60601-1-4 wird nach dem unter Kapitel 3.1.4 vorgestelltem Verfahren (vgl. Abbildung 3.5) durchgeführt. Als Kritikalität wird das von der Funktionseinheit ausgehende Risiko für den Patienten, Anwender oder Dritte betrachtet, das entsprechend der Definition in Schadensausmaß und Schadenshäufigkeit eingeteilt wird. In Handbuch SI wird hierfür eine Skala „niedrig“, „mittel“ und „hoch“ angesetzt<sup>24</sup>, diese ist vergleichbar mit den in Kapitel 3.1.4 definierten Regionen „akzeptiert“, „ALARP“ und „nicht akzeptiert“. Die Festlegung wird in QPL3.1 definiert, wobei für Medizinprodukte eine Aufteilung der Kritikalität in Auftretenswahrscheinlichkeit und Schadenshäufigkeit vorzunehmen ist.

Würde man in der Kritikalitäten/Methoden-Matrix als Methode das „Prinzip der integrierten Sicherheit“ (siehe Abbildung 3.7) verwenden, könnte der Prozeß des Risikomanagements durch Umsetzung des Handbuchs SI nachgestellt werden. Als Qualitätsziel würde man in QPL2.1 u.a. die „Beherrschung aller risikobehafteten Funktionen“ definieren.

Mit entsprechendem Aufwand wäre es möglich eine Zuordnung zwischen den einzelnen Punkten der Risikoanalyse und des Handbuchs SI bzw. Submodells QS festzulegen. Allerdings wäre es aufgrund der allgemein gehaltenen Festlegungen des Handbuchs SI und Submodells QS nötig, zusätzlich Aktivitäten zu definieren, die eine problemlose Umsetzung ermöglichen, was den Rahmen dieser Arbeit sprengen würde. Erschwerend kommt hinzu, daß die Anforderungen an die Dokumentation in der von der Norm geforderten Art und Weise nicht im V-Modell erstellt wird.

Tabelle 5.10 zeigt die Zuordnung zu den Checklistenpunkten. Falls keine eindeutige Zuordnung möglich war, wurde keine Zuordnung anzugeben und das Feld freigelassen. Die Checkliste ist in drei Bereiche unterteilt: dem „Risikomanagement-Plan“, dem „Risikomanagement-Prozeß“ und der „Risikomanagement-Zusammenfassung“. Die Bereiche sind in der Tabelle durch vorangestellte Überschriften unterteilt.

---

<sup>23</sup>Anmerkung: EN1441 definiert hierfür einen Fragenkatalog und verweist alternativ auf Methoden wie die Fehlerbaumanalyse (FTA) oder FMEA (vgl. Kapitel 3.1.5).

<sup>24</sup>Die Einteilung wurde nur als Beispiel gewählt und ist auf das jeweilige Projekt abzustimmen

Anforderung	Anforderung EN60601-1-4	Anforderung V-Modell
<b>Risiko-Management-Plan (RMM Plan)</b>	52.202.1 52.210.2	
Geltungsbereich	52.202 a)	
Entwicklungs-Lebenszyklus	52.202 b)	V-Modell
Verantwortung des Managements (ISO 9001, 4.1)	52.202 c)	PHb_7.1, PHb_7.2
Risiko- Management- Prozess Planung	52.202 d) 52.204.3.1.1 52.204.3.2.3 etc.	
Anforderungen für Reviews	52.202 e) 52.210.5 52.202.3 (2)	PrPl_2
Änderungen der RA Konfigurationsmanagement der RA	52.202.3	KPl_3.1
<b>Risiko- Management- Prozess (RA)</b>	52.204.1	
Kriterien für die Risikoeinstufung: a) Schadensausmaß, b) Schadenshäufigkeit c) Risikograph und Akzeptanzbereiche	52.201.3 b) 52.204.3.2.1 52.204.3.2.2 52.204.3.2.4 52.204.4.2	QPl_3.1
Gefährdungsanalyse	52.204.1 a) 52.201.3 a) 52.204.3.1 52.204.3.1.2 52.204.3.1.3 52.204.3.1.10	Kritikalitäten/Funktionen-Matrix
Risiko-Abschätzung	52.204.3.2.1 52.204.3.1.6 e)	Kritikalitäten/Funktionen-Matrix
Risiko-Beherrschung	52.204.1 b) 52.201.3 e) 52.204.1 52.204.4.1	Kritikalitäten/Methoden-Matrix
Beurteilung der Wirksamkeit der Risiko-Beherrschung	52.201.3 d) 52.209.1 52.204.3.1.9	

Anforderung	Anforderung EN60601-1-4	Anforderung V-Modell
Methoden zur RA je nach Fortschritt des Entwicklungslebenszyklus	52.204.3.1.7 52.204.3.1.8	
<b>Risiko-Management-Zusammenfassung (RMM-Report)</b>		
Gefährdungen / Ursachen	6.8.201	Kritikalitäten/Funktionen-Matrix
Risikoabschätzung und Beurteilung der Effektivität der Methoden zur Risikoanalyse je nach Phase der Entw.	52.204.3.2.5 52.204.4.6	
Maßnahmen bzw. risikobezogene Anforderungen	52.201.3 c)	
Risiko-Beherrschung	52.204.4.1 52.210.6 52.204.3.1.10 52.209.3	
Dokumentation der Restrisiken in der Risikomanagementzusammenfassung und in der Gebrauchsanweisung, so wie eine Liste der Fehlermeldungen und Warnhinweise	6.8.201 52.204.3.1.6 c) 52.204.4.5	
Verifizierung des RMM Plans. Review der. Einhaltung des Entwicklungslebenszyklus	52.201.3 c) 52.202.3 52.203.5 52.204.2 52.212.1	
Qualifikation des Personals	52.205	Rollenkonzept, PHb.7.1
Abschließende Bemerkung über die Vollständigkeit und den Abschluss der Softwarevalidierung und Freigabe der Software	52.210.6 52.210.1	

Tabelle 5.10: Zuordnungstabelle Risikomanagement

## 5.4 Bewertung

Das V-Modell stellt aufgrund der stark risikoorientierten Vorgehensweise<sup>25</sup> in vielerlei Hinsicht eine gute Ausgangsbasis für die Entwicklung richtlinienkonformer Software dar. Bei

<sup>25</sup>vgl. [CH99]

Anwendung des V-Modells als Vorgehensmodell werden automatisch die Anforderungen der Zertifizierungsstelle im Hinblick auf das Projektmanagement, das Konfigurationsmanagement, die Qualitätssicherung und die Systemerstellung erfüllt. Hierbei stellen die Anforderungen des V-Modells eher eine obere denn eine untere Schranke dar, so daß an manchen Stellen nicht jede Aktivität bis ins kleinste Detail ausformuliert in den Zertifizierungsprozeß einfließen sollte. Allerdings ist hervorzuheben, daß die Anforderungen an die Dokumentation von Seiten der Normen und Guidelines stetig steigen<sup>26</sup>.

Die Vorgaben des Handbuch SI sind zudem eine gute Grundlage für das Risikomanagement, so daß gezeigt ist, daß auch dieser Prozeß sich in das Vorgehensmodell integrieren läßt. Wie in Kapitel 3.1.4 gezeigt, stellen die Normen hier viel detailliertere Anforderungen. Den Anforderungen liegen meist informelle Lösungsansätze bei, die aufgrund der großen Verbreitung einen allgemeinen Zuspruch gefunden haben. Beispielsweise ist der Risikomanagement-Prozeß in Abbildung 3.7 Teil des informativen Anhangs der EN60601-1-4. Bei der Umsetzung des Risikomanagements sollte also ruhig nach diesen Vorschlägen vorgegangen werden. Immerhin sind diese Verfahren auch den Zertifizierungsstellen bestens bekannt, wodurch sich eine Zeit- und Kostenersparnis ableiten läßt. Gegen die Anwendung des V-Modells für den Bereich Risikomanagement spricht zudem, daß die Anforderungen sehr allgemein gehalten sind. Für die Umsetzung bedeutet dies, daß man zusätzliche Anforderungen beachten muß, die man allerdings letztendlich nicht direkt verwerten kann, da die Vorgaben der Norm und nicht die des V-Modells zu erfüllen sind.

Abhilfe könnte hierbei eine Erweiterung des V-Modells schaffen, indem man die Anforderungen der Norm in ein Handbuch einarbeitet. So könnte man zusätzliche Aktivitäten beschreiben, die Dokumentation entsprechend der normativen Forderungen definieren und zusätzliche Aspekte wie die Ursachen- und Gefährdungsanalyse direkter ansprechen (in der jetzigen Regelung ergaben sich diese vollständig aus der Norm).

Wie bereits im Kapitel 5.3.3 erklärt, gehen die Änderungsregelungen des Konfigurationsmanagements über die des V-Modells hinaus. Von Seiten des Gesetzgebers wird hier ein zusätzlicher Prozeß definiert, der die Sperrung und Freigabe des Produktes im Falle eines Vorkommnisses beschreibt. Jede Änderung muß im Zusammenhang mit einem Vorkommnis, nachdem die Gefährdung gemindert und beherrschbar gemacht wurde, erneut validiert werden. Der Prozeß der Änderung nach Auslieferung des Produktes wird im V-Modell durch die „Software-Pflege und -Änderung (SWPÄ)“ geregelt. Für Medizinprodukte gilt generell, daß deren Lebenszyklus nicht nach Auslieferung des Produktes endet. Deshalb müßten nach V-Modell alle Medizinprodukte die Durchführungsbedingung der „erhöhten Wartbarkeitsanforderung“ während des Tailorings mit einbeziehen, deren Regelung (SWPÄ) sehr allgemein gehalten sind.

In Bezug auf das Tailoring ist zu beachten, daß der Einbezug der Aktivität KM 2.4 „Konfiguration fortschreiben“ die Aktivitäten KM 3 „Änderungsmanagement (Konfigurationssteuerung)“ nach sich zieht (diese werden in Tabelle T.16<sup>27</sup> als „nicht erforderlich“ markiert). Außerdem ist die Umsetzung der Aktivität KM 3 für das Konfigurationsmanagement anzuwenden.

---

<sup>26</sup>vgl. Anforderungen FDA in Kapitel 3.2

<sup>27</sup>Handbuch „Tailoring und projektspezifisches V-Modell“

Weiterhin stellt sich die Frage, weshalb nicht die Aktivität SE 2.2 „Wirksamkeitsuntersuchung durchführen“ als zusätzliche Anforderung einer erhöhten „Kritikalität“ mit einbezogen wurde. Aus Sicht der Medizinprodukte könnte diese Aktivität dazu benutzt werden, um die verschiedenen Lösungsvorschläge gegeneinander im Bezug auf die Sicherheit zu beurteilen<sup>28</sup>.

Das V-Modell ist generell für die Entwicklung von Medizinprodukten nicht lebensgerecht. Beispielsweise basierten die Definitionen des Alarmalgorithmus im Beispielprojekt auf einer visuellen Beurteilung, deren mathematische Definition zudem zirkulär ist (vgl. [Gol00] Kapitel 6.4). Um dieses Risiko in den Griff zu bekommen, wurden vorab Prototypen erstellt, anhand deren, zusammen mit Experten, eine Lösung erarbeitet wurde.

Als Vorgehensmodell würde sich meiner Meinung nach, beispielsweise eine Mischform aus Spiralmodell und V-Modell besser eignen, indem vorab die Risiken über das Spiralmodell ausgewertet werden und anschließend die Entwicklung über das V-Modell durchgeführt werden könnte.

---

<sup>28</sup>Die entsprechende Regelung hierfür wird in Aktivität SE 2.1 getroffen.



# Kapitel 6

## Unterstützung konformer Entwicklung durch LabVIEW

In diesem Kapitel werden die von LabVIEW angebotenen Werkzeuge zur Unterstützung eines qualitativen Entwicklungsprozesses auf ihre Tauglichkeit untersucht. Der erste Abschnitt stellt die wesentlichen Eigenschaften von LabVIEW vor. In Unterpunkt 2 wird das Metrik Tool - ein Werkzeug um Softwaremetriken in „Bildercode“ (sogenannten Programmiersprachen der 4. Generation) zu ermöglichen - vorgestellt. Unterpunkt 3 stellt die Einbindung von Source Code Control Systemen vor und Unterpunkt 4 die Möglichkeit des Dokumentationstools. In Unterpunkt 5 wird eine von National Instruments vorgeschlagene Entwicklungsstrategie vorgestellt. Das Kapitel wird durch eine Zusammenfassung abgeschlossen.

### 6.1 Was ist LabVIEW

LabVIEW ist eine von National Instruments Ende der achtziger Jahre entwickelte graphische Programmiersprache. In LabVIEW werden Programme grafisch datenflußorientiert mit Hilfe von Ikonen und „Wires“ programmiert. Ein solches Programm nennt man „Virtuelles Instrument“ (VI), woraus sich auf die Herkunft schließen läßt: Labore mit Mess-, Steuer- und Regelinstrumenten. Ein VI besteht aus einem sogenannten „Front Panel“ und einem „Diagramm“. Das „Front Panel“ (siehe Abbildung 6.2) ist die Schnittstelle des Programms mit dem Benutzer. LabVIEW stellt hierfür einen umfangreichen Satz an Elementen (Schalter, Graphen, Listen, ... ) bereit, der sich zusätzlich noch erweitern läßt. Der eigentliche Quellcode ist das „Diagramm“ (siehe Abbildung 6.1). Dieses besteht aus mehreren Blockdiagrammkomponenten (Strukturen, Operatoren, VIs, ..) , die über Wires miteinander verbunden sind. Jede Blockkomponente wird durch ein Ikon visualisiert, das eine Anzahl von „Terminals“ - das sind die eigentlichen Kommunikationspunkte, die Quellen oder Senken sein können - beinhaltet. Der Datenfluß von der Quelle zur Senke wird durch „Wires“ festgelegt. Jedes virtuelle Instrument ist ein ablauffähiges Programm, das sich einzeln testen läßt. Dieses strukturierte Verfahren führt schnell zu einer sicheren Beherrschung auch komplexer Applikationen. Das Einsatzgebiet wurde seit Beginn der Einführung stark

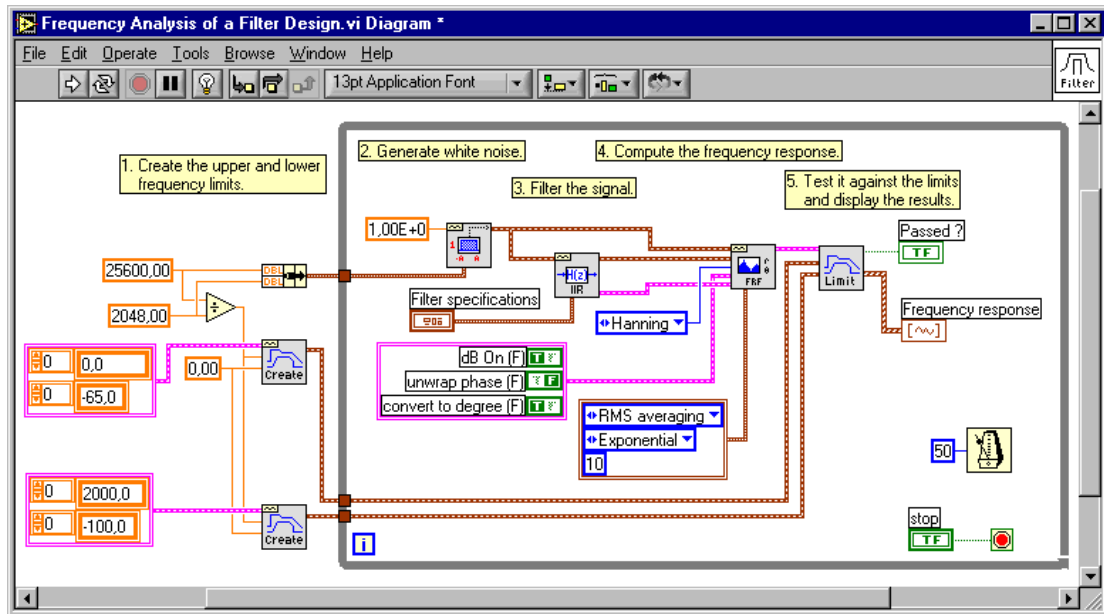


Abbildung 6.1: LabVIEW Diagramm

erweitert, so daß LabVIEW heute in der Medizintechnik, Physik, Bildverarbeitung, Kommunikationstechnik oder Signalanalyse eingesetzt wird. Weitere Bereiche werden durch Toolkits erschlossen. Das sind Erweiterungspakete, die nicht im Standardumfang von LabVIEW enthalten sind (z.B. DB-Anbindung, ...). Nebenbei sollte vielleicht erwähnt werden, daß LabVIEW Programme seit vielen Jahren plattformunabhängig<sup>1</sup> auf Windows, Macintosh, Solaris, HP-UX und neuerdings sogar Linux ausgeführt werden können.

Dieses Kapitel gibt einen Überblick über die in LabVIEW Professional integrierten Tools - das VI Metrik Tool, das Source Code Control und das Documentation Tool.

## 6.2 Das VI Metrik Tool

Die am häufigsten verwendete Maßeinheit zur Messung von Software-Komplexität ist Source Lines of Code (LOC). Dies läßt sich darauf zurückführen, daß diese Metrik sehr einfach zu bestimmen ist. Zwar können in LabVIEW keine LOC gemessen werden, dafür kann hier die Metrik „number of nodes“ gemessen werden. Als „node“ werden alle Blockdiagrammkomponenten mit Ausnahme von Beschriftungen und Graphiken bezeichnet. Insbesondere sind das Funktionen, VIs und Strukturen (z.B. Schleifen und Sequenzen).

Der Einsatz dieser Methode erfolgt typischerweise für Schätzungen zukünftiger Projekte. Um diese Methode optimal zu nutzen, empfiehlt es sich, eine „Wissensbasis“ der vergangenen und zukünftigen Projekte anzulegen. Aufbauend auf dieser, können Schätzungen über die „number of nodes“ des neuen Projektes vorgenommen werden. Für größere Projekte muß hierfür zuerst eine Zerlegung des Projektes in Teilprojekte vorgenommen werden,

<sup>1</sup>Mit Einschränkung auf Plattformspezifischen Technologien wie ActivX

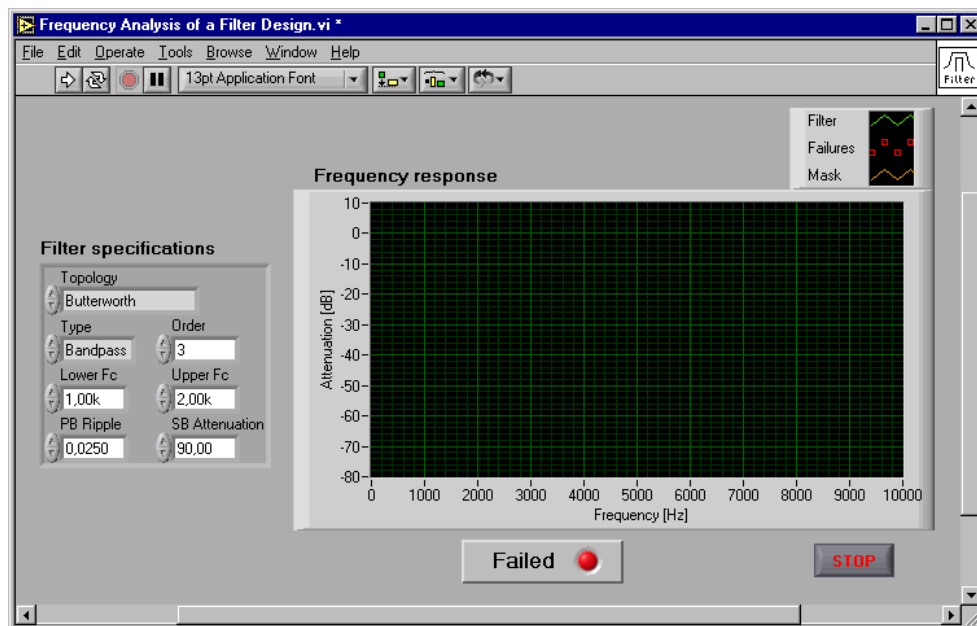


Abbildung 6.2: LabVIEW Front Panel

die dann mit bereits durchgeführten Aufgaben vergangener Projekte verglichen werden können.

Für die Metrik „number of nodes“ gilt dieselbe Problematik wie für LOC. Diese wurde in der Literatur bereits ausführlich diskutiert und kann beispielsweise unter [pro98] nachgelesen werden.

Das VI Metrik Tool stellt neben den „number of nodes“ noch weitere Statistiken bereit. Im einzelnen sind das: die Anzahl Strukturen, die Anzahl der Blockdiagramme incl. Subdiagramme (z.B. der Schleifen, Sequenzen,..), die maximale Blockdiagrammtiefe, die Diagrammweite und Höhe (in Pixel), Anzahl der „wire“ Quellen, die Anzahl der Control- und Indicatorelemente des Front Panels, die Anzahl der lesenden und schreibenden Zugriffe (Bezug ist die Eigenschaft des Elements) auf ein Oberflächenelement, globale/lokale Lese- und Schreibverbindungen, Anzahl Code Interface Nodes (CINs), shared lib Aufrufe, Anzahl der eingehenden und ausgehenden Terminals am Connector Block des VI's. In Abhängigkeit des Projekts kann eines (oder mehrere) dieser Maße eine sinnvolle Ergänzung sein.

## 6.3 Source Code Control

Die Professional Version von LabVIEW ist mit einem in die Entwicklungsumgebung integrierten Source Code Control (SCC) System ausgestattet. Losgelöst von der Benutzerschnittstelle werden drei verschiedene SCC-Systeme zur Unterstützung des Konfigurationsmanagements unterstützt. Zum einen kann ein plattformunabhängiges integriertes (Built-In) SCC-System verwendet werden, zum anderen bietet LabVIEW für die Windows Plattformen eine Schnittstelle zu *Microsoft<sup>TM</sup> Visual SourceSafe* und für die Solaris Plattform

zu Rational ClearCase. Alle drei Systeme erfüllen die Anforderungen eines Konfigurationsmanagements. Das Built-In SCC-System hat gegenüber den beiden anderen Produkten den Vorteil, daß keine zusätzlichen Lizenzkosten durch den Erwerb entstehen. Andererseits bieten externe Systeme einen höheren Sicherheitsstandard als das Built-In System, dessen Sicherheit sich auf das Dateisystem stützt (Anforderung Zugriffskontrolle im KM Plan). Ein weiterer Nachteil des Built-In Systems ist, daß dieses die Dateien nicht komprimiert oder als Differenzen speichern kann. Mit allen drei Systemen ist es möglich VIs zu Projektgruppen zusammenzufassen, wodurch sich der Projektverlauf (vgl. FDA Anforderung „Revision History“) sehr einfach für die einzelnen Module erzeugen läßt<sup>2</sup>.

## 6.4 Documentation Tool

Die Dokumentation von Software läßt sich grundsätzlich in zwei Kategorien einteilen: Dokumentation, die im Entwicklungsprozeß anfällt und Benutzerdokumentation. Beide unterscheiden sich aufgrund der unterschiedlichen Zielgruppe wesentlich voneinander. Die Dokumentation des Entwicklungsprozesses zielt im wesentlichen auf Personen im Projekt (Entwickler, Tester, ..), die Anwenderdokumentation spricht den reinen Endbenutzer an.

Der Dokumentationsprozeß sowohl von Entwicklungsprozeß als auch Benutzerdokumentation wird in LabVIEW durch das Dokumentation Tool<sup>3</sup> unterstützt. Diese kann zur Erstellung einer Online Dokumentation im HTML Format oder für Hilfedateien im RTF Format (aus dieser wird über einen Hilfe Compiler die eigentliche Hilfedatei erzeugt) benutzt werden. Über ein Interface kann der Detaillierungsgrad gewählt werden, wobei entweder aus einer Liste vordefinierter „Dokumentationsprofile“ gewählt oder ein individuelles Profil erstellt werden kann. Als Auswahlmöglichkeiten stellen sich „Front Panel“, „Block Diagramm“, „Connector Pane“, „VI Beschreibung“, „Controls und Indikatoren“, Dateinamen und -pfade sowie eine Liste aller aufgerufenen SubVI's bzw. deren Dokumentation. Obwohl in LabVIEW jedes Element dokumentiert werden kann, ist es bisher nicht möglich, die Beschreibungstexte der Diagrammkomponenten in die Dokumentation einfließen zu lassen. Alternativ kann man allerdings die Beschreibung als Textlabel in das Diagramm einfügen, welches wiederum in die Dokumentation eingebunden werden kann. Der folgende Abschnitt erläutert die Unterstützung für die Erstellung der Implementierungs- und Benutzerdokumentation.

Die Entwickler-Dokumentation sollte zum einen die von dem jeweiligen VI erfüllte Aufgabe in der VI Beschreibung eingetragen und zum anderen die Schnittstellenelemente mit einer kurzen Beschreibung dokumentiert werden. Die Dokumentation kann dann durch Auswahl des Dokumentationsprofils „Using as a SubVI“ erstellt werden. Der Vorteil hierbei ist, daß die Dokumentation strukturell an die Hilfe von LabVIEW angepaßt ist und sich die Zielgruppe „LabVIEW Programmierer“ damit schnell zurechtfinden. Das Documentation Tool eignet sich ebenfalls zur Erstellung einer Anwendungsdokumentation. Hierfür wird für alle VIs, deren „Front Panel“ zur Interaktion mit dem Benutzer eingesetzt wird (sogenannte „top level VIs“), eine Beschreibung beigefügt. Das Dokumentationsprofil „Using the panel“

---

<sup>2</sup>In LabVIEW werden alle Funktionen (VIs) in separaten Dateien gespeichert.

<sup>3</sup>ab Version 6i ist dieses in die Print Funktion integriert

erstellt dann die Benutzerdokumentation.

## 6.5 Entwicklungsstrategie

Neben den Tools gibt National Instruments auch einen sehr interessanten Ansatz vor, wie LabVIEW bereits während der Entwurfsphase zur Unterstützung des Entwicklungsprozesses eingesetzt werden kann. Hierbei wird auf Basis der Anforderungen, die vorab bestimmt werden müssen, eine grobe Systemstruktur entworfen, die durch eine Zerlegung in die benötigten Funktionsblöcke bestimmt ist<sup>4</sup>. Nach der Zerlegung der obersten Ebene können die gefundenen Funktionalitätsblöcke als „Stub VIs“ auf dem Diagramm des „top level“ VIs erzeugt werden. Für jeden „Stub“ werden die ermittelten Ein- und Ausgänge erzeugt und die Funktionalität der VIs sowie der Ein- und Ausgänge dokumentiert. Nach jeder Verfeinerungsstufe sollte man die benötigten Informationen bestimmen und falls nötig durch hinzufügen neuer Verbindungen ergänzen. Das Ziel ist, die einzelnen Aufgaben soweit herunter zu brechen, daß diese in handhabbaren Teilen vorliegen und bearbeitet werden können (work breakdown structur). Die Gefahr dieses Verfahrens ist, daß man sich zu schnell in die Implementierungsphase begibt bzw. blockweise vorgegangen wird.

## 6.6 Zusammenfassung

LabVIEW bietet bereits in der Grundvariante gute Unterstützung für den Einbezug qualitativer Maßnahmen in den Entwicklungsprozeß. Hierbei macht man sich unter anderem die bessere Lesbarkeit der graphischen Sprache zu Nutze. Von Seiten National Instruments wird LabVIEW sogar für den Entwurf der Programme vorgeschlagen. Falls sich das Programm in voneinander unabhängige Funktionsblöcke zerlegen läßt, können mehrere Programmierer auch ohne Source Code Control System gleichzeitig an einem Entwurf bzw. einer Implementierung arbeiten.

Neben den Entwurfsphasen werden auch die abschließenden Testphasen unterstützt. Das integrierte Debugging Tool unterstützt Black- Grey- und White-Box Tests. Das Einbinden von Testtreibern ist ebenfalls problemlos möglich. Für Performance-Messungen ist ein Profiling Tool in die Entwicklungsumgebung integriert.

LabVIEW bietet neben der Entwicklungsumgebung in der Professional Version zusätzliche Tools, die das Projekt- und Konfigurationsmanagement unterstützen und vereinfachen. Zudem kann der Dokumentationsaufwand verringert werden. Allerdings ist für Medizinprodukte die erstellte Dokumentation i.a. nicht ausreichend, da insbesondere bei der Gebrauchsanweisung darauf zu achten ist, daß alle ermittelten Gefährdungen ausreichend dokumentiert und für den Benutzer übersichtlich und klar strukturiert dargestellt werden. Für diese Aufgabe empfiehlt sich der Einsatz eines Textverarbeitungsprogramms.

---

<sup>4</sup>Dies entspricht einem „top down“, was für die meisten Anwendungsfälle empfohlen wird. Sonderfälle wie Gerätetreiber lassen sich nach [pro98] leichter „bottom up“ entwickeln



# Kapitel 7

## Zusammenfassung

Ausgangspunkt für diese Arbeit ist ein im Rahmen des Projekts „Online Monitoring“ des Sonderforschungsbereichs 386 „Statistische Analyse diskreter Strukturen“ entwickelter Softwareprototyp „Trium CTG Online“, das eine online-Datenerfassung samt Alarmgenerierung und Browser-fähiger Visualisierung für Kardiotokogramme bietet. Die Software wurde unter Leitung von Herrn Dr. Martin Daumer zusammen mit Herrn Dimitri Golias im Rahmen einer Diplomarbeit nahezu ausschließlich mit der graphischen Programmiersprache „LabVIEW“ von National Instruments entwickelt.

In dieser Arbeit wird an diesem konkreten Beispiel vorgeführt, welche gesetzlichen Anforderungen für die Erstellung von Medizinprodukten inklusive Software durch das Medizinproduktegesetz (MPG) erfüllt werden müssen. Für die Inverkehrbringung muß ein Konformitätsbewertungsverfahren durchgeführt werden, um zu zeigen, daß das Medizinprodukt die grundlegenden Anforderungen des MPGs erfüllt.

Für die Erfüllung der Anforderungen muß ein Risikomanagementprozeß nach DIN EN 60601-1-4 durchgeführt werden. Das Risikomanagement stellt einen phasenübergreifenden Prozeß dar, der aus Risikoanalyse, Risikobewertung und Risikobeherrschung besteht. Der Gesamtprozeß wird auf einen, vom Hersteller wählbaren, Software-Entwicklungslebenszyklus angewendet. Es wurde gezeigt, daß das V-Modell aufgrund der risikoorientierten Vorgehensweise einen geeigneten Software-Entwicklungslebenszyklus für diesen Prozeß darstellt. Die Zuordnungslisten zeigen die Rahmenpunkte für die Zertifizierung medizinischer Software.

Die Anwendbarkeit des V-Modell als Vorgehensmodell für die MPG-konforme Erstellung von Medizinprodukten ist - bei all seinen Stärken hinsichtlich eines kontrollierten, zertifizierbaren Prozesses - vor allem hinsichtlich zweier Aspekte eingeschränkt. Einmal sind dies die bekannten Schwächen des V-Modells in den dem eigentlichen Entwicklungsprozess vor- und nachgelagerten Phasen (z.B. Prototyping und Pflege und Änderung); vor allem letztere spielen bei Medizinprodukten jedoch eine wichtige Rolle. Weiterhin weist das V-Modell Defizite bei der Umsetzung des Riskiomanagements auf:

Zwar bietet das V-Modell geeignete Schnittstellen für den Risikomanagementprozeß (Handbuch SI), doch sollte man besser eine Umsetzung der Vorgaben nach EN 60601-1-4 anstreben, da die Anforderungen von Seiten des V-Modells zu allgemein sind. Für einen vernünft-

tigen Einsatz des V-Modells als Risikomanagement für Medizinprodukte, sollten die Anforderungen der Norm in ein Handbuch eingearbeitet werden oder alternativ die Norm als Grundlage benutzt werden. Da die Norm selbst auch nur Anforderungen stellt, scheint es sinnvoller, diese in ein Handbuch auszulagern, da somit insbesondere auch Aktivitäten und Checklisten mit in den Prozeß einfließen könnten.

Neben den Entwicklungsprozessen wurde auch gezeigt, daß die Entwicklungsumgebung mithilfe einer Zahl brauchbarer Werkzeuge die die Erstellung richtlinienkonformer Software unterstützen.

Angefangen bei der strukturierten Programmierung, die jedem LabVIEW Programm zugrunde liegt, wird das qualitative Entwickeln durch Werkzeuge wie das Metrik Tool, das Source Code Control System und das Dokumentations-Tool unterstützt.

Begleitend zu dieser Diplomarbeit konnte die Software an vielen Stellen überarbeitet werden sowie mit Unterstützung der Firma „Eurocat“ wichtige Teile des Zertifizierungsprozesses für das Medizinprodukt „Trium CTG Online“ durchlaufen werden. Die Zertifizierung des gesamten Systems soll demnächst durchgeführt werden.

# Anhang A

## Risikoanalyse Plan

### A.1 Zweck und Geltungsbereich

Dieses Dokument beinhaltet die Feststellung der Risiken, deren Bewertung, und die Festlegung der Maßnahmen die zur Risikominderung umgesetzt werden sollen.

### A.2 Kriterien für die Risikoeinstufung

#### A.2.1 Schadensausmaß

Beschreibung	Abkürzung	Kriterien	Beispiel
Unwesentlich	Unwes.	Kurzzeitiges Unwohlsein	Mattigkeit, Konzentrationsstörungen
Geringfügig	Gering.	Vorübergehende Beeinträchtigung der Gesundheit in Form von kurzzeitiger Überbeanspruchung	starke Mattigkeit, starke Müdigkeit, starkes Durstgefühl
Kritisch	Krit.	Dauerhafte Beeinträchtigung der Gesundheit	Herzstörungen (operativer Eingriff nötig)
Katastrophal	Katast.	Schwere Schäden oder Tod	Behinderung des Ungeborenen; Unfruchtbarkeit der Patientin

### A.2.2 Schadenshäufigkeit

Hinweis: Bei der Abschätzung der Schadenshäufigkeit ist zu berücksichtigen wie viele Produkte in Verkehr gebracht werden sollen (geplanter Absatz in der Produktlebenszeit)! Als Kriterien für die Einteilung wird die Anzahl Patientinnen herangezogen (1 Anwendung = 1 Patientin). Implizit wird somit die Laufzeit, die Anzahl der Betten und Kopien mitbewertet.

Beschreibung	Abkürzung	Kriterien	Beispiel
Unvorstellbar	Unvor.	1 mal bei 1000000 Anwendungen	Höhere Gewalt
Unwahrscheinlich	Unwahr.	1 mal bei 10000 Anwendungen	Fehler in Standard Algorithmen
Entfernt vorstellbar	Entf.	1 mal bei 1000 Anwendungen	Fehler in den Berechnungsroutinen, Datenübertragungsfehler
Gelegentlich möglich	Gel.	1 mal bei 100 Anwendungen	Missachtung von Warnhinweisen, Bedienfehler
Wahrscheinlich	Wahr.	1 mal bei 10 Anwendungen	Eingabefehler, Ablesefehler, falsche Einheiten ausgewählt
Häufig	häuf.	1 mal bei 5 Anwendungen	

### A.2.3 Risikograph und Akzeptanzbereiche

häuf.		1		
Wahr.				
Gel.		6	2	
Entf.	1	4	10	2
Unwahr		3		3
Unvor.				
	Unwes	Gering	Krit	Katastr

## A.2.4 Akzeptanzkriterien und Zielsetzungen für die Risikominderung

### A.2.4.1 Risiken vor Umsetzung der Risikomindernden Maßnahmen

1. Einfrieren des Bildschirms am Serverhost
2. Unterbrechung der Netzverbindung
3. Ausfall CTG Auslesegerät / CTG Gerät
4. Ausfall *Trium CTG Online*
5. Berechnungsfehler (Fehler im Algorithmus für FIGO Berechnung)
6. Signalausfall am CTG Auslesegerät
7. Verzögerungen zwischen Aufnahme und Visualisierung
8. Verfälschte Darstellung der Anzeige im Browser
9. Archivierung der Daten schlägt fehl
10. Ausfall Signalanzeige
11. Datenverfälschung
12. Zuordnungsfehler (Patientin ↔ Bett)
13. Bett wird innerhalb der „Warteperiode“ erneut belegt
14. Zugang zum System nicht möglich
15. nicht konforme Schnittstellenumsetzung
16. mehr als 10 Benutzer
17. Farbenblindheit des Arztes
18. Fehlfunktion durch Firewall
19. Fehlfunktion durch Viren auf *CTG Online* Server
20. Fehler bei Signaldarstellung
21. Startkonfiguration
22. Verfahren Dokumentation
23. Räumliche Trennung
24. Aufsichtspflicht

25. Rechneruhr falsch eingestellt

Anz. Der Funktionen	Bereich
5	Nicht akzeptierbarer Bereich
19	ALARP Bereich
8	Akzeptierter Bereich

#### A.2.4.2 Risiken nach Umsetzung Risikomindernden Maßnahmen

Die Risiken nach der Umsetzung der risikomindernden Maßnahmen werden akzeptiert wenn möglichst keine Funktionen im „Nicht akzeptierbarer Bereich“ und möglichst wenige im „ALARP“ - Bereich liegen:

- Unterbrechung der Netzverbindung
- Ausfall CTG Auslesegerät / CTG Gerät
- Datenverfälschung
- Zuordnungsfehler (Patientin ↔ Bett)
- nicht konforme Schnittstellenumsetzung
- mehr als 10 Benutzer
- Startkonfiguration

Anz. Der Funktionen	Bereich
0	Nicht akzeptierbarer Bereich
10	ALARP Bereich
22	Akzeptierter Bereich

Sollten die angegebenen Grenzen nicht erreicht werden, sind zusätzliche risikomindernde Maßnahmen durchzuführen !

### A.3 Risiken

Im folgenden sind alle Gefährdungen bzw. deren Ursachen tabellarisch aufgelistet und bewertet. Sofern möglich sind in weiteren Unterabschnitten jeweils ausführliche Bewertungen vorgenommen. Weiterhin sind, falls erforderlich, die risikomindernden Maßnahmen aufgezeigt.  
en:name:signalkorrelation

### A.3.1 Hauptgefährdungen

- Erhebliche Fehlzuordnungen, welche zu einer medizinisch fehlindizierten Therapie mit potentieller Gesundheitsgefährdung der Patientin führen könnten, müssten vom Arzt aufgrund eigener Kenntnis der Krankengeschichte und/oder durch das Gespräch mit dem Patienten erkannt werden.
- Im schlimmsten Fall kann es durch eine falsche Darstellung zu einer Fehldiagnose kommen und so im schlimmsten Fall den Tod der Patientin und/oder des Föten verursachen
- In diesem Fall kann die Möglichkeit bestehen, dass der behandelnde Arzt auf Grundlage des Fehlers eine fehlerhafte Therapieentscheidung trifft und so eine Gesundheitsbeeinträchtigung der Patientin oder des Ungeborenen eintritt.
- Ein deutlich höheres Risiko stellt die zu späte Erkennung pathologischer Zustände dar, wodurch bleibende Schäden aufgrund einer Mangelversorgung oder Quetschungen die Folge sein können.

### A.3.2 Risiken die sich aus peripheren Einflüssen ergeben

Lfd. Nr. / Funktion	Gefährdung des Patienten	Ursache	Bewertung Ausmaß Häufigkeit Einstufung	Maßnahme
(1.01/12) manuelle Eingabe von Patientendaten (Info.00x)	Fehlzuordnung Bett ↔ Patientin	Fehlerhafte Eingabe/Speicherung der eingegebenen Daten	Gering Gel. ALARP	Zuordnung erfolgt anhand der Betten; Hinweise in GA
(1.02/15) Schnittstelle zwischen CTG Aufnahme und <i>Trium CTG Online</i>	Fehldiagnose	falsche Schnittstellenumsetzung	Kritisch Entf. ALARP	Anforderungsspezifikation und Designspezifikation beschreiben Schnittstelle; Aufnahmegerät muß diese Schnittstelle erfüllen
(1.03/13) Folgebelegung desselben Bettes innerhalb 10 Durchläufen	Fehlzuordnung Fehldiagnose	Randbedingung nicht erfüllt	Gering, Entf. Akz.	Hinweise in GA

Lfd. Nr. / Funktion	Gefährdung des Patienten	Ursache	Bewertung  Ausmaß Häufigkeit Einstufung	Maßnahme
(1.04/11) Da- tenverfälschung Sicherheit	Fehldiagnose	Verfälschung Daten von außen(Fehl- konfiguration); Mutwillig durch dritte	kritisch Entf. ALARP	Authentifizierung, Verschlüsselung, Hinweise in GA
(1.04/11) Da- tenverfälschung Übertragung	Fehldiagnose	Datenverfälsch- ung durch Übertragungs- fehler	kritisch Entf. ALARP	Übertragung von Bildern; PtP Proto- koll TCP (gesicherte Übertragung)
(1.05/7,8) Leistungsanfor- derung	Fehldiagnose	Überlastung Netz/Server führt zu verzöger- ter/unvollständi- ger/gestörter Anzeige	Gering gel. ALARP	Hinweise in GA; Übertragung von Bildern macht Punktstörungen unmöglich
(1.06/6) Si- gnalausfall CTG Gerät	keine Diagnose möglich;Ausfall wird u.U nicht erkannt, da 0en durch Schätz- werte ersetzt werden	Signalausfall am CTG Gerät / CTG Aus- lesegerät z.B. Transducer gelöst	katast. Entf. nicht akzeptiert	Einführung eines neuen Klassifika- tors „Signalausfall“; Designspezifikation
(1.07/9) Archi- vierung schlägt fehl	Verlust Doku- mentation	Archivverzeich- nis voll/keine Schreibrechte	gering Unwahr- scheinlich Akz.	Das System schreibt Logmeldungen, die Hinweise darauf geben; Hinweis in GA
(1.08/10) Ausfall Signal- anzeige	Fehldiagnose; Anzeige fehler- haft	löschen der Ana- lysedatei (von außen); schlim- mer: Verkürzen der Analysedatei (z.B. kopieren einer anderen Datei auf die Analssedatei)	Katast. Unwahr. ALARP	Neustart <i>Trium</i> <i>CTG Online</i> ; Verstößt gegen Definition der Schnittstelle in Anforderungsspezi- fikation; Hinweis in GA

Lfd. Nr. / Funktion	Gefährdung des Patienten	Ursache	Bewertung  Ausmaß Häufigkeit Einstufung	Maßnahme
(1.09/2,14) Netzverbin- dung	keine Diagnose möglich, kein Zugang zum System mgl	Störung Netz- verbindung	Gering Gel ALARP	Erkennung durch stehende Uhranzei- ge und Fötenbild bzw. Fehlermeldung am Bildschirm des Clientrechners (IE), vorübergehend muß Diagnose über Pa- pierstreifen des CTG Gerätes durchgeführt werden
(1.10/3)Ausfall CTG Gerät/CTG Auslesegerät	Fehldiagnose	Ausfall CTG Gerät/CTG Auslese- gerät/Verbindung CTG Auslese- gerät und <i>Trium CTG Online</i>	Kritisch Entf. ALARP	
(1.11/16) Mehr als 10 Benutzer	Fehldiagnose	Verzögerte Übertragung von Bildern	Gering Entf. Akz.	Beschränken der max. Anzahl gleich- zeitiger Zugriff auf G Web Server. Bei mehr als 10 Server Push Verb. wird die älteste terminiert. Der Benutzer erhält eine Fehlermeldung (5)

Lfd. Nr. / Funktion	Gefährdung des Patienten	Ursache	Bewertung  Ausmaß Häufigkeit Einstufung	Maßnahme
(1.12/17) Far- benblindheit des Arztes	Alarm wird nicht erkannt	Ampel unter- scheidet farblich nach Alarmen	Gering Entf. Akz.	Arzt muß anhand der unterschiedlichen Graustufen Alarmwert erken- nen. Eine örtliche Umsetzung analog einer Straßenampel wurde angedacht, wird jedoch in dieser Version nicht imple- mentiert; Hinweis in GA
(1.13/18) Fehl- funktion durch Firewall	Fehldiagnose / Einsatz nicht mgl.	Ausfiltern von Javascript be- einträchtigt Funktionalität; Funktion nicht möglich, falls HTTP nicht akzeptiert wird	Unwes. Entf. Akz.	Hinweis in GA
(1.14/19) Fehl- funktion durch Viren auf <i>CTG</i> <i>Online</i> Server	Fehldiagnose / Einsatz nicht möglich	Fehlfunktion durch Beschädi- gung der Pro- grammdateien (insb. Lab- VIEW RunTime Engine)	Gering Unwahr. Akz.	Einsatz von Vi- renscannern; keine unnötigen Program- me auf Serverrech- ner; Hinweis in GA

Lfd. Nr. / Funktion	Gefährdung des Patienten	Ursache	Bewertung  Ausmaß Häufigkeit Einstufung	Maßnahme
(1.15/21) Konfigurationsdatei nicht vorhanden	belegte Betten werden nicht angezeigt	Konfigurationsdatei nicht gefunden; Eingabe- und/oder Archivverzeichnis nicht gefunden/vorhanden bzw. nicht existierender Pfadeintrag	Kritisch Entf. ALARP	Überprüfung beim Start des Programmes. Wird die Konfigurationsdatei nicht gefunden oder kann der Parameter input- bzw. output-dir nicht gefunden werden, oder ist das angegebene Verzeichnis nicht vorhanden, wird eine Messagebox am Bildschirm angezeigt. Anschließend wird das Programm beendet.
(1.16/21) Frame 0: CopyServer2.vi, FigoServer.vi, ArgusOnline1Bed2-X.vi (0;X;7), ArgusOnline-All5.vi	Fehlzuordnung Patientin ↔ Bett	Parameter in Konfigurationsdatei nicht vorhanden oder falsch gesetzt: Anzeige von Klassifizierungswerten wird ausgeblendet, falsche Bettenbezeichnung	Gering gel. ALARP	Vernünftige default Werte; Ausschluß unvernünftiger Werte; Eintrag in Logdatei „ctgonline.log“
(1.17/9) zu (1.07) check-DirSize.vi	keine Beurteilung möglich; keine retrospektive Aussage (z.B. für rechtliche Fragen) mgl.	Kein Plattenplatz vorhanden: Aufzeichnung bzw. Archivierung kann nicht erfolgen	Kritisch Entf. ALARP	Überprüft den noch vorhandenen Plattenplatz und schreibt frühzeitig Warnungen und Alarmer in die Datei ctgonline.log; Papierstreifen!

Lfd. Nr. / Funktion	Gefährdung des Patienten	Ursache	Bewertung  Ausmaß Häufigkeit Einstufung	Maßnahme
(1.18/6) zu (1.06) Copy- Server.vi	Pathologischer Zustand wird nicht erkannt	Klassifikator Signalausfall falsch einge- stellt (Grenzen können in ct- gonline.cfg konfiguriert werden)	katast. Entf. nicht Akz.	Es wird sicherge- stellt, daß gilt: 10 < SIGNALAUSFALL- WARNUNG < 180 und SIGNALAUS- FALLWARNUNG < SIGNALAUSFALL- ALARM
(1.19/11) zu (1.04) Sicher- heit	Fehldiagnose	Unerlaubter Zu- griff dritter	kritisch Entf ALARP	Apache Proxyser- ver verschlüsselt Datenübertragung; Authentifizierung durch G Web Server
(1.20/12) Kom- mentare in das System einpfle- gen „kommen- tar.html“	Retrospektive Rekonstruktion nicht möglich	Kommentar wird falschem Bett zugeordnet (Mehrbettan- sicht), da dieses voreingestellt war	Gering gel. ALARP	Funktion setBed: Beim Laden wird Bett auf Indexwert -1 (keine Vorein- stellung) gesetzt; Funktion send: Ab- frage ob ein Bett ausgewählt wird, falls nicht, wird eine MessageBox erzeugt, die den Benutzer darauf hinweist, daß kein Bett gewählt wurde
(1.21)/22) Ver- fahren	Rekonstruktion der Aufzeich- nung nicht möglich	Es wird keine Dokumentation erstellt / Do- kumentation wird verspätet eingepflegt	Gering gel. ALARP	Es obliegt der Ver- antwortung des Arztes Daten zu dokumentieren; Wer- den Kommentare nachträglich einge- pflegt muß eine zeit- liche Korrespondenz angegeben werden um den Bezug wieder herzustellen

Lfd. Nr. / Funktion	Gefährdung des Patienten	Ursache	Bewertung  Ausmaß Häufigkeit Einstufung	Maßnahme
(1.22/23) räumliche Trennung	Pathologischer Zustand kann nicht behandelt werden	Arzt ist nicht im Haus	Kritisch häuf. N.A. <sup>1</sup>	Dieses Problem kann nicht vom System gelöst werden. Es liegt in der Verant- wortung des Arztes einen Vertreter im KH zu haben, falls dieser nicht in- nerhalb des KH ist. Wird der verantwor- tliche Arzt unterwegs alarmiert und beur- teilt das CTG als pathologisch muss er diesen erreichen und alarmieren können.
(1.23/24) Nachweis der Aufsichtspflicht	Haftung im Schadensfall	Es liegt kein Nachweis der Überwachung vor	Krit. Entf. ALARP <sup>2</sup>	Arzt kann Alarme kommentieren; Ein- träge in Logdatei zeigen ob Arzt „On- line“. Alarmierung wird typischerweise von Personal, das vor Ort ist ausgelöst.
(1.24/25) Rech- neruhr falsch eingestellt	Haftung im Schadensfall; Fehlinterpreta- tion (Annahme die Aufzeich- nung ist bereits beendet)	Abweichung der Uhrzeit in Verlauf und auf Bettenanzeige von lokaler Zeit	Gering Entf. Akz	Hinweis in GA

### A.3.3 Risiken die sich aus Internen Einflüssen ergeben:

---

<sup>1</sup>falls das System über eine Wählverbindung benutzt wird, bei Einsatz im Intranet wäre die Häufigkeit Unwahrscheinlich

<sup>2</sup>stellt keine direkte Gefährdung der Patientin dar

Lfd. Nr. / Funktion / Gefährdung z.B. [a,b,c].	Gefährdung des Patienten	Ursache	Bewertung  Ausmaß Häufigkeit Einstufung	Maßnahme
(2.01/1) Einfrieren Serverbildschirm	Fehlinterpretation - es wird nicht erkannt, daß ständig dasselbe Bild übertragen wird	Bildschirm am Server „eingefroren“	Kritisch Entf. ALARP	Animiertes Element stellt „laufenden Betrieb“ dar; Hinweise in GA
(2.02/2,4) Zugang zum System nicht möglich	keine online Diagnose möglich	Authentifizierungsfehler; Ausfall Web/Proxy Server, <i>Trium CTG Online</i> , Netzwerkverbindung	Gering Gel ALARP	Auswertung über Papierstreifen CTG Gerät; Hinweise in GA; Fehlermeldung falls Client bereits Online
(2.03/5) Umsetzung FIGO Alg	Kein Alarm bei pathologischem Zustand der Patientin	Algorithmus falsch umgesetzt	Katast Unwahr ALARP	Studie vergleicht Ergebnisse des Algorithmus mit denen von erfahrenen Gynäkologen
(2.04/4) Ausfall CTG Online	Fehldiagnose	Ausfall CTG Online	Gering Unwahr Akz.	Zugang zum System nicht möglich, falls Ausfall bei aktiver Verbindung wird Warnhinweis gegeben (siehe Ausfall Netzverbindung) bzw. stehen Uhrzeit und Fötus; Hinweise in GA

(2.05/1)zu (2.01)	Kritischer Zustand wird nicht erkannt	Bilder für den rotierenden Föten werden nicht gefunden/wurden gelöscht; Systemausfall wird u.U. nicht erkannt	Katast. Unwahr. ALARP	Beim Start wird überprüft, ob alle Bilddateien vorhanden sind, falls nicht: Eintrag in Logdatei „ctgonline.log“, es wird eine Messagebox angezeigt und anschließend das Programm beendet. Hinweis in GA
(2.06/20) readSignal- For1Bed.vi	Fehldiagnose durch verfremdete Darstellung	gleichzeitige Lese- und Schreiboperationen auf die Datenaustauschdateien	kritisch gel. nicht Akzeptiert	Operationen werden durch Semaphoren gekapselt
(2.07/20) CopyServer.vi	keine FIGO Bewertung/ Datenanzeige	Figoserver/ Einzel- und Mehrbettansicht kann Analysedatei nicht finden	Kritisch Entf. ALARP	Datenaustausch zwischen CopyServer und folgenden Modulen wird über eine Datei die in der globalen Variable CtgBed spezifiziert wird gespeichert.

## A.4 Änderungen

Wann, Wer	Was
21.11.2000 CH	Grundversion
11.12.2000 CH	Einordnung Risiken abgeglichen mit RA Report
29.12.2000 CH	Risiken 16 - 19 eingefügt und bewertet
19.01.2001 CH	Neubewertung (1.06) Gefährdung geändert (1.07) Hinweis in GA eingefügt (1.12)
4.2.2001 CH	Wartezeit (1.03) von 100 auf 10 Durchläufe verkürzt Risiken aus Grey Box Analyse mit eingefügt.



# Anhang B

## Risikoanalyse Report

### B.1 Zweck und Geltungsbereich

Dieses Dokument beinhaltet die Verifizierung der Umsetzung und Wirksamkeit der risikomindernden Maßnahmen und eine erneute Bewertung des verbleibenden Risikos.

### B.2 Kriterien für die Risikoeinstufung

(siehe Risiko Analyse Plan)

#### B.2.1 Risikograph und Akzeptanzbereiche

##### B.2.1.1 Risikograph vor Umsetzung der Risikomindernden Maßnahmen

häuf.		1		
Wahr.				
Gel.	6		2	
Entf.	1	4	10	2
Unwahr		3		3
Unvor.				
	Unwes	Gering	Krit	Katastr

### B.2.1.2 Risikograph nach Umsetzung der Risikomindernden Maßnahmen

häuf.				
Wahr.				
Gel.		2		
Entf.	1	11	5	
Unwahr		3	5	1
Unvor.			2	2
	Unwes	Gering	Krit	Katastr

## B.2.2 Akzeptanzkriterien und Zielsetzungen für die Risikominderung

### B.2.2.1 Risiken vor Umsetzung der Risikomindernden Maßnahmen

1. Einfrieren des Bildschirms am Serverhost
2. Unterbrechung der Netzverbindung
3. Ausfall CTG Auslesegerät / CTG Gerät
4. Ausfall *Trium CTG Online*
5. Berechnungsfehler (Fehler im Algorithmus für FIGO Berechnung)
6. Signalausfall am CTG Auslesegerät
7. Verzögerungen zwischen Aufnahme und Visualisierung
8. Verfälschte Darstellung der Anzeige im Browser
9. Archivierung der Daten schlägt fehl
10. Ausfall Signalanzeige
11. Datenverfälschung
12. Zuordnungsfehler (Patientin ↔ Bett)
13. Bett wird innerhalb der „Warteperiode“ erneut belegt
14. Zugang zum System nicht möglich
15. nicht konforme Schnittstellenumsetzung
16. mehr als 10 Benutzer
17. Farbenblindheit des Arztes

18. Fehlfunktion durch Firewall
19. Fehlfunktion durch Viren auf *CTG Online* Server
20. Fehler bei Signaldarstellung
21. Startkonfiguration
22. Verfahren Dokumentation
23. Räumliche Trennung
24. Aufsichtspflicht
25. Rechneruhr falsch eingestellt

Anz. Der Funktionen	Bereich
5	Nicht akzeptierbarer Bereich
19	ALARP Bereich
8	Akzeptierter Bereich

### B.2.2.2 Risiken nach der Umsetzung der Risikomindernden Maßnahmen

Die Risiken nach der Umsetzung der risikomindernden Maßnahmen werden akzeptiert wenn möglichst keine Funktionen im „Nicht akzeptierbarer Bereich“ und möglichst wenige im „ALARP“ - Bereich liegen. Funktionen im nicht akzeptierten bzw. ALARP Bereich:

- Ausfall CTG Auslesegerät / CTG Gerät
- nicht konforme Schnittstellenumsetzung
- Unterbrechung der Netzverbindung
- Ausfall Signalanzeige
- Startkonfiguration
- Datenverfälschung
- Verfahren Dokumentation
- Aufsichtspflicht

Anz. Der Funktionen	Bereich
0	Nicht akzeptierbarer Bereich
8	ALARP Bereich
25	Akzeptierter Bereich

### **B.3 Rest - Risiken**

Im folgenden werden die Restrisiken bewertet. Einträge der Form (x.xx/x) in der Spalte Validierung verweisen auf definierte Tests im Kapitel Testspezifikation der Design Spezifikation.

### B.3.1 Risiken die sich aus peripheren Einflüssen ergeben

Lfd. Nr. / Funktion	Bewertung vor Maß- nahme Ausmaß Häufigkeit Einstufung	Validierung bzw. Referenz auf Test	Bewertung nach Maß- nahme Ausmaß Häufigkeit Einstufung	Ergebnis bzw. Beurteilung
(1.01/12) ma- nuelle Eingabe von Patien- tinnendaten (Info.00x)	Gering Gel. ALARP	Eingabe kann nachträglich be- arbeitet werden; falls Info.xxx über externes System erzeugt wird, kei- ne Validierung möglich; Hinweis in GA 2.6	Gering Entf. Akz.	Zuordnung er- folgt anhand der Betten;
(1.02/15) Schnittstelle zwischen CTG Aufnahme und <i>Trium CTG Online</i>	Kritisch Entf. ALARP	Testspezifikation (2.01, 2.05)	Kritisch Entf. ALARP	Datenaufnahmegerät muß Definiti- on der Afo einhalten. Die Verantwortung liegt hier beim Hersteller des Datenaufnahme- gerätes

Lfd. Nr. / Funktion	Bewertung vor Maß- nahme Ausmaß Häufigkeit Einstufung	Validierung bzw. Referenz auf Test	Bewertung nach Maß- nahme Ausmaß Häufigkeit Einstufung	Ergebnis bzw. Beurteilung
(1.03/13) Fol- gebelegung desselben Bet- tes innerhalb 10 Durchläufen	Gering Entf. Akz	Hinweis in GA 2.6	Gering Entf. Akz	Mißachtet der Anwender die Wartezeit, wer- den die Daten der nachfolgen- de Patientin an die der vor- ausgehenden angehängt; <sup>1</sup> Die Daten (incl. Kommentare) der nachfolgen- den Patientin werden in die- sem Fall der vorausgehen- den Patientin zugeordnet.
(1.04/11) Da- tenverfälschung Sicherheit	kritisch Entf. ALARP	Testspezifikation (7.01, 7.02) Au- thentifizierung, Verschlüsselung, Hinweise in GA 2.2, 2.3	Kritisch Unwahr. Akz	Maßnahme erfolgreich
(1.04/11) Da- tenverfälschung Übertragung	kritisch Entf. ALARP	Testspezifikation (6.05) Protokoll TCP, Übertra- gung von Bildern robust gegen Punktstörungen, Flächenstörungen werden erkannt	Gering Entf. Akz	Maßnahme erfolgreich

<sup>1</sup>Die Ampelanzeige könnte in diesem Fall eine „zu kritische“ Beurteilung angeben, da die FIGO Richtlinien einen Zeitraum von 30-40 min. als Bewertungsgrundlage nehmen. Die Diagrammanzeige (Base-,Floatingline,Ak/Dezelerationen sind hiervon nur kurzzeitig betroffen (Länge des Fensters DMW-Algorithmus)

<b>Lfd. Nr. / Funktion</b>	<b>Bewertung vor Maß- nahme</b> Ausmaß Häufigkeit Einstufung	<b>Validierung</b> bzw. Referenz auf Test	<b>Bewertung nach Maß- nahme</b> Ausmaß Häufigkeit Einstufung	<b>Ergebnis</b> bzw. Beurteilung
(1.05/7,8) Leistungsanfor- derung	Gering Gel. ALARP	Testspezifikation 8.01 8.02	Gering Entf. Akz	Übertragungsra- te 9600 bit/sec ausreichend; Hinweis in GA 1.6.1; Maßnah- me erfolgreich
(1.06/6) Si- gnalausfall CTG Gerät	Katast. Entf. nicht akzep- tiert	Einführung eines neuen Klassifi- kators „Signal- ausfall“; Desi- gnspezifikation (M 1.07)	Gering Entf. Akz.	Signalausfall wird erkannt; Schwelle ist konfigurierbar; Maßnahme erfolgreich
(1.07/9) Archi- vierung schlägt fehl	gering Unwahr- scheinlich akz.	Testspezifikation (2.04)	gering Unwahr- scheinlich akz.	Das System schreibt Log- meldungen, die Hinweise darauf geben; Hinweis in GA (4.3);Maßnahme erfolgreich
(1.08/10) Ausfall Signal- anzeige	Katast. Unwahr. ALARP	Hinweis in GA 2.6	Katast. Unwahr. ALARP	Maßnahme erfolgreich
(1.09/2) Netz- verbindung	Krit. Gel. N.A.	(6.01, 6.03) Uhrzeit und rotierendes Fötensbild bleiben stehen (GA 5.1.1). Erkennung durch Fehlermeldung am Bildschirm (nur IE)	Krit. Entf. ALARP	Stehende Uhr- zeit und rotieren- der Fötus läßt Fehler erkennen, Dignose kann über Papier- streifen des CTGs durch- geführt werden; Maßnahme durchgeführt

Lfd. Nr. / Funktion	Bewertung vor Maß- nahme Ausmaß Häufigkeit Einstufung	Validierung bzw. Referenz auf Test	Bewertung nach Maß- nahme Ausmaß Häufigkeit Einstufung	Ergebnis bzw. Beurteilung
(1.10/3 Aus- fall CTG Gerät/CTG Auslesegerät	Kritisch Entf. ALARP	Arzt/Personal erkennt aufgrund der Kenntnisse der Bettbelegung den Ausfall; Hinweis in GA (5.4.4)	Kritisch Entf. ALARP	Maßnahme erfolgreich
(1.11/16) Mehr als 10 Benutzer	Gering Entf. Akz.	(8.01)	Gering Entf. Akz.	Maßnahme erfolgreich; Hinweis in GA 4.5.2
(1.12/17) Far- benblindheit des Arztes	Gering Entf. Akz.	Akzeptanz durch einen farbenblin- den Arzt	Gering Entf. Akz.	Maßnahme erfolgreich
(1.13/18) Fehl- funktion durch Firewall	Unwes. Entf. Akz.	Aufgrund der An- zahl unterschiedli- cher Firwalls am Markt läßt sich das Verhalten nicht für alle Produkte te- sten. Ein einfacher Test: Javascript am Browser deaktivie- ren	Unwes. Entf. Akz.	Maßnahme erfolgreich; Hinweis in GA 4.4
(1.14/19) Fehl- funktion durch Viren auf CTG Online Server	Gering Unwahr. Akz.	Aufgrund der Vielfältigkeit und häufig neu erschei- nenden Viren kann kein Testszenario angegeben werden;	Gering Unwahr. Akz.	Maßnahme erfolgreich; Hinweis in GA 4.4
(1.15/21) Konfigurati- onsdatei nicht vorhanden	Kritisch Entf. ALARP	(3.01) a (GA 4.1)	Gering Entf. Akz.	Maßnahme erfolgreich

Lfd. Nr. / Funktion	Bewertung vor Maß- nahme Ausmaß Häufigkeit Einstufung	Validierung bzw. Referenz auf Test	Bewertung nach Maß- nahme Ausmaß Häufigkeit Einstufung	Ergebnis bzw. Beurteilung
(1.16/21) Initialisie- rung: Copy- Server2.vi, FigoServer.vi, ArgusOnline1Bed2- X.vi (0<X<7), ArgusOnline- All5.vi	Gering gel. ALARP	Parameter in Kon- figurationsdatei entfernen oder falsch setzen; GA 4.1	Gering gel. ALARP	Maßnahme durchgeführt
(1.17/9) zu (1.07) check- DirSize.vi	Kritisch Entf. ALARP	Kein Plattenplatz vorhanden;	Kritisch Unwahr. Akz.	Hinweis in GA 4.3; Maßnahme erfolgreich
(1.18/6) zu (1.06) Copy- Server.vi	katast. Entf. nicht Akz.	Parameter verändern	katast. Unvor. Akz.	Maßnahme erfolgreich
(1.19/11) zu (1.04) Sicher- heit	kritisch Entf ALARP	entspricht dem heutigen Stand der Technik	kritisch Entf ALARP	Maßnahme er- folgreich (GA 2.2)
(1.20/12) Kom- mentare in das System einpfle- gen „kommen- tar.html“	Gering gel. ALARP	(4.03)	Gering Entf. Akz.	Maßnahme erfolgreich
(1.21/22) Verfahren Dokumentation	Gering gel. ALARP		Gering gel. ALARP	Stellt keine „aktive“ Gefähr- dung dar. Insofern ist die Bewertung eher als zu hoch eingestuft.
(1.22/23) räumliche Trennung	Kritisch häuf. N.A. <sup>2</sup>	Hinweis in GA 1.2	Kritisch Unwahr. Akz.	Maßnahme durchgeführt

<sup>2</sup>falls das System über eine Wählverbindung benutzt wird, bei Einsatz im Intranet wäre die Häufigkeit Unwahrscheinlich

<b>Lfd. Nr. / Funktion</b>	<b>Bewertung vor Maß- nahme</b> Ausmaß Häufigkeit Einstufung	<b>Validierung</b> bzw. Referenz auf Test	<b>Bewertung nach Maß- nahme</b> Ausmaß Häufigkeit Einstufung	<b>Ergebnis</b> bzw. Beurteilung
(1.23/24) Nachweis der Aufsichtspflicht	Krit. Entf. ALARP <sup>3</sup>		Krit. Entf. ALARP	Hinweis in GA 1.2
(1.24/25) Rech- neruhr falsch eingestellt	Gering Entf. Akz	(0.04)	Gering Entf. Akz	Hinweis in GA 2.6

---

<sup>3</sup>stellt keine direkte Gefährdung der Patientin dar

**B.3.2 Risiken die sich aus Internen Einflüssen ergeben:**

<b>Lfd. Nr. / Funktion</b>	<b>Bewertung vor Maßnahme</b> Ausmaß Häufigkeit Einstufung	<b>Validierung</b> bzw. Referenz auf Test	<b>Bewertung nach Maßnahme</b> Ausmaß Häufigkeit Einstufung	<b>Ergebnis</b> bzw. Beurteilung
(2.01/1) Einfrieren Serverbildschirm	Kritisch Entf. ALARP	(2.06)	Kritisch Unwahr. Akz	Einfrieren wird erkannt; Hinweis in GA 5.1.1; Maßnahme erfolgreich
(2.02/2,4) Zugang zum System nicht möglich	Gering Gel ALARP	Auswertung über Papierstreifen CTG Gerät; Hinweise in GA 5.2.7; Fehlermeldung	Gering Entf. Akz.	Maßnahme erfolgreich
(2.03/5) Umsetzung FIGO Alg	Katast Unwahr ALARP	Testspezifikation (1.01); Studie vergleicht Ergebnisse des Algorithmus mit denen von erfahrenen Gynäkologen	Krit. Unwahr Akz.	Maßnahme erfolgreich
(2.04/4)	Gering Unwahr Akz.	Zugang zum System nicht möglich, Falls Ausfall bei aktiver Verbindung wird Warnhinweis gegeben (siehe Ausfall Netzverbindung); Hinweise in GA 5.2.7	Gering Unwahr Akz.	Maßnahme erfolgreich
(2.05/1)zu (2.01)	Katast. Unwahr. ALARP	(2.06) Hinweis in GA 5.1.1	Katast. Unvor. Akz.	Maßnahme erfolgreich
(2.06/20) readSignalFor1Bed.vi	kritisch gel. nicht Akzeptiert		kritisch Unvor. Akz.	Maßnahme erfolgreich
(2.07/20) CopyServer.vi	Kritisch Entf. ALARP		Kritisch Unvor. Akz.	Maßnahme erfolgreich.

## B.4 Änderungen

<b>Wann, Wer</b>	<b>Was</b>
24.11.2000 CH	Grundversion
19.01.2001 CH	(1.02) Ergebnis korrigiert (1.03) Anmerkung bzgl. Diagnose (1.04) Hinweis GA eingefügt (1.08) (2.01) Schadensausmaß geändert

# Abbildungsverzeichnis

3.1	Checkliste zur Zweckbestimmung . . . . .	14
3.2	Schematische Darstellung des Konformitätsbewertungsverfahrens (Quelle: Kursunterlagen „CE-Zertifizierung medizinisch genutzter Software“ TÜV Akademie) . . . . .	17
3.3	Schematischer Aufbau der Risikomanagement-Dokumentation nach EN60601-1-4 . . . . .	23
3.4	Vorschlag eines Entwicklungs-Lebenszyklus nach EN 60601-1-4 Anhang DDD	25
3.5	Risikograph . . . . .	26
3.6	Beispiel Gefährdung (Quelle: Kursunterlagen „CE Zertifizierung medizinisch genutzter Software“ TÜV Akademie) . . . . .	27
3.7	Flußdiagramm des Risikoanalyse Verfahrens (Quelle: Bild CCC.2 EN60601-1-4) . . . . .	28
3.8	Determining Level of Concern (aus Guidance FDA) . . . . .	33
3.9	Dokumentation in a Premarket Submission (Quelle: [FDA99] Abb. 1-1) . .	36
3.10	Off the Shelf Software . . . . .	37
4.1	Abwicklung der Teilaktivität SE 1 . . . . .	40
4.2	Funktionsüberblick Subsystem SE . . . . .	42
4.3	Produktfluß für Aktivität SE 1.4 „Randbedingungen definieren“ . . . . .	45
4.4	SE- und QS-Zusammensammenarbeit bezüglich Kritikalität . . . . .	49
5.1	Schematische Architekturübersicht . . . . .	52
5.2	Dokumentenstruktur . . . . .	55
6.1	LabVIEW Diagramm . . . . .	88
6.2	LabVIEW Front Panel . . . . .	89



# Tabellenverzeichnis

3.1	Übersicht über die Anhänge . . . . .	19
3.2	Tabelle Verantwortung des Managements . . . . .	25
4.1	SSI.1: Festlegung von Kritikalität für technische Systeme (aus Handbuch SI)	47
5.1	Klassifizierung . . . . .	59
5.2	Definition von Tests, Testumgebung, Testmethode und Durchführung . . .	61
5.3	Zuordnungstabelle Submodell Projektmanagement . . . . .	70
5.4	Zuordnungstabelle Submodell Konfigurationsmanagement . . . . .	73
5.5	Produkt-Phasenzuordnung . . . . .	74
5.6	Zuordnungstabelle Anforderungsspezifikation . . . . .	76
5.7	Zuordnungstabelle Designspezifikation . . . . .	78
5.8	Zuordnungstabelle Testpläne . . . . .	79
5.9	Zuordnungstabelle Testkonzept . . . . .	80
5.10	Zuordnungstabelle Risikomanagement . . . . .	83



# Literaturverzeichnis

- [60697] Ergänzungsnorm programmierbare elektrische systeme. In *DIN EN 60601-1-4 Medizinische elektrische Geräte*. VDE, Frankfurt am Main, 1997.
- [93498] *Richtlinie 93/42/EWG des Rates über Medizinprodukte*. 1998.
- [Alp94] Marcel Alper. *Professionelle Softwaretest*. Vieweg, 1994.
- [Bal96] Helmut Balzert. *Lehrbuch der Software-Technik: Software-Entwicklung*. Spektrum Akademischer Verlag, 1996.
- [Bal98] Helmut Balzert. *Lehrbuch der Software-Technik: Softwaremanagement, Software-Qualitätssicherung, Unternehmensmodellierung*. Spektrum Akademischer Verlag, 1998.
- [BfA] *BfArM: Medizinprodukte*. [http://www.bfarm.de/de\\_ver/medizinprod/](http://www.bfarm.de/de_ver/medizinprod/).
- [CH99] T. Creter and J. Hofmann. Software als medizinprodukt. Technical report, Eurocat, 1999.
- [CHKT99] T. Creter, J. Hofmann, W. Kexel, and P. Thun. Richtlinienkonforme entwicklung von medizinprodukten. Technical report, Eurocat, 1999.
- [Dau98] Martin Daumer. Verfahren und vorrichtung zur drifterkennung. Deutsche patent anmeldung nr. 198 27 508, 1998. PCT/DE 99/01820.
- [DIM] *DIMDI Informationssystem Medizinprodukte*. <http://www.dimdi.de/germ/mpg/fr-mpg.htm>.
- [DW00] W. Dröschel and M. Wiemers. *Das V-Modell 97*. Oldenbourg Verlag, München, Wien, 2000.
- [en197] *EN1441 Medizinprodukte Risikoanalyse*. CEN, 1997.
- [eur] *Eurocat Software*. <http://www.eurocat.de/de/software.html>.
- [FDA97a] FDA/CDRH. *Design Control Guidance for Medical Device Manufacturers*, 1997.
- [FDA97b] FDA/CDRH. *Guidance for Industry: General Principles of Software Validation*, 1997.

- [FDA98] FDA/CDRH. *Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices*, 1998.
- [FDA99] FDA/CDRH. *Guidance: Off-The-Shelf Software Use in Medical Devices*, 1999.
- [for] *Forum Medizintechnik Online: Organisation*. <http://www.forum-medtech-pharma.de/merkblatt.htm>.
- [Gni99] J. Gnirs. Intrapartale Überwachung. In H. Schneider, P. Husslein, and Schneider KTM, editors, *Geburtshilfe*, pages 601–651. Springer Verlag, Heidelberg, 1999.
- [Gol00] D. Golias. Computer-gestützte ctg-analyse. Diplomarbeit, Technische Universität München, Institut für Informatik, Februar 2000.
- [Hof98] M. Hofmann. Risikomanagement - gesetzliche verpflichtung zum vorteil des unternehmens nutzen. *Management & Krankenhaus*, (9), 1998.
- [IP98] Luigi Lo Iacono and Frank Pascher. *Dokumentbasierte Software-Entwicklung am Beispiel des V-Modells*. <http://www.ti.et-inf.unisiegen.de/courses/SoDoM/Referate/V-Modell/v-modell.htm>, 1998.
- [JJ00] Rahman Jamal and Hans Jaschinski. *Virtuelle Instrumente in der Praxis*. Hüthig, Heidelberg, 2000.
- [JP97] Rahman Jamal and H. Pichlik. *LabVIEW: Programmiersprache der vierten Generation*. Prentice Hall, München, 1997.
- [Kne98] Peter L. Knepell. *Integrating Risk Management with Design Control*. Digital Media Canon Communications LLC, October 1998. <http://www.devicelink.com/mddi/archive/98/10/011.html>.
- [KNSS00] Prof. Dr. Eckhard Knappe, Prof. Dr. Günter Neubauer, Dr. Thomas Seeger, and Dr. Kevin Sullivan. *Die Bedeutung Von Medizinprodukten Im Deutschen Gesundheitswesen*. 2000. <http://www.bvmed.de/innovation.htm>.
- [MT00] Dieter H. Müller and T. Tietjen. *FMEA Praxis*. Carl Hanser Verlag, 2000.
- [Pic01] Herbert Pichlik. Bilder-code, grafische programmierumgebung national instruments labview 6.i. *c't*, (3):88, 2001.
- [por] *Portfolioanalyse*. <http://www.fh-deggendorf.de/doku/fh/meile/kapitel1/kap8/8seite3.html>.
- [pro98] *Professional G Developers Tools Reference Manual*. National Instruments, 1998. Part Number 321393B-01.
- [Rei00] Martin Reichmann. *Zur Einsetzbarkeit des V-Modells bei kleinen und mittleren Software-Herstellern*. Institut für Wirtschaftsinformatik und Anwendungssysteme, Juli 2000. <http://www.v-modell.iabg.de/diplom2.htm>.

- [Sch96] R. Schneeberger. *Qualitätsmanagement mit MS-Office: Einführung eines QM-Systems nach ISO 9000; Total Quality Management; QM-Verfahren und -Dokumentation*. Markt&Technik, 1996.
- [SS93] Rini Suhr and Roland Suhr. *Software Engineering: Technik u. Methodik*. Oldenbourg, 1993.
- [std99] *stdSEM Homepage*. 1999. <http://www-wnt.gsi.de/stdsemdemo/STDSEM/GENERAL/Default.htm>.
- [UT96] Carlo Ungermann and Frank J. Tesch. *Qualitätsmanagement bei der Softwareerstellung [Leitfaden für die Umsetzung der DIN EN ISO 9000]*. VDI Verlag, 1996.
- [VG93] VDI-GIS. *Software-Zuverlässigkeit*. VDI Verlag, 1993.
- [vm] *V-Modell Leitseite*. <http://www.v-modell.iabg.de/>.
- [vmb] *Der V-Modell Browser*. <http://www.scope.gmd.de/vmodel/de/vm.intro.html>.
- [war] *Software-Wartung*. <http://www.blazey.org/swtarch.htm>.