Gestaltung regulatorischer Vorgaben bei der Entwicklung medizinischer Software

Projektarbeit

Donau Universität Krems

Dr.-Karl-Dorrek-Straße 30

A-3500 Krems

Institut für Informationstechnologien im Gesundheitswesen

Prof. Dr. Christian Johner

Kaiser-Joseph-Str. 274

D-79098 Freiburg

Universitätslehrgang Professional M. Sc.

Informationstechnologien im Gesundheitswesen

Verfasser: Bernhard Fischer

Matrikelnummer: 0664130

Abgabedatum: 24. September 2007

Begutachter: Prof. Dr. Christian Johner

Inhaltsverzeichnis

Abstract

Die Erstellung von Medizingeräten unterliegt einer Vielzahl von regulatorischen Anforderungen. Auf Grund des technischen Fortschritts sind immer mehr Medizingeräte mit Software ausgestattet. Die Praxis zeigt, dass viele Medizinprodukteherstellter Probleme bei der Erfüllung der regulatorischen Anforderungen an medizinische Software haben. Dies betrifft sowohl die Frage, welche Standards einzuhalten sind, als auch die korrekte Berücksichtigung der in den einschlägigen Standards geforderten Vorgaben.

In dieser Arbeit wird zunächst eine Ist-Aufnahme der einzuhaltenden Standards vorgenommen und die dort aufgefundenen Forderungen beschrieben. Basierend auf diesen Forderungen werden Prozesselemente und Verfahren beschrieben, die eine zu den Standards konforme Entwicklung medizinischer Software gewährleisten. Ergänzt werden diese Prozesse durch eine Beschreibung der Dokumente, die bei der Entwicklung medizinischer Software erforderlich sind.

1 Einleitung

1.1 Problemstellung

Der Einsatz medizinischer Technik hat in der modernen Medizin seinen festen Stellenwert. In den letzten Jahren hat der Teil der medizinischen Geräte, die ohne Software nicht mehr auskommen, beständig zugenommen. Die Entwicklung von Software für die Medizintechnik unterliegt jedoch Vorgaben, die für andere Anwendungsbereiche von geringerer Relevanz sind. Daher sind diese Vorgaben vielfach nicht oder unvollständig bekannt und werden nicht angemessen bei der Softwareentwicklung berücksichtigt. Genügen die Medizingeräte aber nicht den notwendigen Standards, kann dies zu Problemen bei der Zulassung des Medizinproduktes oder sogar zur Gefährdung von Patienten führen.

1.2 Ziel der Arbeit

Ziel der Arbeit ist es, die für die Entwicklung medizinischer Software erforderlichen Vorgaben prozessorientiert darzustellen. Diese Darstellung ist einerseits in der Softwareentwicklung nicht ungewöhnlich und wird andererseits in verschiedenen internationalen Normen explizit gefordert. Dabei definieren diese Prozesse Aktivitäten und legen Produkte fest, die Eingaben oder Ergebnisse dieser Aktivitäten sind. Zudem regeln sie die Reihenfolge, in der diese Aktivitäten durchzuführen sind. Dabei liegt der Fokus dieser Arbeit auf den eng mit der eigentlichen Softwareentwicklung in Zusammenhang stehenden Verfahren. Daher werden etwa Anforderungen an ein Qualitätsmanagementsystem nicht detailliert dargestellt.

1.3 Vorgehen

In dieser Arbeit wird zunächst beschrieben, wie es zu den vereinheitlichten Warenverkehrsvorschriften in Europa gekommen ist und sodann in Grundzügen ausgeführt, welche Vorschriften bei der Entwicklung medizinischer Software in Europa zu berücksichtigen sind. Anschließend werden die für die USA geltenden Vorschriften erläutert.

Basierend auf den zuvor beschriebenen Vorschriften werden Prozesse und Verfahren beschrieben, die ein Rahmenwerk für die Erstellung medizinischer Software vorgeben. Ergänzt wird diese Darstellung durch die Beschreibung der Dokumente, die bei der Softwareentwicklung medizinischer Software erforderlich sind.

2 Die Entwicklung Europäischer Vorgaben

Medizinische Therapie und Diagnostik sind heute ohne den Einsatz moderner technischer Geräte und Hilfsmittel nicht mehr denkbar. Damit moderne medizinische Technologie auch das hält, was sie verspricht und der therapeutische Nutzen nicht durch Risiken und Gefahren aufgezehrt wird, bedarf es gesetzlicher Regelungen, die die Sicherheit und Effektivität des medizinischen Gerätes sicherstellen.

Traditionell ist die Abwehr von Gefahren, wie sie bei dem unkontrollierten Einsatz medizinischer Geräte denkbar sind, Aufgabe des Staates. Diese Aufgabe wird durch die staatlichen Stellen häufig unter einem präventiven Standpunkt erfüllt, in dem das In-Verkehr-Bringen und Betreiben potentiell gefährlicher Produkte von einer Zulassung und von der Erfüllung von Sicherheitsvorschriften abhängig gemacht wird.

In diesem Kapitel wird erläutert, welche Vorschriften für die Erstellung medizinischer Software berücksichtigt werden müssen. Dazu wird zunächst ausgeführt, wie europäisches Recht die Erstellung medizinischer Geräte beeinflusst. Anschließend wird das deutsche Medizinproduktegesetz und dessen Bezug auf das europäische Recht beleuchtet. Daran anschließend wird kurz auf die Verfahren zur Feststellung der Konformität des Medizinproduktes mit den europäischen Vorgaben und die Bedeutung der Benannten Stellen eingegangen. In dem anschließenden Kapitel werden dann die für die Erstellung von Software einschlägigen europäischen Normen ausgeführt und deren Inhalte beschrieben. Im Anschluss wird erläutert, inwieweit sich amerikanischen Vorgaben für Medizinprodukte von europäischen Vorgaben unterscheiden.

2.1 Harmonisierung nationaler Vorschriften und Normen

Durch Artikel 2 des Vertrags von Rom wurde der Europäischen Wirtschaftsgemeinschaft (EWG) die Aufgabe übertragen, "eine harmonische Entwicklung des Wirtschaftslebens innerhalb der Gemeinschaft, eine beständige und ausgewogene Wirtschaftsausweitung, eine größere Stabilität, eine beschleunigte Hebung der Lebenshaltung und engere Beziehungen zwischen den Staaten zu fördern, die in dieser Gemeinschaft zusammengeschlossen sind".

Dieses Ziel soll durch die Öffnung der Grenzen, die zu Freizügigkeit und einem freien Waren- und Dienstleistungsverkehr führen soll, sowie durch die Schaffung solidarischer Strukturen, durch die Einführung einer gemeinsamen Politik und die Einsetzung entsprechender Finanzinstrumente verwirklicht werden.

In ihrem Weißbuch über die Vollendung des Binnenmarkts[1] von 1985 stellte die Kommission fest, dass allzu viele Hindernisse der Verwirklichung eines großen Wirtschaftsraums im Wege stehen. In diesem Weißbuch wurden die verschiedenen nationalen Warenverkehrsvorschriften, die zugleich Sicherheitsvorschriften darstellen, als entscheidendes Problem zur Vollendung des Binnenmarktziels identifiziert[2] und die Schaffung einheitlicher europäischer technischer Produktstandards als Weg zur Vollendung des Binnenmarksziel vorgeschlagen. Um langwierige Entscheidungsprozeduren zu vermeiden wurde weiter vorgeschlagen, dass durch den Rat nur grundlegende Rechtsvorschriften festgelegt werden, und ansonsten technische Fragen durch eine Kompetenzübertragung nach Artikel 135 EWG-Vertrag delegiert[3].

Dieser Absichtserklärung folgte am 7. Mai 1985 die „Entschließung des Rates über eine neue Konzeption auf dem Gebiet der technischen Harmonisierung und Normung“[4]. Dieses „neue Konzept“ stützt sich auf die folgenden Grundprinzipien:

- Die Harmonisierung der Rechtsvorschriften beschränkt sich auf die Festlegung der grundlegenden Sicherheitsanforderungen oder sonstigen Anforderungen im Interesse des Gemeinwohls, denen die in den Verkehr gebrachten Waren genügen müssen. Diese bewusst abstrakt gehaltenen Sicherheitsziele sollen durch europäische harmonisierte Normen konkretisiert werden.
- Den privatrechtlichen europäischen Normungsgremien wird ein Normungsauftrag zur Ausarbeitung von technischen Spezifikationen erteilt, die die in den Richtlinien festgelegten grundlegenden Anforderungen konkretisieren. Diese so erarbeiteten Normen werden im Amtsblatt der EWG veröffentlicht und von den nationalen Normungsgremien übernommen.

Diese technischen Spezifikationen erhalten jedoch keinerlei obligatorischen Charakter, sondern bleiben freiwillige Normen. Werden Erzeugnisse hingegen nach harmonisierten Normen hergestellt, so wird eine Übereinstimmung mit den in der Richtlinie aufgestellten grundlegenden Anforderungen angenommen (Vermutungswirkung). Maßgeblich ist aber immer die tatsächliche Erfüllung der grundlegenden Anforderungen. In den Fällen, in denen der Hersteller nicht nach den harmonisierten Normen produziert, liegt die Beweislast für die Übereinstimmung mit den grundlegenden Anforderungen bei ihm.

[1] [KOM(85)].

[2] ebenda, S. 19 ff.

[3] ebenda, S. 20, Rn. 70.

[4] Entschließung des Rates (85/C 136/01) – Amtsblatt C 136 vom 4. Juni 1985.

2.2 Das Konformitätsbewertungsverfahren

Nicht nur die unterschiedlichen nationalen Warenverkehrsvorschriften und technischen Normen stellten Hindernisse im innergemeinschaftlichen Warenverkehr dar, sondern auch die unterschiedlichen Prüf- und Zertifizierungsverfahren, mit denen der Hersteller die Einhaltung der Vorschriften und Normen nachweisen musste. Im Rahmen der Neuen Konzeption wird jedoch die Frage, mit welchen Prüfverfahren der Hersteller die Erfüllung der grundlegenden Anforderungen nachweisen muss, nicht angesprochen. Ein systematische Vereinheitlichung dieser Konformitätsbewertung erfolgte im Rahmen des von der Kommission vorgelegten „Globalen Konzepts für Zertifizierung und Prüfwesen“[5]. In diesem „Globalen Konzept“ spielt die Konformitätsbewertung für den Nachweis der Erfüllung der grundlegenden Anforderungen eine Schlüsselrolle. Einheitliche Konformitätsverfahren sollen eine einheitliche Rechtsanwendung bei der Prüfung der Konformität gewährleisten. Weiterhin wird die wichtige Frage behandelt, welche Anforderungen an die Zertifizierungsstellen (sog. Benannte Stellen) gestellt werden müssen.

Das von der EG-Kommission vorgelegte Konzept ist vom Rat in zwei Entscheidungen angenommen worden[6]. Das „globale Konzept“ stützt sich auf die folgenden Prinzipien:

- **Zertifizierung**. Der Hersteller weist durch die Durchführung von Konformitätsbewertungsverfahren die Konformität seines Produktes mit den grundlegenden Anforderungen nach. Diese Konformität muss, um Vertrauen in die Erfüllung der grundlegenden Anforderungen zu erzeugen, gegebenenfalls durch unabhängige und sachverständige Institutionen, so genannte Benannte Stellen, bestätigt werden. Ein Zertifikat dient als Nachweis der Konformität mit grundlegenden Anforderungen.
- **Akkreditierung**. Ist für das Konformitätsverfahren eine Benannte Stelle erforderlich, so sollen die Mitgliedsstaaten nur kompetente und sachverständige für diese Aufgabe zulassen. Damit die Kompetenz der einzelnen Zertifizierungsstellen nach einheitlichen Kriterien überprüft werden kann, werden die Anforderungen an diese Stellen wiederum durch harmonisierte Normen definiert[7].

---

[5] Ein globales Konzept für Zertifizierung und Prüfwesen, KOM(89) 209 endg. vom 15. Juni 1989, ABI. EG 1989, C 213/3 und C 276/3.

[6] Entschließung des Rates zu einem „Gesamtkonzept für die Konformitätsbewertung“ vom 12.Dezember 1989 (ABl. EG 1990, C 10/1), sowie im „Beschluss des Rates über die in den technischen Harmonisierungsrichtlinien zu verwendenden Module [...]“ vom 13. Dezember 1990 (Beschluss 90/465 EWG, ABl. EG L 220/30), abgeändert durch Beschluss vom 27. März 1993 (Beschluss 90/683 EWG, ABl. EG L 380/13).

[7] Solche harmonisierte Normen sind bspw. EN 45001 – allgemeine Kriterien zum Betreiben von Prüflaboren, EN 45002 - allgemeine Kriterien zum Begutachten von Prüflaboren, EN 45003 - allgemeine Kriterien für Stellen, die Prüflabore akkreditieren, EN 45011 - allgemeine Kriterien für Stellen, die Produkte zertifi-

- **Modulares Konzept**. Der Hersteller kann bei der Wahl des Konformitätsbewertungsverfahrens in den einzelnen Richtlinien zwischen insgesamt acht so genannten Modulen wählen, die mit den Buchstaben A bis H bezeichnet sind. Diese acht verschiedenen Arten von Konformitätsbewertungsverfahren sind an spezifische Produkteigenschaften, sowie das Risikopotenzial des Produkts geknüpft. Sie werden in jeder einzelnen Richtlinie produktspezifisch vorgeschrieben. Dabei unterscheidet das Modulare Konzept innerhalb des Herstellprozesses zwischen der Produktentwurfsstufe[8] und der Produktfertigungsstufe. Grundsätzlich sollen beide Stufen geprüft werden, wobei sich die Intensität der Prüfung nach dem Risikopotenzial richtet.

2.3 Europäische Richtlinien für Medizinprodukte

Basierend auf der oben erläuterten Harmonisierungskonzeption wurden mehrer europäische Richtlinien erlassen, die den Markt für Medizinprodukte regeln. Diese Richtlinien folgen dem oben ausgeführten Konzept:

- Festsetzung abstrakt beschriebener Sicherheitsziele,
- deren Konkretisierung durch harmonisierte Normen[9] und
- der Nachweis der Konformität durch den Hersteller im Rahmen von Konformitätsbewertungsverfahren nach dem „Globalen Konzept".

Ein gemeinsames Merkmal der medizinprodukterechtlichen Richtlinien ist, dass sie sich als so genannte sektorale Richtlinien qualifizieren lassen. Sektorale Richtlinien zeichnen sich dadurch aus, dass in ihnen verschiedene Produkte zusammengefasst sind, für die sich einheitliche Schutzziele definieren lassen und die zusätzlich einer einheitlichen Normung zugänglich sind. Demgegenüber haben so genannte horizontale Richtlinien, wie etwa die Richtlinie über elektromagnetische Verträglichkeit, einen breiten Anwendungsbereich und können auf eine Vielzahl von Produkten angewendet werden. Sofern ein Produkt sowohl unter eine sektorale, als auch unter eine horizontale Richtlinie fällt, sind die Regelungen der sektoralen Richtlinie vorrangig.

Dennoch bleibt der Hersteller zur Prüfung verpflichtet, ob neben den Regelungen der jeweiligen sektoralen Richtlinie noch grundlegende Anforderungen anderer Richtlinien anzuwenden sind, so dass es im Einzelfall zur Anwendung mehrerer Richtlinien kommen kann.

Im Bereich der Medizinprodukte wurden bisher 3 Richtlinien erlassen. Dies sind:

---

zieren, EN 45012 - allgemeine Kriterien für Stellen, die Qualitätssicherungssysteme zertifizieren und EN 45014 – allgemeine Kriterien für Konformitätserklärungen von Anbietern

[8] Produktentwicklung bis zur Erstellung eines für die spätere Herstellung repräsentativen Prototyps.

[9] die im Amtsblatt der EG veröffentlicht werden.

- Richtlinie 90/385 über aktive implantierbare medizinische Geräte (AIMD).
- Richtlinie 93/42 über allgemeine Medizinprodukte (MDD)
- Richtlinie 98/79 über In-vitro-Diagnostik (IVD).

2.4 Das Medizinproduktegesetz

Entsprechend der Pflicht der BRD, die europäischen Richtlinien gemäß Art. 189 Abs. 3 EGV in nationales Recht umzusetzen, erfolgte die Umsetzung der drei oben genannten Richtlinien in nationales Recht durch das Medizinproduktegesetz.

Die Bundesregierung beabsichtigte, die Richtlinie über aktive implantierbare medizinische Geräte in einem Medizinproduktegesetz direkt in nationales Recht umzusetzen. Ein entsprechender Gesetzesentwurf wurde aber zurückgezogen, da es im europäischen Verfahren bei der Beratung zu einer Richtlinie über allgemeine Medizinprodukte zu zahlreichen Änderungen kam. Ein Medizinproduktegesetz, das nur die Richtlinie über aktive implantierbare medizinische Geräte umgesetzt hätte, wäre so schon vor dem In-Kraft-Treten veraltet gewesen. Da aber die in der Richtlinie genannte Frist für die Umsetzung ablief, erlangt die Richtlinie über aktive implantierbare medizinische Geräte durch Bekanntmachung des Bundesministers für Gesundheit bis zur ihrer rechtsgültigen Umsetzung direkt Geltung[10].

Bei der Umsetzung der Richtlinie über allgemeine Medizinprodukte gab es diese Probleme nicht. Das Medizinproduktegesetz trat am 1. Januar 1995 in Kraft. Einige Vorschriften dieses Gesetzes traten bereits einen Tag nach Verkündigung in Kraft. Um jedoch den Herstellern eine angemessene Zeit zur Umstellung zu ermöglichen, wurde bis zur endgültigen Anwendung des Gesetzes eine Übergangszeit bis zum 13. Juni 1998 festgelegt.

Eine Umsetzung der Richtlinie über In-vitro-Diagnostik erfolgte mit dem am 1. Januar 2002 in Kraft getretenen zweiten Medizinprodukte-Änderungsgesetz. Da bis zu diesem Zeitpunkt die europäische Richtlinie bereits umgesetzt sein musste, entschied sich die Bundesregierung auch in diesem Fall dafür, bis zu der Umsetzung der Richtlinie in nationales Recht, die europäische Richtlinie direkt anzuwenden.

Zweck des Medizinproduktegesetzes ist es, nur medizinisch und technisch unbedenkliche Medizinprodukte in Verkehr zu bringen. Daher wurden für den Hersteller die Erfüllung grundlegender Anforderungen gefordert, die abstrakt die Sicherheit des Produktes sicherstellen. Wie diese Forderungen umzusetzen sind, ist nicht im Gesetz selbst festgelegt, sondern an eine nachrangige

[10] Nach den in dem Ratti-Urteil des Europäischen Gerichtshofs aufgestellten Grundsätzen können sich Bürger der Europäischen Union direkt auf die Vorschriften der Richtlinie berufen, wenn die Umsetzung der Richtlinie nicht fristgerechte erfolgt ist (EuGH Rs. 148/78 Slg. 1979, S. 1629 ff.).

Verordnung delegiert. In der Medizinprodukt-Verordnung (MPV) ihrerseits wird aber lediglich wieder auf die europäischen Richtlinien zurückverwiesen.

Mit dem zweiten Medizinprodukt-Änderungsgesetz erfolgte nun eine Neustrukturierung des Medizinproduktegesetzes. In diesem Gesetz werden die grundlegenden Anforderungen, die Klassifizierungsregeln und das Konformitätsbewertungsverfahren durch eine unmittelbare Rückverweisung auf die Richtlinie in das Gesetz integriert, daher ist die Rückverweisung durch die Medizinprodukt-Verordnung nicht mehr erforderlich.

2.5 Festlegung der Zweckbestimmung

Der Hersteller des Medizinprodukts muss das konkrete Einsatzgebiet eines medizinischen Produktes festlegen. Es bekommt somit eine Zweckbestimmung. Zweckbestimmung ist nach § 3 Nr. 10 MPG die Verwendung, für die das Medizinprodukt in der Kennzeichnung, der Gebrauchsanweisung oder den Werbematerialien […] bestimmt ist. Diese Zweckbestimmung schließt in vielen Fällen eine Kombination mit einem anderen Gerät ein.

2.6 Software als Medizinprodukt

Das Medizinproduktegesetz definiert Medizinprodukte als 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:

- der Erkennung, Verhütung, Überwachung, Behandlung oder Linderung von Krankheiten,
- der Erkennung, Überwachung, Behandlung, Linderung oder Kompensierung von Verletzungen oder Behinderungen,
- der Untersuchung, der Ersetzung oder der Veränderung des anatomischen Aufbaus oder eines physiologischen Vorgangs oder
- 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[11].

[11] §3, Nr.1, MPG, vom 02.08.1994, zuletzt geändert am 13.12.2001, zit. nach [Schorn], S. 53.

Zubehör für Medizinprodukte[12] sind Gegenstände, Stoffe, Zubereitungen aus Stoffen sowie Software, die selbst keine Medizinprodukte nach Nummer 1 sind, aber vom Hersteller dazu bestimmt sind:

- mit einem Medizinprodukt verwendet zu werden, damit dieses entsprechend der von ihm festgelegten Zweckbestimmung des Medizinproduktes angewendet werden kann, oder
- die für das Medizinprodukt festgelegte Zweckbestimmung zu unterstützen.

Aus dieser Legaldefinition kann man also entnehmen, das eine Software dann als Medizinprodukt im Sinne des MPG angesehen werden kann, wenn es:

- selbst ein Medizinprodukt ist (etwa eine Software, die einen Behandlungsplan für die Strahlentherapie erstellt),
- Bestandteil oder Komponente eines Medizinproduktes ist (etwa Steuerungssoftware für ein Medizinprodukt),
- Zubehör für ein Medizinprodukt ist.

[12] §3, Nr.9, MPG, vom 02.08.1994, zuletzt geändert am 13.12.2001, zit. nach [Schorn], S. 55.

3 Vorgaben für den europäischen Markt

Werden Medizinprodukte unter Berücksichtigung der einschlägigen harmonisierten Normen hergestellt, so wird eine Übereinstimmung mit den grundlegenden Anforderungen angenommen (Vermutungswirkung). Alle für Medizinprodukte harmonisierten Normen sind vom Europäischen Rat veröffentlicht und über das Internet zugänglich[13]. Diese Fundstelle enthält auf 33 Seiten eine Vielzahl von Normen, die teils nur für bestimmte Arten von Medizinprodukten zutreffend sind, teils aber auf alle Arten von Medizinprodukten angewendet werden sollen. Solche Normen sind also auch auf die Entwicklung von Software anzuwenden. Für die Softwareentwicklung sind die folgenden Normen relevant:

- DIN EN ISO 13485: Qualitätsmanagement (s. Kapitel 3.1).
- DIN EN ISO 14971: Risikomanagement (s. Kapitel 3.2).
- DIN EN ISO 60601-1-4: Sicherheit für programmierbare elektrische medizinische Geräte (s. Kapitel 3.3).
- DIN EN ISO 62304: Software-Lebenszyklus-Prozesse (s. Kapitel 3.4).
- DIN EN ISO 60601-1-6: Gebrauchstauglichkeit (s. Kapitel 3.5).

Zusätzlich zu diesen Normen muss folgendes berücksichtigt werden:

- In den „Medical Devices Guidance Documents“ werden verbindliche Anleitungen der Europäischen Union veröffentlicht, die in Zusammenarbeit mit Herstellern und Benannten Stellen erstellt wurden (s. Kapitel 3.6).
- Die Benannten Stellen nehmen sowohl am nationalen als auch am internationalen Erfahrungsaustausch teil. Die dort gefassten Beschlüsse und Dokumente müssen von dem Benanten Stellen angewendet werden, und daher von den Herstellern berücksichtigt werden (s. Kapitel 3.7).
- In der „Global Harmonization Task Force“ haben sich Repräsentanten zuständiger Behörden und der Industrie aus verschiedenen Ländern zusammengeschlossen, um Regeln zu erarbeiten, die als Leitlinien für Medizinprodukte gelten konnten (s. Kapitel 3.8).

[13] http://ec.europa.eu/enterprise/newapproach/standardization/harmstds/reflist/meddevic.html (letzter Zugriff: 05.06.2007) .

3.1 Qualitätsmanagement

Unter einem Qualitätsmanagementsystem versteht man einen „Teil des Managementsystems einer Organisation, der sich in Bezug auf Qualitätsziele auf das Erreichen von Ergebnissen richtet, um (...) die Erfordernisse, Erwartungen und Anforderungen interessierter Parteien zu erfüllen“.[14]. Die ISO-9000-Familie hat sich weltweit als Standard für Qualitätsmanagementsysteme durchgesetzt.

Die Normenreihe DIN EN ISO 9000ff:2000 besteht aus 3 Teilen. Die ISO 9000:2000 beschreibt Grundlagen für Qualitätsmanagementsysteme und legt die Terminologie für solche Systeme fest[15]. Von zentraler Bedeutung ist die Norm DIN EN ISO 9001:2000, die Minimalforderungen an ein zertifizierungsfähiges Qualitätsmanagementsystem festlegt[16]. Sie wird ergänzt durch die Norm DIN EN ISO 9004:2000, die einen Leitfaden zur Leistungsverbesserung eines Qualitätsmanagementsystems bereitstellt. Daher bietet diese Norm Anregungen und Orientierung zur Umsetzung eines umfassenden prozessorientierten Qualitätsmanagementsystems[17].

Die Norm DIN EN ISO 13485 wurde auf der Grundlage der DIN EN ISO 9001:2000 erarbeitet, jedoch wurden insbesondere die Anforderungen für „Kundenzufriedenheit“ und „ständige Verbesserung“ modifiziert, und die dokumentarischen Anforderungen an den Entwicklungsprozess verschärft. Ansonsten sind die Anforderungen in beiden Normen weitgehend identisch. Die Anforderungen des Qualitätsmanagementsystems werden in den nachfolgenden Kapiteln kurz beschrieben.

3.1.1 Grundsätze des Qualitätsmanagements

Nach der DIN EN ISO 9000:2000 basiert das Qualitätsmanagement auf acht Grundsätzen[18]:

- Kundenorientierung: Verstehen von Kundenerfordernissen, Erfüllen der Kundenanforderungen und Versuchen, diese Anforderungen zu übertreffen.
- Führung: Schaffen und Erhalten eines internen Umfeldes, in dem sich Personen voll und ganz für das Erreichen der Organisationsziele einsetzen können.
- Einbeziehung von Personen: Vollständiges Einbeziehen von Personen, um ihre Fähigkeiten für die Organisation zu nutzen.

[14] [ISO 9000], Abschnitt 2.11, S. 19.

[15] [ISO 9000], Abschnitt 0.1, S. 8.

[16] [ISO 9001], Abschnitt 0.1, S. 75.

[17] [ISO 9004], Abschnitt 0.3, S. 142.

[18] [ISO 9000], Abschnitt 0.2, S.9.

- Prozessorientierter Ansatz: Leiten und Lenken der Tätigkeiten und zugehörigen Ressourcen als Prozesse, um die gewünschten Ergebnisse effizienter zu erreichen.
- Systemorientierter Managementansatz: Erkennen, Verstehen, Leiten und Lenken der in Wechselbeziehung stehenden Prozesse einer Unternehmung als System.
- Ständige Verbesserung: Ständige Verbesserung der Gesamtleistung der Organisation.
- Sachbezogener Ansatz zur Entscheidungsfindung: Entscheidungen werden auf der Grundlage der Analyse von Daten und Informationen getroffen.
- Lieferantenbeziehung zum gegenseitigen Nutzen: Beziehungen zwischen Organisation und Lieferanten zum gegenseitigen Nutzen erhöhen die Wertschöpfungsfähigkeit beider Seiten.

3.1.2 Prozessorientierung

Eine herausragende Rolle in der DIN EN ISO 9000ff:2000 spielt die Prozessorientierung. Unter Prozessen versteht die DIN EN ISO 9000:2000 „jede Tätigkeit oder jeder Satz von Tätigkeiten, die bzw. der Ressourcen verwendet, um Eingaben in Ausgaben umzuwandeln“[19]. Diese Definition ist sehr abstrakt. Nach dieser Definition können bereits einfache Verknüpfungen weniger Tätigkeiten, die ein Ergebnis erzeugen, als Prozess aufgefasst werden. Dennoch bleibt der Zuschnitt der Prozesse, die eine Organisation verwenden will, offen. Die Norm macht hierzu keine Vorgaben.

Als prozessorientierten Ansatz bezeichnet die Norm die Anwendung eines Systems von Prozessen in einer Organisation, gepaart mit dem Erkennen der Wechselwirkungen zwischen diesen Prozessen und dem Management dieser Prozesse[20]. Die ISO 9001:2000 stellt die folgenden Anforderungen an die Prozessorientierung[21]:

- Die erforderlichen Prozesse und ihre Anwendung in der Organisation sind zu erkennen.
- Die Abfolge und Wechselwirkung der Prozesse ist aufzuzeigen.
- Die erforderlichen Kriterien und Methoden zur Durchführung und Lenkung der Prozesse sind zu definieren.
- Die benötigten Ressourcen und Informationen zur Durchführung und Überwachung der Prozesse sind bereitzustellen.
- Die Prozesse sind zu überwachen, zu messen und zu analysieren.

[19] [ISO 9001], Abschnitt 0.2, S.75, dritter Absatz.

[20] [ISO 9001], Abschnitt 0.2, S.75, zweiter Absatz.

[21] [ISO 9001], Abschnitt 4.1, S.81.

- Es sind die erforderlichen Maßnahmen zu treffen, um die geplanten Ergebnisse zu erzielen.
- Die Prozesse sind in Übereinstimmung mit den Anforderungen der Norm zu leiten und zu lenken.

3.1.3 Allgemeine Anforderungen

In der Norm wird gefordert, dass das Qualitätsmanagementsystem dokumentiert sein muss[22]. Die Dokumentation zum Qualitätsmanagementsystem muss mindestens folgende Informationen enthalten:

- die Qualitätspolitik und die Qualitätsziele des Unternehmens,
- das Qualitätsmanagement-Handbuch,
- die von der Norm geforderten dokumentierten Verfahren,
- die von der Norm geforderten dokumentierten Aufzeichnungen,
- alle Dokumente, die von dem Unternehmen zur Planung, Durchführung und Lenkung der Prozesse benötigt werden.

Das Qualitätsmanagement-Handbuch beschreibt das Qualitätsmanagementsystem überblicksartig. Es dient vor allem der externen Darlegung der Organisation sowie der Abläufe und Zuständigkeiten gegenüber Kunden und anderen Anspruchsgruppen. Zudem dient es als ständige Referenz bei der Verwirklichung und Aufrechterhaltung des Qualitätsmanagementsystems.

Das Qualitätsmanagement-Handbuch enthält üblicherweise folgende Informationen[23]:

- Die Qualitätspolitik und die Qualitätsziele des Unternehmens.
- Die für das Qualitätsmanagementsystem erforderlichen Verfahren, oder Verweise auf die Dokumentation dieser Verfahren.
- Eine Beschreibung der Wechselwirkung der Prozesse des Qualitätsmanagementsystems (Prozesslandschaft).

Für die Lenkung qualitätsrelevanter Dokumente, wie etwa Verfahrensanweisungen oder Arbeitsanweisungen, aber auch Anforderungs- und Designdokumente ist ein dokumentiertes Verfahren einzuführen. Diese Dokumente müssen[24]

- vor der Freigabe auf Angemessenheit geprüft werden,

[22] [ISO 9001], Abschnitt 4.2.1, S.82.

[23] [ISO 9001], Abschnitt 4.2.2, S.82f.

[24] [ISO 9001], Abschnitt 4.2.3, S.83.

- bewertet, ggf. aktualisiert und dann erneut freigegeben werden,
- mit Revisionsstand gekennzeichnet werden,
- aktuell verfügbar sein und
- lesbar und leicht erkennbar sein

Für die Lenkung von Qualitätsaufzeichnungen, wie etwa Prüfprotokolle, ist ebenfalls ein dokumentiertes Verfahren erforderlich[25]. In diesem Verfahren sind die Lenkungsmaßnahmen festzulegen, die für die Kennzeichnung, die Aufbewahrung und die Wiederauffindbarkeit erforderlich sind.

3.1.4 Verantwortung der Leitung

Bei der Einführung, der Umsetzung, Lenkung und Weiterentwicklung eines Qualitätsmanagementsystems kommt der obersten Leitung eine zentrale Rolle zu. Daher wird in der Norm gefordert, dass die oberste Leitung ihre Verpflichtung bezüglich der Entwicklung und Verwirklichung des Qualitätsmanagementsystems nachweist, indem sie

- der Organisation die Bedeutung der Erfüllung der Kundenanforderungen sowie der gesetzlichen und behördlichen Anforderungen vermittelt,
- die Qualitätspolitik und Qualitätsziele festlegt,
- Managementbewertungen durchführt und
- die Verfügbarkeit von Ressourcen sicherstellt.

3.1.5 Kundenbezogene Prozesse

Damit die Organisation eine qualitätsgerechte Leistung erbringen kann, ist es entscheidend, zu Beginn die Kundenerfordernisse korrekt verstanden und erfasst zu haben. Die Anforderungen des Kunden, sowie etwaiger weiterer Anspruchsgruppen müssen ermittelt, in geeigneter Form dokumentiert und innerhalb der Organisation kommuniziert werden[26].

Bei der Ermittlung der Anforderungen ist wichtig, dass alle Anforderungen des Kunden – auch die vorausgesetzten und nicht ausgesprochenen – vollständig und richtig identifiziert werden. Die so aufgenommenen Kundenanforderungen müssen einer Bewertung unterzogen werden, um sicherzustellen, dass die Kundenanforderungen das Produkt korrekt spezifizieren[27] und

[25] [ISO 9001], Abschnitt 4.2.4, S.83.

[26] [ISO 9001], Abschnitt 7.2.1, S.88.

[27] [ISO 9001], Abschnitt 7.2.2a, S.88.

durch die Organisation umgesetzt werden können[28]. Die Ergebnisse dieser Bewertung müssen aufgezeichnet werden[29]. Dies lässt sich praktisch nur durchführen, wenn die Kundenanforderungen dokumentiert werden, auch wenn dies explizit nicht in der Norm gefordert wird.

3.1.6 Entwicklung

Die Entwicklung eines neuen Produktes muss geplant und gelenkt werden. Dazu gehört auch, dass der Entwicklungsprozess detailliert beschrieben ist und weiterhin für jeden Teilprozess („Phase“) eine geeignete Bewertung (Verifizierung und/oder Validierung) des Entwicklungsergebnisses vorgesehen ist. Zudem sind die Verantwortlichkeiten und Befugnisse der beteiligten Gruppen festzulegen[30].

Die Entwicklung eines Produktes soll nur auf Grundlage eindeutiger Vorgaben erfolgen. Daher sind vor der Entwicklung des Produktes Vorgaben an das zu entwickelnde Produkt zu ermitteln oder festzulegen. Dazu gehören Funktions- und Leistungsbeschreibungen, gesetzliche und behördliche Anforderungen sowie interne Richtlinien, Unterlagen und Erkenntnisse vorangegangener Entwicklungen[31].

Alle Entwicklungsergebnisse müssen freigegeben werden und vor der Freigabe einer Verifizierung unterzogen werden. Dabei sind die Entwicklungsergebnisse darauf zu prüfen, ob sie die Entwicklungsvorgabe erfüllen, Abnahmekriterien für das Produkt enthalten sowie Merkmale für den sicheren und bestimmungsgemäßen Gebrauch enthalten[32]. Eine Verifizierung muss gemäß zuvor festgelegten Regeln erfolgen. Die Ergebnisse der Verifizierung müssen aufgezeichnet werden[33].

An geeigneten Stellen im Entwicklungsprozess, die Norm spricht von Phasen, müssen systematische Entwicklungsbewertungen vorgenommen werden. Die Norm spezifiziert nicht näher, an welchen Stellen dies zu geschehen hat. Häufig erfolgt dies etwa nach Abschluss aller Designaktivitäten. Bei dieser Bewertung ist insbesondere zu beachten, ob alle Produktanforderungen erfüllt werden können und ob mögliche Probleme für die nachfolgenden Entwicklungsschritte erkennbar sind und anschließend geeignete Maßnahmen vorzuschlagen[34].

---

[28] [ISO 9001], Abschnitt 7.2.2c, S.88.

[29] [ISO 9001], Abschnitt 7.2.2, S.88.

[30] [ISO 9001], Abschnitt 7.3.1, S.89.

[31] [ISO 9001], Abschnitt 7.3.2, S.89f.

[32] [ISO 9001], Abschnitt 7.3.3, S.90.

[33] [ISO 9001], Abschnitt 7.3.5, S.90.

[34] [ISO 9001], Abschnitt 7.3.4, S.90.

Zudem muss eine Entwicklungsvalidierung gemäß festgelegter Regeln durchgeführt werden, um sicherzustellen, dass das Produkt in der Lage ist, die Anforderungen für die festgelegte Anwendung oder den beabsichtigten Gebrauch zu erfüllen.

3.1.7 Qualitätsmanagement für Medizingeräte

Wie bereits oben erwähnt, hat sich das technische Komitee TC210, das für Qualitätsmanagementsysteme medizinischer Geräte zuständig ist, auf Grund der großen Verbreitung der Normenreihe DIN EN ISO 9000:2000 entschlossen, die Normenreihe DIN EN ISO 9000:2000 als Grundlage der eigenen Norm zu verwenden.

Die Norm DIN EN ISO 13485 ist derzeit in der Version 2003 gültig. Diese Norm definiert Anforderungen an ein Qualitätsmanagementsystem einer Organisation, welche Ihre Fähigkeit zur Bereitstellung von Medizinprodukten darlegen muss, die sowohl Kundenanforderungen, als auch zutreffenden gesetzlichen Anforderungen genügen[35]. Primäres Ziel der Norm ist die Harmonisierung der für Medizinprodukte geltenden Anforderungen an Qualitätsmanagementsysteme. Daher werden einige Anforderungen der DIN EN ISO 9000 ausgeschlossen, die für Medizinprodukte als nicht geeignet betrachtet werden. Dies betrifft vor allem die in der DIN EN ISO 9000 geforderte Kundenorientierung (Kapitel 5.2) und Kundenzufriedenheit (Kapitel 8.2.1) sowie den Verbesserungsprozess (Kapitel 8.5). Als Begründung dafür wird in der Norm angegeben, dass „Kundenzufriedenheit“ zu subjektiv ist[36] bzw. dass die ständige Verbesserung des Qualitätsmanagementsystems kein angemessenes Ziel von Bestimmungen für Medizinprodukte sein kann[37].

Die Norm [ISO 9001] fordert lediglich für sechs Prozesse dokumentierte Verfahren, nämlich:

- Lenkung von Dokumenten[38],
- Lenkung von Aufzeichnungen[39],
- Interne Audits[40],
- Lenkung fehlerhafter Produkte[41],
- Korrekturmaßnahmen[42] und

[35] [ISO 13485], S. 7.

[36] [ISO 13485], S. 64.

[37] [ISO 13485], S. 67.

[38] [ISO 9001], Kapitel 4.2.3.

[39] [ISO 9001], Kapitel 4.2.4.

[40] [ISO 9001], Kapitel 8.2.2.

[41] [ISO 9001], Abschnitt 8.3.

- Vorbeugemaßnahmen[43].

Von der Norm [ISO 13485] werden darüber hinaus folgende dokumentierte Verfahren gefordert:

- Design- und Entwicklungsplanung. Die Organisation muss dokumentierte Verfahren für das Design und die Entwicklung festlegen. Bei der Design- und Entwicklungsplanung muss die Organisation weiterhin die Design- und Entwicklungsphasen festlegen. Für jede Phase muss die angemessene Bewertung und Verifizierung festgelegt werden. Weiterhin muss das Planungsergebnis dokumentiert werden und mit dem Fortschreiten von Design und Entwicklung aktualisiert werden[44].
- Beschaffungsprozess. Die Organisation muss dokumentierte Verfahren einführen, um sicherzustellen, dass die beschafften Produkte die festgelegten Beschaffungsanforderungen erfüllen[45].
- Identifikation. Die Organisation muss das Produkt mit geeigneten Mitteln während der Produktrealisierung identifizieren und muss dokumentierte Verfahren für eine solche Produktidentifizierung festlegen[46].
- Rückverfolgbarkeit. Die Organisation muss dokumentierte Verfahren für die Rückverfolgbarkeit erarbeiten. In dem Verfahren müssen der Umfang der Rückverfolgbarkeit und die erforderlichen Aufzeichnungen festgelegt werden[47].
- Produkterhaltung. Die Organisation muss dokumentierte Verfahren zur Erhaltung der Konformität des Produktes während der internen Verarbeitung und der Auslieferung zum vorgesehenen Bestimmungsort festlegen[48].
- Rückmeldung. Die Organisation muss ein dokumentiertes Verfahren für ein Rückmeldesystem einführen, damit frühzeitig Warnungen betreffend Qualitätsproblemen verarbeitet werden können und als Vorgabe für Korrektur- und Vorbeugemaßnahmen verwendet werden können[49].
- Datenanalyse. Die Organisation muss dokumentierte Verfahren zur Ermittlung, Erfassung und Analyse geeigneter Daten festlegen, um die Eignung und Wirksamkeit des

---

[42] [ISO 9001], Abschnitt 8.5.2.

[43] [ISO 9001], Abschnitt 8.5.3.

[44] [ISO 13485], Abschnitt 7.3.1, S. 18.

[45] [ISO 13485], Abschnitt 7.4.1, S. 21.

[46] [ISO 13485], Abschnitt 7.5.3.1, S. 23f.

[47] [ISO 13485], Abschnitt 7.5.3.2, S. 24.

[48] [ISO 13485], Abschnitt 7.5.5, S. 24f.

[49] [ISO 13485], Kapitel 8.2.1, S. 26.

Qualitätsmanagements darzulegen und zu beurteilen, ob eine Verbesserung des Qualitätsmanagementsystems erfolgen kann[50].

In allen anderen wesentlichen Punkten stimmt die DIN EN ISO 13485:2003 mit DIN EN ISO 9001:2000 überein.

3.2 Risikomanagement

Die Norm [ISO 14971] legt ein Verfahren fest, mit dem Gefährdungen erkannt, Risiken abgeschätzt, bewertet, kontrolliert und die Wirksamkeit dieser Kontrolle überwacht werden kann[51]. Die Norm kann damit als Verfahren für das wirksame Management der mit dem entwickelten Produkt in Zusammenhang stehenden Risiken dienen. Das Verfahren basiert auf der Tatsache, dass ein Risiko als aus zwei Komponenten bestehend angesehen werden kann[52]:

- Die Wahrscheinlichkeit des Auftretens eines Schadens (Schadenswahrscheinlichkeit)
- Die Folgen des Schadens (Schadenshöhe)

Die Vertretbarkeit eines Risikos ist im Wesentlichen durch diese beiden Komponenten beeinflusst. Die Norm fordert, dass durch die Organisation ein Risikomanagementprozess festgelegt und aufrechterhalten wird. Dieser Prozess muss dokumentiert werden und die folgenden Elemente beinhalten:

- Risikoanalyse
- Risikobewertung
- Risikokontrolle

Damit der Risikomanagementprozess angemessen durchgeführt werden kann, ist es erforderlich, dass die Organisation[53]:

- Ihre Grundsätze zur Festlegung vertretbarer Risiken unter Berücksichtigung einschlägiger Normen und Vorschriften bestimmt,
- die Verfügbarkeit der benötigten Mittel sicherstellt,
- das erforderliche, ausgebildete Personal bereitstellt und
- die Ergebnisse der Risikomanagementaktivitäten in regelmäßigen Abständen überprüft, um die Wirksamkeit des Risikomanagementprozesses sicherzustellen.

---

[50] [ISO 13485], Abschnitt 8.4, S. 28.

[51] [ISO 14971], Abschnitt 1, S. 4.

[52] [ISO 14971], Einleitung, S. 3.

[53] [ISO 14971], Abschnitt 3.3, S. 7.

Die oben angeführten Punkte müssen in der Risikomanagementakte dokumentiert werden.

3.2.1 Risikomanagementakte

Alle für das zu entwickelnde Medizinprodukt durchgeführten Aktivitäten müssen in der Risikomanagementakte dokumentiert werden[54].

3.2.2 Risikomanagementplan

Die Organisation muss für das zu entwickelnde Medizinprodukt einen Risikomanagementplan erstellen. Der Risikomanagementplan ist Bestandteil der Risikomanagementakte. Der Plan muss Folgendes enthalten[55]:

- Anwendungsbereich des Planes, wobei insbesondere die Lebenszyklusprozesse aufzuführen sind, für die der Plan gilt,
- einen Verifizierungsplan,
- die Anforderungen an die Bewertung der Risikoaktivitäten,
- Kriterien für die Vertretbarkeit von Risiken und
- Die Zuordnung von Verantwortlichkeiten

3.2.3 Risikoanalyse

Um mögliche Gefährdungen analysieren zu können ist es zunächst erforderlich, den bestimmungsgemäßen Gebrauch und den vorhersehbaren Missbrauch zu beschreiben. Dazu wird gefordert, eine Liste aller quantitativen und qualitativen Merkmale zu erarbeiten, die die Sicherheit des Medizinproduktes beeinflussen. Diese Daten sind in der Risikomanagementakte zu dokumentieren[56].

Darauf aufbauend ist eine Liste der bekannten und vorhersehbaren Gefährdungen zu erarbeiten, die sowohl den Normalfall des Medizingerätes als auch das Verhalten des Medizingerätes in Fehlersituationen berücksichtigt. Diese Daten sind in der Risikomanagementakte zu dokumentieren[57].

---

[54] [ISO 14971], Abschnitt 3.6, S. 7.

[55] [ISO 14971], Abschnitt 3.5, S. 7.

[56] [ISO 14971], Abschnitt 4.2, S. 10.

[57] [ISO 14971], Abschnitt 4.3, S. 10.

In Anschluss daran ist für jede zuvor festgestellte Gefährdung das Risiko dieser Gefährdung, also die Auftretenswahrscheinlichkeit und die Folgen, abzuschätzen. Zur Risikoeinschätzung können unterschiedliche Verfahren verwendet kommen, die Norm fordert kein bestimmtes Verfahren. Die Einschätzung der Risiken ist in der Risikomanagementakte zu dokumentieren[58].

3.2.4 Risikobewertung

Für jede während der Risikoanalyse identifizierte Gefährdung muss – unter Anwendung der im Risikomanagementplan festgelegten Kriterien – entschieden werden, ob das eingeschätzte Risiko so gering ist, dass eine Risikominderung nicht erforderlich ist, oder ob Maßnahmen zur Risikominderung festgelegt werden müssen. Die Risikobewertung ist in der Risikomanagementakte zu dokumentieren[59].

3.2.5 Risikokontrolle

Wenn eine Risikominderung erforderlich ist, muss der Hersteller Maßnahmen festlegen, um das Risiko auf ein vertretbares Maß zu reduzieren. Eine Maßnahme kann dabei die Wahrscheinlichkeit des Auftretens oder den Schweregrad des möglichen Schadens verringern. Dazu ist eines der aufgeführten Verfahren in der angeführten Reihenfolge anzuwenden:

- Zunächst muss versucht werden, das Risiko durch eine Änderung des Designs zu beseitigen oder zu verringern.
- Ist dies nicht möglich, sind Schutzvorrichtungen oder Schutzmaßnahmen vorzusehen.
- Ist auch dies nicht möglich, sind Sicherheitsinformationen vorzusehen.

Die ausgewählten Maßnahmen zur Risikokontrolle sind in der Risikomanagementakte zu dokumentieren[60].

Jedes Restrisiko, das nach der Durchführung der Maßnahmen zur Risikokontrolle verbleibt, muss anhand der im Risikomanagementplan festgelegten Kriterien bewertet werden. Die Bewertung ist in der Risikomanagementakte zu dokumentieren. Ist das verbleibende Risiko nicht vertretbar, müssen weitere Maßnahmen zur Risikominderung festgelegt werden[61].

---

[58] [ISO 14971], Abschnitt 4.4, S. 10f.

[59] [ISO 14971], Abschnitt 5, S. 11.

[60] [ISO 14971], Abschnitt 6.2, S. 11

[61] [ISO 14971], Abschnitt 6.4, S. 12.

Die zur Risikominderung festgelegten Maßnahmen müssen umgesetzt werden, und die Wirksamkeit der Maßnahmen muss verifiziert werden. Sowohl die Umsetzung, als auch Verifizierung muss in der Risikomanagementakte dokumentiert werden[62].

Ist das Restrisiko nach den festgelegten Kriterien weiterhin nicht vertretbar, weitere Maßnahmen zur Risikominderung aber nicht praktikabel, muss durch eine Risiko/Nutzen-Analyse bestimmt werden, ob der medizinische Nutzen das Restrisiko überwiegt. Die Ergebnisse der Bewertung müssen in der Risikomanagementakte dokumentiert werden[63].

Nachdem alle Maßnahmen der Risikokontrolle umgesetzt und verifiziert wurden, muss entschieden werden, ob das verbleibende Gesamtrestrisiko des Medizinproduktes, unter Zugrundelegung der festgelegten Kriterien, vertretbar ist. Die Ergebnisse der Bewertung müssen in der Risikomanagementakte dokumentiert werden[64].

Alle Ergebnisse des Risikomanagementprozesses müssen in einem Risikomanagementbericht aufgezeichnet werden. Dieser Bericht muss für jede Gefährdung

- die Rückverfolgbarkeit auf die Risikoanalyse,
- die Risikobewertung,
- die Durchführung und Verifizierung der Maßnahmen zur Risikokontrolle und
- die Bewertung, dass das Restrisiko vertretbar ist, enthalten.

3.3 Programmierbare elektrische medizinische Systeme

Bei der Norm DIN EN ISO 60601-1-4:1996+A1:1999 handelt es sich um eine Ergänzungsnorm zu EN 60601-1: Medizinische elektrische Geräte – Teil 1: Allgemeine Festlegungen für die Sicherheit. Diese Norm legt Anforderungen für den Entwicklungsprozess programmierbarer elektrischer medizinischer Geräte (PEMS) fest. Zweck dieser Norm ist es, als Anleitung für Sicherheitsanforderungen zu dienen, die den Zweck haben, Risiken zu reduzieren und zu beherrschen[65]. Diese Norm geht der [ISO 14971] zeitlich voraus, so dass es mit dieser Norm zahlreiche Überschneidungen gibt.

Die Norm fordert zunächst, dass für die Entwicklung eines PEMS ein Entwicklungsprozess für das Design definiert wird[66], der weiter in Teilprozesse[67] unterteilt ist. Weiterhin werden integrale

[62] [ISO 14971], Abschnitt 6.3, S. 12.

[63] [ISO 14971], Abschnitt 6.5, S. 12.

[64] [ISO 14971], Abschnitt 7, S. 12f.

[65] [ISO 60601-1-4], Abschnitt 1.201, S. 5.

[66] Die Norm spricht von einem Entwicklungs-Lebenszyklus.

Teilprozesse für das Risikomanagement und Problemlösung verlangt, die sich über den gesamten Entwicklungsprozess erstrecken. Zudem muss der Entwicklungsprozess Anforderungen an die Dokumentation enthalten[68]. Die Norm stellt weitere Anforderungen an die erforderlichen Prozesse.

3.3.1 Risikomanagementprozess

Für den Risikomanagementprozess muss ein Risikomanagementplan erstellt werden. Dieser Plan muss die folgenden Informationen enthalten:

- anzuwendender Entwicklungsprozess,
- Verantwortung des Managements,
- Risikomanagementprozess und
- Anforderungen an Reviews

Der Risikomanagementprozess muss weiterhin Verfahren zur Risikoanalyse und Risikobeherrschung enthalten[69].

Innerhalb der Risikoanalyse müssen für alle vernünftigerweise vorhersehbaren Umstände die Gefährdungen für Patienten, Anwender, Servicepersonal, Unbeteiligte sowie Umgebung und Umwelt ermittelt werden[70]. Als Ursachen müssen sowohl menschliche Eigenschaften, Fehler sowie Umgebungsbedingungen als auslösende Ursachen betrachtet werden[71]. Zudem müssen die vernünftigerweise vorhersehbaren Folgen von Ereignissen, die in einer Gefährdung resultieren, betrachtet werden[72]. Die in der Risikoanalyse eingesetzten Verfahren werden in der Norm nicht festgelegt, jedoch müssen diese Verfahren in der Risikomanagementdokumentation enthalten oder referenziert werden[73]. Weiterhin müssen die identifizierten Gefährdungen und ihre auslösenden Ursachen ebenfalls in der Risikomanagementdokumentation festgehalten werden[74].

---

[67] Die Norm sagt, dass eine Unterteilung in Phasen und Aufgaben erforderlich sei, mit jeweils klar definierten Eingängen, Ausgängen und Tätigkeiten. Diese Definition kann also durchaus als Teilprozess aufgefasst werden.

[68] [ISO 60601-1-4], Abschnitt 52.203.4, S. 10.

[69] [ISO 60601-1-4], Abschnitt 52.204.1, S. 10.

[70] [ISO 60601-1-4], Abschnitt 52.204.3.1, S. 10f.

[71] [ISO 60601-1-4], Abschnitt 52.204.3.1.5, S. 11.

[72] [ISO 60601-1-4], Abschnitt 52.204.3.1.4, S. 11.

[73] [ISO 60601-1-4], Abschnitt 52.204.3.1.8, S. 11.

[74] [ISO 60601-1-4], Abschnitt 52.204.3.1.10, S. 11.

Für jede ermittelte Gefährdung muss das zugehörige Risiko abgeschätzt werden[75]. Diese Abschätzung muss auf einem Verfahren beruhen, das sowohl die Wahrscheinlichkeit der Gefährdung als auch das Schadensausmaß berücksichtigt[76]. Das Verfahren muss dokumentiert werden[77].

Nachdem die Risiken identifiziert und abgeschätzt wurden, fordert die Norm, dass die Risiken beherrscht werden[78], d.h. wenn das Risiko nicht akzeptabel ist, müssen Maßnahmen getroffen werden, die das Risiko der Gefährdung auf ein akzeptables Maß reduzieren. Sowohl die gefundenen Maßnahmen als auch die Beurteilung der Wirksamkeit müssen dokumentiert werden[79].

Die bereits erwähnte Risikomanagementdokumentation muss also die folgenden Informationen enthalten:

- die ermittelten Gefährdungen und die zugehörigen auslösenden Ursachen,
- eine Abschätzung des Risikos,
- einen Verweis auf die angewendeten Sicherheitsmaßnahmen,
- die Beurteilung der Wirksamkeit der Risikobeherrschung und
- einen Verweis auf die durchgeführte Verifizierung.

3.3.2 Problemlösungsprozess

Auch der Problemlösungsprozess[80] muss als Teil des Entwicklungsprozesses definiert sein. Der Problemlösungsprozess kann – abhängig vom Problem – die folgenden Eigenschaften besitzen[81]:

- Einen Bericht von Sicherheits- oder Leistungsfähigkeitsproblemen erlauben
- Für jedes eine Beurteilung bezüglich der mit dem Problem verbundenen Risiken erlauben
- Die Handlungen festlegen, die zur Lösung jedes Problems führen
- Für jede Tätigkeit die Verfahren für die Validierung bzw. Verifizierung festlegen

---

[75] [ISO 60601-1-4], Abschnitt 52.204.3.2, S. 11.

[76] [ISO 60601-1-4], Abschnitt 52.204.3.2.2 / 52.204.3.2.3, S. 11.

[77] [ISO 60601-1-4], Abschnitt 52.204.3.2.4 / 52.204.3.2.5 S. 11.

[78] [ISO 60601-1-4], Abschnitt 52.204.4, S. 11.

[79] [ISO 60601-1-4], Abschnitt 52.204.4.6, S. 11.

[80] Die Norm spricht von einem definierten System für die Problemlösung innerhalb und zwischen allen Phasen und Aufgaben des Entwicklungs-Lebenszyklusses.

[81] [ISO 60601-1-4], Abschnitt 52.203.6, S. 10.

3.3.3 Entwicklungsprozess

Weiterhin müssen noch, ebenfalls unter dem Gesichtspunkt der Sicherheit, die folgenden Teilprozesse vorhanden sein:

- Erstellung der Systemspezifikation[82]: Für das PEMS und jedes seiner Subsysteme muss eine Spezifikation erstellt werden. Diese Spezifikation muss die risikobezogenen Funktionen detailliert aufführen. Zudem muss die Spezifikation die zur Beurteilung der Risiko-Beherrschungsmaßnahmen notwendigen Informationen enthalten.
- Erstellung der Systemarchitektur[83]: Für das PEMS und jedes seiner Subsysteme muss eine Architektur festgelegt werden. Dabei muss die Architektur der Systemspezifikation genügen. Weiterhin muss die Spezifikation der Architektur die Anforderungen zur Risikobeherrschung[84] sowie die Zuordnung der Risiko-Beherrschungsmaßnahmen zu Subsystemen berücksichtigen[85].
- Design und Implementierung: Das PEMS ist in Subsysteme und Komponenten zu zerlegen, wobei jedes Subsystem eine Design- und Prüfspezifikation besitzen muss[86].
- Verifikation: Es muss ein Verifizierungsplan erstellt werden, um zu zeigen, wie die Sicherheitsanforderungen verifiziert werden[87]. Die Verifizierung muss nach dem Verifizierungsplan durchgeführt werden und die Ergebnisse müssen ebenfalls dokumentiert werden[88]. Die bei der Verifizierung eingesetzten Verfahren und Techniken müssen dokumentiert werden[89].
- Validierung: Es muss ein Validierungsplan erstellt werden, um zu zeigen, dass die richtigen Sicherheitsanforderungen aufgestellt wurden[90]. Die Validierung muss nach dem Validierungsplan durchgeführt werden und die Ergebnisse der Validierung müssen dokumentiert werden[91]. Die bei der Validierung eingesetzten Verfahren und Techniken müssen dokumentiert werden[92].

---

[82] [ISO 60601-1-4], Abschnitt 52.206, S. 12.

[83] [ISO 60601-1-4], Abschnitt 52.207, S. 12.

[84] [ISO 60601-1-4], Abschnitt 52.207.3, S. 12.

[85] [ISO 60601-1-4], Abschnitt 52.207.5, S. 12f.

[86] [ISO 60601-1-4], Abschnitt 52.208, S. 13.

[87] [ISO 60601-1-4], Abschnitt 52.209.2, S. 13.

[88] [ISO 60601-1-4], Abschnitt 52.209.3, S. 13.

[89] [ISO 60601-1-4], Abschnitt 52.209.4, S. 13.

[90] [ISO 60601-1-4], Abschnitt 52.210.2, S. 13.

[91] [ISO 60601-1-4], Abschnitt 52.210.3, S. 13.

[92] [ISO 60601-1-4], Abschnitt 52.210.7, S. 13.

3.4 Software-Lebenszyklus-Prozess

Die Norm EN ISO 62304 ist aus der Kenntnis entstanden, das die Einhaltung von bestimmten Prozessen bei der Entwicklung und Wartung von Software für medizinische Produkte die Risiken für Patienten und andere Personen verringert.[93] Daher stellt die Norm ISO 62304 solche Anforderungen an die Prozesse der Softwareentwicklung, die bei angemessener Umsetzung erwarten lassen, dass die Software über das erwartete Maß an Sicherheit und Zuverlässigkeit verfügt. Die Norm fordert jedoch kein bestimmtes Vorgehensmodell bei der Softwareentwicklung[94]. Die Einhaltung der Norm definiert jedoch sowohl Abhängigkeiten zwischen den Prozessen als auch Anforderungen an die geforderten Prozesse selbst. Dazu werden die Prozesse in Aktivitäten zergliedert.

3.4.1 Allgemeine Anforderungen

Es sind keine Verfahren bekannt, die sicherstellen, dass durch ihren Einsatz eine geforderte Sicherheit oder Qualität eines Produktes tatsächlich vorhanden ist. Es gibt jedoch Prinzipien, von denen man nach dem Stand der Technik vermutet, dass der sachgerechte Einsatz dieser Prinzipien hilft, die Sicherheit oder Qualität eines Produktes tatsächlich zu verbessern.

Für die Softwaretechnik wird dies von den folgenden drei Prinzipien vermutet, die daher in der Norm gefordert sind. Dies sind:[95]

- Qualitätsmanagement,
- Risikomanagement und
- Softwaretechnik.

Anforderungen an ein Qualitätsmanagementsystem sind bereits in der [ISO 13485] festgelegt worden. In der EN ISO 62304 werden daher keine spezifischen Angaben für ein Qualitätsmanagement gemacht und lediglich die Anwendung der [ISO 13495] gefordert.[96]

Auch für den Risikomanagementprozess verzichtet die Norm darauf, einen eigenen Prozess für das Software-Engineering zu definieren.[97] Da es bereits die Norm [ISO 14971] für das Risikomanagement von Medizinprodukten gibt, fordert die Norm lediglich den Einsatz dieser Norm. Damit das Risikomanagement an allen wesentlichen Aktivitäten der Softwareentwicklung betei-

---

[93] [ISO prEN 62304], Anhang A, S. 31.

[94] Die Norm spricht durchgehend von einem „Lebenszyklus-Modell der Softwareentwicklung“.

[95] [ISO prEN 62304], Anhang B, S. 36.

[96] [ISO prEN 62304], Abschnitt 4.1, S. 11.

[97] [ISO prEN 62304], Abschnitt 4.2, S. 12.

ligt wird, wird lediglich bei den betreffenden Aktivitäten der Einsatz des Risikomanagement nochmals explizit gefordert. Jedoch macht die Norm teils spezifische Ergänzungen zu dem allgemeinen Risikomanagementprozess (s. Kapitel 3.4.6).

Das Risiko einer Gefährdung wird üblicherweise als Kombination angegeben, bestehend aus der Wahrscheinlichkeit des Auftretens eines Ausfalls kombiniert mit der Schwere der Schädigung, die sich durch den Ausfall ergibt. Es war aber im Normenausschuss keine Übereinstimmung über Verfahren zu erzielen, über die die Wahrscheinlichkeit des Auftretens eines Softwareausfalles bestimmt ist. Daher geht die Norm davon aus, dass ein Ausfall eintreten wird, und klassifiziert Software lediglich nach dem Schadensausmaß, der sich durch den Ausfall ergibt.[98] Die Software muss einer der folgenden Sicherheitsklassen zugeordnet werden:

- Klasse A: keine Verletzung ist möglich.
- Klasse B: keine schwere Verletzung ist möglich.
- Klasse C: Tod oder schwere Verletzung ist möglich.

3.4.2 Entwicklungsprozess

Der Hersteller muss seinen Softwareentwicklungsprozess im Softwareentwicklungsplan dokumentieren.[99] Dieser Prozess muss für alle Sicherheitsklassen des zu entwickelnden Softwaresystems angemessen sein und die folgenden Informationen enthalten:

- das Prozessmodell mit allen benutzten Prozessen[100],
- eine Strukturierung der Prozesse in Aktivitäten und Aufgaben,
- die Ausgaben der Aktivitäten und Aufgaben und
- ein Verfahren für die Dokumentation der Zusammenhänge zwischen Anforderungsmanagement, Prüfungsaktivitäten und Risikokontrollmaßnahmen.

Der Plan muss weiterhin:

- die für Systeme der Klasse C benutzten Normen, Methoden und Werkzeuge beschreiben[101],
- die für die Softwareintegration benutzen Verfahren beschreiben [102];

---

[98] [ISO prEN 62304], Abschnitt 4.3, S. 12.

[99] [ISO prEN 62304], Abschnitt 5.1, S. 12f.

[100] Also außer dem Softwareentwicklungsprozess mindestens noch Konfigurationsmanagementprozess, Änderungsmanagementprozess und Problemlösungsprozess.

[101] Mit „beschreiben“ ist gemeint, dass die Beschreibung entweder in dem Plan eingeschlossen oder in ihm referenziert wird.

- die für die Verifikation erforderlichen Aufgaben und Akzeptanzkriterien beschreiben[103],
- die für das Risikomanagement erforderlichen Aufgaben beschreiben[104],
- die für das Konfigurationsmanagement erforderlichen Aufgaben und Arten von Konfigurationselementen beschreiben[105],
- die für den Problemlösungsprozess erforderlichen Aufgaben beschreiben[106] und
- die während der Softwareentwicklung erzeugten Arten von Dokumenten beschreiben[107].

Soweit sich während der Entwicklung Änderungen ergeben, muss der Softwareentwicklungsplan angepasst werden.

3.4.2.1 Anforderungsanalyse

Jedes System[108] muss über Software-Systemanforderungen verfügen, die das System in dem für die Erstellung notwendigen Umfang beschreiben. Diese Anforderungen müssen von den Systemanforderungen an das Gesamtsystem abgeleitet sein.[109]

Typische Systemanforderungen sind[110]:

- Anforderungen an die Funktionalität und die Leistungsfähigkeit,
- Beschreibung der Schnittstellen mit Ein- und Ausgaben des Systems,
- Alarme, Warnungen und Benutzermeldungen,
- Anforderungen an Datensicherheit und Gebrauchstauglichkeit und
- Anforderungen an Installation, Betrieb und Wartung.

Dem System muss eine Sicherheitsklasse zugeordnet werden (s. 3.4.1). Für Systeme der Sicherheitsklasse B und C müssen Risikokontrollmaßnahmen in die Anforderungen einbezogen werden. Soweit erforderlich müssen die Anforderungen des Gesamtsystems ggf. angepasst werden.

---

[102] [ISO prEN 62304], Abschnitt 5.1.5, S. 14.

[103] [ISO prEN 62304], Abschnitt 5.1.6, S. 14.

[104] [ISO prEN 62304], Abschnitt 5.1.8, S. 14.

[105] [ISO prEN 62304], Abschnitt 5.1.10, S. 14f.

[106] [ISO prEN 62304], Abschnitt 5.1.12, S. 15.

[107] [ISO prEN 62304], Abschnitt 5.1.9, S. 14.

[108] Wenn nichts explizit anders erwähnt, ist mit System immer ein Software-System gemeint.

[109] [ISO prEN 62304], Abschnitt 5.2, S. 15. Natürlich ist dies nur möglich, wenn das Software-System, eine Teil eines Gesamtsystem ist.

[110] [ISO prEN 62304], Abschnitt 5.2.3, S. 15f.

Die Systemanforderungen müssen verifiziert werden. Dabei ist sicherzustellen, dass die Anforderungen[111]:

- die Anforderungen aus Gesamtsystem und Risikokontrollmaßnahmen korrekt spezifizieren,
- auf Anforderungen aus dem Gesamtsystem oder anderen Quellen zurückverfolgt werden können und
- verständlich, widerspruchsfrei und prüfbar sind.

3.4.2.2 Erstellung der Softwarearchitektur

Für Systeme der Sicherheitsklasse B und C muss eine Architektur erstellt und dokumentiert werden[112]. Diese Aktivität fordert eine strukturelle Zerlegung des Systems in Komponenten, eine Beschreibung der Eigenschaften dieser Komponenten und der Beziehung zwischen diesen Komponenten. Für Systeme der Klasse C muss die Aufteilung so gewählt werden, dass sie die Sicherheitsanforderungen wirksam umsetzt[113].

Sofern SOUP-Komponenten[114] eingesetzt werden, müssen Funktions- und Leistungsanforderungen für diese Komponente definiert werden[115]. Weiterhin müssen die für die Komponente benötigte Hardware und Software spezifiziert werden, die für den bestimmungsgemäßen Gebrauch erforderlich sind[116].

Die erstellte Architektur muss verifiziert werden. Dabei ist sicherzustellen, dass die Architektur:

- die Anforderungen für System, Gesamtsystem und Risikokontrollmaßnahmen korrekt spezifiziert,
- die Schnittstellen zwischen den einzelnen Komponenten unterstützt und
- die richtige Funktion der SOUP-Komponenten unterstützt.

---

[111] [ISO prEN 62304], Abschnitt 5.2.7, S. 16f.

[112] [ISO prEN 62304], Abschnitt 5.3, S. 17.

[113] [ISO prEN 62304], Abschnitt 5.3.6, S. 17.

[114] SOUP: Software unbekannter Herkunft. Software, die nicht entwickelt wurde, um in das in Entwicklung befindliche Medizingerät eingefügt zu werden, und für die der Entwicklungsprozess unbekannt ist.

[115] [ISO prEN 62304], Abschnitt 5.3.4, S. 17.

[116] [ISO prEN 62304], Abschnitt 5.3.5, S. 17.

3.4.2.3 Erstellung des Feindesigns[117]

Für Systeme der Sicherheitsklasse B und C muss die Architektur solange verfeinert werden, bis sie durch nicht weiter aufteilbare Softwarekomponenten dargestellt wird[118]. Jeder so definierten Komponente ist eine Sicherheitsklasse zuzuordnen. Für jede Komponente der Sicherheitsklasse C und alle Schnittstellen dieser Komponente muss ein detailliertes Design erstellt werden[119]. Das Design muss verifiziert werden. Dabei ist sicherzustellen, dass das Design:

- die Softwarearchitektur korrekt implementiert und keine Widersprüche zu der Architektur enthält und
- im erforderlichen Maße Zuverlässigkeitsfaktoren enthält[120].

3.4.2.4 Implementierung[121]

Jede Softwarekomponente muss implementiert werden. Für Komponenten der Sicherheitsklasse B oder C muss[122]:

- ein Verifizierungsprozess festgelegt werden,
- überprüft werden, ob die Anforderungen einschließlich der Risikokontrollmaßnahmen korrekt implementiert wurden,
- überprüft werden, ob die im Design beschriebenen Schnittstellen korrekt implementiert sind und
- überprüft werden, ob vorgegebene Programmierverfahren und Programmierrichtlinien eingehalten werden.

Für Komponenten der Sicherheitsklasse C muss zudem ein Verifizierungsplan festgelegt werden. Weiterhin ist für solche Komponenten explizit zu prüfen, ob die Komponente[123]:

- mit dem detaillierten Design übereinstimmt,
- Datenfluss und Kontrollfluss korrekt implementiert sind und

---

[117] Die Norm spricht von „detailliertem Design der Software“

[118] Solche Software-Komponenten, in der Norm Software-Einheiten genannt, sind Softwarekomponenten, für die keine weitere Verfeinerung vorgesehen ist. Die Entscheidung, eine Komponente nicht weiter zu zerlegen, kann aus Gründen des Designs, der Prüfung oder des Konfigurationsmanagements erfolgen.

[119] [ISO prEN 62304], Abschnitt 5.4, S. 18.

[120] Die Norm enthält eine Anzahl von Beispielen zu Zuverlässigkeitsfaktoren, die eingesetzt und überprüft werden können, s. [ISO prEN 62304], Abschnitt 5.4.5, S. 18.

[121] [ISO prEN 62304], Abschnitt 5.5, S. 18f.

[122] [ISO prEN 62304], Abschnitt 5.5.3, S. 19.

[123] [ISO prEN 62304], Abschnitt 5.5.4, S. 19.

- vorgegebene Verfahren zur Fehlerbehandlung richtig umgesetzt sind.

3.4.2.5 Software-Integration

Alle Softwarekomponenten sind gemäß den Festlegungen des Integrationsplans zu integrieren[124]. Für Komponenten der Sicherheitsklasse B und C muss verifiziert werden, dass alle Softwareeinheiten und Teilkomponenten korrekt integriert wurden.

Weiterhin ist für Komponenten der Sicherheitsklasse B und C eine Integrationsprüfung durchzuführen, die prüft, ob die Komponenten wie beabsichtigt funktionieren[125]. Dieser Integrationstest kann zusammen mit dem Software-Systemtest durchgeführt werden[126].

3.4.2.6 Prüfung[127]

Die Software muss basierend auf den Anforderungen[128] getestet werden. Für Komponenten der Sicherheitsklasse B und C ist für jede Anforderung eine Anzahl von Prüfungen zu definieren, die die Anforderung in dem erforderlichen Umfang prüfen[129]. Soweit Abweichungen während der Prüfung identifiziert wurden, sind diese in den Problemlösungsprozess einzubringen.

Die Prüfspezifikation muss verifiziert werden. Dabei ist darauf zu achten, dass die Softwareanforderungen in dem erforderlichen Umfang geprüft werden und die eingesetzten Prüfstrategien angemessen sind[130].

Für jede durchgeführte Prüfung[131] müssen die Ergebnisse der Prüfung aufgezeichnet werden. Die Aufzeichnung muss Angaben zu der Version der geprüften Software, den durchgeführten Prüfungen, den Prüfergebnissen und dem Prüfer enthalten.[132] Soweit erforderlich sind ebenfalls

---

[124] [ISO prEN 62304], Abschnitt 5.6.1, S.19.

[125] [ISO prEN 62304], Abschnitt 5.6.3, S. 20.

[126] [ISO prEN 62304], Abschnitt 5.6.4, Anmerkung, S. 20.

[127] Die Norm verlangt nur für Komponenten bzw. Systeme der Sicherklass B und C eine Prüfung. Aus allgemeinen Gründen wird man aber in der Regel auch für andere Komponenten und System auf Prüfungen nicht verzichten wollen.

[128] Gemeint sind die in der Aktivität „Analyse der Software-Anforderungen“ identifizierten und dokumentierten Software-Anforderungen.

[129] [ISO prEN 62304], Abschnitt 5.7.1, S. 21.

[130] [ISO prEN 62304], Abschnitt 5.7.4, S. 21.

[131] Dies betrifft auch Prüfungen nach der Lösung von Softwareproblemen innerhalb des Problemlösungsprozesses, s. [ISO prEN 62304], Abschnitt 9,10, S. 30.

[132] [ISO prEN 62304], Abschnitt 5.7.5, S. 21.

die Hardware- und Softwarekonfiguration und die benutzten Softwarewerkzeuge zu dokumentieren.[133]

3.4.2.7 Freigabe

Bevor die Software eingesetzt werden kann, muss sie freigegeben werden. Bevor die Freigabe erfolgen kann, müssen folgende Voraussetzungen erfüllt sein:

- die Verifizierung ist abgeschlossen und die Ergebnisse der Verifizierung wurden vollständig bewertet [134],
- eventuelle Abweichungen[135] wurden bewertet[136],
- die Dokumentation ist vollständig[137],
- die Software und die zugehörige Dokumentation wurden unter Konfigurationskontrolle gestellt,
- die Software, der zugehörige Quellcode und die Dokumentation wurden archiviert[138],
- es ist sichergestellt, dass die Software bei Bedarf erneut erstellt werden kann[139].

3.4.3 Wartungsprozess

Die Norm verlangt einen Wartungsprozess, durch den alle Rückmeldungen nach der Freigabe der Software verarbeitet werden. Die Norm fordert dabei, dass der Hersteller aktiv nach Rückmeldungen über das freigegebene Softwareprodukt sucht[140]. Der verwendete Wartungsprozess muss dokumentiert werden und Folgendes enthalten: [141]

- Verfahren über die Verarbeitung von Rückmeldungen[142] (also Empfang, Aufzeichnung, Bewertung, Lösung und Verfolgung);

---

[133] [ISO prEN 62304], Abschnitt 9.10, S. 30. In vielen Fällen wird dies aber wohl bereits in der Prüfspezifikation dokumentiert sein.

[134] [ISO prEN 62304], Abschnitt 5.8.1, S. 22.

[135] Die Norm spricht von „Anomalien“. Da es sich aber um Abweichungen zwischen spezifizierten und beobachtetem Verhalten handelt, scheint mir Abweichungen passender.

[136] [ISO prEN 62304], Abschnitt 5.8.3, S. 22.

[137] [ISO prEN 62304], Abschnitt 5.8.4, S. 22.

[138] [ISO prEN 62304], Abschnitt 5.8.7, S. 22.

[139] [ISO prEN 62304], Abschnitt 5.8.5, S. 22.

[140] [ISO prEN 62304], Abschnitt 6.2.1.1, S. 23.

[141] [ISO prEN 62304], Abschnitt 6.1, S. 23.

[142] Das sind Problemberichte und Änderungsanforderungen.

- Verwendung des Problemlösungsprozesses für die Analyse der Rückmeldungen[143];
- Verwendung des Problemlösungsprozesses für die Lösung von Problemberichten;
- Verwendung des Risikomanagementprozesses;
- Verwendung des Konfigurationsmanagementprozesses für die Handhabung von Änderungen an der bestehenden Software.

Der Wartungsprozess gilt für alle Komponenten und Systeme, unabhängig von der Sicherheitsklassifizierung. Rückmeldungen müssen entweder als Problemberichte[144] oder als Änderungsanforderungen klassifiziert werden. Die Rückmeldungen einschließlich der Analyse, Bewertung und der Lösung müssen dokumentiert werden.[145]

Für die Durchführung von Änderungsanforderungen ist ein definierter Änderungsprozess zu benutzen[146]. Änderungsanforderungen müssen vor ihrer Umsetzung hinsichtlich ihrer Auswirkung analysiert und bewertet werden. Vor der Benutzung des geänderten Softwaresystems ist eine weitere Prüfung und Freigabe erforderlich.

3.4.4 Problemlösungsprozess

Alle Probleme[147] in dem Softwaresystem müssen innerhalb eines definierten Problemlösungsprozesses bearbeitet werden. Für jedes Problem ist ein Problembericht zu erstellen, der Typ, Umfang und Kritikalität des Problems dokumentiert[148]. Soweit angemessen, müssen interessierte Parteien über bestehenden Probleme informiert werden[149].

Nachdem das Problem bekannt ist, muss es untersucht werden und, soweit erforderlich, Maßnahmen getroffen werden, um das Problem einer Lösung zuzuführen.[150] Jeder Problembericht

---

[143] Die Rückmeldungen können als Problemberichte interpretiert werden, und werden dann innerhalb des Problemlösungsprozesses gelöst.

[144] Problemberichte sind Rückmeldungen über tatsächliche oder mögliche Schadensereignisse bzw. wirkliche oder vermeintliche Abweichungen von der Spezifikation (s. [ISO prEN 62304], Abschnitt 6.2.1.3, S. 23).

[145] [ISO prEN 62304], Abschnitt 6.2.5, S. 24.

[146] Bei diesem Prozess kann es sich entweder um den Softwareentwicklungsprozess oder einen eigenen Änderungsprozess handeln.

[147] Die Norm weißt explizit darauf hin, dass Probleme sowohl vor als auch nach der Freigabe entstehen können. Daher kann der Problemlösungsprozess auch bereits während der Entwicklung des Softwaresystems eingesetzt werden, sofern kein alternativer Prozess dafür vorgesehen ist.

[148] [ISO prEN 62304], Abschnitt 9.1, S. 29.

[149] [ISO prEN 62304], Abschnitt 9.2, S. 29.

[150] [ISO prEN 62304], Abschnitt 9.3, S. 29.

ist auf mögliche Sicherheitsprobleme zu bewerten. Der Status eines Problemberichts muss verfolgt werden. Ist es erforderlich zur Lösung eines Problems die Implementierung zu ändern, so ist zuvor eine Änderungsspezifikation zu erstellen, die die geplante Änderung beschreibt. Vor der Umsetzung ist jede Änderungsspezifikation zu überprüfen und zu genehmigen[151]. Alle zur Umsetzung der Änderungsspezifikation erforderlichen Aktivitäten müssen zuvor identifiziert werden.[152] Vor der Benutzung des geänderten Softwaresystems ist eine weitere Prüfung und Freigabe erforderlich[153].

Alle in Zusammenhang mit einem Problembericht stehenden Unterlagen, einschließlich der Prüfungsunterlagen, müssen aufbewahrt werden[154]. Zudem müssen alle Problemberichte daraufhin analysiert werden, ob in den Problemberichten Trends zu entdecken sind[155].

3.4.5 Konfigurationsmanagementprozess

Alle Konfigurationselemente, aus denen das System besteht, sind einschließlich der Versionen dieser Elemente zu dokumentieren[156]. Dies schließt SOUP-Konfigurationselemente ein[157].

Konfigurationselemente dürfen nur als Reaktion auf eine genehmigte Änderungsspezifikation[158], mit anschließender Umsetzung[159], Verifikation[160] und erneuter Freigabe, geändert werden.

Jede Änderung an der bestehenden Konfiguration muss so dokumentiert werden, dass sie auf die zugehörigen Änderungsspezifikationen, Problemberichte und Änderungsanforderungen zurückverfolgt werden kann[161].

---

[151] [ISO prEN 62304], Abschnitt 9.6, S. 29f.

[152] [ISO prEN 62304], Abschnitt 8.2.2, S. 28. Die Norm weist darauf hin, dass nicht gefordert wird, dass die Implementierung der Änderung ein integraler Bestandteil eines Änderungskontrollprozesses sei. Die Änderung kann durchaus innerhalb des Softwareentwicklungsprozesses umgesetzt werden.

[153] [ISO prEN 62304], Abschnitt 9.7, S. 30.

[154] [ISO prEN 62304], Abschnitt 9.7, S. 30.

[155] [ISO prEN 62304], Abschnitt 9.8, S. 30.

[156] [ISO prEN 62304], Abschnitt 8.1.3, S. 27.

[157] Für SOUP-Elemente muss Titel, Hersteller und die eindeutige Kennzeichnung dokumentiert werden, s. [ISO prEN 62304], Abschnitt 8.1.1, S. 27.

[158] [ISO prEN 62304], Abschnitt 8.2.1, S. 28.

[159] [ISO prEN 62304], Abschnitt 8.2.2, S. 28.

[160] [ISO prEN 62304], Abschnitt 8.2.3, S. 28.

[161] [ISO prEN 62304], Abschnitt 8.2.4, S. 28.

3.4.6 Risikomanagementprozess

Die Norm verzichtet darauf, einen eigenen Risikomanagementprozess für die Softwareentwicklung zu definieren, und verweist insoweit auf die DIN EN ISO 14971:2000[162]. Jedoch ergänzt die Norm diesen Prozess um weitere Anforderungen.

Jede Komponente des Softwaresystems muss hinsichtlich der Frage, ob die Komponente zu einer Gefährdung beitragen kann, untersucht und entsprechend klassifiziert werden[163]. Für Komponenten, die der Sicherheitsklasse B und C zugeordnet wurden, sind die möglichen Ursachen der Gefährdung zu identifizieren[164]. Falls eine SOUP-Komponente zu einer Gefährdung beitragen kann, sind die von dem Hersteller der SOUP-Komponente herausgegeben Informationen angemessen zu berücksichtigen[165]. Alle identifizierten Ursachen möglicher Gefährdungen[166], sowie die möglichen Folgen dieser Gefährdungen[167] müssen dokumentiert werden.

Für Komponenten, die der Sicherheitsklasse B und C zugeordnet wurden, sind für jede Ursache, die zu einer Gefährdung führen kann, angemessene Maßnahmen festzulegen[168]. Werden die Maßnahmen durch Software umgesetzt, müssen diese Maßnahmen durch Softwareanforderungen an das Softwaresystem beschrieben werden[169], und die Umsetzung dieser Maßnahmen muss nach dem in der Norm beschriebenen Entwicklungsverfahren erfolgen[170] (s. Kapitel 3.4.2). Die Risikokontrollmaßnahme muss überprüft werden, um mögliche neue Gefährdungen, die durch die Maßnahme möglich sind, zu identifizieren und zu bewerten[171].

---

[162] [ISO prEN 62304], Abschnitt 4.2, S. 12.

[163] [ISO prEN 62304], Abschnitt 7.1, S. 25, siehe auch [ISO prEN 62304], Abschnitt 4.3, S. 12.

[164] [ISO prEN 62304], Abschnitt 7.1.2, S. 25.

[165] [ISO prEN 62304], Abschnitt 7.1.4, S. 25

[166] [ISO prEN 62304], Abschnitt 7.1.5, S. 25

[167] [ISO prEN 62304], Abschnitt 7.1.6, S. 26

[168] [ISO prEN 62304], Abschnitt 7.2.1, S. 26. Die angesprochenen Maßnahmen können sowohl in Hardware, in Software, in der Arbeitsumgebung oder durch die Bedienungsanleitung umgesetzt werden.

[169] [ISO prEN 62304], Abschnitt 7.2.2, S. 26.

[170] Gemeint ist, das die Maßnahmen zur Risikominimierung als integraler Teil des Softwaresystems betrachtet werden sollen, und daher in gleicher Weise umgesetzt werden sollen.

[171] [171] [ISO prEN 62304], Abschnitt 7.3.1, S. 26

3.5 Gebrauchstauglichkeit

Die Norm DIN EN 60601-1-6[172] entstand aus der Erfahrung, dass bei der Benutzung medizinischer Geräte in zunehmendem Maße Fehler auftreten, die auf die mangelnde Gebrauchstauglichkeit dieser Geräte zurückzuführen ist. Die Norm verlangt daher einen Prozess zur Analyse, Entwicklung, Gestaltung, Verifizierung und Validierung der Gebrauchstauglichkeit und beschreibt Anforderungen an einen solchen Prozess[173]. Dieser Prozess hat daher den primären Zweck Gefährdungen für Patienten, Anwender und andere Personen zu vermeiden, soweit die Gefährdungen mit der Gebrauchstauglichkeit in Verbindung stehen[174].

Alle Ergebnisse des Ergonomieprozesses müssen in der Ergonomieakte dokumentiert werden. In dieser Akte müssen zudem die folgenden Informationen dokumentiert werden:

- die Anwendung des Gerätes, einschließlich des medizinischen Zwecks, der Anwendungumgebung und des Anwenderprofils[175], zudem muss eine Zusammenfassung dieser Informationen in der Gebrauchsanleitung enthalten sein und
- die Hauptbedienfunktionen des Gerätes[176].

Die Gebrauchstauglichkeit muss einer Risikoanalyse nach DIN EN ISO 14791:2000 unterzogen werden. Daher müssen insbesondere die folgenden Punkte berücksichtigt werden[177]:

- die Spezifikation des Gerätes, einschließlich der Anwendungsumgebung und des Anwenderprofils,
- vorhersagbare Benutzungsfehler und
- Informationen über bekannte Fehler für gleichartige Benutzerschnittstellen und Geräte sowie Ergebnisse der Überprüfung der Benutzerschnittstellen des zu entwickelnden Gerätes.

Innerhalb des Ergonomieprozesses muss die Gebrauchstauglichkeit der Benutzerschnittstelle entwickelt und dokumentiert werden[178]. Diese Spezifikation muss Folgendes berücksichtigen[179]:

---

[172] DIN EN 60601-1-6 (VDE 0750-1-6) Medizinische elektrische Geräte – Teil 1-6: Allgemeine Festlegung für die Sicherheit – Ergänzungsnorm: Gebrauchstauglichkeit (IEC 60601-1-6:2004)

[173] [60601-1-6], Einleitung, S. 6.

[174] [60601-1-6], Abschnitt 46.201, S. 11.

[175] [60601-1-6], Abschnitt 46.202.2.1, S. 12.

[176] [60601-1-6], Abschnitt 46.202.2.2, S. 12.

[177] [60601-1-6], Abschnitt 46.203.2.3, S. 13.

[178] Diese Spezifikation kann in andere Spezifikationen integriert werden, wie etwa die Systemanforderungen.

[179] [60601-1-6], Abschnitt 46.203.3, S. 13f.

- die Spezifikation des Softwaresystems,
- Gefährdungen, die sich aus der korrekten Benutzung des Gerätes ergeben und
- Gefährdungen, die sich aus vorhersagbaren Fehlbedienungen ergeben.

Die Spezifikation der Gebrauchstauglichkeit muss Folgendes enthalten:

- Typische Benutzerszenarien für das Gerät,
- Anforderungen an die Benutzerschnittstelle für die Hauptbedienfunktionen und
- Benutzeraktionen für die Hauptbedienfunktionen,

Die Benutzerschnittstelle muss verifiziert[180] und validiert werden. Für die Validierung ist ein Validierungsplan erforderlich, in dem Folgendes behandelt werden muss:

- Benutzungsszenarien für den schlechtesten Fall, basierend auf der Spezifikation der Gebrauchstauglichkeit,
- vorhersagbare Benutzungsfehler und
- Ergebnisse der Risikoanalyse[181].

3.6 Medical Devices Guidance Documents

Bei den „Medical Devices Guidance Documents“ handelt es sich um nicht verbindliche Anleitungen der Europäischen Union, die in Zusammenarbeit mit Herstellern und Benannten Stellen erstellt wurden[182]. Dennoch wird unterstellt, dass den in diesen Dokumenten aufgestellten Forderungen nachgekommen wird[183]. Diese Anleitungen beschäftigen sich mit sehr unterschiedlichen Dingen, wie der Klassifikation von Medizingeräten, dem Verfahren der Konformitätsbewertung, der klinischen Erprobung und anderem. Jedoch enthalten sie bis auf MEDDEV 2.1/1 keine Anforderungen an die Softwareentwicklung. In MEDDEV 2.1/1 finden sich Angaben zu der Frage, wann Software als Medizingerät gilt. Dort ist festgelegt[184], dass Software, die die Funktionsfähigkeit eines medizinischen Gerätes beeinflusst entweder Teil eines Medizingerätes oder selbst ein Medizingerät ist. Handelt es sich hingegen um ein Vielzweckgerät, muss entschieden wer-

---

[180] [60601-1-6], Abschnitt 46.205.4, S. 13f.

[181] [60601-1-6], Abschnitt 46.205.5, S. 13f.

[182] http://ec.europa.eu/enterprise/medical_devices/meddev/index.htm, letzter Zugriff 13.08.2007.

[183] Due to the participation of the aforementioned interested parties and of experts from Competent Authorities, it is anticipated that the guidelines will be followed within the Member States and, therefore, ensure uniform application of relevant Directive provisions.

[184] http://ec.europa.eu/enterprise/medical_devices/meddev/2_1-1___04-1994.pdf, Kapitel I, 1.1 (f), S. 5f, letzter Zugriff 13.08.2007, letzter Zugriff 14.08.2007.

den, ob die Software für diagnostische oder therapeutische Zwecke eingesetzt wird. In diesem Fall muss die Software als Medizingerät behandelt werden, andern falls nicht.

3.7 Nationaler und internationaler Erfahrungsaustausch

Die Allgemeinen Akkreditierungsregeln sowie die Bestimmungen in den Bescheiden über die Akkreditierung und Benennung legen fest, dass die Benannten Stellen verpflichtet sind, sich am nationalen Erfahrungsaustausch (EK-Med) zu beteiligen[185]. Soweit im nationalen Erfahrungsaustauschkreis keine Vertretungsregelung getroffen wird, gilt die Verpflichtung auch für die Teilnahme am europäischen Erfahrungsaustausch[186]. Weiterhin wird gefordert, dass die Benannten Stellen die dort gefassten Beschlüsse und Dokumente anwenden[187].

Die Ergebnisse des nationalen Erfahrungsaustauschkreises werden als Sammlung der Antworten und Beschlüsse des EK-Med bekannt gemacht[188]. Die Dokumente sind nach Themenbereichen geordnet, die sich primär an den Artikeln der Richtlinie 93/42/EWG beziehungsweise den Paragraphen des Medizinproduktegesetzes (MPG) orientieren. Die Dokumente spiegeln den Sachverhalt zu einem bestimmten Zeitpunkt wider. Aus Kapazitätsgründen können sie nicht immer sofort an neue Gegebenheiten – z.B. gesetzliche oder normative Änderungen – angepasst werden. Für die Entwicklung von Software kommen die folgenden Antworten und Beschlüsse in Betracht:

- Mindestvoraussetzungen für Zertifizierungen nach [ISO 13485][189]. In diesem Dokument wird nachdrücklich darauf hingewiesen, dass eine Zertifizierung nach DIN EN ISO 13485:2003 nur ausgesprochen werden darf, wenn die zu zertifizierende Organisation die Anforderungen der Norm in ihrem Qualitätsmanagementsystem vollständig und nachweislich erfüllt. Die Nichterfüllung von elementaren Anforderungen, wie[190]:
    - die Einführung aller von der Norm geforderten Verfahren,
    - die Festlegung der Abfolge und Wechselwirkung der Prozesse,

---

[185] Antworten und Beschlüsse der EK-MED, 3.13 B.14, Teilnahme am europäischen Erfahrungsaustausch, http://www.zlg.de/download/ab/313_0306_B14.pdf, letzter Zugriff 14.08.2007.

[186] Die Akkreditierung erfolgt durch die Zentralstelle der Länder für Gesundheitsschutz bei Arzneimitteln und Medizinprodukten (ZLG), s. http://www.zlg.de, letzter Zugriff 14.08.2007.

[187] Die bei dem internationalen Erfahrungsaustausch entstandenen Dokumente sind unter http://www.team-nb.org/ zu finden, die nationalen Dokumente sich über http://www.zlg.de/ zugänglich.

[188] http://www.zlg.de/cms.php?PHPSESSID=4c73a5229737a88551e122c95cc70c4c&mapid=334, letzter Zugriff 14.08.2007.

[189] http://www.zlg.de/download/ab/305-0304.E11.pdf, letzter Zugriff 14.08.2007.

[190] zu Einzelheiten siehe Kapitel 3.1 Qualitätsmanagement.

- die Messung und Analyse von Prozessen,
- die Festlegung von (messbaren) Qualitätszielen und
- das Vorhandensein der von der Norm geforderten Aufzeichnungen und dokumentierten Anforderungen

stellen eine wesentliche Nichtkonformität dar, die eine Zertifizierung verhindern.

- Zertifizierung von vom Medizinprodukt unabhängiger Software[191]. In diesem Dokument dokumentiert der EK-Med seine Auffassung zu der Frage, wann Software als Medizinprodukt gilt. Inhaltlich gehen diese Festlegungen aber nicht über die in Kapitel 2.6 gemachten Feststellungen hinaus.

Von den Ergebnissen des internationalen Erfahrungsaustauschkreises ist für die Entwicklung von Software nur ein Beschluss von Relevanz[192]. In der Empfehlung "NB_MED/2.2/REC4 Software and Medical Devices" finden sich die folgenden Angaben:

- In Kapitel 3.1 finden sich zahlreiche Angaben zu der zu der Frage, wann Software als Medizinprodukt gelten. Inhaltlich gehen auch diese Feststellungen nicht über die in Kapitel 2.6 gemachten Feststellungen hinaus. Es werden aber zahlreiche Beispiele angeführt, die die dort gemachten Feststellungen illustrieren.[193].
- Kapitel 3.2 beschäftigt sich mit den Verfahren zur Feststellung der Konformität mit den grundlegenden Anforderungen. Dabei soll sichergestellt werden, dass[194]:
  - die Entwicklung Verfahren benutzt, die auf dem Konzept eines Entwicklungs-Lebenszyklus basiert und Verfahren für die Entwicklungsplanung, Risikomanagement, Verifikation und Validierung einsetzt,
  - Verfahren zur Dokumentenlenkung und zum Konfigurationsmanagement umgesetzt sind,
  - die Verantwortung des Managements festgelegt wurde und die Festlegung der erforderlichen Ressourcen durchgeführt wurde sowie
  - ein Qualitätsmanagement eingerichtet wurde, das angemessen Verfahren zur Entwicklungslenkung, Dokumentenlenkung und Lenkung von Qualitätsaufzeichnungen enthält.

---

[191] http://www.zlg.de/download/ab/307-1100.A01.pdf, letzter Zugriff 14.08.2007.

[192] [NB-MED-2.2/REC4].

[193] [NB-MED-2.2/REC4], Kapitel 3.1, S. 2ff.

[194] [NB-MED-2.2/REC4], Kapitel 3.2, S. 5ff.

- In Kapitel 3.3 werden noch Hinweise zum Änderungsmanagement gemacht. Es wird darauf hingewiesen, dass bei Änderungen an der Software sichergestellt sei muss, dass[195]:
    - das Medizingerät immer noch die grundlegenden Anforderungen erfüllt,
    - die Änderungen unter Verwendung des Konfigurationsmanagements dokumentiert werden,
    - die Änderungen validiert und verifiziert werden,
    - mögliche Sicherheitsrisiken, die durch die Änderungen verursacht sind, angemessen berücksichtigt werden und
    - durch das Konfigurationsmanagement eine klare Identifikation und Kontrolle der Softwareversionen sichergestellt ist.

3.8 Global Harmonization Task Force (GHTF)

Die „Global Harmonization Task Force“ (GHTF) wurde im Jahre 1992 mit den Ziel zu gegründet, die Anforderungen an die Entwicklung von Medizinprodukte weltweit einheitlich zu gestalten. Repräsentanten zuständiger Behörden und der Industrie aus den USA, Kanada, Australien, Japan und Europa schlossen sich zusammen, um gemeinsame Regeln zu erarbeiten, die als Leitlinien für Medizinprodukte gelten können. Um diesen Aufgaben nachzukommen wurde von der GHTF fünf Studiengruppen gebildet. Dies sind:

- Die Studiengruppe 1 beschäftigt sich mit dem Vergleich der verschiedenen regulatorischen Anforderungen in den verschiedenen Ländern und der Identifikation derjenigen Elemente die für eine Harmonisierung geeignet sind. Zudem ist diese Gruppe für die Harmonisierung der erforderlichen Informationen für die Zulassung zuständig.
- Die Studiengruppe 2 beschäftigt sich mit der Vereinheitlichung von Medizinprodukte-Beobachtungs- und –Meldungssystemen.
- Die Studiengruppe 3 ist für die Untersuchung der in den verschiedenen Ländern vorhandenen Qualitätsmanagementsysteme zuständig.
- Die Studiengruppe 4 ist für die Untersuchung der verschiednen Anforderungen an Audits und Auditoren in den unterschiedlichen Qualitätsmanagementsystemen zuständig.

[195] [NB-MED-2.2/REC4], Kapitel 3.3, S. 10f.

- Die Studiengruppe 5 beschäftigt sich mit den Anforderungen an klinische Sicherheit sowie Leistungsanforderungen an Medizingeräte. Zudem versucht diese Gruppe weltweit einheitliche Definitionen für häufig verwendete Begriffe zu etablieren.

Schon die Zusammensetzung der GHTF ist klar, dass die dort aufgestellten Leitlinien nicht verbindlich sein können. Aber die Zielsetzung der Gruppe macht auch deutlich, das eine Orientierung an diesen Vorgaben hilfreich ist, da sich die unterschiedlichen Gruppen darüber haben einigen können, da die dort verabschiedeten Dokumente letztendlich als Konsens aller beteiligten Gruppen aufgefasst werden können. Alle Dokumente sind über das Internet zugänglich. Von den dort[196] aufgefundenen Dokumenten sind die folgenden für die Softwareentwicklung bedingt relevant:

- SG1/N41R9:2005: Essential Principles of Safety & Performance of Medical Devices[197].
- SG3/N15R8:2005: Implementation of Risk Management Principles and Activities Within a Quality Management System[198].

3.8.1 Essential Principles of Safety and Performance

In diesem Dokument werden generelle Anforderungen an die Sicherheit von Medizingeräten beschrieben. Der überwiegende Teil der Feststellungen in diesem Dokument befasst sich mit chemischen, physikalischen und biologischen Risiken, und ist daher nicht für die Softwareentwicklung relevant. Es werden aber auch einige allgemeine Anforderungen an das Risikomanagement gestellt, die aber auch bereits durch die harmonisierten Normen abgedeckt sind:

- Medizingeräte sollen so entwickelt und produziert werden, dass bei bestimmungsgemäßen Gebrauch die Sicherheit von Patienten und Benutzern nicht gefährdet werden, und soweit Risiken verbleiben, diese Risiken gegen den Nutzen für den Patienten abgewogen werden[199].
- Es ist erforderlich, sowohl Sicherheitsprinzipien einzusetzen, als auch den allgemein anerkannten Stand der Technik bei der Entwicklung und Produktion zu berücksichtigen. Soweit Risikokontrollmaßnahmen erforderlich sind, soll der Hersteller diesen Prozess lenken, so dass die verbleibenden Risiken akzeptabel sind[200].

---

[196] http://www.ghtf.org/index.html, letzter Zugriff 14.08.2007.

[197] [SG1/N41R9].

[198] [SG3/N15R8].

[199] [SG1/N41R9], Kapitel 5.1, S 8.

[200] [SG1/N41R9], Kapitel 5.2 S. 8f.

3.8.2 Implementation of Risk Management Principles and Activities

Von Medizinherstellern wird verlangt, sowohl über ein Qualitätsmanagementsystem als auch über ein Risikomanagementsystem zu verfügen. Da sowohl Qualitätsmanagement als auch Risikomanagement vollständig in den Entwicklungs- und Produktionsprozess des Medizingerätes integriert sein soll, ist es sinnvoll über eine Integration dieser beiden Systeme nachzudenken. Der Leitfaden gibt Hinweise, wie eine Integration zwischen diesen beiden Systemen durchgeführt werden kann. Der überwiegenden Teil der Forderungen dieses Leitfadens sind aber bereits durch die Berücksichtigung von [ISO 13485] und [ISO 14971] erfüllt. Die wesentlichen Aussagen des Leitfadens sind:

- Die für das Risikomanagement erforderlichen Aktivitäten sollten als Verfahren innerhalb des Qualitätsmanagements definiert werden. Die Dokumente und Aufzeichnungen des Risikomanagement sollen als Dokumente und Aufzeichnungen des Qualitätsmanagements gelenkt werden[201].
- Das Top Management ist verantwortlich für die Einführung, Umsetzung und Aufrechterhaltung des Risikomanagements innerhalb der Organisation einschließlich der dafür notwendigen Aktivitäten und Ressourcen[202].
- Die erforderlichen Aktivitäten des Risikomanagements sollen den gesamten Lebenszyklus des Medizingerätes überdecken.[203].
- Die Entwicklungsplanung sollte die Koordination mit den zugehörigen Risikomanagementaktivitäten sicherstellen. Dazu ist es erforderlich, die Beziehungen zwischen Entwicklungs- und Risikomanagementaktivitäten zu identifizieren und die notwendigen Ressourcen zu planen[204].
- Entwicklungsvorgaben müssen beabsichtigten Gebrauch, Funktionalität, Leistungsanforderungen, Sicherheit, regulatorische Anforderungen sowie Risikokontrollmaßnahmen angemessen berücksichtigen. Bei allen vorgesehenen Änderungen müssen auch die möglichen Risiken betrachtet werden, um die Sicherheit und Leisitung des Gerätes nicht zu beeinträchtigen[205].

[201] [SG3/N15R8], Kapitel 3.1, S.7.

[202] [SG3/N15R8], Kapitel 4, S.7f.

[203] [SG3/N15R8], Kapitel 6, S.8.

[204] [SG3/N15R8], Kapitel 7.1, S.9.

[205] [SG3/N15R8], Kapitel 7.2, S.9f.

- Die als Entwicklungsvorgaben definierten Risikokontrollmaßnahmen müssen durch die Entwicklung verfolgt und in den Entwicklungsergebnissen identifiziert werden und hinsichtlich der angemessenen Umsetzung bewertet werden[206].
- Durch Entwicklungsreviews soll festgestellt, werden ob alle verbleibenden Restrisiken angemessen kommuniziert wurden und für das Gerät angemessen sind. Für die Entwicklungsreviews sollen risikobezogene Aufgaben definiert werden. In diesen Aufgaben soll ermittelt werden, ob[207]:
    - alle Gefährdungen identifiziert wurden, deren Risiko korrekt ermittelt wurde und ggf. die erforderlich Risikokontrollmaßnahmen festgelegt wurden und
    - die festgelegten Risikokontrollmaßnahmen wirksam sind.
- Durch Verifizierung soll der objektive Nachweis geführt werden, dass die identifizierten Risiken berücksichtigt wurden sowie die vorgesehenen Risikokontrollmaßnahmen umgesetzt wurden und wirksam sind[208].
- Durch die Validierung soll überprüft werden, inwieweit das Medizingerät Benutzeranforderungen erfüllt, für den beabsichtigten Gebrauch geeignet ist und inwieweit die verbleibenden Restrisiken den vorgegebenen Abnahmekriterien genügen[209].
- Die Erfahrung hat wiederholt gezeigt, dass selbst triviale Änderungen an dem Medizingerät nicht vorhergesehene und teilweise katastrophale Konsequenzen haben kann. Alle vorgesehen Änderungen sollen daher hinsichtlich ihrer Wirkung auf die Sicherheit des Gerätes bewertet werden[210].

[206] [SG3/N15R8], Kapitel 7.3, S.10f.

[207] [SG3/N15R8], Kapitel 7.4, S.11f.

[208] [SG3/N15R8], Kapitel 7.5, S.12.

[209] [SG3/N15R8], Kapitel 7.6, S.12.

[210] [SG3/N15R8], Kapitel 7.7, S.12f.

4 Vorgaben für den amerikanischen Markt

Die Anforderungen an Medizinprodukte sind in dem „Federal Food, Drug, and Cosmetic Act", zuletzt geändert am 31. Dezember 2004[211], in Abschnitten 513 bis 523 festgelegt. Die amerikanische Gesundheitsbehörde „Food and Drug Administration" (FDA) ist für die Umsetzung dieser Forderungen, und damit für die Sicherheit, Verträglichkeit und Wirksamkeit von Medizinprodukten, die in den USA verkauft werden, zuständig. Zur Präzisierung der gesetzlichen Forderungen hat die FDA Verordnungen erlassen, die die Anforderungen an das Gesetz näher bestimmen[212]. Für Medizingeräte werden 33 Verordnungen aufgeführt, die teils nur für bestimmte Arten von Medizinprodukten zutreffend sind, teils auf mehrere Arten von Medizinprodukten angewendet werden sollen. Diese Verordnungen werden ergänzt durch Verordnungen für die Zulassung von Geräten. Für die Entwicklung von Software ist aber lediglich die Verordnungen CFR 21, Part 820, „Quality System Regulation" relevant.

Die Vorstellungen der FDA werden teilweise durch so genannte Guidance-Dokumente präzisiert[213]. Diese Dokumente dokumentieren die Vorstellungen der FDA zu einem bestimmten Thema, sind aber nicht eigentlich verbindlich. Da die FDA aber diese konkretisierten Vorstellungen bei der Zulassung berücksichtigen wird, werden sie zweckmäßigerweise bei der Umsetzung der FDA-Anforderungen berücksichtigt. Einige dieser Anleitungen sind auch für die Softwareentwicklung relevant sind. Dieses sind:

- Design Control Guidance for Medical Device Manufacturers[214],
- General Principles of Software Validation - Final Guidance for Industry and FDA Staff[215],
- Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices - Guidance for Industry and FDA Staff[216].
- Medical Device Use-Safety: Incorporating Human Factors Engineering into Risk Management[217],
- Do It By Design - An Introduction to Human Factors in Medical Devices[218],

---

[211] [FDA-Act].

[212] [21CFR820].

[213] http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfGGP/Search.cfm, letzter Zugriff 17.07.2007.

[214] [FDA-DesignGuide].

[215] [FDA-Validation].

[216] [FDA-Premarket].

[217] [FDA-HumFactors].

- Guidance for Off-the-Shelf Software Use in Medical Devices[219],
- Guidance for Industry - Cyber security for Networked Medical Devices Containing Off-the-Shelf (OTS) Software[220],

4.1 Zulassung von Medizinprodukten in den USA

Zur Zulassung eines Medizinprodukts durch die amerikanische Bundesgesundheitsbehörde FDA gibt es je nach Produkt und Risikoklasse[221] grundsätzlich zwei unterschiedliche Verfahren, die Zulassung nach §510(k) und die Zulassung durch Premarket Approval.

4.1.1 Zulassung nach §510(k)

Bei der Zulassung nach §510 (k) des "Federal Food, Drug and Cosmetic Act" handelt es sich um eine vereinfachtes, rein formales Zulassungsverfahren. Medizinprodukte können nach diesen Verfahren unter den folgenden Voraussetzungen zugelassen werden:

- Es handelt sich um ein Produkt der Risikoklasse I oder II.
- Ein vergleichbares Produkt ist vor dem 28.05.1976 in den USA auf dem Markt gewesen[222]
- Es ist keine klinische Studie erforderlich.

4.1.2 Zulassung durch Premarket Approval (PMA)

Produkte, die nicht nach §510(k) zugelassen werden können, also insbesondere alle Medizinprodukte der Klasse III, sog. "significant risk devices", müssen nach dem PMA[223]/IDE[224]-Verfahren[225] zugelassen werden. Dazu fordert das FDA im Normalfall vom Antragsteller die Durchführung einer klinischen Studie und gewährt auf Antrag eine Ausnahmegenehmigung zum Einsatz des Produkts bei einer bestimmten Anzahl von Patienten und festgelegten Krankenhäusern bzw. Ärzten ("Investigators"). Aus rechtlicher Sicht dient sie auch dazu, den Hersteller wäh-

---

[218] [FDA-DoIt].

[219] [FDA-OTS].

[220] [FDA-Cybersecurity]

[221] [21CFR860]

[222] ("substantially equivalent / predicate Device").

[223] PMA = Premarket Approval

[224] IDE = Investigational Device Exemption

[225] Geregelt in [21CFR814]

rend der Studie vor Produkthaftungsklagen zu schützen. Weiterhin ist zum Einsatz des Produkts im Rahmen der IDE die Zustimmung der zuständigen Ethikkommission (HEC oder IRB) einzuholen.

Die Zulassung gemäß PMA gliedert sich in folgende Teile:

- Erstellung der Antragsunterlagen mit Studienprotokoll und produktspezifischen Informationen,
- IDE-Antragstellung bis Genehmigung,
- Durchführung der IDE-Studie,
- Studien-Abschlussbericht mit Anerkennung der gewonnenen Daten durch FDA,
- Antrag auf PMA-Zulassung unter Zugrundelegung der IDE Daten,
- PMA-Erteilung.

4.2 21 CFR Part 820 - Quality System Regulation

Bei der „Quality System Regulation“[226] handelt es sich um eine Verordnung zur Einführung von so genannter „Good Manufacturing Practice“ bei der Herstellung, Entwicklung, Validierung, Verpackung, Lagerung und Installation von Medizingeräten, und gilt daher auch für die Entwicklung medizinischer Software. Allerdings enthält die Verordnung keine spezifischen Anforderungen an die Softwareentwicklung.

Die Verordnung weist darauf hin, dass die Nichteinhaltung einer laut der Verordnung anzuwendenden Bestimmung bedeutet, dass das Gerät nach Paragraph 501(h) unstatthaft verändert wurde. In diesem Fall werden der für die Nichteinhaltung verantwortlichen Person gesetzliche Maßnahmen angedroht[227].

4.2.1 Anforderungen an das Qualitätsmanagement

Die Verordnung stellt in Subchapter B Anforderungen an das Qualitätsmanagement[228]. Die in diesem Kapitel aufgestellten Forderungen sind durch die Verwendung der DIN EN ISO 13485:2003 bereits abgedeckt. Im Einzelnen ist in Unterkapitel B Folgendes gefordert:

- Festlegen einer Qualitätspolitik (s. [ISO 13485), Abschnitt 5.3),

[226] [21CFR820].

[227] [21CFR820], Sect.1 (3) (c), S. 12.

[228] Die Verordnung spricht von „Quality Systems Requirements“. Inhaltlich handelt es sich um Anforderungen an ein Qualitätsmanagementsystem.

- Festlegen einer angemessenen Organisationsstruktur, Festlegen von Befugnissen und Bereitstellen von Ressourcen (s. [ISO 13485), Abschnitt 5.5 und 6),
- Überprüfung der Eignung und Wirksamkeit des Qualitätsmanagementsystems (s. [ISO 13485), Abschnitt 4.1 und 8),
- Festlegung von Qualitätspraktiken, -ressourcen und –aktivitäten durch einen Qualitätsplan (s. [ISO 13485), Kapitel 5),
- Festlegung der für das Qualitätssystem relevanten Verfahren (s. [ISO 13485), Abschnitt 4),
- Durchführen von Audits, zur Überprüfung der Leistung des Qualitätssystems (s. [ISO 13485), Abschnitt 8.2.2),
- Bereitstellen des erforderlichen Personals (s. [ISO 13485), Abschnitt 6.2) und
- Schulung des Personals (s. [ISO 13485), Abschnitt 6.2.2).

4.2.2 Entwicklungslenkung

In Subchapter C werden Anforderungen an die Entwicklungslenkung gestellt, um sicherzustellen, dass die Entwicklungsanforderungen erfüllt werden. Geräte der Klasse II und III, sowie mit Computer-Software automatisierte Geräte der Klasse I unterliegen der Entwicklungslenkung, daher kann davon ausgegangen werden, dass diese Verfahren grundsätzlich bei der Entwicklung medizinischer Software einzuhalten sind. Im Einzelnen sind gefordert[229]:

- die Planung der Entwicklungstätigkeiten einschließlich Festlegung der Schnittstellen zu anderen Teilen, die einen Beitrag zu den Entwicklungsprozessen leisten[230] (s. [ISO 13485), Abschnitt 7.1 und 7.3.1),
- ein Verfahren zur Ermittlung der Anforderungen und des vorgesehenen Gebrauchs des Systems, einschließlich eines Verfahrens zur Berücksichtigung von unvollständigen Anforderungen[231] (s. [ISO 13485], Abschnitt 7.2.1, 7.2.2 und 7.3.2),
- ein Verfahren, durch das die Entwicklungsergebnisse (Design output) in einer Form dokumentiert werden, die eine Überprüfung mit den Entwicklungsvorgaben erlauben. Dieses Verfahren muss Annahmekriterien enthalten. Das Entwicklungsergebnis muss do-

[229] Die Klassifikation der medizinischen Geräte ist in [21CFR860) geregelt.

[230] [21CFR820], Sec. 30 (b).

[231] [21CFR820], Sec. 30 (c).

kumentiert, überprüft und vor der Freigabe genehmigt werden[232] (s. [ISO 13485], Abschnitt 7.3.3),

- ein Verfahren, um sicherzustellen, dass formale Reviews des Entwicklungsfortschritts zu bestimmten Zeitpunkten innerhalb des Entwicklungsprozesses vorgesehen und durchgeführt werden[233] (s. [ISO 13485], Abschnitt 7.2.3),
- ein Verfahren zur Überprüfung der Geräteentwicklung. Dieses Verfahren muss bestätigen, dass das Entwicklungsergebnis den Anforderungen der Entwicklungsvorgaben genügt[234] (s. [ISO 13485], Abschnitt 7.3.5),
- ein Verfahren zur Validierung. Dieses Verfahren muss sicherstellen, dass das Gerät den Benutzeranforderungen genügt und für die beabsichtigte Verwendung (intended use) geeignet ist. Soweit angemessen, muss dieses Verfahren Softwarevalidierung und Risikoanalyse mit einschließen[235] s. [ISO 13485], Abschnitt 7.3.6),
- ein Verfahren zur Identifikation, Dokumentation, Überprüfung, Genehmigung und Freigabe von Entwicklungsänderungen[236] (s. [ISO 13485], Abschnitt 7.37),
- das Pflegen einer Entwicklungsentstehensakte (Design history file). Diese Akte muss alle notwendigen Aufzeichnungen enthalten, oder darauf verweisen, die erforderlich sind, um zu belegen, dass die Entwicklung in Übereinstimmung mit den Vorschriften von Sec. 820.30 durchgeführt wurden[237].

4.2.3 Dokumentenlenkung

Subchapter D[238] fordert ein Verfahren zur Lenkung von Dokumenten. Im Einzelnen sind gefordert:

- Die Anforderungen zur Lenkung von Dokumenten (document approval and distribution) decken sich im Wesentlichen mit den Anforderungen aus [ISO 13485], Abschnitt 4.2.3. Zusätzlich wird gefordert, dass die Genehmigung des Dokumentes einschließlich Datum und Unterschrift der genehmigenden Person(en) dokumentiert werden muss[239].

---

[232] [21CFR820], Sec. 30 (d).

[233] [21CFR820], Sec. 30 (e).

[234] [21CFR820], Sec. 30 (f).

[235] [21CFR820], Sec. 30 (g).

[236] [21CFR820], Sec. 30 (i).

[237] [21CFR820], Sec. 30 (j).

[238] [21CFR820], Sec. 40.

[239] [21CFR820], Sec. 40 (a).

- Die Anforderungen zur Änderung von Dokumenten (document changes) decken sich ebenfalls weitgehend mit den Anforderungen aus [13485]. Es wird wieder gefordert, die Genehmigungen mit Datum und Unterschrift der genehmigenden Person(en) zu dokumentieren[240].

4.2.4 Beschaffung

Subchapter E fordert ein Verfahren, durch das sichergestellt wird, dass die beschafften Waren und Dienstleistungen mit den spezifizierten Anforderungen übereinstimmen.

- Es wird gefordert, für Lieferanten, Auftragsnehmer und Berater Anforderungen festzulegen, die von diesen erfüllt werden müssen, die Erfüllung dieser Anforderungen zu bewerten und diese Bewertung zu dokumentieren, sowie das Maß an Kontrolle festzulegen, das auf der Basis der durchgeführten Bewertung erforderlich ist (Evaluation)[241] (s. [ISO 13485), 7.4.1).
- Für jedes beschaffte Produkt und jede Dienstleistung müssen die erforderlichen Daten festgelegt werden, die die erforderlichen Anforderungen präzise beschreiben (Purchasing data). Soweit möglich, soll sichergestellt werden, dass der Hersteller bei Änderungen der Anforderungen durch Lieferanten, Auftragsnehmer und Berater über die Änderungen informiert wird[242] (s. [ISO 13485), 7.4.2)..

4.2.5 Identifikation und Rückverfolgbarkeit

Subpart F fordert ein Verfahren zur Identifikation des Medizinproduktes über die gesamte Produktion hinweg, von Empfang, Produktion, Verteilung bis zur Installation. Da Softwaresysteme im herkömmlichen Sinne nicht produziert werden, betrifft dies also nur Empfang (für extern erstellten Komponenten und SOUP), Verteilung und Installation. Im Einzelnen sind gefordert (s. [ISO 13485), Abschnitt 7.5.3):

- Ein Verfahren, zur Produktidentifikation über alle Stufen hinweg[243].
- Soweit das Medizingerät zu einer wesentlichen Verletzung von Patient oder Anwender[244] führen kann, muss ein Verfahren festgelegt werden, das die Identifikation von Los, Charge, Einheit und soweit erforderlich Komponenten über Kontrollnummern erlauben[245].

---

[240] [21CFR820], Sec. 40 (b).

[241] [21CFR820], Sec. 50 (a).

[242] [21CFR820], Sec. 50 (b).

[243] [21CFR820], Sec. 60.

[244] Die Verordnung spricht von „significant injury of the user“.

4.2.6 Herstell- und Prozesskontrolle

Subpart G fordert, dass die Herstellprozesse definiert, umgesetzt, gelenkt und überwacht werden, um sicherzustellen, dass das Gerät mit seinen Spezifikationen übereinstimmt[246]. Anschließend werden Anforderungen an diese Prozesse und an die Inspektions-, Mess- und Prüfeinrichtungen dieser Prozesse definiert[247]. Dadurch soll sicherstellt werden, dass diese Einrichtungen für den vorgesehenen Zweck geeignet sind und die notwendige Genauigkeit haben. Zudem wird weiterhin ein Verfahren zur Prozessvalidierung gefordert, soweit ein Prozess durch nachfolgende Inspektion und Prüfung nicht vollständig verifiziert werden kann[248]. Da Software keine Produktion im eigentlichen Sinn benötigt, entfallen die Anforderungen dieses Kapitels für die Softwareentwicklung.

4.2.7 Abnahme

Subpart H fordert ein Verfahren für alle notwendigen Abnahmetätigkeiten. Diese Abnahmetätigkeiten schließen alle erforderlichen Überprüfungstätigkeiten ein[249]. Im Einzelnen wird gefordert:

- ein Verfahren zu Prüfung von Lieferungen (Wareneingangskontrolle)[250] (s. [ISO 13485), 7.4.3),
- ein oder mehrere Verfahren zur Prüfung während der Herstellung, soweit dies angebracht ist[251] (s. [ISO 13485), 7.5.1),
- ein Verfahren zur Abnahme des fertigen Gerätes[252] und
- die Dokumentation der durchgeführten Abnahmetätigkeiten, einschließlich Datum, Ergebnis und Unterschriften der Personen, die die Abnahme durchgeführt haben. Diese Aufzeichnungen sind Teil des DMR[253].

---

[245] [21CFR820], Sec. 65.

[246] [21CFR820], Sec. 65.

[247] [21CFR820], Sect. 72.

[248] [21CFR820], Sect. 75.

[249] [21CFR820], Sect. 80 (a).

[250] [21CFR820], Sect. 80 (b).

[251] [21CFR820], Sect. 80 (c).

[252] [21CFR820], Sect. 80 (d).

[253] Device Master Record – übersetzt als Gerätehauptakte

4.2.8 Nicht-konforme Produkte

Die Verordnung fordert in Subchapter I Verfahren für die Lenkung von Produkten, die nicht den Anforderungen genügen. Das Kapitel bezieht sich jedoch ausschließlich auf Produkte[254], und damit nicht auf Software, da Software keinen Herstellprozess im eigentlichen Sinn benötigt[255].

4.2.9 Korrektur- und vorbeugende Maßnahmen

Die Verordnung fordert in Subchapter J Verfahren für Korrektur und Vorbeugungsmaßnahmen. Die dort aufgestellten Forderungen sind bereits in der [ISO 13485] gefordert, vor allem in Abschnitt 8.5.2 (Korrekturmaßnahmen) und Abschnitt 8.5.3 (Vorbeugemaßnahmen). Im Einzelnen ist in Subchapter J Folgendes gefordert:

- ein Verfahren für die Durchführung von Korrektur- und vorbeugenden Maßnahmen[256] ,
- die Analyse aller vorhandenen Qualitätsaufzeichnungen, um potentielle und existierende Qualitätsprobleme zu identifizieren[257],
- die Untersuchung der Ursache von Nicht-Übereinstimmungen, die sich auf Produkte, Prozesse und das Qualitätsmanagementsystem beziehen[258],
- die Festlegung der notwendigen Aktionen für Nacharbeit und Korrekturmaßnahmen[259],
- die Verifizierung oder Validierung der festgelegten Maßnahmen[260],
- die Umsetzung und Dokumentation der festgelegten Maßnahmen[261] und
- die Weiterleitung der erforderlichen Informationen an die betroffenen Stellen[262].

---

[254] [21CFR820], Sect. 3 (r) : Product means component, manufacturing material, in-process devices, finished devices and returned devices ("Produkt meint Bauteil, Fertigungsmaterial, in Bearbeitung befindliche Geräte, fertige Geräte und Rückwaren"), eigene Übersetzung.

[255] Die dort verlangten Verfahren decken sich aber weitgehend mit den Forderungen in [ISO 13485], Abschnitt 8.3

[256] [21CFR820], Sect. 100 (a).

[257] [21CFR820], Sect. 100, (a) (1).

[258] [21CFR820], Sect. 100, (a) (2).

[259] [21CFR820], Sect. 100, (a) (3).

[260] [21CFR820], Sect. 100, (a) (4).

[261] [21CFR820], Sect. 100, (a) (5) und (b).

[262] [21CFR820], Sect. 100, (a) (6).

4.2.10 Aufzeichnungen

Alle erforderlichen Aufzeichnungen müssen an einem Ort geführt werden, der für den FDA-Inspektor zugänglich sein muss. Von Aufzeichnungen, die in automatisierten Datenverarbeitungssystemen gespeichert sind, müssen Sicherungskopien erstellt werden[263].

4.2.10.1 Gerätehauptakte (Device Master Record)

Sect. 820.181 fordert das Führen einer Gerätehauptsakte. Dabei sind die Anforderungen an die Dokumentenlenkung zu berücksichtigten (s. Kapitel 4.2.3). Die Gerätehauptsakte muss die folgenden Informationen enthalten:

- Spezifikationen.
- Spezifikation der eingesetzten Prozesse,
- Qualitätssicherungsverfahren und zugehörige Spezifikationen einschließlich Abnahmekriterien und
- Verfahren und Methoden zu Installation, Instandhaltung und Wartung.

4.2.10.2 Geräteentstehungsakte

Sect. 820.184 fordert weiterhin das Führen einer Geräteentstehungsakte (Device History Record / DHR). Die Akte enthält alle Daten, die von nach Sect. 820.60 Identification und Sect 820.65 Traceability geforderten Verfahren kommen. Die Geräteentstehungsakte muss insbesondere folgende Informationen enthalten:

- Herstelldatum und Herstellmenge,
- Aufzeichnungen, die belegen, dass gemäß DMR produziert wurde und
- die Identifizierung der Produkte

4.2.10.3 Qualitätssystemsakte

Sect. 820.186 fordert das Führen einer Qualitätssystemsakte. Dieses Dokument muss alle nicht produktspezifischen Verfahren dokumentieren.

4.2.11 Beanstandungen und Beanstandungsakte

Sect. 820.186 fordert ein Verfahren für den Empfang, die Überprüfung und Auswertung von Beanstandungen. Das Verfahren muss sicherstellen, dass:

[263] [21CFR820], Sect. 180.

- alle Beanstandungen einheitlich und zeitgerecht bearbeitet werden[264],
- alle Beanstandungen beurteilt werden, um ggf. nach Verordnung 803 oder 804 an die FDA weitergeleitet zu werden[265], solche Beanstandungen[266] müssen von einer benannten Person umgehend überprüft beurteilt und untersucht werden,
- alle Beanstandungen überprüft werden, um festzustellen, ob eine Untersuchung erforderlich ist[267].
- alle Beanstandungen, die auf ein mögliches Versagen des Gerätes hinweisen, müssen untersucht werden[268],
- alle Beanstandungen mit den zugehörigen Untersuchungen in der Beanstandungsakte geführt werden.

4.2.12 Wartung

Soweit Wartung eine spezifizierte Anforderung ist, muss ein Verfahren zur Ausführung und Überwachung der Wartung festgelegt und umgesetzt werden[269]. Wartungsberichte müssen statistisch analysiert werden[270]. Wartungsberichte müssen dokumentiert werden. Da Software nicht altert, entfällt auch die Notwendigkeit der Wartung.

4.2.13 Statistische Verfahren

Soweit angemessen, müssen statistische Verfahren zur Festlegung, Kontrolle, Verifizierung und Akzeptanz von Prozessmerkmalen und Prozessfähigkeit festgelegt und umgesetzt werden[271].

4.3 Design Control Guidance

Diese Anleitung[272] soll den Herstellern von Medizingeräten helfen, die Anforderungen an die Lenkung der Entwicklung innerhalb des Qualitätsmanagements besser zu verstehen und damit

[264] [21CFR820], Sect. 198 (a).
[265] [21CFR820], Sect. 198 (a) (3).
[266] [21CFR820], Sect. 198 (d).
[267] [21CFR820], Sect. 198 (b).
[268] [21CFR820], Sect. 198 (c).
[269] [21CFR820], Sect. 200 (a).
[270] [21CFR820], Sect. 200 (b).
[271] [21CFR820], Sect. 250.
[272] [FDA-DesignGuide].

angemessen umzusetzen. Das Dokument bezieht sich sowohl auf die Entwicklung des Gerätes als auch die Festlegung der dazu erforderlichen Herstellungsprozesse[273]. Allerdings sind die Angaben allgemein auf die Lenkung der Entwicklung von Medizingeräte gerichtet, die Anleitung enthält daher ebenfalls keine softwarespezifischen Vorgaben.

Unter Entwicklungslenkung[274] wird ein zusammenhängender Satz aus Verfahren und Arbeitsweisen verstanden, die in den Entwicklungsprozess eingebunden sind. Entwicklungslenkung macht systematische Bewertungen zu einem integrierten Bestandteil der Entwicklung. Als Resultat werden Unzulänglichkeiten in den Entwicklungsvorgaben und Abweichungen zwischen Entwicklungsvorschlägen und Anforderungen sichtbar gemacht. Daher ist es möglich diese Unzulänglichkeiten frühzeitig im Entwicklungsprozess zu korrigieren. Entwicklungslenkung verbessert damit die Wahrscheinlichkeit, dass die Benutzeranforderungen und die Anforderungen aus dem beabsichtigten Gebrauch angemessen in das Medizinprodukt transferiert werden.

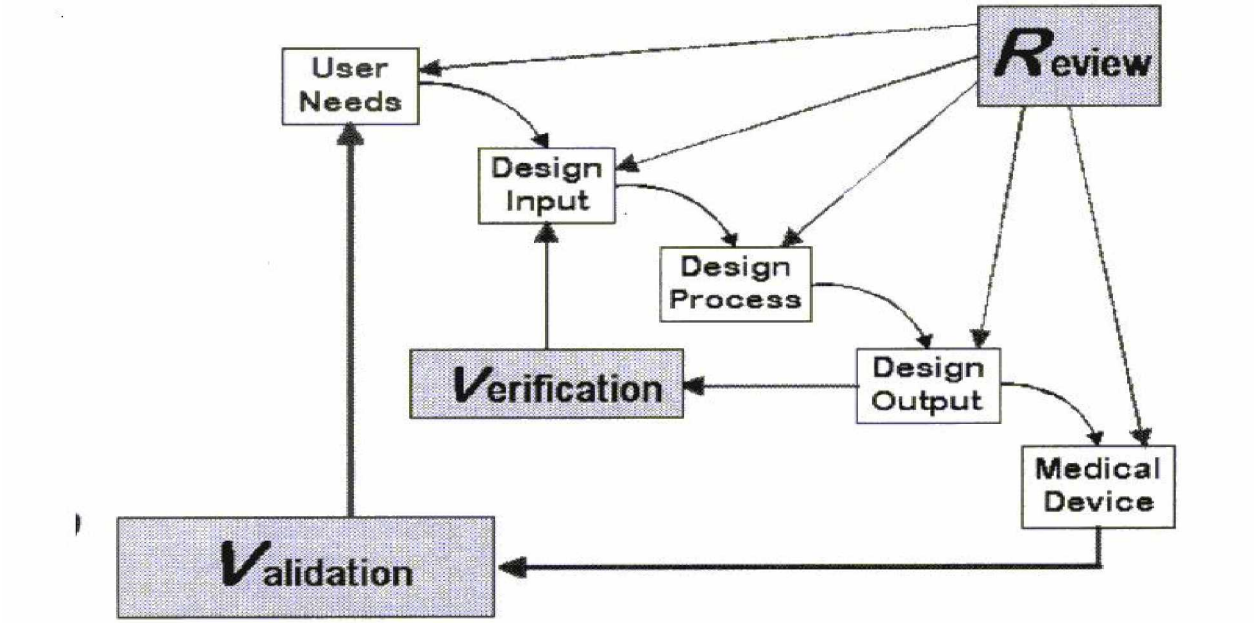

Abbildung 1: Validierung, Verifikation und Reviews im Entwicklungsprozess[275]

Die obige Abbildung illustriert dieses Vorgehen:

[273] Diese Teile sind für diese Arbeit irrelevant, da Software keinen eigentlichen Herstellungsprozess benötigt.

[274] Design Control wird hier als Entwicklungslenkung übersetzt, wie auch allgemein Design als Entwicklung in diesem Zusammenhang übersetzt wird. Dies entspricht Terminologie aus [ISO 9001] und [ISO 13485]

[275] [FDA-DesignGuide], S. XX

- Benutzeranforderungen und Anforderungen des beabsichtigten Gebrauchs werden einem Review unterzogen und damit auf Angemessenheit geprüft, bevor aus diesen Angaben Entwicklungsvorgaben[276] abgeleitet werden.
- Die auf Angemessenheit und Vollständigkeit geprüften Entwicklungsvorgaben werden in den Entwicklungsprozess[277] gegeben. Durch ein Review wird sichergestellt, das der Entwicklungsprozess den Vorgaben entspricht, und damit prinzipiell angemessene Ergebnisse liefert.
- Bei der Durchführung des Prozesses fallen Entwicklungsergebnisse[278] an, die einem Review unterzogen werden. Zudem werden die Ergebnisse gegen die Vorgaben verifiziert, um sicherzustellen, dass die im Prozess erstellten Ergebnisse die Anforderungen angemessen umsetzen.
- Aus den Entwicklungsergebnissen entsteht letztendlich das Medizingerät. Durch die Validierung wird sichergestellt, dass das fertige Medizingerät den Benutzeranforderungen und dem beabsichtigten Gebrauch genügt.
- Reviews begleiten die Entwicklung in jedem Schritt.

4.3.1 Entwicklungsplanung

Eine Entwicklungsplanung[279] ist erforderlich, um sicherzustellen, dass der Entwicklungsprozess angemessen kontrolliert wird und die erzielte Gerätequalität die vorgegebenen Kriterien erfüllt. Die Entwicklungsplanung muss mit den restlichen Anforderungen an die Entwicklungslenkung konsistent sein. Die folgenden Elemente werden typischerweise in einem Entwicklungsplan festgelegt – und daher erwartet:

- Beschreibung der Zielvorgaben für Design und Entwicklung;
- Festlegung der organisatorischen Verantwortlichkeiten,
- Festlegung der wichtigsten durchzuführenden Aufgaben mit den Ergebnissen und den Verantwortlichkeiten für jede Aufgabe,
- Festlegung der wichtigsten Review- und Entscheidungspunkte (Meilensteine),
- Auswahl der Reviewer, Zusammensetzung der Reviewteams und Festlegung der Verfahren, die bei den Reviews Verwendung finden,

---

[276] [FDA-DesignGuide] spricht von „design input“.

[277] [FDA-DesignGuide] spricht von „design process“

[278] [FDA-DesignGuide] spricht von „design output“

[279] [FDA-DesignGuide] spricht von “Design and development planning.”, s. S. 9ff.

- Lenkung der Entwicklungsdokumentation und
- Festlegung der Benachrichtigungsaktivitäten.

4.3.2 Entwicklungsvorgaben

Unter Entwicklungsvorgaben versteht man die Anforderungen, die als Startpunkt des Gerätedesigns benutzt werden[280]. Daher hat die Qualität dieser Anforderungen eine besonders hohe Bedeutung. Sind wesentliche Anforderungen nicht bis zur Validierung festgelegt, kann dies teures Redesign zur Folge haben, bevor das Produkt fertig gestellt ist und genutzt werden kann.

Unabhängig davon, ob die Idee eines Produktes über den Kontakt durch Kunden, aus der Forschung oder der klinischen Aktivität kommt, so führt die Produktidee üblicherweise zu einem Konzept-Dokument, das einige der gewünschten Vorstellungen an das neue oder verbesserte Gerät spezifiziert. Solche Konzept-Dokumente sind erfahrungsgemäß selten in sich schlüssig. Bevor solche Dokumente als Entwicklungseingaben benutzt werden können, müssen sie überarbeitet und erweitert werden und dann in eine Spezifikation mit vollständigen Entwicklungsanforderungen umgewandelt werden.

Entwicklungsvorgaben müssen möglichst umfangreich sein. Dabei werden gewöhnlich drei unterschiedliche Kategorien von Anforderungen unterschieden. Typischerweise hat jedes Produkt Anforderungen jedes Typs, nämlich:

- funktionale Anforderungen, die spezifizieren, was das Gerät tut, und sich dabei auf die operationalen Möglichkeiten des Gerätes mit Ein- und Ausgaben beziehen.
- Leistungsanforderungen, die angeben, wie oft oder wie gut eine bestimmte Leistung erbracht werden muss. Dabei werden also Punkte wie Geschwindigkeit, Antwortzeiten, Genauigkeit aber auch operationale Grenzen angesprochen.
- Schnittstellenanforderungen, die solche Anforderungen spezifizieren, die kritisch für die Verträglichkeit des Gerätes mit externen Systemen sind. Insbesondere wird hier spezifiziert, welche Eigenschaften durch externe Systeme vorgegeben sind, und daher außerhalb des Einflusses der Entwicklung liegen. Eine wichtiges Beispiel einer solche Schnittstelle ist die Benutzer- bzw. Patientenschnittstelle.

[280] [21CFR820], Sect. 3(f).

4.3.3 Entwicklungsergebnisse

[21CFR820] definiert Entwicklungsergebnisse[281] als Ergebnis von Entwicklungsbemühungen in jeder Entwicklungsphase. Die Qualitätsanforderungen an die Entwicklungsergebnisse kann in zwei Teile aufgeteilt werden[282]:

Die Entwicklungsergebnisse sollten in Begriffen definiert werden, die eine Überprüfung der Übereinstimmung mit den Entwicklungsvorgaben erlauben. Dies wirft zwei Fragen auf:

- Woraus leiten sich die Entwicklungsergebnisse her?
- Sind Form und Inhalt der Entwicklungsergebnisse angemessen?

Der erste Punkt ist wichtig, da typische Entwicklungsprojekte umfangreiche Daten produzieren, von denen Teile nicht als Entwicklungsergebnisse klassifiziert werden sollen (may not). Andererseits müssen die Entwicklungsergebnisse hinreichend umfangreich sein, um wirksam zu sein. Als Regel gilt, dass ein Produkt einer Entwicklungsaktivität als Entwicklungsergebnis qualifiziert ist, wenn es im Entwicklungsplan aufgeführt ist. Das Entwicklungsergebnis einer Aktivität[283] ist häufig Entwicklungsvorgabe einer anderen Aktivität. Beispiele sind:

- Ergebnisse der Risikoanalyse
- Softwarequellcode
- Ergebnisse von Verifikationsaktivitäten

4.3.4 Review

[21CFR820] definiert ein Review als dokumentierte, umfangreiche und systematische Untersuchung von Teilen der Entwicklung mit dem Ziel, Unangemessenheit in den Entwicklungsanforderungen aufzuzeigen, der Fähigkeit des Entwicklungsprodukts, diesen Anforderungen zu genügen und andere Probleme zu entdecken[284]. Im Allgemeinen haben Reviews den folgenden Zweck:

- die Bereitstellung einer systematischen Beurteilung der Entwicklungsergebnisse,

---

[281] [21CFR820], 3(g) *Design output* means the results of a design effort at each design phase and at the end of the total design effort.

[282] [FDA-DesignGuide], S. 19.

[283] [FDA-DesignGuide] spricht an dieser Stelle von “phase”, und meint damit eine CCCCC

[284] [21CFR820] 3(h): Design review means a documented, comprehensive, systematic examination of a design to evaluate the adequacy of the design requirements, to evaluate the capability of the design to meet these requirements, and to identify problems.

- die Bereitstellung von Rückmeldungen an Entwickler über existierende oder zu erwartende Probleme sowie Beurteilung des Projektfortschritts und
- die Bestätigung, dass das Projekt eine Aktivität oder Phase korrekt abgeschlossen hat, und damit die nachfolgende Aktivität oder Phase der Entwicklung durchgeführt werden kann.

In der Praxis überlappen sich Reviews, Verifikations- und Validierungstätigkeiten.

Üblicherweise werden Verifikationstätigkeiten vor Reviews durchgeführt und die Verifikationsergebnisse werden mit den verifizierten Entwicklungsergebnissen den Reviewteilnehmern zugeleitet. Alternativ können bestimmte Verifikationstätigkeiten als Teile des Entwicklungsreviews angesehen werden, insbesondere dann, wenn die Verifikationstätigkeiten komplex sind.

Analog benötigt Validierung üblicherweise eine Anzahl unterschiedlicher Tätigkeiten einschließlich der Feststellung, dass die angemessenen Verifikations- und Reviewtätigkeiten durchgeführt worden sind. Daher ist häufig ein Review als Abschluss der Validierung gewünscht um sicherzustellen, dass die Validierung vollständig und angemessen durchgeführt wurde.

Verifizierungsaktivitäten sollten auf allen Stufen und Ebenen der Geräteentwicklung durchgeführt werden. Die Basis der Verifikation bildet eine dreistufige Vorgehensweise[285], bestehend aus Tests, Inspektionen und Analysen. Jedes Vorgehen, das Konformität mit den Entwicklungsvorgaben sicherstellt, ist eine akzeptable Methode zur Verifizierung der Entwicklung bezüglich der zugehörigen Anforderungen. Eine bestimmte Methode der Verifizierung wird von dem Leitfaden weder empfohlen noch verlangt.

4.3.5 Verifizierung und Validierung

[21CFR820] definiert Verifizierung als „Bestätigung durch Untersuchung und Bereitstellung von objektivem Nachweis, dass vorgegebene Anforderungen erfüllt werden“[286]. Verifizierung und Validierung sind verbundene[287] Konzepte mit bedeutenden Unterschieden.

Validierung wird in [21CFR820] definiert als „Bestätigung durch Untersuchung und Bereitstellung von objektivem Nachweis, dass die besonderen Anforderungen für einen bestimmten beabsichtigten Gebrauch gleich bleibend erfüllt werden“[288]. Entwicklungsvalidierung wird weiter definiert

[285] [FDA-DesignGuide], S. 30, spricht von einem “three-pronged approach”

[286] [21CFR820] 3(aa), Verification means confirmation by examination and provision of objective evidence that specified requirements have been fulfilled.

[287] [FDA-DesignGuide] spricht auf S. 29 von „associated concepts“.

[288] [21CFR820] 3(z), Validation means confirmation by examination and provision of objective evidence that the particular requirements for a specific intended use can be consistently fulfilled.

als „Bereitstellung von objektiven Nachweis, dass die Gerätespezifikationen mit Benutzeranforderungen und beabsichtigtem Gebrauch übereinstimmen“[289].

Während Verifikation eine detaillierte Untersuchung verschiedener Aspekte der Entwicklung ist, ist die Entwicklungsvalidierung eine kumulative Addition aller Bemühungen sicherzustellen, dass die Entwicklung mit Benutzeranforderungen und beabsichtigtem Gebrauch übereinstimmt, unter Voraussetzung der erwarteten Abweichungen und der Benutzerumgebung.

Die Validierungsplanung sollte bereits in den frühen Entwicklungsstadien beginnen. Die Validierungsmethoden und Akzeptanzkriterien sollten festgelegt werden. Für komplexe Entwicklungen ist eine organisatorische und zeitliche Festlegung von Ressourcen und Verantwortlichkeiten sinnvoll. Der Validierungsplan soll einem Review unterzogen werden und (damit) auf Angemessenheit und Vollständigkeit geprüft werden.

Die Validierung kann Mängel in den ursprünglichen Annahmen bezüglich der Benutzeranforderungen oder des beabsichtigten Gebrauchs entdecken. Daher sollte ein formales Review im Anschluss an die Validierung vorgenommen werden, um solche Mängel zu lösen. Wie bei der Verifikation sind Maßnahmen erforderlich, wenn Mängel oder Unzulänglichkeiten bei der Validierung entdeckt werden, um die entdeckten Mängel zu beseitigen.

Die Validierungsdokumentation enthält die Zusammenstellung der Ergebnisse der Validierungsaktivitäten. Für eine komplexe Entwicklung mag es sinnvoll sein, die Ergebnisse in einzelnen Dokumenten zu halten und eine Zusammenfassung der Validierungsergebnisse als Report zu erstellen.

4.3.6 Entwicklungsänderungen

Es werden hauptsächlich zwei administrative Elemente mit der Verfolgung von Entwicklungsänderungen verlangt:

- Dokumentenlenkung: Es ist erforderlich, die Entwicklungsdokumente korrekt zu nummerieren und den Zustand und die Versionsgeschichte nachvollziehbar zu machen.
- Änderungskontrolle: Es ist erforderlich, die festgestellten Abweichungen und die aus Verifikation und Review resultierenden Maßnahmen zu dokumentieren und deren Umsetzung zu verfolgen.

Für kleine Entwicklungsprojekte kann es ein angemessener Prozess zur Verwaltung von Änderungen sein, lediglich Entwicklungsänderungen, die Durchführung der Verifikation und die zuge-

[289] [21CFR820] (2), Design validation means establishing by objective evidence that device specifications conform with user needs and intended use(s).

hörige Dokumentation zu dokumentieren. Die Verfolgung von Entwicklungsänderungen wird verlangt, damit:

- Maßnahmen, zur Beseitigung von Problemen bis zur vollständigen Umsetzung verfolgt werden,
- Änderungen so umgesetzt werden, dass das ursprüngliche Problem gelöst ist und kein neues Problem in das Gerät hineingebracht wird,
- die Entwicklungsdokumentation vollständig aktualisiert wird, um den geänderten Entwicklungsstand zu reflektieren und
- die Kommunikation und Koordination von Entwicklungsänderungen durchgeführt wird.

4.3.7 Entwicklungsentstehungsakte

[21CFR820] definiert die Entwicklungsentstehungsakte (Design History File / DHF) als eine Sammlung von Akten[290] , die die Entwicklungsgeschichte eines fertig gestellten Gerätes beschreibt[291], d.h. die DHF enthält oder referenziert alle Dokumente, die notwendig sind, um zu zeigen, dass das Gerät in Übereinstimmung mit dem Entwicklungsplan und den Anforderungen entwickelt wurde. Weder [ISO 9001] noch [ISO 13485] verlangen ein solches Dokument. [FDA-DesignGuide][292] führt aus, dass der hauptsächliche Nutznießer der Entwicklungsentstehungsakte der Hersteller sei. Denn nur bei Vorliegen dieser Informationen ist es bei Bedarf möglich, genau nachzuvollziehen, wie bestimmte Anforderungen für das Gerät festgelegt und umgesetzt wurden. Die folgenden Informationen sind üblicherweise in der Entwicklungsentstehungsakte enthalten:

- Entwicklungsplan mit Entwicklungsaufgaben und Ergebnisse,
- Kopien der genehmigten Entwicklungsvorgabedokumente und der Entwicklungsergebnisdokumente,
- Dokumente der Entwicklungsreviews und
- Validierungsdokumente.

[290] [21CFR820] 3(e), spricht von “compilation of records”.

[291] [21CFR820] 3 (e).

[292] [FDA-DesignGuide], S. 43f.

4.4 Premarket Submissions for Software

Diese Anleitung[293] gibt dem Hersteller Hinweise über den Umfang der Dokumentation, die die FDA bei der Genehmigung eines Medizingerätes, das Software enthält, für erforderlich ansieht. Der Umfang der Dokumentation richtet sich dabei nach dem Gefährdungsgrad[294] des Gerätes. Der Gefährdungsgrad ist nicht mit der Klassifizierung des Medizingerätes nach 21 CFR 860 gleichzusetzen, vielmehr ist hierfür der Grad der Patientengefährdung vor der Anwendung jeglicher Risikokontrollmaßnahmen zu ermitteln. Die Software muss dabei einer der folgenden Gefährdungsklassen zugeordnet werden[295]:

- Major: Ein Fehler der Software kann Tod oder schwerwiegende Verletzungen[296] verursachen,
- Moderate: Ein Fehler der Software kann eine leichte Verletzung verursachen,
- Minor: Es wird nicht erwartet, dass Fehler der Software eine Verletzung verursachen können.

Die Anleitung gibt weiterhin Hinweise zur Festlegung des Gefährdungsgrads an Hand einiger Schlüsselfragen. Die FDA hält die folgenden Dokumente, abhängig von dem ermittelten Gefährdungsgrad der Software für erforderlich:

4.4.1 Funktionale Anforderungen

Unabhängig von dem ermittelten Gefährdungsgrad ist eine Dokumentation der wesentlichen Funktionen des Systems, die durch Software gesteuert werden, erforderlich. Weiterhin soll in diesem Dokument die Umgebung beschrieben werden, in der diese Software betrieben werden soll.[297].

4.4.2 Gefährdungsanalyse

Unabhängig von dem ermittelten Gefährdungsgrad ist eine Dokumentation der durchgeführten Gefährdungsanalyse erforderlich. Dieses Dokument soll sowohl den beabsichtigten Gebrauch als auch alle Hard- und Softwarerisiken berücksichtigen. Zusätzlich sollen alle vorhersehbaren

[293] [FDA-PreMarket].

[294] Level of Concern (LOC).

[295] Im Wesentlichen entsprechen die Gefährdungsklassen den Sicherheitsklassen der EN IS0 62304.

[296] Das Dokument spricht von „Serious Injury“

[297] [FDA-Premarket], S. 10f.

Gefährdungen berücksichtigt werden, auch solche die aus vorsätzlichen und versehentlichen Missbrauch resultieren[298].

4.4.3 Softwareanforderungsspezifikation

Die „Software Requirement Specification“ (SRS) dokumentiert alle Software-Anforderungen. Das Dokument legt also fest, was das Softwaresystem tut. Typische Bestandteile sind funktionale Anforderungen und Schnittstellendefinitionen[299].

Die Anleitung schlägt vor, bei dem Gefährdungsgrad „Minor“ eine Zusammenfassung des SRS zu dokumentieren und andernfalls die vollständige SRS einzureichen.

4.4.4 Softwarearchitektur

Das „Architecture Design Chart“ beschreibt die Beziehungen der wesentlichen funktionalen Einheiten einschließlich der notwendigen Hardware- und Softwareschnittstellen. Der Umfang der Dokumentation soll so ausgelegt werden, dass es möglich ist, die Struktur der Software zu den Funktionen in Beziehung zu setzen, die von der Software erfüllt werden soll[300].

Die Anleitung hält das Architekturdokument bei dem Gefährdungsgrad „Major“ und „Moderate“ für erforderlich, andernfalls kann es entfallen.

4.4.5 Softwaredesignspezifikation

In der “Software Design Specification“ (SDR) wird die Implementierung der Anforderungen an die Software beschrieben[301]. Die Anleitung hält fest, das SRS (s. Kapitel 4.4.3) und SDS so aufgefasst werden können, dass die SRS beschreibt, was die Software leisten soll und die SDS beschreibt, wie die Software dies tut[302].

Die Anleitung hält die SDS für den Gefährdungsgrad „Major“ und „Moderate“ erforderlich, andernfalls kann sie entfallen.

---

[298] [FDA-Premarket], S. 11.

[299] [FDA-Premarket], S. 11ff. Inhaltlich entspricht das Dokument also im Wesentlichen dem Anforderungsdokument der Anforderungsanalyse nach [ISO prEN 62304], Anschnitt 5.2.

[300] [FDA-Premarket], S. 13.

[301] [FDA-Premarket], S. 13.

[302] „In terms of the relationship between the SRS and the SDS, the SRS describes what the Software Device will do and the SDS describes how the requirements in the SRS are implemented”.

4.4.6 Anforderungsnachverfolgung

Die “Traceability Analysis” verbindet Softwareanforderungen, Designspezifikationen und Testspezifikationen[303]. Weiterhin bietet die “Traceability Analysis” die Möglichkeit, identifizierte Risiken mit der Implementierung und dem Test der Maßnahmen zur Risikoverringerung zu verbinden.

Die Anleitung hält die “Traceability Analysis” unabhängig vom Gefährdungsgrad für erforderlich.

4.4.7 Softwareentwicklungs-Lebenszyklus

Für die Gefährdungsklasse “Major” und “Moderate” ist die Einreichung einer Übersicht über den benutzten Softwareentwicklungs-Lebenszyklus erforderlich[304]. Diese Übersicht sollte alle Prozesse enthalten, die erforderlich sind, um die verschiedenen Aktivitäten innerhalb der Softwareentwicklung zu lenken. Für die Gefährdungsklasse “Major” ist weiterhin eine Liste der innerhalb der Softwareentwicklung erzeugten Dokumente sowie eine Beschreibung der angewendeten Kodierrichtlinien erforderlich.

4.4.8 Verifikation und Validierung

Unter Verifikation versteht die Anleitung die durch Untersuchung und Bereitstellung objektiver Nachweise erlangte Bestätigung, dass vorgegebene Anforderungen erfüllt sind[305]. In der Softwareentwicklung kann Verifikation als Bestätigung aufgefasst werden, dass die Ergebnisse einer bestimmten Entwicklungsphase alle Anforderungen erfüllen, die als Input an diese Phase gestellt wurden. Testen ist eine von mehreren möglichen Verifizierungsaktivitäten.

Validierung meint hingegen die Bereitstellung objektiver Beweise, dass die Spezifikationen mit Benutzeranforderungen und beabsichtigtem Gebrauch übereinstimmen[306].

Die Anleitung empfiehlt einen unterschiedlichen Umfang an Dokumentation für die vorgenommenen Verifikations- und Validierungstätigkeiten, basierend auf dem Gefährdungsgrad[307]:

- Minor: Es ist eine Dokumentation über den Systemtest und ggf. Integrationstest erforderlich. Die Dokumentation soll die pass/fail-Kriterien und eine Zusammenfassung der Ergebnisse enthalten.

---

[303] [FDA-Premarket], S. 13f.

[304] [FDA-Premarket], S. 14.

[305] [21CFR820] 3 (aa).

[306] [21CFR820] 3 (z)(2).

[307] [FDA-Premarket], S.14f.

- Moderate: Es ist eine Zusammenfassung aller Verifizierungs- und Validierungsaktivitäten mit den Ergebnissen dieser Aktivitäten erforderlich. Die Dokumentation muss die pass/fail-Kriterien enthalten. Es muss zudem sichergestellt sein, dass diese Aktivitäten durch die „Traceability Analysis“ auf Designanforderungen zurückgeführt werden können.
- Major: Es sind alle Informationen für den Gefährdungsgrad “Moderate” erforderlich. Weiterhin wird eine Beschreibung aller Test benötigt, die fehlgeschlagen sind. Weiter sind alle Änderungen zu dokumentieren, die auf Grund nicht bestandener Tests durchgeführt wurden, und ob die durchgeführten Änderungen wirksam sind. Weiterhin sollten Beispiele des Integrationstests und eine Zusammenfassung der Ergebnisse dokumentiert werden.

4.4.9 Versionsgeschichte

Es soll die Versionsgeschichte aller während der Entwicklung erstellten Versionen dokumentiert werden. Dies erfordert die Angabe von Datum, Versionsnummer und die Angabe eine kurzen Beschreibung der durchgeführten Änderungen[308].

4.4.10 Abweichungen

Für die Gefährdungsklasse “Major” und “Moderate” ist die Einreichung einer Übersicht über alle noch vorhandenen Softwareabweichungen erforderlich. Diese Liste soll die folgenden Informationen enthalten[309]:

- Problembeschreibung,
- Einfluss auf die Systemleistung,
- Einfluss auf die Gerätesicherheit,
- Plan oder Zeitrahmen für die Problembeseitigung.

4.5 General Principles of Software Validation;

Diese Anleitung beschreibt allgemeine Validierungsprinzipien, die die FDA bei der Validierung von Software für medizinische Geräte für anwendbar hält[310]. Die Anleitung äußert sich aber nicht

[308] [FDA-Premarket], S. 15.

[309] [FDA-Premarket], S. 15.

[310] [FDA-Validation], S. 1. In diesem Dokument geht es aber primär nicht um die Validierung an sich, sondern um die erforderlichen Aktivitäten und Aufgaben, die letztendlich erst eine erfolgreich Validierung erlauben.

nur zu Validierung. Auch andere Aktivitäten, wie Planung, Verifikation, Konfigurationsmanagement und weiteren Aspekte des Software-Engineering, die die FDA für wesentlich für die Entscheidung hält, ob eine Software validiert ist, werden erwähnt. Die Anleitung empfiehlt weiterhin eine Integration der Aktivitäten der Softwareentwicklung und des Risikomanagements. Basierend auf dem beabsichtigtem Gebrauch und den Sicherheitsrisiken, die sich daraus ergeben, sollen der erforderliche Aufwand und die notwendigen Techniken festgelegt werden. Obwohl diese Anleitung kein bestimmtes Vorgehensmodell festlegt, oder bestimmte Techniken oder Methoden fordert, wird empfohlen, Softwarevalidierungs- und –verifikationsaktivitäten während der gesamten Softwareentwicklung durchzuführen.

Software Validierung wird als ein entscheidendes Werkzeug angesehen um sicherzustellen, dass die Qualität der Software angemessen ist. Software-Validierung kann die Benutzbarkeit und Verlässlichkeit der Software erhöhen und zudem zu einer Verringerung von Fehlerraten und Rückrufen sowie einer Verringerung des Patientenrisikos führen[311].

Zu jeder der üblichen Aktivitäten innerhalb des Lebenszyklus eines Softwareproduktes gibt es typische Aufgaben, die die Entscheidung unterstützen, dass eine Software als validiert gelten kann. Diese spezifischen Aufgaben, sowie die Reihenfolge und die Häufigkeit in der sie ausgeführt werden, sind durch die Wahl des verwendeten Lebenszyklusmodells und das Sicherheitsrisiko, das durch Software gegeben ist, bestimmt. Für bestimmte Anwendungen mit geringer Gefährdung können diese Aufgaben möglicherweise ganz entfallen. Jedoch sollte bei der Entwicklung der Anwendung der Einsatz solcher Aufgaben bedacht werden, und die Entscheidung über den Einsatz dokumentiert werden[312].

Die folgenden Aktivitäten werden in der Anleitung als üblich bei der Entwicklung von Software angesehen[313]:

- Entwicklungsplanung[314],
- Erstellung der Systemanforderungen,
- Softwareanforderungsspezifikation,
- Softwaredesignspezifikation,
- Implementierung,
- Test,

[311] [FDA-Validation], S. 9f.

[312] [FDA-Validation], S. 14.

[313] [FDA-Validation], S. 14.

[314] [FDA-Validation] spricht von „Quality Planning“ meint aber die Planung aller erforderlichen Entwicklungsaktivitäten.

- Installation,
- Betrieb und Support,
- Wartung und
- Außerdienststellung

In den nachfolgenden Kapiteln werden diese Aktivitäten näher betrachtet

4.5.1 Entwicklungsplanung

In der Entwicklungsplanung soll ein Plan erstellt werden, der die folgenden Informationen enthält[315]:

- das gewählte Vorgehensmodell mit den für die Entwicklung erforderlichen Aktivitäten und den spezifischen Aufgaben innerhalb jeder Aktivität,
- die benötigten Ressourcen,
- die Aufzählung aller wesentlichen Qualitätsmerkmale, die bei der Entwicklung zu berücksichtigen sind,
- die Ein- und Ausgaben einer jeden Aufgabe,
- Rollen, Ressourcen und Verantwortlichkeiten für jede Aufgabe,
- das Vorgehen für die Dokumentation und die Lösung von Abweichungen,
- Risiken und Voraussetzungen der Entwicklung,
- die Benutzeranforderungen und
- Anforderungen an die Durchführung von Reviews, insbesondere Designreviews.

Das Management muss die für die Entwicklung angemessen Entwicklungsumgebung und die erforderlichen Ressourcen bereitstellen[316]. Dazu gehört die Bereitstellung der folgenden Pläne[317]:

- Risikomanagementplan,
- Konfigurationsmanagementplan,
- Qualitätssicherungsplan, einschließlich
    1. Verifikations- und Validierungsaufgaben einschließlich Abnahmebedingungen

[315] [FDA-Validation], Kapitel 5.2.1, S. 15f., siehe auch [21CFR820], 20(b)(1) und (2)

[316] [FDA-Validation], S. 15.

[317] [FDA-Validation], S. 15f.

2. Anforderungen an Entwicklungsreviews
3. Anforderungen an alle weiteren Reviews und

- Problemmanagementverfahren.

4.5.2 Review

Entwicklungsreviews sind ein grundlegendes Werkzeug für die Handhabung und Bewertung von Entwicklungsprojekten. Die Forderungen des Qualitätsmanagementsystems verlangen, dass wenigstens ein formales Entwicklungsreview während des Entwicklungsprozesses durchgeführt wird. Jedoch wird empfohlen, solche Reviews an allen sinnvollen Stellen einzusetzen, etwa am Ende eine jeden Aktivität. Solche Reviews sind besonders am Ende der Anforderungsanalyse wichtig. An dieser Stelle entdeckte Probleme können so beseitigt werden, bevor Ressourcen in die Entwicklung fehlerhafter Anforderungen gesteckt werden, und verringern so die Wahrscheinlichkeit wesentliche Punkte bei der Entwicklung zu vergessen.

4.5.3 Anforderungen

Die Festlegung der Anforderungen an die Software beinhaltet die Identifikation, Analyse und Dokumentation von Informationen über das Medizingerät und dessen beabsichtigten Gebrauch. Die Anforderungsspezifikation sollte die folgenden Teile enthalten[318]:

- alle Softwareeingaben und –ausgaben, einschließlich der zugehörigen Grenzen und Defaultwerte,
- eine vollständige Liste der Funktionen, die die Software ausführt,
- alle Leistungsanforderungen, die die Software erfüllen soll, einschließlich Durchsatz, Zeitvorgaben, Zuverlässigkeit und Antwortzeiten,
- die fachliche Definition der Benutzschnittstellen und einer Beschreibung, wie Benutzer mit dem System interagieren,
- eine Beschreibung aller weiteren Schnittstellen,
- das verwendete Fehlerkonzept und der Umgang mit diesen Fehlern,
- vorgesehene Hardwareplattform und zugehöriges Betriebssystem und
- alle sicherheitsrelevanten Anforderungen und Funktionen, die in der Software umgesetzt werden[319].

[318] [FDA-Validation], Kapitel 5.2.2, S. 16.

Die Qualitätsanforderungen[320] verlangen ein Verfahren für den Umgang mit unvollständigen, missverständlichen und widersprüchlichen Anforderungen. Jede aufgeführte Anforderung sollte hinsichtlich Angemessenheit, Vollständigkeit, Konsistent, Testbarkeit, Richtigkeit und Klarheit ausgewertet werden[321]. Die Anforderungen sollen aus den Anforderungen an das Gesamtsystem[322] sowie Ergebnissen der Risikoanalyse abgeleitet sein[323].

4.5.4 Design

Im Designprozess werden die Anforderungen in ein Softwarekonzept übertragen. Die Designspezifikation beschreibt, was die Software tun soll und wie sie dies tun soll. Häufig ist es hilfreich, wenn die Designspezifikation zusätzlich zu den Einzelheiten des Designs auch noch eine Zusammenfassung der Designinformationen enthält. Dies kann insbesondere dann hilfreich sein, wenn die Software komplex ist, oder wenn sich beteiligte Personen in das Design einarbeiten sollen oder müssen. Die Designspezifikation muss so vollständig sein, dass der Programmierer nicht gezwungen ist, Ad-hoc-Entscheidungen über das Design zu treffen. Typische Aufgaben in dieser Aktivität sind[324]:

- Aktualisierung der Software-Risikoanalyse,
- Rückverfolgung der Designelemente auf Softwareanforderungen,
- Bewertung des Softwaredesigns,
- Schnittstellendesign,
- Erstellung des Modultestplans,
- Erstellung des Integrationstestplans und
- Erstellung der Testspezifikation für den Modul-, Integrations-, System- und Abnahmetest.

Die Designspezifikation sollte Folgendes enthalten[325]:

- die Software Risikoanalyse,
- das benutzte Entwicklungsverfahren und die verwendeten Kodierungsrichtlinien,

---

[319] Es wird ind [FDA-Validation] angenommen, das diese Sicherheitsanforderungen an die Software aus der Risikoanalyse abgeleitet sind.

[320] [21CFR820], 30(c).

[321] Bei dem erwähnten Verfahren wird es sich regelmäßig um ein Review handeln.

[322] Insoweit die Software nicht bereit das Medizingerät ist.

[323] [FDA-Validation], S. 17.

[324] [FDA-Validation], S. 17f.

[325] [FDA-Validation], S. 18.

- die Beschreibung des Systemumfelds,
- die verwendete Hardware,
- die logische Struktur der Anwendung einschließlich des verwendeten Kontrollflusses und der eingesetzten Algorithmen,
- die erforderlichen Datenstrukturen und der verwendeter Datenfluss,
- die Definition der benötigten Variablen und die Beschreibung der beabsichtigten Verwendung,
- die erforderlichen Fehler-, Alarm- und Warnmeldungen,
- jegliche unterstützende Software, wie Betriebsystem, Treibersoftware und Ähnliches,
- alle erforderlichen Kommunikationsverbindungen, sowohl via Hardware als auch via Software,
- alle erforderlichen oder vorgesehenen Sicherheitsvorgaben und
- alle weiteren vorgesehenen Einschränkungen und Begrenzungen.

4.5.5 Implementierung

Die Implementierung[326] ist diejenige Aktivität, die das zuvor erstellte Design in Quellcode umsetzt. Bei dieser Aktivität wird häufig eine Hochsprache zum Einsatz kommen, aber auch die Verwendung von Assemblercode ist möglich. Die Entscheidung für die Wahl der Programmiersprache und der verwendeten Entwicklungsumgebung sollte dokumentiert werden. Sofern der eingesetzte Compiler verschiedene Stufen der Fehlerüberprüfung anbietet, sollte die strengste Stufe benutzt werden. Wird diese Stufe nicht verwendet, sollten die Gründe dafür dargelegt werden. Die Ergebnisse des Kompilierungsvorgangs einschließlich alle Warnungen sollte dokumentiert werden.[327]

Die Verwendung von Kodierungsrichtlinien wird empfohlen. Kodierungsrichtlinien sollten Angaben zu Klarheit, Stil, Komplexitätsmanagement und Kommentierung enthalten. Kommentare sollen Angaben zu dem Modul[328], Ein- und Ausgaben, verwendeten Variablen, Datentypen und Operationen enthalten.

[326] In der Literatur findet man auch die Begriffe Kodieren oder Programmieren.

[327] [FDA-Validation], Kapitel 5.2.4, S. 20f.

[328] Bei objektorientierter Programmierung also meistens Angaben zu der Klasse.

Der erstellte Quellcode sollte auf Übereinstimmung mit dem Design geprüft werden. Quellcodebewertungen erfolgen häufig in der Form von Codewalkthroughs oder Codeinspektionen. Solche Verfahren stellen ein äußerst wirksames Mittel zur Fehlererkennung bereit.

Eine Analyse des erstellten Quellcodes sollte durchgeführt werden, um sicherzustellen, dass der erstellte Code korrekt die Spezifikationen umsetzt und dabei die vorgegeben Regeln einhält. Diese Analyse sollte dokumentiert werden und die folgenden Informationen enthalten[329]:

- Das Softwaredesign ist vollständig umgesetzt worden,
- jedes Modul und jede Funktion im Quellcode kann zurückverfolgt werden auf eine Element in der Designspezifikation oder der Risikoanalyse,
- Tests für jedes Modul und jede Funktion können auf Elemente in der Designspezifikation oder der Risikoanalyse zurückverfolgt werden.

4.5.6 Entwicklertests

Um die Software zu testen, muss die Software unter kontrollierten Bedingungen mit vorgegebenen Eingaben ausgeführt werden. Die dabei beobachteten Ausgaben werden dabei mit erwarteten Ausgaben verglichen und anschließend einschließlich eventuell auftretender Abweichungen dokumentiert[330].

Ein grundlegendes Element des Softwaretests ist daher das erwartete Ergebnis. Die für die Festlegung des erwarteten Ergebnisses notwendigen Informationen muss die Softwarespezifikation liefern. Daher müssen die Informationen der Spezifikation hinreichend präzise sein. Der durchzuführende Softwaretest soll die folgenden Grundsätze berücksichtigen:

- das erwartete Ergebnis ist durch die Spezifikation vorgegeben,
- der Testfall hat eine hohe Wahrscheinlich einen Fehler aufzudecken,
- der Testfall ist unabhängig von der Kodierung,
- sowohl die Sachkenntnis der Benutzers als auch des Entwickler wird eingesetzt,
- der Tester verwendet andere Werkzeuge als die Entwickler und
- es werden sowohl normale Abläufe als auch Fehlerszenarien bei der Testausführung berücksichtigt.

---

[329] [FDA-Validation], S. 21.

[330] [FDA-Validation], Kapitel 5.2.5, S. 18ff. Allerdings werden – entgegen des Titels dieses Kapitels, große Teile dieser Tests gerade nicht von dem Entwickler ausgeführt, sondern von separaten Testabteilungen. Außerdem gibt es gute Gründe, den Entwickler den eigenen Quellcode nicht testen zu lassen, sondern andere Mitarbeiter dafür heranzuziehen.

Softwaretests beginnen üblicherweise nach Abschluss von vorbereitenden Aufgaben, wie Softwareinspektionen, mit den Modultests[331]. Modultests werden regelmäßig als so genannte „White-Box“-Tests durchgeführt, d.h. bei der Spezifikation der Tests wird die Struktur des zu testenden Codes berücksichtigt. Der Umfang, in dem die Struktur des Moduls berücksichtigt wird, kann durch Metriken spezifiziert werden. Häufig verwendete Metriken[332] sind Anweisungsabdeckung, Zweigabdeckung, Bedingungsabdeckung und Pfadabdeckung. Vielfach schließt sich an den Modultest ein Integrationstest an, durch den die unterschiedlichen Module integriert werden[333].

Bei der Spezifikation des Systemtests sind folgende Fälle zu berücksichtigen[334]:

- Test der Standardszenarien, wie sie im klinischen Alltag regelmäßig vorkommen,
- Test mit allen zulässigen Eingaben unter Berücksichtigung der in der Spezifikation vorgegebenen Grenzwerte,
- Test auf Robustheit durch die geplante Eingabe unzulässiger Werte,
- Test auf Effizienz durch Ermittlung von Antwortzeiten und Durchsatz,
- Verhalten und Stressbedingungen, d.h. Verhalten bei geringer Überschreitung der vorgegebene Randbedingungen, wie Anzahl Benutzer, verarbeitete Daten, etc. und
- Bedienbarkeit und Benutzerfreundlichkeit.

Typische Aufgaben in dieser Testaktivität sind[335]:

- Die Testplanung,
- Die Ausführung von Modultests, Integrationstest, Funktionaler Tests, Systemtests und Abnahmetests,
- Die Bewertung der Testergebnisse,
- Die Fehlerbewertung und –beseitigung und

[331] [FDA-Validation], S.22. Das ist in der Realität häufig anders. Es ist nicht ungewöhnlich, dass der Entwickler kodiert und gleichzeitig für den erstellten Code Modultests schreibt. Erst nach Abschluss des Moduls findet eine Codeinspektion für produktiven Code und Testcodes statt.

[332] Für den Kontrollfluss.

[333] Bei der objektorientierten Programmierung, wo üblicherweise Module mit Klassen gleichgesetzt werden, wird der Integrationstest, der die korrekte Zusammenarbeit der verschiedenen Klassen testet, häufig gemeinsam mit dem Modultest durchgeführt. Integrationstests testen dann häufig das Zusammenspiel größerer Teile, wie etwa Komponenten.

[334] [FDA-Validation], S. 24f.

[335] [FDA-Validation], S. 26.

- Die Analyse der Rückverfolgbarkeit von Modultest zu Feindesign, Integrationstests zu Grobdesign und Systemtest zu Softwareanforderungen.

4.5.7 Vor-Ort-Test

Testen vor Ort ist ein wesentlicher Teil der Softwarevalidierung. Die Qualitätsanforderungen verlangen Installations- und Inspektionsverfahren, als auch die zugehörige Dokumentation, um die angemessene Installation nachzuweisen[336]. Die für den Vor-Ort-Test benutzte Terminologie ist uneinheitlich[337].

Der Vor-Ort-Test sollte einem zuvor definierten und freigegebenen Plan folgen. Die Testausführung sollte mit den benutzten Verfahren, den Eingabedaten und den Testergebnissen aufbewahrt werden. Weiter sollte die getestete Konfiguration mit den verschiedenen Hardware- und Softwareversionen überprüft und dokumentiert werden. Typische Aufgaben des Vor-Ort-Tests sind[338]:

- die Ausführung von Abnahmetests,
- die Auswertung des Testergebnisse,
- die Fehlerbewertung und ggf. Problembeseitigung und
- die Erstellung eines Testabschlussberichts.

4.5.8 Wartung und Softwareänderungen

Für Software bedeutet der Begriff Wartung etwas anderes als für Hardware. Softwarewartung beinhaltet Maßnahmen zur Beseitigung von Fehlern[339], Maßnahmen zur Verbesserung der Leistung, der Wartbarkeit oder anderer Eigenschaften der Software[340], sowie Maßnahmen um die Software in einer geänderten Umgebung ausführbar zu machen[341].

Werden Änderungen an der Software vorgenommen, müssen im erforderlichen Umfang Regressionstests vorgenommen werden, um zu zeigen, dass die an den Änderungen beteiligten Teile der Software nicht nachteilig beeinflusst wurden. Der durch die Änderung notwendige Validierungsaufwand ist durch die Art der Änderung festgelegt. Eine sorgfältige und vollständige

---

[336] [21CFR820], 170.

[337] [FDA-Validation], S. 27 nennt „beta test, site validation, user acceptance test installation verification and installation testing“ als mögliche Begriffe.

[338] [FDA-Validation], S. 28.

[339] corrective maintenance (dtsch. Fehlerbeseitigung).

[340] perfective maintenance (dtsch. Produktpflege).

[341] adaptive maintenance.

Dokumentation des Designs und der Beziehungen zwischen den einzelnen Teilen der Software kann den notwendigen Validierungsaufwand einschränken. Zusätzlich zu den Verifikations- und Validerungsaufgaben sollten bei Softwareänderungen die folgenden Aufgaben Berücksichtigung finden[342]:

- die Überprüfung und gegebenenfalls Ergänzung des Softwarevalidierungsplans.
- die Bewertung der Abweichungen: Soweit möglich, sollen identifizierte Abweichungen grundsätzlich gelöst werden. Sofern Trends bei bestimmten Fehlern festgestellt werden, muss durch Korrekturmaßnahmen sichergestellt werden, dass solche und ähnliche Probleme nicht mehr auftreten.
- Problemidentifikation und Lösungsverfolgung: Alle aufgetretenen Probleme müssen dokumentiert werden. Die Lösung jedes Problems muss verfolgt werden, um sicher zu stellen, das es beseitigt ist und um Trends zu identifizieren.
- Vorgeschlagene Änderungseinschätzung: Alle vorgeschlagenen Änderungen und Verbesserungen müssen hinsichtlich des Einflusses auf das System bewertet werden. Diese Informationen werden benötigt, um den Umfang der erforderlichen Verifikations- und Validierungsaufgaben festzulegen.
- Verifikation und Validierung: Für alle freigegebenen Softwareänderungen sind die erforderlichen Verifikations- und Validierungsaufgaben durchzuführen, um zu zeigen, das die durchgeführten Änderungen das System nicht nachteilig beeinflusst haben.
- Aktualisierung der Dokumentation.

4.6 An Introduction to Human Factors in Medical Devices

Der Zweck dieses Handbuches ist es, Hersteller zu ermutigen, die Sicherheit von Medizingeräten durch den Einsatz einer systematisch und sorgfältig entwickelten Benutzerschnittstelle zu verbessern[343]. Das Handbuch führt weiter aus, dass die Anwender von Medizingeräten sich erheblich in ihren physischen, sensorischen und mentalen Fähigkeiten unterscheiden. Zudem werden Medizingeräte in den unterschiedlichsten Umgebungen benutzt, in denen teilweise die Leistung durch Umwelteinflüsse, wie Lärm, schlechte Lichtverhältnisse, Hitze und Schmutz gefährdet ist. Ein Medizingerät kann nur dann sicher und effektiv benutzt werden, wenn die Wechselbeziehungen zwischen der Betriebsumgebung, der Leistungsfähigkeit des Benutzers, den

[342] [FDA-Validation], Kapitel 5.2.7, S. 28f.

[343] [FDA-DoIt], S. 1, Introduction.

verschiedenen Belastungsgraden, unter denen der Benutzer das Gerät benutzt und dem Design des Gerätes bei der Entwicklung des Gerätes angemessen berücksichtigt[344].

4.6.1 Die Benutzerschnittstelle

Dieser Abschnitt beschreibt Probleme, die bei unangemessener Gestaltung der Benutzerschnittstelle auftreten können und gibt Faustregeln, die bei der Gestaltung der Benutzerschnittstelle berücksichtigt werden sollen[345]:

- Alle Aspekte der Benutzerschnittstelle sollten soweit wie möglich mit den Benutzerwartungen übereinstimmen.
- Alle Benutzereingaben und Anzeigen sollten die wesentlichen Fähigkeiten des Benutzers, wie Kraft, Geschicklichkeit, Gedächtnis, Reichweite, Sehkraft und Hörvermögen angemessen berücksichtigen.
- Die Eingabe- und Anzeigeelemente sollten in sinnvollen Gruppen zusammengefasst werden, und der Zusammenhang zwischen Eingabeelementen und zugehörigen Anzeigeelementen klar und unmissverständlich sein.
- Die Größe und Farbe von Anzeigeelementen sollten so gewählt werden, das sie aus verschiedenen Entfernungen, und verschiedenen Winkeln und unter verschiedene Lichtverhältnissen gut lesbar sind.
- Abkürzungen, Symbole und Text sollten konsistent verwendet werden, mit dem Benutzerhandbuch übereinstimmen und der Fachterminologie entsprechen.
- Wenn möglich sollten Eingabeelemente einen taktilen Feedback geben.
- Das System sollte immer Informationen über die aktuell durchgeführte Aktion geben und in Fehlersituationen Hilfestellung anbieten.
- Es sollte berücksichtigt werden, auf Fehlersituationen durch visuelle oder akustische Signale aufmerksam zu machen.

4.6.2 Human Factors Engineering

Das Handbuch führt „Human Factors Engineering“ als eine Methodologie ein, die wesentlich für das wirksame Design der Benutzschnittstelle ist. Dieser Prozess besteht aus den folgenden Aktivitäten[346]:

---

[344] [FDA-DoIt], S. 3ff., Why Human Factors Engineering is important.

[345] [FDA-DoIt], S. 6ff, The User Interface.

[346] [FDA-DoIt], S. 17ff0, Human Factors Engineering.

- Durchführung von Studien, um festzustellen, wie die vorgesehenen Benutzer mit medizinischen Geräten umgehen, unter welchen Umweltumgebungen das Gerät benutzt wird und welche typischen Probleme bei der Verwendung oder bei Konkurrenzprodukten auftreten. Wichtig ist, dass der Hersteller anschließend eine möglichst genaue Kenntnis über den Umgang mit vergleichbaren Geräten hat[347].
- Entwicklung und Festlegung des Bedienkonzepts: Parallel soll Bedienkonzept entwickelt werden. Dabei sollen Informationen aus der Literatur, Leitfaden zur Benutzerführung, zur Ergonomie von Geräten und Geräteinformationen verwendet werden. Auch Informationen über Beschwerden und Rückrufe sollten bei der Entwicklung des Bedienkonzepts berücksichtigt werden[348].
- Analyse der Aufgaben, Gefährdungen und Funktionen: Nachdem das Bedienkonzept festgelegt wurde, und empirische Informationen über Benutzer und Umgebung vorliegen, können nun die Informationen, wie Benutzeranforderungen und Benutzungsanforderungen, mögliche Gefährdungen, Anforderungen an Schulung und an Abläufe festgelegt werden[349].
- Entwicklung der Benutzerschnittstelle: Das Ergebnis der vorhergehenden Aktivität ist eine in sich konsistente Benutzschnittstelle, die die spezifizierten Benutzeranforderungen und die identifizierten Risiken bei der Benutzung berücksichtigt.
- Durchführung von Tests: Die spezifizierte Benutzerschnittstelle sollte nun Tests unterzogen werden, um sicherzustellen, dass in den vorherigen Schritten die richtigen Informationen ermittelt wurden und diese Informationen vollständig und angemessen berücksichtigt wurden. Dazu wird häufig ein Prototyp entwickelt, der in unterschiedlichen Szenarien geprüft wird. Bei der Prüfung der Benutzerschnittstelle sollten möglich alle verschiedenen Benutzergruppen eingeschlossen werden[350].
- Festlegen der endgültigen Spezifikation: Basierend auf den Ergebnissen der durchgeführten Tests sollte die Benutzerschnittstelle nochmals überprüft werden, bevor diese dann endgültig zur Entwicklung freigegeben wird.

[347] [FDA-DoIt], S. 20ff.

[348] [FDA-DoIt], S. 18ff,

[349] [FDA-DoIt], S. 23ff.

[350] [FDA-DoIt], S. 28,

4.7 Medical Device Use Safety

Die Anleitung beschreibt, wie Risiken, die auf die Benutzung des Medizingerätes zurückzuführen sind, innerhalb des Risikomanagementprozesses berücksichtigt werden sollen[351]. Die Beschäftigung mit den Risiken, die aus dem Gebrauch herrühren, setzt ein gründliches Verständnis der Verwendung des Gerätes voraus. Wesentliche Teile dieses Verständnis sind[352]:

- Kenntnis über die verschiedenen Benutzergruppen des Gerätes,
- Sowohl die übliche Geräteverwendung, aber auch mögliche, aber ungewöhnliche Arten der Geräteverwendung,
- die Eigenschaften des Gerätes,
- die Eigenschaften der Umgebung, unter denen das Gerät betrieben wird und
- die Beziehungen zwischen Benutzer, Umgebung und Gerät.

4.7.1 Gefährdungen

Eine Gefährdung ist eine mögliche Ursache eines Schadens. Gefährdungen, die aus der Verwendung des Gerätes resultieren, entstehen aus folgenden Gründen:

- Das Gerät wird auf Arten benutzt, die nicht vorhergesehen wurden,
- das Gerät wird auf Arten benutzt, die zwar vorhergesehen wurden, aber nicht hinreichend überwacht werden[353],
- das Gerät benötigt physische, sensorische oder kognitive Fähigkeiten, über die der Benutzer nicht verfügt,
- das Gerät benötigt physische, sensorische oder kognitive Fähigkeiten, über die der Benutzer in einer bestimmten Umgebung nicht verfügt,
- die Benutzung des Gerätes entspricht nicht den Erwartungen des Benutzers,
- die Umgebung beeinflusst die Gerätefunktion, und dieser Einfluss wird nicht vom Benutzer berücksichtigt.

---

[351] [FDA-UseSafety], S. 5ff.

[352] [FDA-UseSafety], S. 5.

[353] [FDA-UseSafety], S. 7. Im Original ist von “inadequately controlled for” die Rede. Ich versteh dies als “nicht hinreichend überwacht“

4.7.2 Beabsichtigter Gebrauch

Die Beschreibung des beabsichtigten Gebrauchs des Medizingerätes ist wesentlich für das Verständnis, wie das Gerät benutzt und eingesetzt wird. Die Beschreibung sollte die folgenden Informationen enthalten[354]:

- Übersicht über die Gerätefunktionen
- Typische Szenarien, in denen das Gerät benutzt wird,
- Anforderungen an den Benutzer für einen sicheren und wirksamen Betrieb des Gerätes,
- Darstellung der vorläufigen Benutzerschnittstelle,
- erwartete Benutzungsumgebung.

4.7.3 Risikomanagementprozess

Risikomanagement kann den Einfluss solcher Gefährdungen verringern, auch wenn das Risiko, das aus solchen Gefährdungen herrührt, schwierig zu bestimmen ist. Bei der Betrachtung von Risiken des Gebrauchs in einem Risikomanagementprozess sollten die folgenden Aufgaben berücksichtigt werden[355]:

- Feststellung von analytisch abgeleiteten und empirisch ermittelten Gefährdungen des Gebrauchs[356],
- Beschreibung der Szenarien, in denen die festgestellten Gefährdungen auftreten,
- Entwicklung und Anwendung von Strategien, zur Steuerung dieser Risiken,
- Nachweis des sicheren und wirksamen Gerätegebrauchs (Validierung)

4.8 Off-the-Shelf Software Use in Medical Devices

Die Bedeutung von „Off-the-shelf“ (OTS) Software nimmt mit der Verwendung standardisierter Hardware zu. Gegen den Einsatz solcher Software ist auch prinzipiell nichts einzuwenden, da der Hersteller sich so auf die Entwicklung der medizinischen Software konzentrieren kann. Jedoch kann der Einsatz solcher Mehrzwecksoftware nicht für die vorgesehenen spezifischen

[354] [FDA-UseSafety], S. 17f

[355] [FDA-UseSafety], S. 15, Abschnitt 5, Apply Human Factors Engineering (HFE) Approaches Within the Risk Management Process.

[356] Es wird kein spezielles Verfahren für die analytische Ermittlung der Gefährdungen empfohlen. Ein mögliches Verfahren ist etwa FMEA.

Zwecke geeignet sein. Zudem verliert der Hersteller die Kontrolle für den Software-Lebenszyklus, trägt aber dennoch die Verantwortung über die fortgesetzte sichere und wirksame Leistung des Medizingerätes. Die Anleitung hilft bei der Frage, welche Unterlagen der Hersteller bei der Verwendung von OTS-Software bereitstellen muss, um einen sicheren Betrieb des Medizingerätes sicherzustellen[357].

Diese Anleitung geht von einem sicherheitsbasierten Ansatz des Risikomanagements aus und ist mit internationalen Normen über Risikomanagement verträglich[358]. Der Umfang der erforderlichen Dokumentation richtet sich nach den Ergebnissen der Risikoanalyse und nach der festgestellten Gefährdungsklasse der Software[359]. Die Liste gibt eine Übersicht über die erforderliche Dokumentation[360]:

- Minor:
    - Risikoanalyse,
    - Basisdokumentation und
    - ggf. Risikokontrollmaßnahmen.
- Moderate:
    - Risikoanalyse,
    - Basisdokumentation,
    - Risikokontrollmaßnahmen und
    - Beschreibung und Rechtfertigung der Restrisiken.
- Major:
    - Risikoanalyse,
    - Basisdokumentation,
    - Risikokontrollmaßnahmen,
    - Beschreibung und Rechtfertigung der Restrisiken und
    - ergänzende Dokumentation

[357] [FDA-OTS], Kapitel 1.1 Introduction and Background, S.1

[358] [FDA-OTS], Kapitel 1.2 Purpose / Scope – Die relevanten Begriffe und Konzepte des Risikomanagements können daher auch den angesprochenen internationalen Normen entnommen werden, etwa [ISO 14971].

[359] zur Festlegung der Gefährdungsklassen siehe [FDA-Premarket], S. 4ff.

[360] [FDA-OTS], Tabelle 1-1, S. 5.

In den nachfolgenden Kapiteln ist ausgeführt, welche Informationen die jeweiligen Dokumente enthalten müssen.

4.8.1 Basisdokumentation

Die Basisdokumentation zu der eingesetzten OTS-Software soll die folgenden Fragen beantworten[361]:

- Um welche Art von Software handelt es sich? Für jedes Teil der OTS-Software sollen Titel, Hersteller, Version, und alle weiteren erforderlichen Informationen zur korrekten Identifizierung der Software festgehalten werden. Zudem soll angegeben werden, welche Benutzerdokumentation bereitgestellt wird, wieso die Software für das Medizingerät geeignet ist und von welchen Beschränkungen beim Einsatz dieser Software ausgegangen wird.
- Welche Anforderungen verlangt die Software? Hier werden Angaben zu den für die OTS-Software erforderlichen Hardwareanforderungen, wie Prozessor, Speicherplatz, Festplattenspeicherbedarf und Softwareanforderungen, wie Betriebssystem, Treiber, und Utilities erwartet.
- Wie werden die erforderlichen Maßnahmen des Benutzers sichergestellt? Hier sollen Angaben darüber gemacht werden, ob die Software installiert oder konfiguriert werden muss, wie dies durchzuführen ist, ob dies ggf. wiederholt werden muss und wie der Benutzer in der Bedienung oder Benutzung der Software geschult werden muss.
- Welche Funktionen werden von dem Medizingerät genutzt? Hier wird dokumentiert, welche Funktionen der OTS-Software genutzt werden, und welche Funktionen damit in dem Medizingerät erfüllt werden[362].
- Wie wird die Funktionalität sichergestellt? Basierend auf dem Gefährdungsgrad des Medizingerätes sollen durchgeführte Test-, Verifikations- und Validierungsaktivitäten, die Ergebnisse der Tests und die bekannten Probleme der OTS-Software aufgeführt werden.
- Wie wird der Einsatz der OTS-Software gelenkt? Es soll beschrieben werden, wie sichergestellt wird, dass keine unzulässigen Versionen benutzt werden. Es sollte weiter beschrieben werden, wie Aktualisierungen der OTS-Software installiert und konfiguriert werden.

[361] [FDA-OTS], Kapitel 2.1, S. 5ff.

[362] Es sollen die in [FDA-Premarket], S.8ff, festgelegten Informationen angeführt werden, siehe auch Kapitel 4.4.

4.8.2 Risikoanalyse

Es wird vom Hersteller erwartet, als Teil der Risikoanalyse des Medizingerätes eine Risikoanalyse zu der eingesetzten OTS-Software durchzuführen[363]. Die folgenden Informationen sollen vom Hersteller bereitgestellt werden:

- Eine Liste aller identifizierten Gefährdungen,
- die Bewertung einer jeden Gefährdung und
- eine Liste aller möglichen Ursachen für jede Gefährdung.

4.8.3 Risikokontrollmaßnahmen

Risikokontrollmaßnahmen haben den Zweck, die Schwere einer Gefährdung, die Wahrscheinlichkeit des Auftretens der Gefährdung oder beides zu verringern. Die Maßnahme kann Änderungen an der Hardware oder der Software beinhalten. Es sollten die folgenden Informationen beigestellt werden[364]:

- Eine Liste aller Gefährdungen, für die Risikokontrollmaßnahmen festgelegt wurden,
- die zur Verringerung der Gefährdung durchgeführten Maßnahmen und
- das noch verbleibende Restrisiko.

4.8.4 Beschreibung der Restrisiken

Der Hersteller soll eine komplette Liste der verbleibenden Risiken erstellen. Das in Zusammenhang mit OTS-Software stehende Risiko soll mit dem Risiko von Alternativen verglichen werden, etwa dem Risiko, die betreffende Software selbst zu entwickeln. Jede Erfahrung mit der Benutzung der betreffenden OTS-Software sollte zudem dargestellt werden[365].

4.8.5 Ergänzende Dokumentation

Für die spezielle Dokumentation wird vom Hersteller erwartet, dass er[366]:

- zusichert, dass bei der Entwicklung der OTS-Software Verfahren eingesetzt wurden, die für den beabsichtigten Einsatz der OTS-Software angemessen und ausreichend sind,

---

[363] [FDA-OTS], Kapitel 2.2, S. 7f.

[364] [FDA-OTS], Kapitel 2.3, S. 8ff.

[365] [FDA-OTS], Kapitel 2.4, S. 11.

[366] [FDA-OTS], Kapitel 2.5, S. 11f.

- nachweist, dass die Verfahren und Ergebnisse der für die OTS-Software durchgeführten Verifikations- und Validierungsaktivitäten für den beabsichtigten Einsatz der OTS-Software angemessen und ausreichend sind und
- darlegt, dass ein angemessener Mechanismus für die Weiterführung von Wartung und Support der OTS-Software existiert, falls der Hersteller der OTS-Software dies nicht mehr tut.

4.9 Cybersecurity for Networked Devices with OTS Software

Diese Anleitung stellt Empfehlungen für Hersteller von Medizingeräten bereit, die OTS-Software[367] beinhalten und an ein Netzwerk angeschlossen werden können. Sicherheitsgefährdungen können immer dann angenommen werden, wenn durch die OTS-Software die Möglichkeit besteht, ohne Autorisierung auf das Netzwerk oder das Medizingerät zuzugreifen. [21CFR820] verlangt in Abschnitt 100, das alle vorliegenden Informationen zu analysieren sind, hier also die möglichen Schwachstellen der Cybersecurity, und anschließend geeignete Aktionen einzuleiten, um die aufgefundenen Probleme zu beseitigen. Die möglicherweise im Zuge dieser Aktionen durchzuführenden Softwareänderungen sind wie alle anderen Softwareänderungen zu behandeln. Das Dokument weist darauf nochmals hin.

[367] OTS-Software ist eine in den FDA-Dokumente benutzte Abkürzung für „Off-the-shelf"-Software.

5 Prozessorientierte Darstellung

Nachdem in den vorherigen Kapiteln die für die Softwareentwicklung einschlägigen Gesetze, Standards, Verordnungen und Anleitungen mit den dazugehörigen Anforderungen übersichtsartig aufgeführt wurden, werden in diesem Kapitel die dort angeführten Vorgaben in einen prozessorientierten Kontext gestellt. Dazu werden die in den Standards geforderten Verfahren prozessorientiert mit den zugehörigen Ein- und Ausgaben beschrieben. Dies kann natürlich keine erschöpfende Beschreibung sein, da in diesem Fall jede einzelne regulatorische Anforderung und Anmerkung bei der Konzeption der Prozesse Berücksichtigung finden müsste. Obwohl auch dies prinzipiell möglich ist, sprengt diese Art der Darstellung den Umfang einer Projektarbeit. Zudem wäre zu überlegen, ob für diese umfangreiche Darstellung ein Textdokument die geeignete Darstellung ist.

In dieser Arbeit werden daher die erforderlichen Prozesse zunächst durch die wesentlichen Anforderungen charakterisiert und sodann die erforderlichen Aufgaben mit den Eingaben und Aufgaben aufgeführt. Wo dies hilfreich erscheint, werden die Ausführungen durch Aktivitätsdiagramme ergänzt.

Bei der Durchsicht der regulatorischen Vorgaben ergeben sich die folgenden Gruppen von Aktivitäten:

1. Aktivitäten, die sich mit der Planung der Entwicklungsaktivitäten, der Feststellung der Qualitätsmaßnahmen und der Ermittlung der benötigten Ressourcen beschäftigen (Entwicklungsplanung),
2. Aktivitäten, die sich im Vorfeld einer Entwicklung mit der Aufnahme von Kundenanforderungen beschäftigen,
3. Aktivitäten, die sich mit der Erfassung, Analyse, Verfolgbarkeit und Änderung von Anforderungen beschäftigen (Anforderungs- und Änderungsmanagement),
4. Aktivitäten, die sich mit der Identifikation und Beurteilung von Risiken und mit Maßnahmen zur Reduzierung von identifizierten Risiken beschäftigen (Risikomanagement),
5. Aktivitäten, die sich mit der Gebrauchtauglichkeit der Software beschäftigen,
6. Aktivitäten, die sich mit Architektur, Design und Implementierung der Software beschäftigen (Softwarewareentwicklung),
7. Aktivitäten, die sich mit der Überprüfung der bei der Entwicklung der Software entstandenen Produkte gegen bestimmte Arten von Anforderungen, wie funktionale Anforderungen, Qualitätsanforderungen, Berücksichtigung von Risikokontrollmaßnahmen, Vollstän-

digkeit oder Widerspruchsfreiheit, beschäftigen (Review, Test, Verifikation und Validierung),

8. Aktivitäten, die sich mit der Identifikation und Rückverfolgbarkeit der Produkte beschäftigen (Konfigurationsmanagement),
9. Aktivitäten, die sich mit der Problembehandlung der Produkte beschäftigen, die dann eventuell zu Änderungen von Anforderungen und Software führen (Problemmanagement),
10. Aktivitäten, die sich mit allgemeinen Anforderungen an das Qualitätsmanagementsystem, also dem Vorliegen von Verfahren zur Lenkung von Dokumenten und Aufzeichnungen, der Durchführung interner Audits und Ähnlichem beschäftigen. Diese Vorgaben sind recht unspezifisch für die Softwareentwicklung und bleiben daher weitgehend unberücksichtigt.

5.1 Methodische Vorüberlegungen

Bevor diese Aktivitäten aber dargestellt werden, bleibt zuvor die Frage zu klären, auf welche Art diese Aktivitäten nun dargestellt werden. Dazu wird kurz der Begriff eines Vorgehensmodells diskutiert, bevor die für uns relevanten Begriffe erläutert werden, mit denen die Anforderungen dargestellt werden.

5.1.1 Definition des Vorgehensmodells

Prozessmodelle, im deutschen Sprachraum auch als Vorgehensmodelle bekannt, haben den Anspruch, den organisatorischen Rahmen für die Softwareentwicklung festzulegen. Was das nun genau heißt, und welche Begriffe zur Beschreibung eines Vorgehensmodells geeignet sind, wird in der Literatur unterschiedlich gesehen. [Balzert] stellt dazu fest: „Jede Software-Erstellung soll in einem festgelegten organisatorischen Rahmen erfolgen. Ein Prozessmodell beschreibt einen solchen Rahmen. Ein definiertes Prozess-Modell soll Folgendes festlegen:

- Reihenfolge des Arbeitsablaufes (Entwicklungsstufen, Phasenkonzepte),
- Jeweils durchzuführende Aktivitäten,
- Definition der Teilprodukte einschließlich Layout und Inhalt,
- Fertigstellungskriterien (Wann ist ein Teilprodukt fertig gestellt?).
- Notwendige Mitarbeiterqualifikationen,
- Verantwortlichkeiten und Kompetenzen,

- Anzuwendende Standards, Richtlinien, Methoden und Werkzeuge.“ [368]

[Versteegen] definiert hingegen etwas allgemeiner: „Ein Prozessmodell ist eine Beschreibung einer koordinierten Vorgehensweise bei der Abwicklung eines Vorhabens. Es definiert sowohl den Input, der zur Abwicklung der Aktivität notwendig ist, als auch den Output, der als Ergebnis der Aktivität produziert wird. Dabei wird eine feste Zuordnung von Workern vorgenommen, die die jeweilige Aktivität ausüben.“ [369]

[Winter] wiederum stellt fest: „Vorgehensmodelle stellen den Rahmen dar, in dem die Entwicklungstätigkeiten organisiert werden [...]. Sie zerlegen den Entwicklungsprozess gewöhnlich in zeitlich aufeinander folgende *Phasen*, die jeweils ein Zeitintervall mit den darin stattfindenden Aktivitäten beschreiben. Als *Aktivität* wird dabei eine inhaltlich zusammenhängende (Teil-) Tätigkeit bezeichnet, die von einigen wenigen Personen in einem bestimmten Zeitraum ausführbar ist. Jede Phase schließt mit einem Meilenstein ab, bei dem überprüft wird, ob die geforderten Ergebnisse erbracht worden sind.

Vorgehensmodelle beschreiben die notwendigen Aktivitäten nebst ihren Voraussetzungen und Ergebnissen und legen somit die Ablauforganisation fest; sie spezifizieren quasi die Geschäftsprozesse der Softwareentwicklung selbst.“[370]

5.1.2 Kernbegriffe von Vorgehensmodellen

Schon diese drei Beispiele zeigen, dass die Vorstellungen, was ein Vorgehensmodell im Einzelnen leisten soll, sich erheblich unterschieden können. Zudem kann sich die Terminologie noch zusätzlich unterscheiden[371]. Dennoch kann man eine – zumindest teilweise - Übereinstimmung zwischen den verschiedenen Definitionen feststellen. In einem Prozessmodell werden üblicherweise die folgenden Begriffe benutzt:

- **Disziplinen** erlauben eine inhaltliche Gliederung der Entwicklungsaktivitäten. Disziplinen findet man sowohl in klassischen Vorgehensmodellen[372], als auch in moderneren Vorgehensmodellen, wie dem V-Modell 97[373] oder RUP[374], auch wenn sie dort teilweise anders

[368] [Balzert2], Kapitel 3.3, S. 98.

[369] [Versteegen], Kapitel 2, S. 21ff.

[370] [Winter], Kapitel 3, S. 27.

[371] Ergebnisse einer Aktivität heißen im „V-Modell 97“ Produkte, im „Rational Unified Process (RUP)“ hingegen Artefakte, und wir haben hier überwiegend von Ergebnissen gesprochen.

[372] In der Literatur findet man mehrere solcher klassischen Modelle, wie das Wasserfallmodell, das allgemeine V-Modell oder das Spiralmodell, vgl. [Pomberger], Kapitel 2, S. 11ff.

[373] [Dröschel], Einführung in das V-Modell Version 97, S. 57ff.

[374] [Versteegen2], Kapitel 3.4, Die Phasen und Workflows des Rational Unified Process, S. 52ff.

genannt werden. In den regulatorischen Anforderungen werden eine Vielzahl von unterschiedlichen Disziplinen aufgeführt, wie etwa Entwicklungsplanung, Anforderungsanalyse, Architekturentwurf und detaillierter Entwurf in [ISO prEN 62304], auch wenn dafür anderen Begriffe, wie Prozesse, Aktivitäten oder Verfahren benutzt werden. Disziplinen benötigen üblicherweise eine Anzahl von Eingaben, bestehen aus einem – mehr oder weniger - komplexen Ablauf, bei dem eine Anzahl von Aktivitäten ausgeführt wird, und erzeugen oder verändern eine Anzahl von Produkten. Es ist also damit klar, dass jede Disziplin als Prozess aufgefasst werden kann.

- **Aktivitäten** beschreiben, was in einem Projekt zu tun ist und legen ggf. fest, welche Voraussetzungen, Ergebnisse und Abhängigkeiten damit verbunden sind. Die Granularität der Aktivitäten ist damit deutlich geringer als die von Disziplinen. Aktivitäten werden benutzt, um die Disziplinen weiter zu strukturieren. Ein Beispiel einer Aktivität ist eine Produktverifizierung oder eine Risikokontrollmaßnahme. Eine bestimmte Aktivität kann prinzipiell in verschiedenen Disziplinen verwendet werden. Auch eine Aktivität verwendet Eingaben und erzeugt Ergebnisse, kann also ebenfalls als (Teil-) Prozess aufgefasst werden.
- **Produkte** beschreiben die grundlegenden Eigenschaften der entstehenden Resultate. In den regulatorischen Anforderungen findet sich häufig eine inhaltliche Charakterisierung der erforderlichen Produkte. In den regulatorischen Anforderungen sind eine Vielzahl von Ergebnissen aufgeführt. Exemplarisch seien nur Entwicklungsplan, Anforderungsspezifikation, Verifikationsplan, Risikomanagementplan oder Geräteentstehungsakte genannt.
- **Methoden** legen fest, wie bestimmte Aktivitäten ausgeführt werden. An einigen Stellen werden in den regulatorischen Anforderungen Vorschläge gemacht, wie bestimmte Aktivitäten ausgeführt werden, etwa wird in [60601-1-4][375] angeführt, dass als Verfahren für die Verifizierung Walkthroughs und Besichtigungen, statische und dynamische Analysen, sowie White- und Blackbox-Prüfungen in Frage kommen.
- **Phasen** stellen eine zeitliche Gliederung des Entwicklungsprozesses dar. Alle Vorgaben weisen darauf hin, dass sie keinen speziellen Softwareentwicklungsprozess fordern, und bleiben daher hinsichtlich der Vorgabe, in welcher Reihenfolge Aktivitäten oder Disziplinen auszuführen seien, überwiegend unbestimmt. Dennoch wird etwa in [21CFR820], ein Verfahren gefordert, um sicherzustellen, dass formale Reviews des Entwicklungsfortschritts zu bestimmten Zeitpunkten innerhalb des Entwicklungsprozesses vorgesehen und durchgeführt werden[376]. Analoge Forderungen finden sich in [ISO 13485][377].

[375] [60601-1-4], Kapitel 52.209.2, Anmerkung, S. 13.

[376] [21CFR820], Sec. 30 (e).

[377] [ISO 13485], Abschnitt 7.2.3

Vorgehensmodelle verwenden üblicherweise zusätzlich Begriffe wie Rollen, Iterationen oder Meilensteine. Auf diese Begriffe können wir aber verzichten, da hier nicht das Ziel verfolgt wird, die regulatorisch vorgegebenen Aktivitäten auf reale Vorgehensmodelle abzubilden.

5.1.3 Softwareentwicklungsprozess

Für den Softwareentwicklungsprozess sind die folgenden Disziplinen erforderlich:

- **Konzepterstellung**. Bevor das Projekt gestartet oder die Produktentwicklung begonnen werden kann, müssen die Kundenanforderungen aufgenommen werden, die Vision eines neuen oder verbesserten Produktes entwickelt und die prinzipielle Machbarkeit des Produktes sichergestellt werden. Zudem muss der beabsichtigte Gebrauch des Gerätes festgelegt werden. Das wesentliche Ergebnis dieser Disziplin ist ein Produktkonzept.
- **Entwicklungsplanung**. Bevor nun die Produktentwicklung beginnen kann, muss festgelegt werden, wie diese Entwicklung von statten gehen soll. Daher müssen die für die Entwicklung des Software-Systems verwendete Prozesse, die benötigten Ressourcen, einzuhaltende Meilensteine, zu verwendende Standards, Regeln und Ähnliches definiert werden.
- **Anforderungsermittlung**. Zweck der Anforderungsermittlung ist es, die in dem Konzept noch unklar und unvollständig formulierten Anforderungen an das Produkt zu analysieren, zu spezifizieren und zu verifizieren. Ergebnis ist eine Spezifikation, die angibt, was das System tun soll. Das wesentliche Ergebnis dieser Disziplin ist die Anforderungsspezifikation (Lastenheft) und eine erste Risikoanalyse.
- **Systemdesign**. Das Ziel der Systemanalyse ist eine Lösungsbeschreibung, die festlegt, wie das System die geforderten Leistungen erbringt. Das wesentliche Ergebnis dieser Disziplin ist die Systemspezifikation (Pflichtenheft) und eine aktualisierte Risikoanalyse.
    - **Architekturkonzeption**. Durch die Architekturkonzeption werden die zentralen Realisierungsentscheidungen getroffen. Weiterhin wird das System hierarchisch in Komponenten zerlegt und die Schnittstellen dieser Komponenten technisch beschrieben. Das wesentliche Ergebnis dieser Aktivität ist die Architekturspezifikation.
    - **Entwurf**. Im Mittelpunkt dieser Disziplin steht die weitere Zerlegung der Komponenten in Softwaremodule und eine Beschreibung der internen Struktur der Komponenten. Das wesentliche Ergebnis dieser Disziplin ist die Designspezifikation.
- **Implementierung und Modultest**. In dieser Disziplin werden die im Design spezifizierten Module implementiert und anschließend in Isolation getestet. Das wesentliche Ergebnis dieser Disziplin ist ein getestetes Modul.

- **Verifizierung**. Durch die Verifizierung wird überprüft, ob das fertige System oder Teile dieses Systems den Vorgaben entsprechen. Hierzu ist zunächst eine Testspezifikation zu erstellen, die festlegt, welche Prüfungen vorzunehmen sind. Häufig werden Modultest, Integrationstest und Systemtest unterschieden.
- **Validierung**. Durch die Validierung wird überprüft, ob das Produkt für den beabsichtigten Zweck geeignet ist. In einer Spezifikation ist zu dokumentieren, welche Überprüfungen hierfür erforderlich sind.
- **Abnahmetest und Freigabe**.
- **Risikokontrollmaßnahmen**. Risikokontrollmaßnahmen sind keine separate Disziplin, sondern sind vollständig in den Entwicklungsprozess eingebettet.
- **Problemlösungsmaßnahmen**.
- **Änderungskontrolle**. Durch eine Änderungskontrolle wird sichergestellt, dass keine unbeabsichtigten Änderungen in das Produkt eingebracht werden.
- **Konfigurationsmanagement**. Konfigurationsmanagement ist bereits während der Entwicklung erforderlich, da alle Produkte vor der Validierung durch das Konfigurationsmanagement identifiziert sein müssen.

5.2 Konzepterstellung

Vor dem eigentlichen Beginn der Produktentwicklung wird der Hersteller Vorstellungen über das zu entwickelnde Produkt entwickeln, grundsätzliche Anforderungen festlegen und Leistungsdaten über das Gerät dokumentieren. Diese Vorstellungen resultieren üblicherweise in ein Gerätekonzept oder Visionsdokument. [ISO 13485][378] fordert den Hersteller auf, solchen Überlegungen vor dem Eingehen von Verpflichtungen anzustellen und dabei insbesondere Kundenanforderungen und Anforderungen, die für den beabsichtigten Gebrauch erforderlich sind, aufzunehmen und zu bewerten. Im Einzelnen sind die folgenden Aktivitäten auszuführen:

- Ermittlung von Kundenanforderungen. [ISO 13485][379] fordert die Ermittlung der vom Kunden festgelegten Anforderungen. Es wird aber nicht näher spezifiziert, wie diese Anforderungen ermittelt werden sollen. Lediglich in Kapitel 7.2.3 werden Regelungen zur Kommunikation mit dem Kunden zu den Punkten Produktinformationen, Anfragen, Änderungen, Rückmeldungen und Maßnahmenempfehlungen verlangt. Es liegt nahe, über diese Kommunikationswege Kundenanforderungen zu ermitteln.

[378] [ISO 13485], Kapitel 7.1, Planung der Produktrealisierung und Kapitel 7.2, Kundenbezogene Prozesse

[379] [ISO 13485], Kapitel 7.2.1 a).

- Ermittlung regulatorischer und gesetzlicher Anforderungen. Der Hersteller[380] soll bereits vor dem Beginn der Produktentwicklung ermitteln, welche gesetzlichen und regulatorischen Anforderungen zu berücksichtigen sind. Soweit es sich um eine Softwareentwicklung handelt, sind die wesentlichen Anforderungen in dieser Arbeit beschrieben. Je nach Art des Medizingerätes müssen aber möglicherweise zahlreiche weitere Vorgaben eingehalten werden. Der Hersteller soll sich möglichst früh darüber informieren, um bewerten zu können, ob er diese Vorgaben einhalten kann.
- Festlegung von Anforderungen der Organisation. Der Hersteller hat möglicherweise Vorgehensweisen für bestimmte Disziplinen oder Aktivitäten intern festgelegt. Es ist auch möglich, dass der Hersteller für die Produktentwicklung erst bestimmte Vorgehensweisen festlegen möchte. Zudem kann der Hersteller Produktanforderungen aller oder bestimmter Arten von Geräten festgelegt haben. Alle diese Anforderungen sollen also bei der Produktentwicklung berücksichtigt werden. Daher sollen solche Anforderungen in dem Produktkonzept berücksichtigt werden[381].
- Ermittlung des beabsichtigten Gebrauchs und dessen Anforderungen. Bereits bei der Konzepterstellung soll der beabsichtigte Gebrauch soweit möglich spezifiziert werden[382]. Auf der Grundlage des beabsichtigten Gebrauchs sollen Anforderungen ermittelt werden, die zur Umsetzung des beabsichtigten Gebrauchs erforderlich sind. Dies schließt folgende Informationen ein[383]:
    - Übersicht über die Gerätefunktionen,
    - Typische Szenarien, in denen das Gerät benutzt wird,
    - Anforderungen an den Benutzer für einen sicheren und wirksamen Betrieb des Gerätes,
    - Darstellung der vorläufigen Benutzerschnittstelle,
    - erwartete Benutzungsumgebung.
- Bewertung der ermittelten Anforderungen. Der Hersteller soll die ermittelten Anforderungen bewerten. Bei der Bewertung soll berücksichtigt werden, ob die Anforderungen ausreichend für eine Bewertung sind und ob der Hersteller in der Lage ist, die ermittelten Anforderungen umzusetzen[384]. Dabei ist also insbesondere zu berücksichtigen, ob der Her-

[380] [ISO 13485], Kapitel 7.2.1 c).

[381] [ISO 13485], Kapitel 7.2.1 d).

[382] [ISO 13485], Kapitel 7.2.1 b).

[383] [FDA-UseSafety], S. 17f.

[384] [ISO 13485], Kapitel 7.2.2.

steller über die erforderlichen Fachkräfte verfügt, ob die Fachkräfte in ausreichendem Maße verfügbar sind und die bisher festgestellten Produktanforderungen durch den Hersteller umsetzbar sind. Das Ergebnis der Bewertung ist die Entscheidung, das Produkt zu entwickeln oder nicht.

Abbildung 2 zeigt die für die Konzepterstellung erforderlichen Aktivitäten im Zusammenhang.

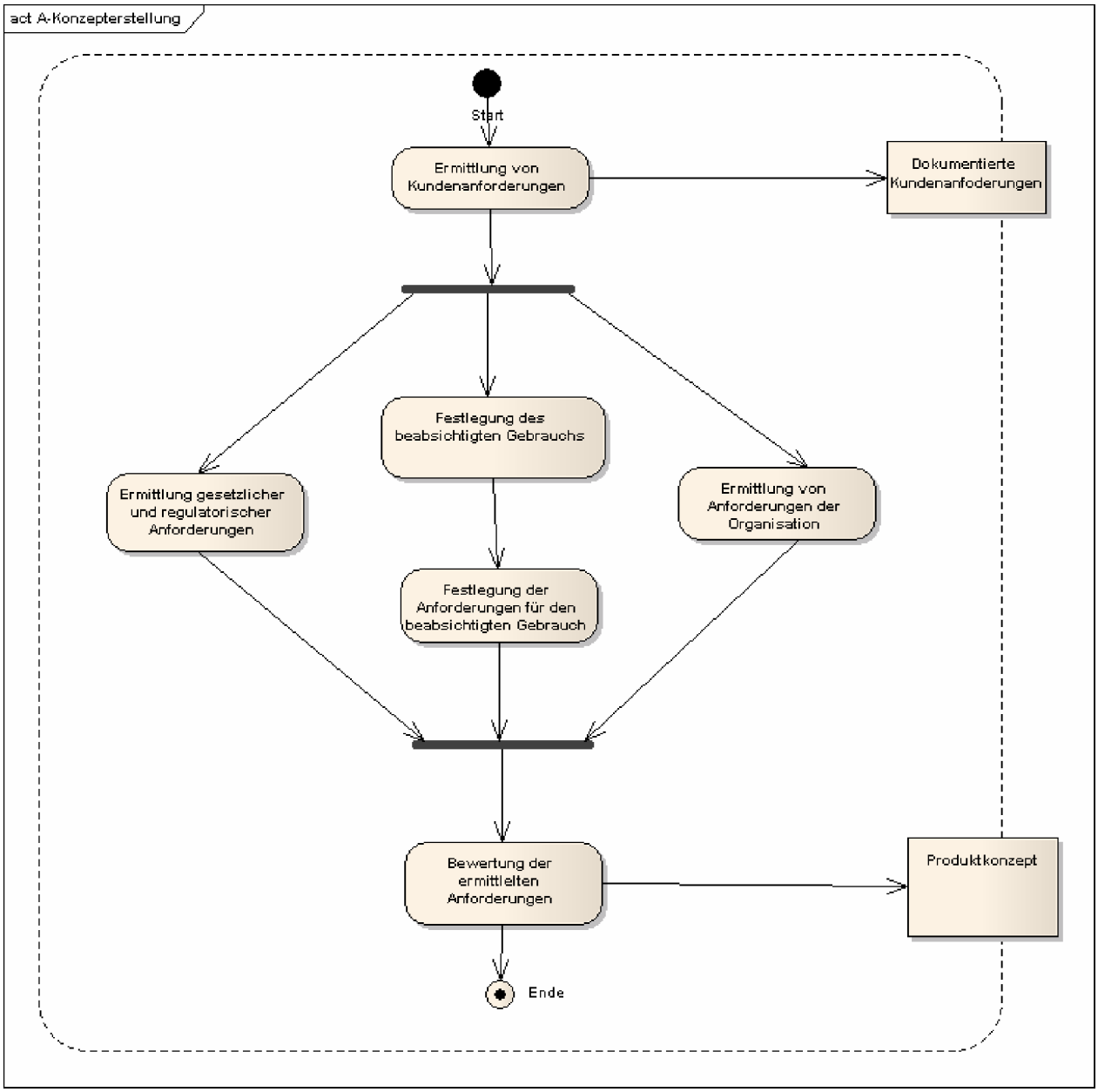

Abbildung 2 : Aktivitätsdiagramm Konzepterstellung

5.3 Entwicklungsplanung

Nachdem das Konzept des Gerätes festgelegt wurde und die Entscheidung, das Gerät zu entwickeln, getroffen wurde, muss die Entwicklung geplant werden. Dazu ist ein Entwicklungsplan zu erstellen, der alle der folgenden Informationen enthält, die zur Durchführung der Produktentwick-

lung erforderlich sind. Sehr viele Dokumente enthalten wesentliche Vorgaben zur Entwicklungsplanung. Die folgende Liste listet alle Dokumente mit den Kapiteln auf, die wesentliche Vorgaben zur Entwicklungsplanung enthalten.

- [ISO 13485]:
    - Kapitel 7.1 Planung der Produktrealisierung
    - Kapitel 7.2.3 Kommunikation mit dem Kunden
    - Kapitel 7.3.1 Design- und Entwicklungsplanung
- [ISO 60601-1-4]:
    - Kapitel 52.203.1. Definition eines Entwicklungslebenszyklus.
    - Kapitel 52.203.2. Aufteilung des Entwicklungslebenszyklus in Phasen und Aktivitäten.
    - Kapitel 52.203.3. Ein integraler Risikomanagementprozess ist erforderlich.
    - Kapitel 52.203.4. Es müssen Anforderungen an die Dokumentation festgelegt werden.
    - Kapitel 52.203.6. Ein Prozess für die Problemlösung ist erforderlich.
    - Kapitel 52.204.2. Der Risikomanagementprozess muss innerhalb des Entwicklungslebenszyklus durchgeführt werden.
    - Kapitel 52.205. Qualifikation des Personals.
    - Kapitel 52.209.2. Erstellung eines Verifizierungsplans.
    - Kapitel 52.210.2. Erstellung eines Validierungsplans.
    - Kapitel 52.210.4. Die Validierungsgruppe muss von der Entwicklungsgruppe unabhängig sein.
- [ISO prEN 62304]:
    - Kapitel 4.1. Risikomanagement.
    - Kapitel 5. Softwareentwicklungsprozess.
    - Kapitel 5.1. Planung der Softwareentwicklung.
    - Kapitel 5.1.1. Softwareentwicklungsplan.
    - Kapitel 5.1.2. Aktualisierung des Softwareentwicklungsplans.
    - Kapitel 5.1.3. Referenz auf die System-Entwicklung im Entwicklungsplan.
    - Kapitel 5.1.4. Planung der Normen für die Softwareentwicklung.

- Kapitel 5.1.5. Planung der Softwareintegration und der Integrationsprüfung.
- Kapitel 5.1.6. Planung der Software-Verifizierung.
- Kapitel 5.1.8. Planung des Risikomanagements.
- Kapitel 5.1.9. Planung der Dokumentation.
- Kapitel 5.1.10. Planung des Konfigurationsmanagements.
- Kapitel 5.1.12. Planung der Problemlösung.
- Kapitel 5.5.2. Festlegung eines Verifizierungsprozesses für Softwareeinheiten.

- [ISO 14971]
  - Kapitel 3.4. Qualifikation des Personals.
- [21CFR820]
  - Kapitel 820.25. Personal.
  - Kapitel 820.30. Entwicklungslenkung.
  - Kapitel 820.30 (i). Entwicklungsentstehungsakte (Design history file).
  - Kapitel 820.40. Dokumentenlenkung.
  - Kapitel 820.181. Produkt-Hauptakte (Device master record).
  - Kapitel 820.184. Produkt-Entstehungsakte (Device history record).
  - Kapitel 820.186. Qualitätssystemakte (Quality system record).
  - Kapitel 820.250. Statistische Methoden.
- [FDA- Premarket]:
  - Software Development Environment Description (s. S. 14f.)
- [FDA- DesignGuide]:
  - Section B: Entwicklungsplanung
- [FDA-Validation]:
  - Kapitel 4.4 Software Life Cycle
  - Kapitel 4.10 Flexibility and Responsibility
  - Kapitel 5.1 Software Life Cycle Activities
  - Kapitel 5.2.1 Quality Planning

Aus den oben aufgeführten Vorgaben ergeben sich die folgenden Anforderungen an die Planung der Entwicklung:

- Es müssen alle erforderlichen Prozesse, die bei der Entwicklung des Software-Systems verwendet werden, festgelegt und dokumentiert werden. Dabei ist auch festzulegen, wie die Aktivitäten und Aufgaben anderer Prozesse die Entwicklung beeinflussen oder in die Entwicklung integriert sind. Bei der Festlegung sind auch die bei der Ausführung der Prozesse anfallenden Produkte festzulegen und zu dokumentieren. Zu den erforderlichen Prozessen, die geplant werden müssen, gehört insbesondere:
    - Die Festlegung und Dokumentation der Verfahren, die die Softwareentwicklung und die Validierung der Entwicklung koordinieren. Die Vorgaben für die Validierung werden im Entwicklungsplan oder einem separaten Validierungsgsplan dokumentiert.
    - Die Festlegung und Dokumentation eines Verfahrens, das beschreibt, wie Komponenten und Subsysteme (einschließlich SOUP) integriert werden und wie die Integration der Komponenten geprüft wird. Die Vorgaben für die Integration werden im Entwicklungsplan, Verifizierungsplan oder einem separaten Integrationsplan dokumentiert.
    - Die Festlegung und Dokumentation des Verfahrens zur Verifikation für jede Aktivität des Lebenszyklus. Dazu gehört auch die Festlegung der Meilesteine, zu denen die Verifizierungsaufgaben durchgeführt werden und die Akzeptanzkriterien für die Verifizierung der zu liefernden Produkte. Die Vorgaben für die Verifizierung werden im Entwicklungsplan oder einem separaten Verifizierungsplan dokumentiert.
    - Die Festlegung und Dokumentation eines Verfahrens für die Problemlösung. Dieses Verfahren muss über alle Phasen und Aktivitäten des Entwicklungsprozesses hinweg verwendet werden.
    - Die Festlegung und Dokumentation eines Verfahrens zum Änderungsmanagement. Dabei müssen auch die SOUP-Konfigurationselemente und Software, die zur Entwicklungsunterstützung verwendet wird, berücksichtigt werden.
    - Die Festlegung und Dokumentation eines Verfahrens für das Konfigurationsmanagement. Dabei müssen auch die SOUP-Konfigurationselemente und Software, die zur Entwicklungsunterstützung verwendet wird, berücksichtigt werden. Software-Komponenten müssen unter das Konfigurationsmanagement gestellt werden, bevor sie verifiziert werden.
    - Die Festlegung und Dokumentation der Aktivitäten und Aufgaben des Software-Risikomanagements. Dies schließt das Management von Risiken, die sich auf SOUP beziehen, ein. Das Risikomanagement muss sich dabei auf den gesamten

Entwicklungsprozess beziehen. Die Vorgaben für das Risikomanagement werden im Entwicklungsplan oder einem separaten Risikomanagementplan dokumentiert.

- Die organisatorische Struktur des Projektes, wie Hauptaufgaben, vorgesehener Zeitrahmen für jede Hauptaufgabe, benötigte Ressourcen und erforderliches Personal und die organisatorischen Verantwortlichkeiten müssen festgelegt und dokumentiert werden.
- Die zeitliche Organisation der Entwicklung muss festgelegt werden, insbesondere wesentliche Review- und Entscheidungspunkte sowie Meilensteine.
- Die im Entwicklungsprozess verwendeten Normen, Methoden und Werkzeuge müssen festgelegt und dokumentiert werden.
- Die Systemanforderungen müssen im Entwicklungsplan dokumentiert werden.[385]
- Es muss ein Verfahren, durch das die Beziehung zwischen Systemanforderungen, Software-Anforderungen, Softwaresystemprüfungen und Risikokontrollmaßnahmen, die in die Software implementiert sind, festgelegt und dokumentiert werden.
- Es muss eine Produktentstehungsakte (DHF) angelegt und gepflegt werden. Dieses Dokument enthält oder referenziert alle notwendigen Aufzeichnungen, um zu dokumentieren, dass die Entwicklung in Übereinstimmung mit den in der Entwicklungsplanung festgelegten Verfahren erfolgt ist.
- Es muss eine Produkthauptakte (DMF) angelegt und gepflegt werden. Dieses Dokument enthält order referenziert alle Spezifikationen und sonstigen Vorgaben, die erforderlichen Qualitätssicherungsverfahren sowie notwenige Verfahren zur Installation und Wartung.
- Bewerten und Freigeben der Entwicklungsplanung.

Es wird durchgehend unterstellt, dass üblicherweise nicht alle Informationen zu Beginn der Entwicklung vorliegen, oder zumindest nicht vollständig vorliegen. Daher wird darauf hingewiesen, dass auch die Änderungen in dem Entwicklungsplan dokumentiert werden müssen.

Das wesentliche Ergebnis dieser Disziplin ist die dokumentierte Entwicklungsplanung. Je nach Strukturierung dieses Dokumentes können weitere Dokumente anfallen, sofern die Inhalte nicht im Entwicklungsplan selbst enthalten sind, sondern dort nur referenziert werden. Teile, die häufig als eigenständige Dokumente gepflegt werden, sind:

- Die Verifikationsaufgaben werden in einem separaten Verifikationsplan definiert.
- Die Validierungsaufgaben werden in einem separaten Validierungsplan definiert.

[385] Es wird bei dieser Anforderung davon ausgegangen, dass die Software Teil eines umfassenderen Systems ist. In diesem Fall sind diese umfassenderen Anforderungen im Entwicklungsplan zu referenzieren. Handelt es sich um eine reine Softwarelösung, gibt es solche Anforderungen nicht.

- Die zeitliche Organisation der Entwicklung wird in einem Projekt- und Meilensteinplan definiert.
- Die Anforderungen an das Risikomanagement werden in einem Risikomanagementplan definiert.

Die beiden untenstehenden Aktivitätsdiagramme geben einen Überblick über die Aktivitäten bei der Entwicklungsplanung.

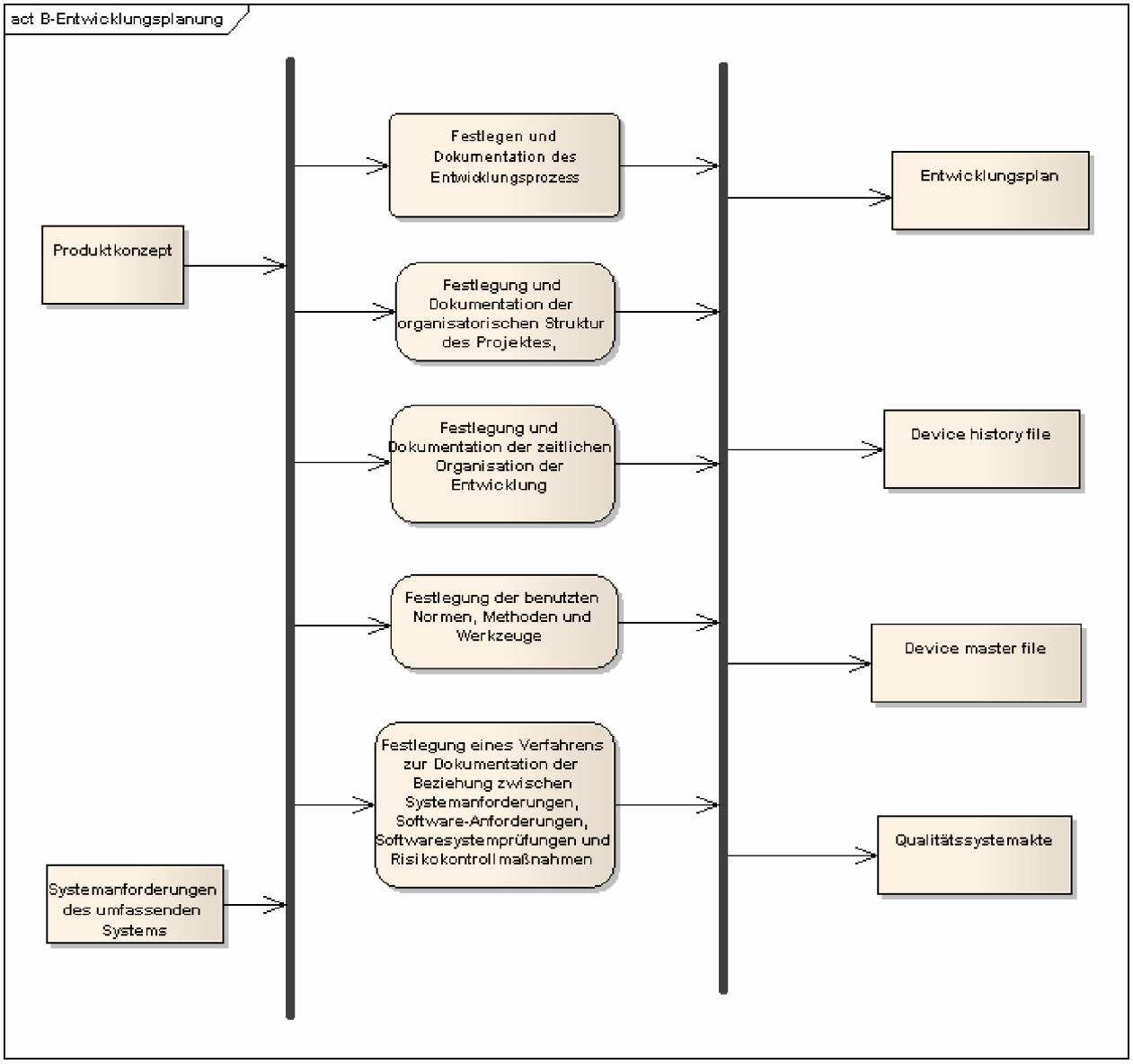

Abbildung 3 : Entwicklungsplanung

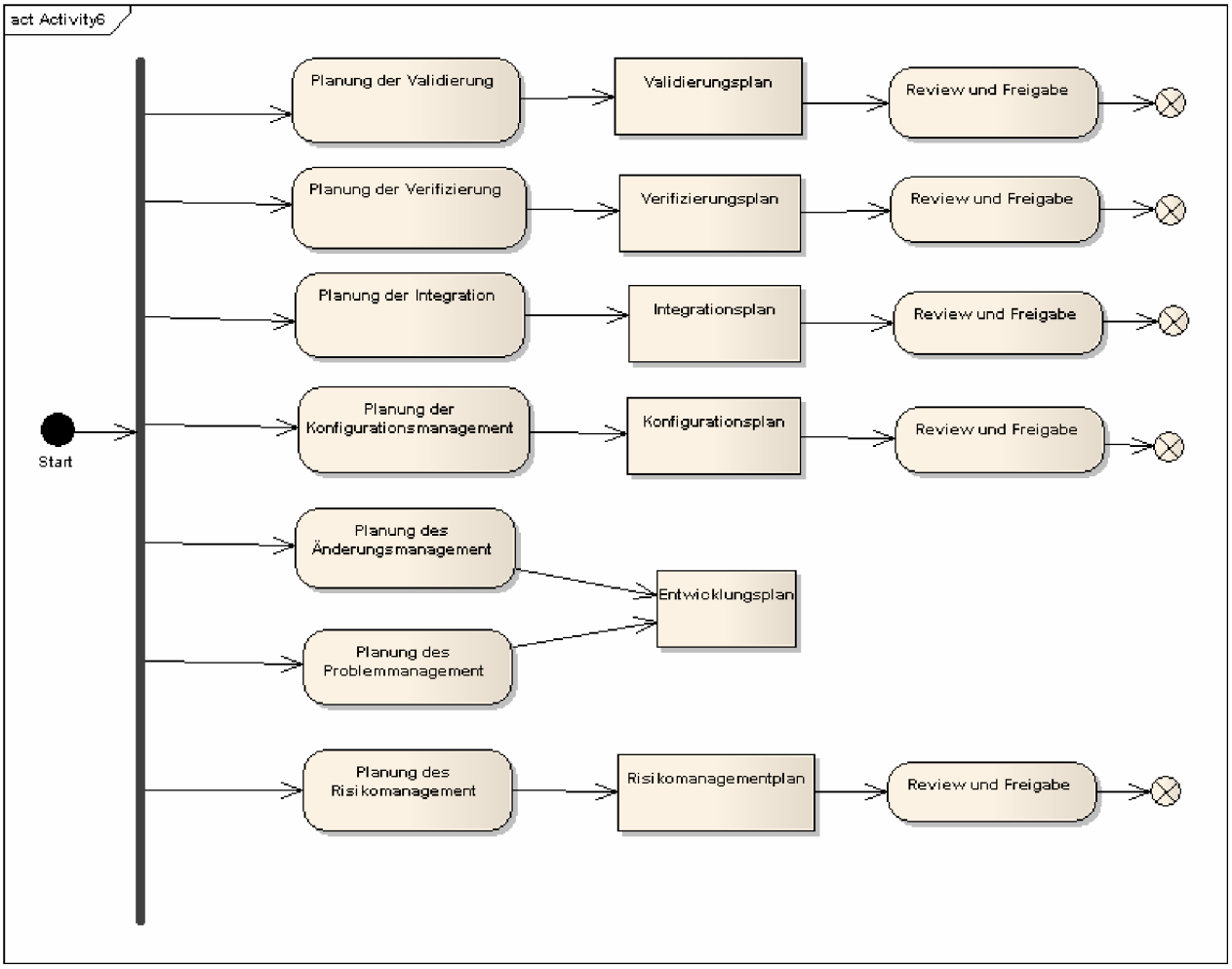

Abbildung 4: Entwicklungsplanung - Prozesse

5.4 Anforderungsanalyse

Im Anforderungsmanagement unterscheidet man generell zwischen Anwenderanforderungen[386] und Systemanforderungen[387]. Anwenderanforderungen beschreiben, was ein System aus Kundensicht leisten soll, wohingegen Systemanforderungen beschreiben, wie diese Anforderungen durch das System geleistet werden.

In den verschiedenen regulatorischen Vorgaben sind die Begriffe jedoch nicht so klar, wie sie sein könnten. [ISO prEN 62304] macht hierzu einige Angaben[388]. Es wird ausgeführt, dass die verschiedenen Begriffe ein Bereich häufiger Verwirrung sind. [ISO prEN 62304] erläutert diese Begriffe wie folgt:

---

[386] Anwenderanforderungen werden häufig in einem Lastenheft dokumentiert.

[387] Systemanforderungen werden hingegen in einen Spezifikationsdokument oder eine Pflichtenheft dokumentiert.

[388] [ISO prEN 62304], Anhang B (informativ), Kapitel B.5.2, S. 40.

- Design-Inputs sind die Übersetzung von Anwender-Bedürfnissen in formal dokumentierte Medizingeräte-Anforderungen.
- Software-Anforderungen sind die formal dokumentierten Spezifikationen dessen, was die Software tut, um die Anwender-Bedürfnisse und die Design-Inputs zu erfüllen.
- funktionale Software-Spezifikationen sind oft Teil der Software-Anforderungen und detaillieren die Funktionen weiter.
- Software-Design-Spezifikationen definieren, wie die Software designt und zerlegt wird und Anforderungen und funktionale Spezifikationen implementiert werden.

Diesen Erläuterungen kann man entnehmen, dass Anwender-Bedürfnisse und Design-Inputs ebenfalls durch die Normen adressiert werden. [21CFR820][389] ergänzt, dass Verfahren vorgesehen werden sollen, um sicherzustellen, dass die ermittelten Anforderungen und den beabsichtigten Gebrauch angemessen berücksichtigen, einschließlich der Benutzer- und Patientenanforderungen. Die folgende Liste listet alle Dokumente mit den Kapiteln auf, die wesentliche Vorgaben zur Anforderungsanalyse enthalten.

- [ISO 13485]
    - Kapitel 7.1 (a) Planung der Produktrealisierung – Produktanforderungen.
    - Kapitel 7.2.1 Ermittlung der Anforderungen an das Produkt.
    - Kapitel 7.3.2 Design- und Entwicklungsvorgaben.
    - Kapitel 8.2.4.1 Erfassung und Messung des Produktes - Allgemeine Anforderungen.
- [ISO 60601-1-4]
    - Kapitel 52.206. Anforderungsspezifikation.
    - Kapitel 52.206.1. Für das System und jedes seiner Subsysteme muss eine Anforderungsspezifikation erstellt werden.
    - Kapitel 52.206.2. Die Anforderungsspezifikation muss die risikobezogenen Funktionen detailliert aufführen.
    - Kapitel 52.206.3. Die Anforderungsspezifikation muss Informationen zu den Risikobeherrschungsmaßnahmen enthalten.
- [ISO prEN 62304]
    - Kapitel 4.3. Softwaresicherheitsklassifizierung für jedes System.

[389] [21CFR820], Section 30 (c) Design Input

- Kapitel 5.1.3 (a). Referenz auf Systemanforderungen im Entwicklungsplan.
- Kapitel 5.2. Analyse der Systemanforderungen.
- Kapitel 5.2.1. Definition der Anforderungen an die Software, abgeleitet aus Systemanforderungen.
- Kapitel 5.2.2. Festlegen von Anforderungen an die Software und an jedes Softwaresystem.
- Kapitel 5.2.3. Inhalt der Anforderungen an die Software.
- Kapitel 5.2.4. Einschluss von Risikokontrollmaßnahmen in die Anforderungen an die Software.
- Kapitel 5.2.6. Aktualisierung der Systemanforderungen bei geänderten oder ergänzten Anforderungen.
- Kapitel 5.2.7. Verifizierung der Anforderungen an die Software.

- [ISO 60601-1-6]
  - Kapitel 46.202.1. Ergonomieprozess – Allgemeines.
  - Kapitel 46.202.2. Informationen für den Ergonomieprozess.
  - Kapitel 46.202.2.1. Spezifikation der Anwendung des Gerätes.
  - Kapitel 46.202.2.2. Festlegen der Hauptbedienfunktionen.
  - Kapitel 46.202.2.3. Spezifikation der Gebrauchstauglichkeit.
- [ISO 14971]
  - Kapitel 4.2. Festlegung des bestimmungsgemäßen Gebrauchs.
- [21CFR820]
  - Kapitel 820.30 (c). Entwicklungsvorgaben.
- [FDA-Premarket]
  - Software Description, S. 10f
  - Software Requirement Specification (SRS), S 11f
- [FDA- DesignGuide]]
  - Section B: Entwicklungsvorgaben (Design Input)
- [FDA-Validation]
  - Kapitel 4.1. Requirements.
  - Kapitel 5.2.2. Requirements.

- [FDA-UseSafety]
    - Kapitel 1.1. Use-Related Hazards.
    - Kapitel 1.2. Use-Scenarios Resulting in Hazards.
    - Kapitel 3.0. Human Factors.
    - Kapitel 3.1. Human Factors Overall Considerations.
    - Kapitel 3.2. Human Factors considerations for the device-user system.
    - Kapitel 3.2.1. Medical Device Use Environment.
    - Kapitel 3.2.2. Medical Device Users.
    - Kapitel 3.2.3. Medical Device User Interfaces.
    - Kapitel 4.0. Advantages and Level of Effort.
    - Kapitel 5.1. Device Use Description.
    - Kapitel 5.2. User Interface Design Information in Standards and Guidelines.
    - Kapitel 5.4. Analytic Human Factors Engineering Approaches.
    - Kapitel 5.5. Empirical Human Factors Engineering Approaches (Use Studies).
    - Kapitel 5.6. Prioritize and Assess Use-related Risk.
    - Kapitel 5.8. Verify and Validate User Interface Design.
    - Kapitel 6.0. Document Risk Management activities for device use.
    - Kapitel 6.1. Device overall.
    - Kapitel 6.2. Device user interface.
    - Kapitel 6.3. Device use.
    - Kapitel 6.4. Device user population.
    - Kapitel 6.5. Device user Environments.
    - Kapitel 6.6. Use-Related risk.
    - Kapitel 6.7. Verification and Validation.

Aus den verschiedenen regulatorischen Vorgaben ergeben sich die folgenden Forderungen an die Anforderungsanalyse:

- Die erforderlichen Anforderungen, wie
    - Kundenanforderungen,
    - Anforderungen an die Gebrauchstauglichkeit,

- regulatorische Anforderungen und
- sonstige Anforderungen

- müssen systematisch ermittelt, dokumentiert und bewertet werden. Die so ermittelten Anforderungen sind auf Vollständigkeit, Eindeutigkeit und Widerspruchsfreiheit zu prüfen. Zudem sollen die Anforderungen in Worten ausgedrückt werden, die Mehrdeutigkeit vermeiden und es ermöglichen, dass Prüfungskriterien festgelegt werden und Prüfungen durchgeführt werden, um festzustellen, ob die Prüfungskriterien eingehalten werden.
- Falls das Softwaresystem lediglich Teil eines Medizingerätes ist, müssen die Anforderungen an das Softwaresystem definiert werden, die von den Anforderungen an das Gesamtsystem abgeleitet sind.
- Die Software-Anforderungen sollen Anforderungen an die Funktionalität und Leistungsfähigkeit, Anforderungen an die Schnittstellen, Ein- und Ausgaben, Datendefinitionen, Anforderungen an die Datensicherung, die Wartung durch den Betreiber, an die Installation und an die Gebrauchstauglichkeit enthalten.
- Bei der Festlegung von Softwareanforderungen muss die Risikoanalyse des Medizingerätes überprüfen, wenn Softwareanforderungen festgelegt werden und muss sie ggf. aktualisieren. Dabei sind die risikobehafteten Funktionen festzulegen, sowie Informationen zu ermitteln, die sicherstellen, dass vorgesehene Risiko-Beherrschungsmaßnahmen die identifizierten Risiken ausreichend verringern.
- Für die Gebrauchstauglichkeit ist die Kenntnis über die verschiedenen Benutzergruppen des Gerätes, die übliche Geräteverwendung, aber auch mögliche, aber ungewöhnliche Arten der Geräteverwendung, die funktionalen Eigenschaften des Gerätes, die Eigenschaften der Umgebung, unter denen das Gerät betrieben wird und die Beziehungen zwischen Benutzer, Umgebung und Gerät zu ermitteln, zu dokumentieren und zu bewerten. Die Gebrauchstauglichkeit ist einer Risikokontrolle zu unterziehen.
- Es muss sichergestellt werden, dass vorhandene Anforderungen ggf. überprüft und aktualisiert werden.
- Der Hersteller muss jedem Software-System eine Software-Sicherheitsklasse bzw. Gefährdungsklasse zuweisen.
- Der Hersteller muss den bestimmungsgemäßen Gebrauch des Medizingerätes festlegen.
- Der Hersteller muss verifizieren und dokumentieren, dass sich Anforderungen nicht gegenseitig widersprechen, in Worten ausgedrückt werden, die Mehrdeutigkeit vermeiden und es ermöglichen, dass Prüfungskriterien festgelegt werden und Prüfungen durchge-

führt werden, um festzustellen, ob die Prüfungskriterien eingehalten werden. Der Hersteller muss die Systemanforderung freigeben.

Die wesentlichen Ergebnisse dieser Disziplin sind:

- die dokumentierte Systemanforderung, einschließlich einer Beschreibung der Schnittstellen. Die Benutzerschnittstelle ist eine dieser Schnittstellen. Schnittstellenbeschreibungen werden häufig als separate Dokumente gepflegt.
- Eine Festlegung des beabsichtigten Gebrauchs, mit vorgesehenen Verwendungsszenarien.
- die aktualisierte Risikomanagementakte bzw. neu erstellte Risikomanagementakte mit einer Bewertung der Risiken und ggf. Risikokontrollmaßnahmen. Dies schließt eine Risikoanalyse der Gebrauchstauglichkeit ein.

Die beiden untenstehenden Aktivitätsdiagramme geben einen Überblick über die Aktivitäten bei der Anforderungsanalyse.

Das untenstehende Aktivitätsdiagramm gibt einen Überblick über die Aktivitäten bei der Anforderungsanalyse.

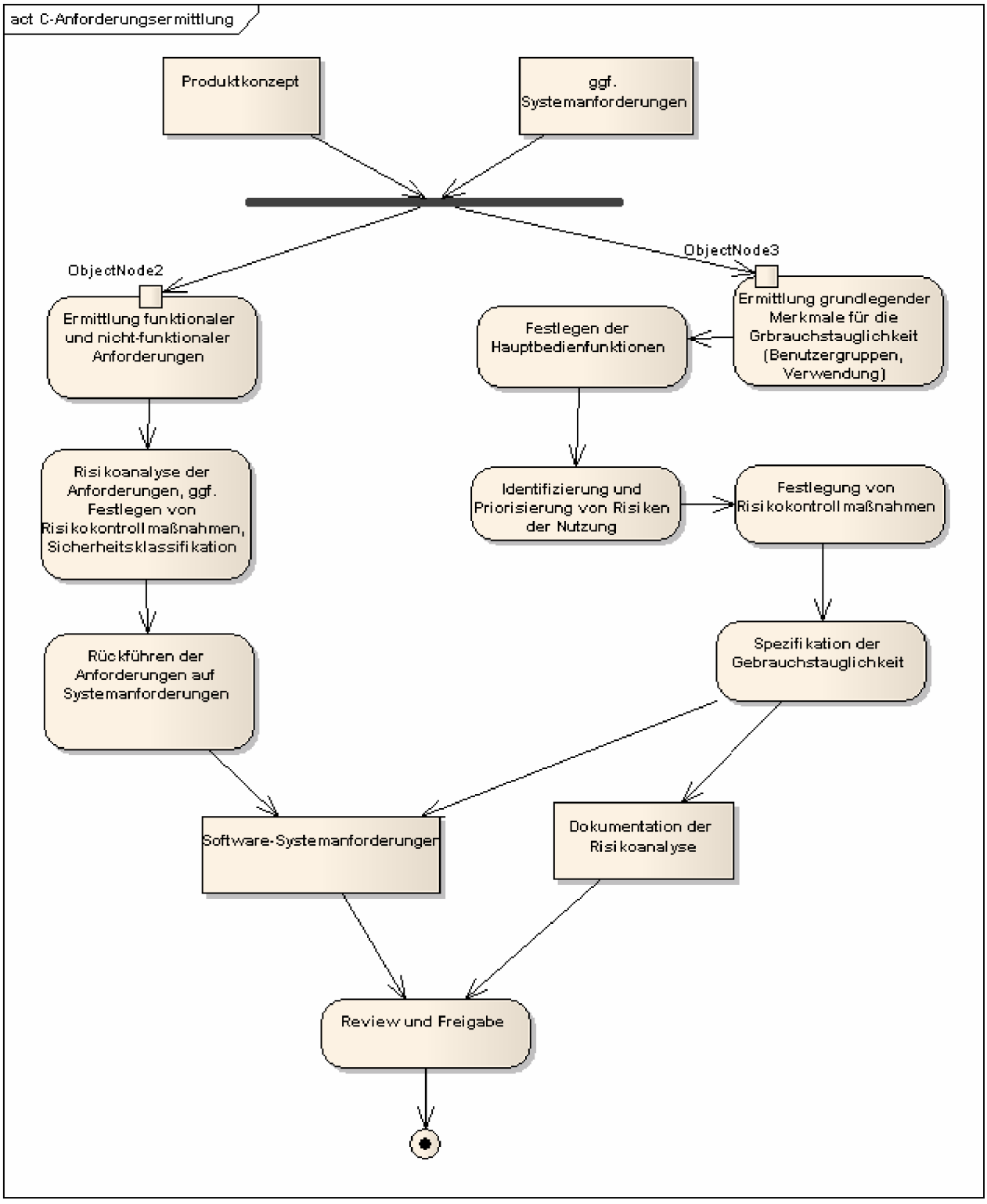

Abbildung 5: Anforderungsanalyse

5.5 Systementwurf

Nachdem Anforderungen an das zu entwickelnde Produkt ermittelt, bewertet und freigegeben wurden, kann nun das System selbst entwickelt werden. Das konkrete Verfahren, durch das das Softwareprodukt spezifiziert wird, wird durch die regulatorischen Anforderungen offen gelassen.

Es können also objektorientierte Verfahren unter Verwendung von Use-Cases, Aktivitätsdiagrammen, Klassendiagrammen und Sequenzdiagrammen eingesetzt werden, oder im Embedded-Bereich sowohl Echtzeit-Erweiterungen der UML wie auch eine Beschreibung durch Statecharts, etwa bei der Verwendung von speicherprogrammierbaren Steuerungen benutzt werden. Das Ergebnis des Systementwurfs wird hier - unabhängig von dem Unfang und der Art der eingesetzten Verfahren - als Designspezifikation bezeichnet. Wie genau die Designspezifikation sein muss, machen die regulatorischen Vorgaben von der Sicherheitsklassifikation des betreffenden Systems abhängig. Die folgende Liste listet alle Dokumente mit den Kapiteln auf, die wesentliche Vorgaben zum Systementwurf enthalten, die aber nicht spezifisch auf Produkte wie Architektur oder detailliertes Design eingehen.

- [ISO 13485]
    - 7.3.3 Design- und Entwicklungsergebnisse
    - 7.3.4 Design- und Entwicklungsbewertung
- [ISO 60601-1-4]
    - 52.208.1 Das System muss in Subsysteme mit einer eigenen Design- und Prüfspezifikation zerlegt werden
- [21CFR820]
    - 820.30 (d)
- [FDA-Premarket]
    - Traceability Analysis, S. 13
- [FDA- DesignGuide]]
    - Section D: Design Output
- [FDA-Validation]
    - 3.5 Design Review
    - 5.2.3 Design
- [FDA-UseSafety]
    - 3.2.3Medical Device User Interfaces

5.5.1 Architekturentwurf

Auch wenn in den regulatorischen Vorgaben keine spezifischen Methoden oder Werkzeuge vorgegeben werden, werden in diesen Dokumenten Prinzipien beschrieben, bei denen Systemdesign angewendet werden sollen. Es wird gefordert, das System hierarchisch in Subsysteme und

Komponenten zu zergliedern, wobei der aus regulatorischen Gründen erforderliche Umfang der Zergliederung von der Gefährdung abhängig ist, die von dem System oder den Komponenten ausgehen kann. Die folgende Liste listet alle Dokumente mit den Kapiteln auf, die wesentliche Vorgaben zur Software-Architektur enthalten.

- [ISO 60601-1-4]:
    - Kapitel 52.207 Architektur.
    - Kapitel 52.207.1 Die Architektur muss den Anforderungen genügen.
    - Kapitel 52.207.2 Für das System und jedes Subsystem muss eine Architektur festgelegt werden.
    - Kapitel 52.207.3 Berücksichtigung der Anforderungen zur Risikobeherrschung.
    - Kapitel 52.207.4 Maßnahmen zur Verringerung der Gefährdungswahrscheinlichkeit (soweit erforderlich).
    - Kapitel 52.207.5 Architektur-Spezifikation muss Risikobeherrschungsmaßnahmen, Ausfälle und Ausfallverhalten berücksichtigen.
    - Kapitel 52.208.1 Zerlegung des Systems in Subsysteme.
- [ISO prEN 62304]
    - Kapitel 5.3 Softwarearchitektur.
    - Kapitel 5.3.1 Umwandlung der Softwareanforderungen in eine Architektur.
    - Kapitel 5.3.2 Dokumentierung der Architektur.
    - Kapitel 5.3.3 Entwicklung einer Architektur für die Schnittstellen zwischen den Softwarekomponenten.
    - Kapitel 5.3.4 Spezifikation der Funktions- und Leistungsanforderungen für SOUP-Komponenten.
    - Kapitel 5.3.5 Spezifikation der Hard- und Software für die SOUP-Komponenten.
    - Kapitel 5.3.6 Festlegung der Architektur, um die Sicherheit zu gewährleisten.
    - Kapitel 5.3.7 Verifizierung der Softwarearchitektur.
- [FDA-Premarket]
    - Architecture Design Chart, S. 13
    - Software Design Specification, S. 13

Eine Beschreibung der Struktur des Systems, in den Vorgaben „Architektur“ genannt, ist in jedem Fall erforderlich[390]. Für die Erstellung der Architektur sind die folgenden Aktivitäten erforderlich:

- Das zu entwickelnde System muss hierarchisch in Subsysteme zerlegt werden. Für jedes Subsystem ist die Gefährdungsklasse festzulegen.
- Die Architektur muss der Anforderungsspezifikation genügen.
- Die Architektur muss festlegen, bei welchen Komponenten es sich um SOUP-Komponenten handelt. Für SOUP-Komponenten ist die erforderliche System-Hardware und Software zu spezifizieren.
- Die Architektur-Spezifikation muss die Anforderungen zur Risiko-Beherrschung berücksichtigen.
- Die Architektur-Spezifikation muss, soweit anwendbar, zur Verringerung der Gefährdungswahrscheinlichkeit Anforderungen für Funktionen hoher Zuverlässigkeit, Redundanz, Divergenz, defensiven Designs sowie zur Begrenzung potentiell gefährlicher Elemente enthalten.
- Die Architektur-Spezifikation muss die Zuordnung von Risiko-Beherrschungsmaßnahmen zu Subsystemen und Komponenten des Systems berücksichtigen.
- Die Softwarearchitektur muss dokumentiert und verifiziert werden.

Das Ergebnis des Architekturentwurfs ist eine Architekturspezifikation, die die oben beschriebenen Informationen in geeigneter Form enthält.

Das untenstehende Aktivitätsdiagramm gibt einen Überblick über die Aktivitäten bei der Anforderungsanalyse.

[390] [60601-1-4], 52.207, [ISO prEn 62304], 5.3, [FDA-Premarket], Architecture Design Chart, S. 13. Nur [60601-1-4] fordert die Architektur in allen Fällen, die beiden Dokumente fordern sie, wenn mindestens eine geringe Gefährdung von dem betreffenden System ausgehen kann.

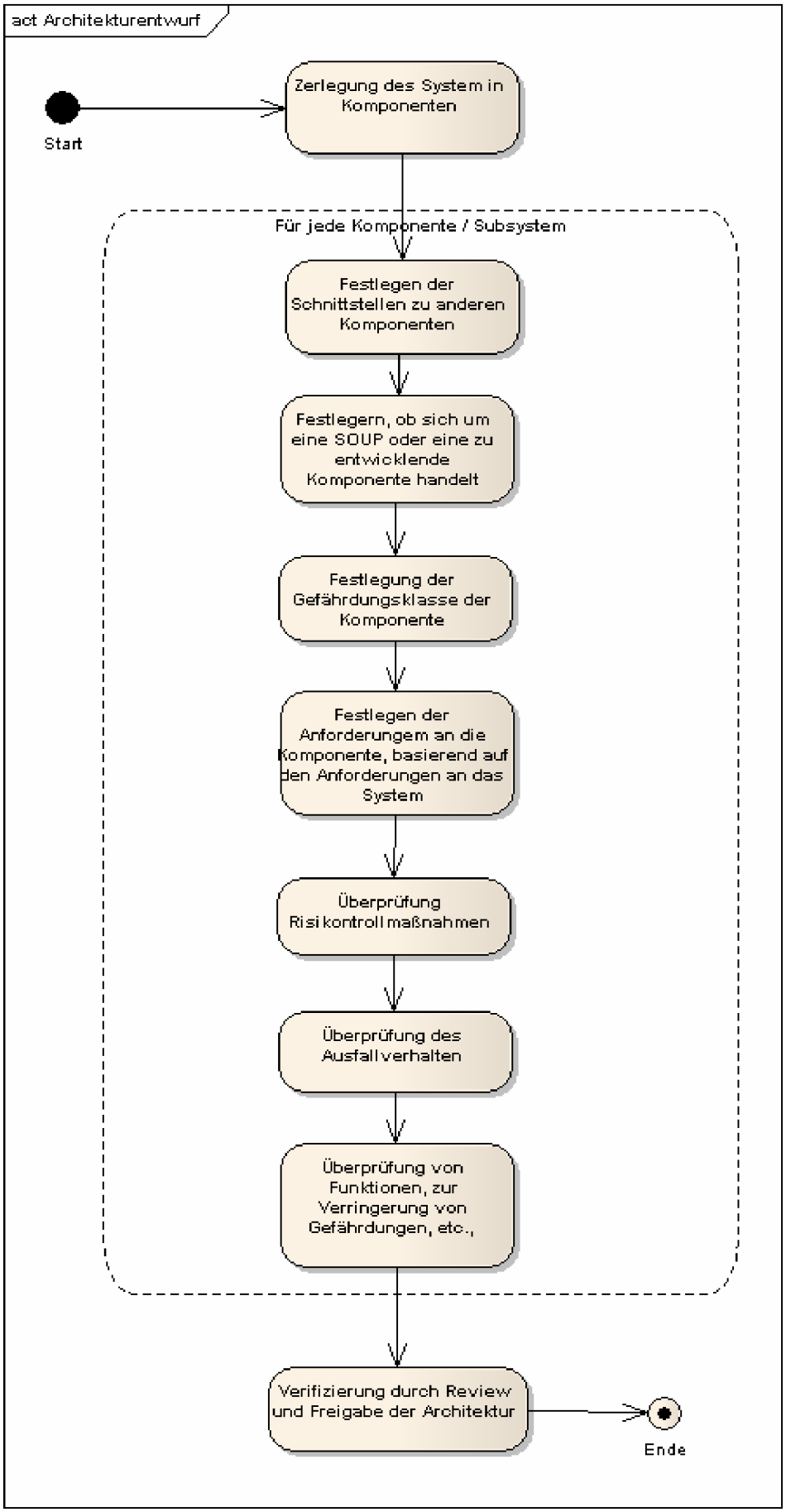

Abbildung 6: Software-Architektur

5.5.2 Detaillierter Entwurf

In Abhängigkeit von der Sicherheitsklasse, die der Komponente bzw. dem System zugeordnet wurde, muss die hierarchische Zerlegung weitergeführt werden. [FDA-Premarket][391] fordert für Komponenten mit der Sicherheitsklasse Moderate und Major eine „Software Design Specification“, die beschreibt, wie die Anforderungen implementiert werden. [ISO prEN 62304] [392] fordert für Komponenten der Sicherheitsklasse B und C[393] ein detailliertes Design.

Die folgende Liste listet alle Dokumente mit den Kapiteln auf, die wesentliche Vorgaben zur Anforderungsanalyse enthalten.

- [ISO prEN 62304]
    - Kapitel 5.4 Detailliertes Design der Software
    - Kapitel 5.4.1 Aufteilung der Softwarekomponenten in Softwareeinheiten
    - Kapitel 5.4.2 Entwicklung eines detaillierten Design für jede Softwareeinheit
    - Kapitel 5.4.3 Entwicklung eines detaillierten Designs für alle Schnittstellen (Hard- und Software)
    - Kapitel 5.4.4 Verifizierung des detaillierten Designs
    - Kapitel 5.4.5 Zusätzliche Verifizierung von Zuverlässigkeitsfaktoren im detaillierten Design
- [FDA-Premarket]:
    - Software Design Specification, S. 13.

Für die Erstellung des detaillierten Designs sind die folgenden Aktivitäten erforderlich:

- Der Hersteller muss die Software-Architektur soweit verfeinern, bis sie durch Software-Einheiten dargestellt wird[394].
- Für jede Software-Einheit der Sicherheitsklasse C muss ein detailliertes Design entwickelt werden[395]. Für alle Schnittstellen zwischen einer Software-Einheit der Sicherheits-

[391] [FDA-Premarket], S. 13.

[392] [ISO prEn 62304], Kapitel 5.4.2.

[393] Die Festlegung der Gefährdungsklasse in [ISO prEN 62304] und die Festlegung des „Levels of Concern“ unterscheidet sich bestenfalls in Details. Für die Betrachtung in dieser Arbeit ist dies jedoch irrelevant und daher werden Minor mit A, Moderate mit B und Major mit C identifiziert.

[394] [ISO prEn 62304], Kapitel 5.4.1.

[395] [ISO prEn 62304], Kapitel 5.4.2.

klasse C und externen (Hardware- oder Software-) Schnittstellen, sowie zu anderen Software-Einheiten muss ein detailliertes Design entwickelt werden[396].

- Für jede Software-Einheit der Sicherheitsklasse C muss verifiziert werden, dass die Architektur korrekt implementiert und frei von Widersprüchen mit der Architektur ist[397].
- Sofern im Design vorhanden, muss der Hersteller bei der Design-Verifizierung Zuverlässigkeitsfaktoren verifizieren, soweit dies angebracht ist. Beispiele für Zuverlässigkeitsfaktoren sind Zuordnung der CPU und Speicherressourcen, Definition von Fehlern und Ausnahmen, Isolierung von Fehlern und Ausnahmen und Wiederaufnahme nach Fehlern.
- Implementierung der beabsichtigten Ereignisse, des Inputs, Outputs, der Schnittstellen, des logischen Flusses, der Zuordnung der CPU und Speicherressourcen, Definition von Fehlern und Ausnahmen, Isolierung von Fehlern und Ausnahmen und Wiederaufnahme nach Fehlern, Initialisierung von Variablen, des Speichermanagements, der kalten und warmen Zurücksetzungen und des Standby und anderer Zustandsänderungen, die einen Einfluss auf die Risikokontrollmaßnahmen haben können.[398]

Das Ergebnis des detaillierten Designs ist eine Designspezifikation, die die oben beschriebenen Informationen in geeigneter Form enthält.

5.6 Implementierung und Modultest

In dieser Disziplin wird jede einzelne Software-Einheit implementiert. Nach der Implementierung muss die erstellte Implementierung hinsichtlich der zuvor festgelegten Akzeptanzkriterien verifiziert werden. Verifizierungsmaßnahmen werden lediglich für Softwareeinheiten der Sicherheitsklasse B und C gefordert. Es ist allerdings nicht verkehrt, Verifizierungsmaßnahmen in jedem Fall durchzuführen. In verschiedenen Dokumenten werden zwar Beispiele für die angemessene Verifizierungsmaßnahmen gemacht, es werden aber keine bestimmten Verifizierungsmaßnahmen zwingend vorgeschrieben. Die folgende Liste listet alle Dokumente mit den Kapiteln auf, die wesentliche Vorgaben zur Implementierung enthalten.

- [ISO prEN 62304]
    - Kapitel 5.5 Softwarekodierung
    - Kapitel 5.5.1 Implementierung jeder Softwareeinheit

[396] [ISO prEn 62304], Kapitel 5.4.3.

[397] [ISO prEn 62304], Kapitel 5.4.4.

[398] [ISO prEn 62304], Kapitel 5.4.5.

- Kapitel 5.5.3 Akzeptanz des Softwarecodes
- Kapitel 5.5.4 Verifizierung des Softwarecodes
- Kapitel 8.2.2 Implementierung von Änderungen

- [FDA-Validation]
  - Kapitel 5.2.4 Construction or Coding

Für den Modultest sind folgende Dokumente zu berücksichtigen:

- ·[ISO prEN 62304]:
  - Kapitel 5.5.2 Festlegung eines Verifizierungsprozesses für Softwareeinheiten
  - Kapitel 5.5.3 (a) Anforderungen und Risikokontrollmaßnahmen sind korrekt implementiert
  - Kapitel 5.5.3 (b) keine Widersprüche mit den Schnittstellen laut detailliertem Design
  - Kapitel 5.5.3 (c) Programmierverfahren und Richtlinien werden eingehalten
  - Kapitel 5.5.4 Verifizierung des Softwarecodes
  - Kapitel 5.5.5 Dokumentierung der Ergebnisse der Softwarecodeverifizierung
- ·[FDA-Validation]:
  - Kapitel 5.2.5 Testing by the Software developer

Nach diesen Vorgaben sind bei Implementierung und Kodierung die folgenden Aktivitäten erforderlich:

- Jede Software-Einheit muss implementiert werden.
- Der Hersteller muss einen Verifizierungsplan für den Software-Code von Software-Einheiten festlegen.
- Es müssen Strategien, Methoden und Verfahren für die Verifizierung der Software-Einheit festgelegt werden. Dies erfolgt am Besten im Rahmen eines Verifizierungsplans. Wenn die Verifizierung durch Test stattfindet, müssen die Testverfahren auf Korrektheit überprüft werden. Dies erfolgt aber üblicherweise im Rahmen der Entwicklungsplanung zu Beginn des Projektes.
- Für die Verifizierung der Softwareeinheiten müssen Akzeptanzkriterien festgelegt werden. Es muss beispielsweise überprüft werden, ob die Anforderungen einschließlich der Risikomaßnahmen korrekt implementiert sind und die Kodierrichtlinien eingehalten werden. Auch die Akzeptanzkriterien werden üblicherweise im Verifizierungsplan definiert oder referenziert.

Das Ergebnis dieser Disziplin ist der verifizierte Software-Code sowie ggf. eine Aufzeichnung der vorgenommenen Verifizierungstätigkeiten.

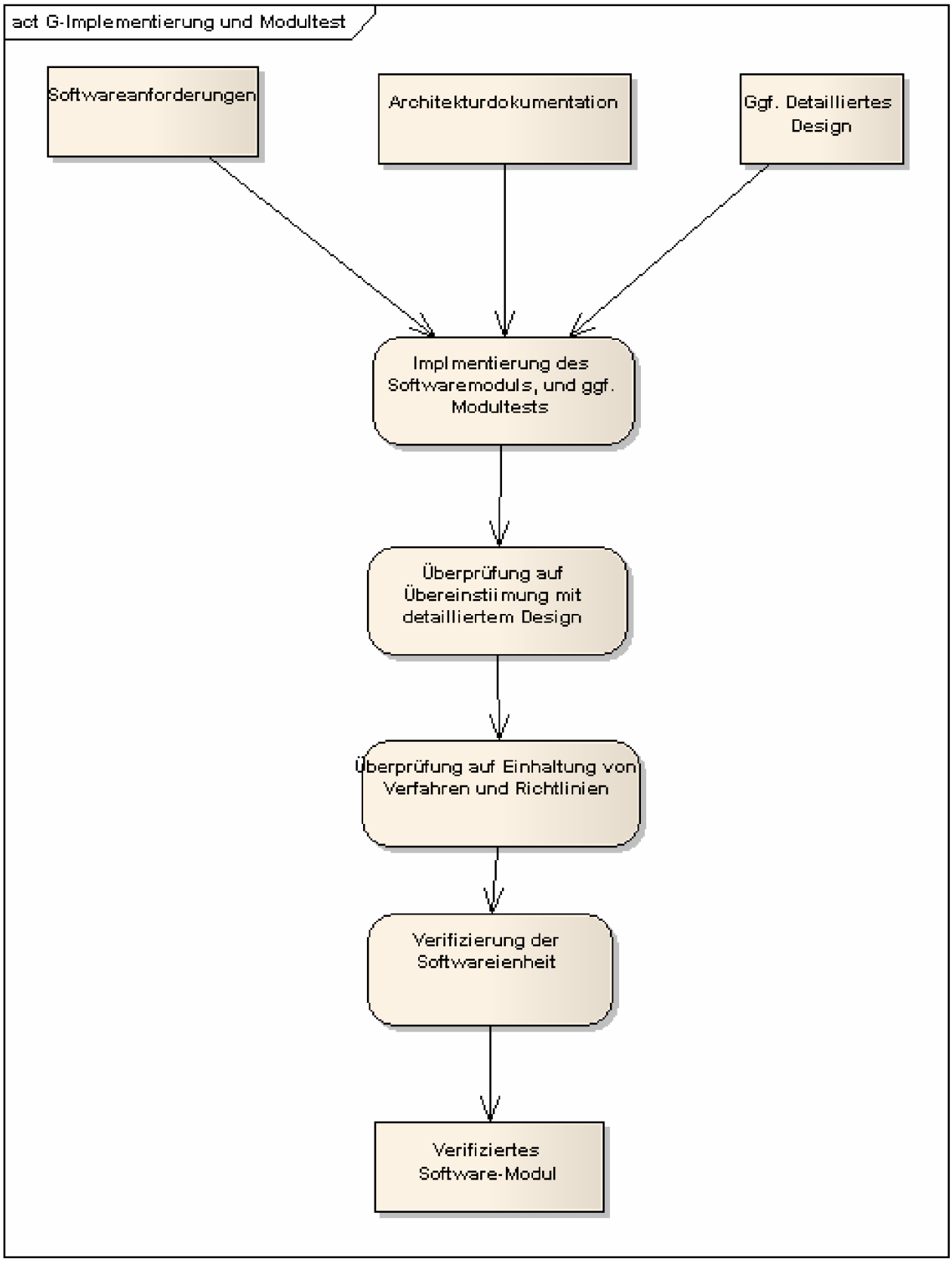

Abbildung 7: Implementierung und Modultest

5.7 Verifizierung

Verifizierung nennt man den Vorgang, durch den der Nachweis erlangt wird, dass das System oder Komponenten vorgegeben Kriterien genügen. Um zu verifizieren, dass das Software-System die vorgegeben Anforderungen erfüllt, muss es unter kontrollierten Bedingungen mit vorgegebenen Eingaben ausgeführt werden. Die dabei beobachteten Ausgaben werden dabei mit erwarteten Ausgaben verglichen und anschließend, einschließlich eventuell auftretender Abweichungen, dokumentiert[399]. In dem Verifizierungsplan wird festgelegt, an welchen Stellen im Entwicklungsprozess solche Verifizierungsaktivitäten vorgesehen sind. Weiter ist im Verifizierungsplan zu notieren, welche Kriterien an die auszuführenden Tests zu stellen sind, üblicherweise basierend auf der Sicherheitsklassifizierung der Komponenten oder des Systems. Üblicherweise werden Modultest, Integrationstest, Systemtest und Abnahmetest unterschieden. Um Dokumente zu verifizieren wird häufig ein Review durchgeführt.

Die folgende Liste listet alle Dokumente mit den Kapiteln auf, die wesentliche Vorgaben zur Verifizierung enthalten, ohne auf bestimmte Produkte detailliert einzugehen.

- [ISO 13485]:
    - Kapitel 7.3.5 Design- und Entwicklungsverifizierung
    - Kapitel 7.6 Lenkung von Erfassungs- und Messmitteln
    - Kapitel 8.1 (a) Messung, Analyse und Verbesserung – Allgemeines
    - Kapitel 8.2.4.1 Erfassung und Messung des Produktes - Allgemeine Anforderungen
- [ISO 60601-1-4]:
    - Kapitel 52.209 Verifizierung
    - Kapitel 52.209.1 Verifizierung der Implementierung der Sicherheitsanforderungen erforderlich
    - Kapitel 52.209.2 Erstellung eines Verifizierungsplans
    - Kapitel 52.209.3 Verifizierung muss nach Verifizierungsplan erfolgen
    - Kapitel 52.212 Bewertung des Systems, ob es nach den Vorgaben der Norm entwickelt wurde

[399] [FDA-Validation], Kapitel 5.2.5, S. 18ff. Allerdings werden – entgegen des Titels dieses Kapitels, große Teile dieser Tests gerade nicht von dem Entwickler ausgeführt, sondern von separaten Testabteilungen. Außerdem gibt es gute Gründe, den Entwickler den eigenen Quellcode nicht testen zu lassen, sondern andere Mitarbeiter dafür heranzuziehen.

- [ISO prEN 62304]:
    - Kapitel 5.1.5 Planung der Softwareintegration und der Integrationsprüfung
    - Kapitel 5.1.6 Planung der Software-Verifizierung
    - Kapitel 5.1.7 Planung der Abdeckung von Anforderungen durch Softwareverifizierung
    - Kapitel 5.1.11 Planung der Konfigurationskontrolle (VOR Verifizierung)
    - Kapitel 5.2.7 Verifizierung von Softwareanforderungen
    - Kapitel 5.3.7 Verifizierung der Softwarearchitektur
    - Kapitel 5.4.4 Verifizierung des detaillierten Designs
    - Kapitel 5.4.5 Zusätzliche Verifizierung des detaillierten Designs
    - Kapitel 5.5.4 Verifizierung des Softwarecodes
    - Kapitel 7.3.1 Verifizierung von Risikokontrollmaßnahmen
    - Kapitel 9.9 Verifizierung der Lösung von Softwareproblemen
    - Kapitel 9.10 Inhalt der Prüfungsdokumentation
- [21CFR820]:
    - Kapitel 820.20 (e) Entwicklungsüberprüfung
    - Kapitel 820.20 (f) Entwicklungsverifizierung
    - Kapitel 820.72 Herstell- und Prozesskontrollen
    - Kapitel 820.90 Nicht-Konforme Produkte
- [FDA-Premarket]:
    - Kapitel Traceability Analysis, S. 13
    - Kapitel Verification Documentation S. 14f
- [FDA- DesignGuide]]
    - Section E: Design Review
    - Sektion F: Design Verification
- [FDA-Validation]
    - Kapitel 4.2 Defect Prevention
- [FDA-UseSafety]
    - Kapitel 5.8 Verification and Validation of User Interface Design

- Kapitel 6.7 Verification and Validation

Es ergeben sich die folgenden Aktivitäten, die üblicherweise zu der Entwicklungsplanung gezählt werden:

- Planung der Verifizierungstätigkeiten. Die Ergebnisse werden im Verifizierungsplan dokumentiert. Darin ist zu planen, zu dokumentieren und zu bewerten:
- wie die Sicherheitsanforderungen über den gesamten Entwicklungsprozess hinweg verifiziert werden,
- die Festlegung und Dokumentation der Verifizierungsstrategien, Aktivitäten und Techniken sowie eingesetzter Werkzeuge,
- die Dokumente und anderen Ergebnisse, wie Software-Code, die eine Verifizierung erfordern.
- die Abdeckungskriterien, für die eine Verifizierung durchgeführt werden soll,
- der Umfang, in dem die Anforderungen für das Softwareprodukt durch Testfälle geprüft werden.
- ein Plan, der spezifiziert, wie die Software-Komponenten (einschließlich SOUP) integriert werden und wie während der Integration Prüfungen durchgeführt werden.

5.7.1 Integrationstest

In dem Integrationstest wird geprüft, ob die, bereits einzeln geprüften Komponenten, spezifikationsgemäß zusammenarbeiten. Die folgende Liste listet alle Dokumente mit den Kapiteln auf, die wesentliche Vorgaben zum Integrationstest enthalten.

- [ISO prEN 62304]:
    - Kapitel 5.6 Software-Integration und Integrationsprüfung
    - Kapitel 5.6.1 Integration der Softwareeinheiten
    - Kapitel 5.6.2 Verifizierung der Softwareintegration
    - Kapitel 5.6.3 Prüfung der integrierten Software
    - Kapitel 5.6.4 Inhalt der Integrationsprüfung
    - Kapitel 5.6.5 Überprüfung der Integrationsprüfung
    - Kapitel 5.6.6 Durchführung von Regressionstests
    - Kapitel 5.6.7 Inhalt von Aufzeichnungen über die Integrationsprüfung

- Kapitel 5.6.8 Verwendung des Problemlösungsprozesses für gefundene Anomalien

Für die Integration von Komponenten in das System sind die folgenden Vorgaben zu berücksichtigen:

- Die Verifizierung muss nach dem zuvor erstellten, bewerteten und freigegebenen Verifizierungsplan durchgeführt werden. Die Ergebnisse der Verifizierungsaktivitäten müssen dokumentiert, analysiert und bewertet werden.
- Für jede Software-Anforderung muss ein Satz von Prüfungen festgelegt und durchgeführt werden; diese Prüfungen werden ausgedrückt durch Input-Stimuli, erwartete Ergebnisse, pass/fail-Kriterien und Verfahren für die Durchführung von Software-Systemprüfungen. Anmerkung: Es ist vertretbar, den Integrationstest und die Software-System-Prüfung in einem einzigen Plan und einem Satz von Aktivitäten zu kombinieren. Es ist weiterhin vertretbar, Software-Anforderungen in früheren Phasen zu prüfen.
- Die gefundenen Anomalien müssen durch den Problemlösungs-Prozess für Software eingegeben werden. Dies bedeutet nicht zwangsläufig, dass der Fehler korrigiert werden muss, lediglich, dass die Art des Problems überprüft und das Problem auf mögliche Sicherheits-Relevanz untersucht wurde, wie in [ISO 14971] spezifiziert.
- Es müssen alle Prüfergebnisse aufgezeichnet werden. Die Aufzeichnungen sollen den Namen des Prüfers, die Spezifikation der Prüffälle, die Prüfumgebung, die erforderlichen Aktionen und die erwarteten und die tatsächlichen Ergebnisse enthalten.
- Wenn im Verlauf der Software-System-Prüfung Änderungen vorgenommen werden, müssen im erforderlichen Umfang Prüfungen wiederholt oder modifizierte oder zusätzliche Prüfungen durchgeführt werden, um zu verifizieren, dass die Änderung für die Korrektur des Problems geeignet ist und um zu zeigen, dass keine unbeabsichtigten Nebeneffekte eingeführt wurden.
- Es muss verifiziert werden, dass alle Softwareanforderungen geprüft oder anderweitig verifiziert wurden, alle durchgeführten Prüfungen sich auf die Software-Anforderungen zurückverfolgen lassen und die angewandten Strategien der Verifizierung angemessen sind und die Prüfergebnisse die erforderlichen pass/fail-Kriterien erfüllen.
- Es muss durch die Software-Integrationprüfung verifiziert werden, dass alle Software-Einheiten einer Software-Komponente korrekt in die Software-Komponente integriert wurden und alle Software-Einheiten, Software-Komponenten und die Unterstützung für manuellen Betrieb des Systems korrekt in das System integriert wurden.
- Durch die System- oder Integrationsprüfung ist zu verifizieren, dass die integrierte Komponente wie spezifiziert funktioniert.

- Wird ein System inkrementell integriert, müssen Regressionstests durchgeführt werden, um zu zeigen, dass vorher integrierte Software weiterhin korrekt funktioniert.

Das untenstehende Aktivitätsdiagramm gibt einen Überblick über die Aktivitäten beim Integrationstest:

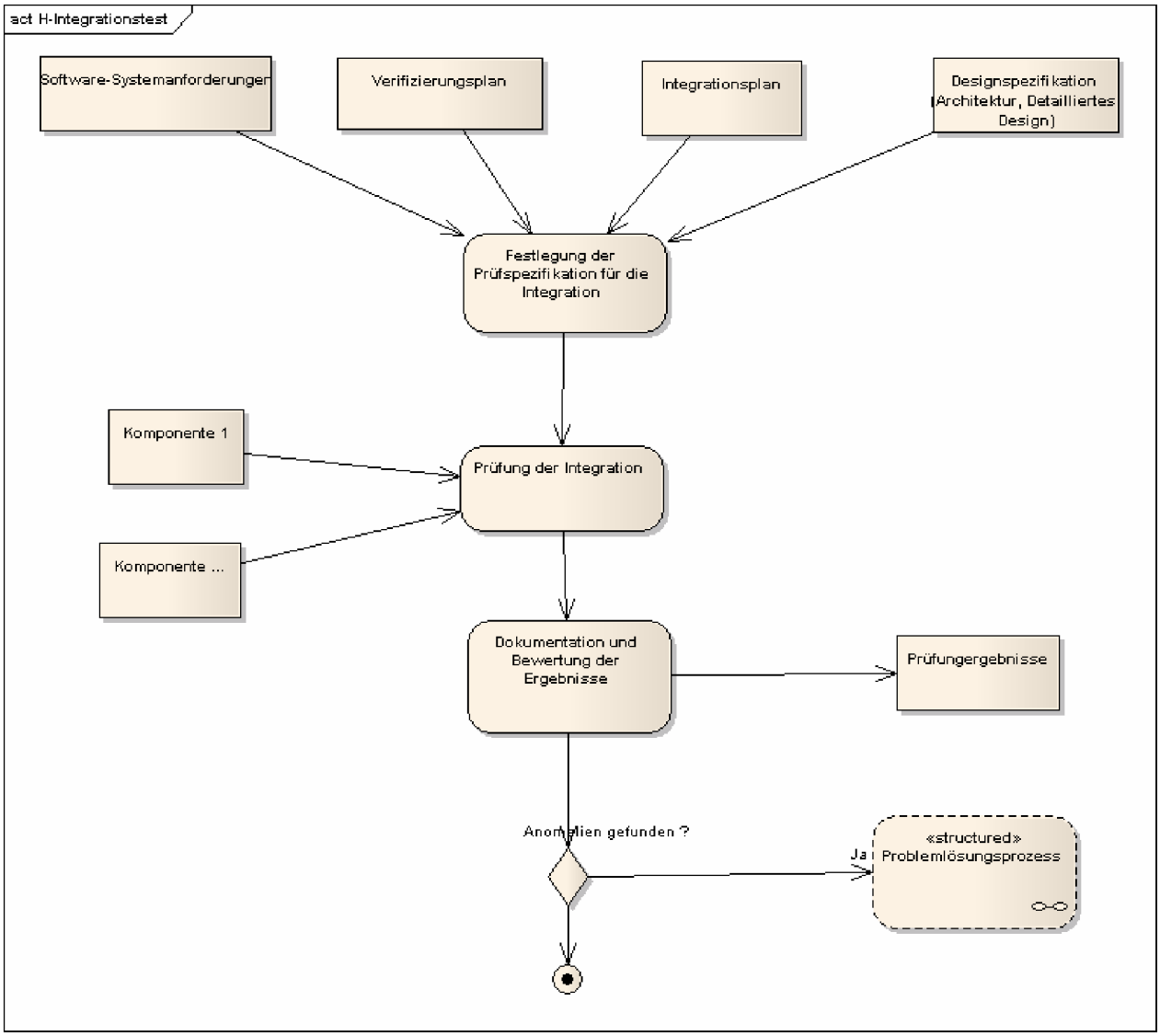

Abbildung 8: Integrationstest

5.7.2 Systemtest

Im Systemtest wird geprüft, ob das System als Ganzes die Anforderungen an das System erfüllt. Daher sind die meisten Verifikationsverfahren anforderungsbasiert. Die folgende Liste listet alle Dokumente mit den Kapiteln auf, die wesentliche Vorgaben zum Systemtest enthalten.

- [ISO 13485]:
    - Kapitel 8.2.4.1 Erfassung und Messung des Produktes - Allgemeine Anforderungen

- [ISO prEN 62304]:
    - Kapitel 5.7 Prüfung des Softwaresystems
    - Kapitel 5.7.1 Festlegen von Prüfungen für jede Software-Anforderung
    - Kapitel 5.7.2 Verwendung des Problemlösungsprozesses für gefundene Anomalien
    - Kapitel 5.7.3 Prüfungswiederholung nach Änderung
    - Kapitel 5.7.4 Verifizierung der Software-System-Prüfungen
    - Kapitel 5.7.5 Aufzeichnung von Daten für jede Prüfung

Die Vorgaben für den Systemtest decken sich weitgehend mit denen des Integrationstests. In vielen Fällen wird der Integrationstest auch zusammen mit dem Systemtest ausgeführt.

5.8 Validierung

Durch die Validierung soll überprüft werden, inwieweit das Medizingerät Benutzeranforderungen erfüllt, für den beabsichtigten Gebrauch geeignet ist und inwieweit die verbleibenden Restrisiken den vorgegebenen Abnahmekriterien genügen[400]. [21CFR820] definiert Validierung als „Bestätigung durch Untersuchung und Bereitstellung von objektivem Nachweis, dass die besonderen Anforderungen für einen bestimmten beabsichtigten Gebrauch gleich bleibend erfüllt werden“[401].

Die folgende Liste listet alle Dokumente mit den Kapiteln auf, die wesentliche Vorgaben zur Validierung enthalten.

- [ISO 13485]:
    - Kapitel 7.3.6 Design- und Entwicklungsvalidierung
- [ISO 60601-1-4]:
    - Kapitel 52.210 Validierung
    - Kapitel 52.210.1 Validierung der Sicherheit nach Zweckbestimmung
    - Kapitel 52.210.2 Erstellung eines Validierungsplans
    - Kapitel 52.210.3 Validierung muss nach dem Validierungsplan durchgeführt werden.

[400] [ISO 13485], Kapitel 7.3.6.

[401] [21CFR820] 3(z), Validation means confirmation by examination and provision of objective evidence that the particular requirements for a specific intended use can be consistently fulfilled.

- Kapitel 52.210.4 Leitung der Validierungsgruppe unabhängig von der Entwicklungsgruppe
- Kapitel 52.210.5 Beschreibung der Abhängigkeiten zwischen Validierung und Entwicklung
- Kapitel 52.210.6 Validierung des eigenen Designs unzulässig

- [ISO prEN 62304]:
  - Kapitel 5.1.3 (b) Referenz des Validierungsplans im Entwicklungsplan
- [ISO 60601-1-6]
  - Kapitel 46.202.5 Validierungsplan für die Gebrauchstauglichkeit
- [21CFR820]:
  - Kapitel 820.20 (g) Entwicklungsvalidierung
- [FDA-Premarket]:
  - Validation Documentation S. 14f
- [FDA- DesignGuide]:
  - Section G: Design Validation
- [FDA-Validation]:
  - Kapitel 4.3 Time and Effort
  - Kapitel 4.4 Software Life Cycle
  - Kapitel 4.5 Plans
  - Kapitel 4.5 Procedures
  - Kapitel 4.7 Software Validation after Change
  - Kapitel 4.8 Validation Coverage
  - Kapitel 4.9 Independence of Review
  - Kapitel 4.10 Flexibility and Responsibility
- [FDA-UseSafety]:
  - Kapitel 5.8 Verification and Validation of User Interface Design
  - Kapitel 6.7 Verification and Validation

Für die Validierung sind die folgenden Vorgaben zu berücksichtigen:

- Die für die Validierung einzuhaltenden Regelungen müssen festgelegt werden. Dies erfolgt meistens in einem Validierungsplan.
- In den Validierungsplan müssen Verfahren eingeschlossen werden, um sicherzustellen, dass die richtigen Sicherheitsanforderungen aufgestellt wurden.
- In den Validierungsplan müssen Verfahren zur Validierung der Benutzerschnittstelle eingeschlossen werden.
- Das zur Durchführung der Validierung eingesetzte Personal muss geplant werden. Niemand darf sein eigenes Design validieren.
- Die Validierung muss gemäß den im Validierungsplan festgelegten Regelungen durchgeführt werden. Die Ergebnisse der Verifizierungsaktivitäten müssen dokumentiert, analysiert und bewertet werden.
- Wurden Änderungen am System durchgeführt, so muss sichergestellt werden, dass das System oder die geänderten Teile erneut validiert werden.

Das untenstehende Aktivitätsdiagramm gibt einen Überblick über die Aktivitäten bei der Validierung:

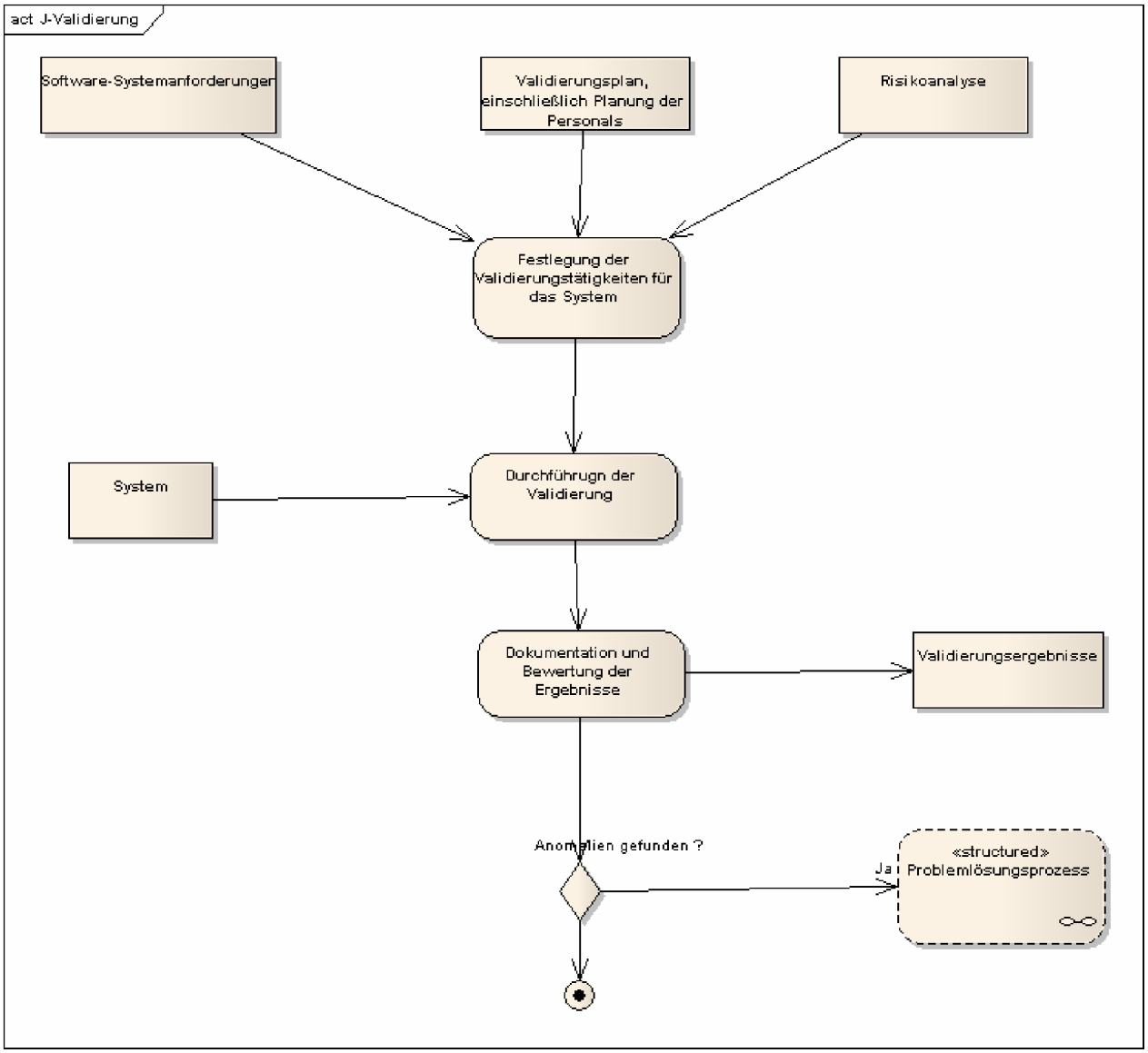

Abbildung 9: Validierung

5.9 Freigabe

Bevor die Software eingesetzt werden kann, muss sie freigegeben werden. Die folgende Liste listet alle Dokumente mit den Kapiteln auf, die wesentliche Vorgaben zur Freigabe enthalten.

- [ISO prEN 62304]:
    - Kapitel 5.8 Software-Freigabe
    - Kapitel 5.8.1 Sicherstellen, dass die Verifizierung der Software vollständig ist
    - Kapitel 5.8.2 Dokumentation bekannter, nicht gelöster Anomalien
    - Kapitel 5.8.3 Bewertung bekannter, nicht gelöster Anomalien
    - Kapitel 5.8.4 Dokumentation freigegebener Versionen

- Kapitel 5.8.5 Dokumentation, wie die freigegebene Software erstellt wurde
- Kapitel 5.8.6 Sicherstellen, dass die Dokumentation vollständig ist
- Kapitel 5.8.8 Wiederholbarkeit der Software-Freigabe sicherstellen

- [FDA-Premarket]:
  - Unresolved Anomalies. S. 15

Nach diesen Vorgaben, sind für die Freigabe die folgenden Aktivitäten erforderlich:

- die Verifizierung ist abgeschlossen und die Ergebnisse der Verifizierung wurden vollständig bewertet,
- eventuelle Abweichungen wurden bewertet,
- die Dokumentation ist vollständig,
- die Software und die zugehörige Dokumentation wurden unter Konfigurationskontrolle gestellt,
- die Software, der zugehörige Quellcode und die Dokumentation wurden archiviert,
- es ist sichergestellt, dass die Software bei Bedarf erneut erstellt werden kann.

Der Hersteller muss geänderte Software-Systeme erneut freigeben. Änderungen können als Teil einer vollständigen erneuten Freigabe eines Software-Systems freigegeben werden, oder als Änderungs-Bausatz, der die geänderten Software-Komponenten und die Werkzeuge enthält, die erforderlich sind, um die Änderungen als Änderungen in ein bestehendes Software-System zu installieren[402].

Das untenstehende Aktivitätsdiagramm gibt einen Überblick über die Aktivitäten bei der Freigabe:

[402] [ISO prEN 62304], Kapitel 6.3.2.

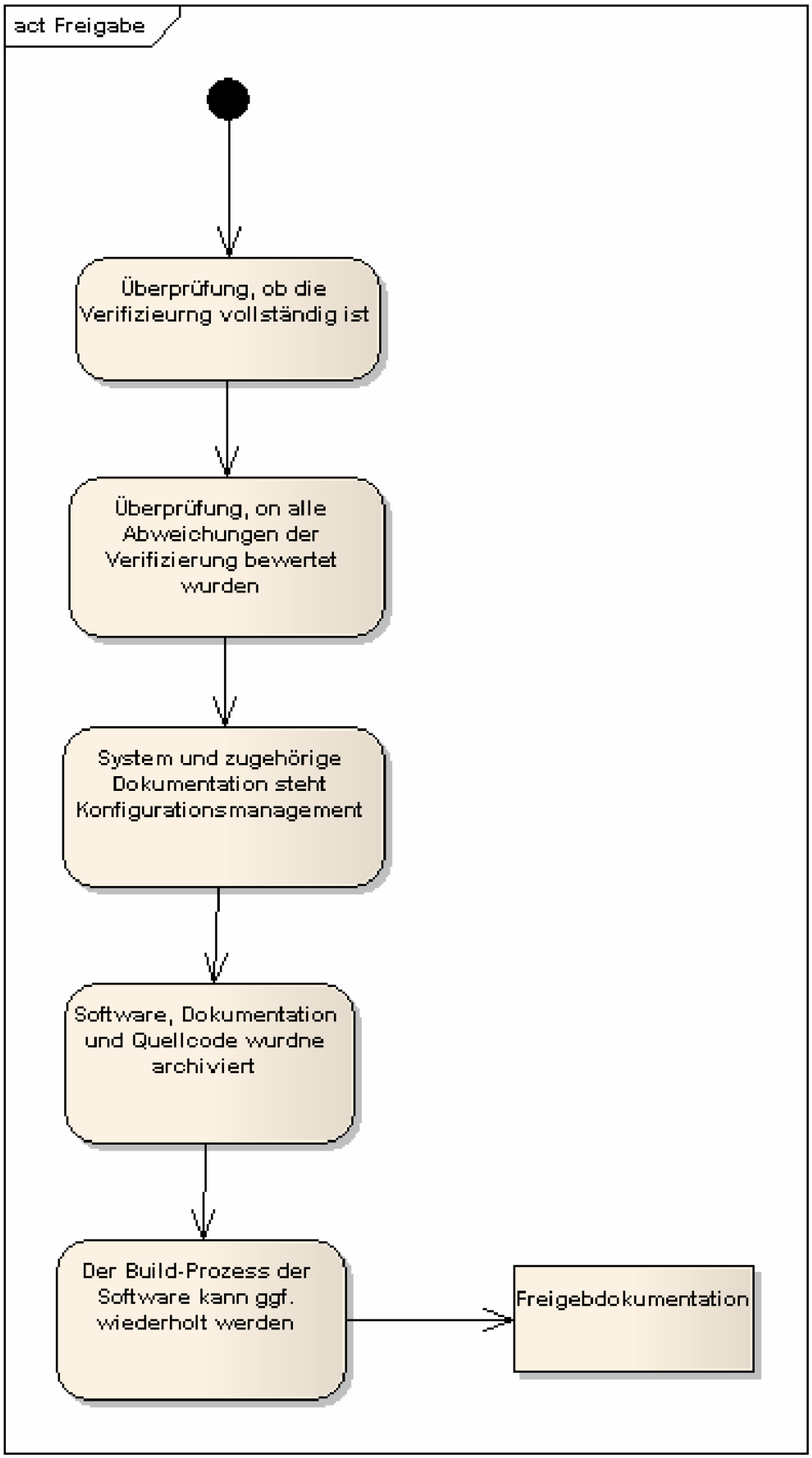

Abbildung 10: Freigabe der Software

5.10 Management von Änderungen

Jede Änderung an einem freigegebenen Software-Produkt muss als eine oder mehrere Änderungsspezifikationen dokumentiert werden. Dabei wird unter einer Änderungsspezifikation die dokumentierte Spezifikation einer Änderung verstanden[403]. Die folgende Liste listet alle Dokumente mit den Kapiteln auf, die wesentliche Vorgaben zum Änderungsmanagement enthalten.

- ISO 13485]:
    - Kapitel 7.2.3 (b) Kommunikation mit dem Kunden: Rückmeldungen und Beschwerden
    - Kapitel 7.3.7 Lenkung von Design- und Entwicklungsänderungen
- [ISO 60601-1-4]:
    - Kapitel 52.211 Änderungen
    - Kapitel 52.211.1 Änderungen des Designs müssen erneut bewertet werden
    - Kapitel 52.211.2 Nach Änderungen müssen alle betroffenen Dokumente überarbeitet werden.
- [ISO prEN 62304]:
    - Kapitel 5.7.3 Prüfungswiederholung der Softwareprüfung nach Änderungen
    - Kapitel 6.2.3 Analyse der Änderungsspezifikation hinsichtlich der Auswirkungen
    - Kapitel 6.2.4 Überprüfung und Genehmigung der Änderungen
    - Kapitel 6.2.5 Dokumentation und Kommunikation von Änderungen (bei freigegebener Software)
    - Kapitel 6.3 Implementierung von Änderungen
    - Kapitel 6.3.1 Verwendung eines Prozesses für die Implementierung von Änderungen
    - Kapitel 6.3.2 Verwendung eines Prozesses für die Implementierung von Änderungen
    - Kapitel 7.4 Risikomanagement von Softwareänderungen
    - Kapitel 7.4.1 Analyse von Änderungen in Hinblick auf Sicherheit
    - Kapitel 7.4.2 Analyse von Änderungen in Hinblick auf bestehende Risikokontrollmaßnahmen

[403] [ISO prEN 62304], Kapitel 6.2.1.4.

- Kapitel 7.4.3 Durchführung von Risikomanagementmaßnahmen
- Kapitel 8.2 Änderungskontrolle
- Kapitel 8.2.1 Genehmigung von Änderungsspezifikationen
- Kapitel 8.2.2 Implementierung von Änderungen, wie in der Änderungsspezifikation gefordert
- Kapitel 8.2.3 Verifizierung von ausgeführten Änderungen
- Kapitel 8.2.4 Bereitstellung von Mitteln für die Rückverfolgung von Änderungen
- Kapitel 9.3 (b) Aktionen, um die Aktionen der Änderungsspezifikation zu dokumentierten
- Kapitel 9.5 Verfolgung und Bericht über den Status der Änderungsspezifikation
- Kapitel 9.6 Lösung des Problems (Überprüfung und Genehmigung der Änderungen)
- Kapitel 9.9 (c) Verifizierung, das Änderungsspezifikationen korrekt implementiert wurden
- Kapitel 9.10 Prüfung der Prüfungsdokumentation nach Änderungen

- [21CFR820]:
  - Kapitel 820.30 (i) Entwicklungsänderungen
- [FDA-Validation]:
  - Kapitel 5.2.7 Maintenance and Software Changes

Wird es während der Entwicklung oder nach Abschluss der Entwicklung notwendig Änderungen oder Ergänzungen vorzunehmen, so sind die folgenden Aktivitäten erforderlich:

- Jede Änderungsanforderung muss zunächst bewertet werden, um festzustellen, in wieweit es die Sicherheit betrifft. Jede Änderungsanforderung, die ein Problem anzeigt, muss als Problembericht aufgezeichnet werden.
- Die Änderung muss spezifiziert werden und die Änderungsspezifikation muss hinsichtlich ihrer Auswirkung auf die Organisation, die freigegebenen Software-Produkte und auf von ihr betroffene Systeme analysiert werden.
- Jede Änderungsspezifikation muss vor der Umsetzung überprüft und freigegeben werden.
- Jede Änderungsanforderungen muss mit den Ergebnissen der Analyse und der Änderungsspezifikation dokumentiert werden.

- Alle relevanten Dokumente im Entwicklungszyklus müssen überarbeitet, ergänzt, bewertet und erneut freigeben werden.
- Führt die Änderung zu einer Änderung der Architektur oder des Designs, so ist die geänderte Designspezifikation so zu behandeln, als ob es sich um ein neues Design handelt.
- Der Hersteller muss geänderte Software-Systeme gemäß Kapitel 5.9 (Software-Freigabe) erneut freigeben.

Das untenstehende Aktivitätsdiagramm gibt einen Überblick über die Aktivitäten bei dem Änderungsmanagement:

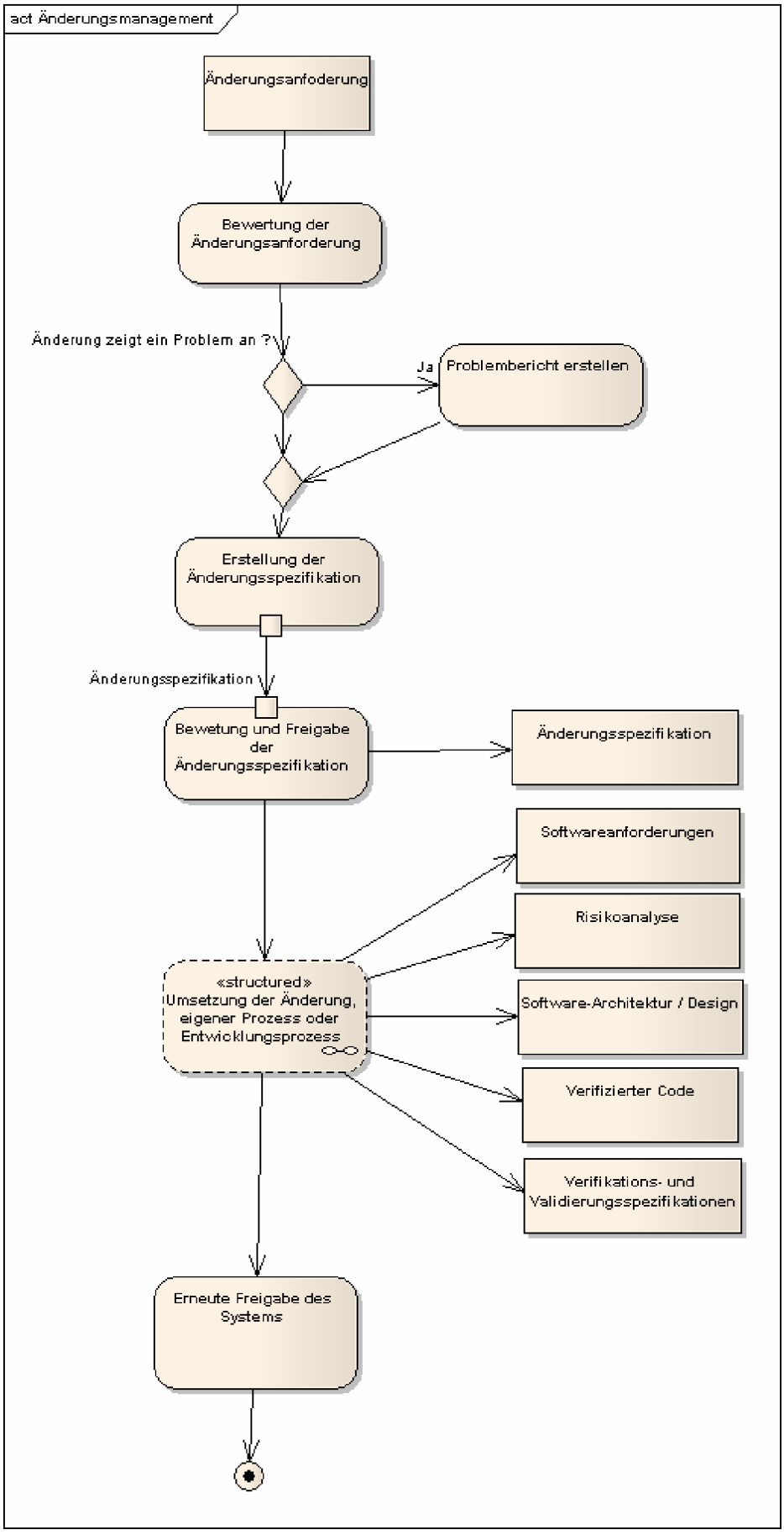

Abbildung 11: Änderungsmanagement

5.11 Problemlösungsverfahren

Der Entwicklungsprozess muss ein Verfahren für die Problemlösung enthalten[404]. Dieses Verfahren muss über alle Phasen und Aktivitäten des Entwicklungsprozesses hinweg verwendet werden, muss innerhalb der Entwicklungsplanung festgelegt und im Entwicklungsplan dokumentiert werden. Weiterhin wird gefordert, dass jedwede Probleme und Nicht-Konformitäten, die während der Entwicklung und während des Betriebes entdeckt werden, in ein dokumentiertes Problemlösungsverfahren für Software einzubringen sind, nachdem diese entdeckt wurden. Wichtig ist dabei, dass die Komponenten eindeutig identifiziert werden können. Dies ist aber erst möglich, nachdem sie unter Konfigurationskontrolle gestellt wurden[405]. Die folgende Liste listet alle Dokumente mit den Kapiteln auf, die wesentliche Vorgaben zum Problemmanagement enthalten.

- [ISO 13485]:
    - Kapitel 7.2.3 (b) Kommunikation mit dem Kunden: Rückmeldungen und Beschwerden
    - Kapitel 8.3 Lenkung fehlerhafter Produkte
- [ISO 60601-1-4]:
    - Kapitel 52.203.6 Integraler Prozess für die Problemlösung erforderlich
- [ISO prEN 62304]:
    - Kapitel 5.1.12 Planung der Problemlösung bei Software
    - Kapitel 5.6.8 Verwendung eines Problemlösungsprozesses für Software
    - Kapitel 5.7.2 Verwendung eines Problemlösungsprozesses für Software
    - Kapitel 6.2 Analyse von Problemen und Änderungen
    - Kapitel 6.2.1 Aufzeichnung und Bewertung von Rückmeldungen
    - Kapitel 6.2.1.1 Suchen von Rückmeldungen
    - Kapitel 6.2.1.2 Aufzeichnung von Rückmeldungen
    - Kapitel 6.2.1.3 Bewertung von Rückmeldungen
    - Kapitel 6.2.1.4 Dokumentation der Rückmeldung

[404] [ISO prEN 62304], Kapitel 5.1.1 und [ISO 60601-1-4], Kapitel 52.203.6.

[405] Daher wird auch gefordert, dass Komponenten und Systeme vor der Durchführung von Verifikationstätigkeiten unter Konfigurationskontrolle gestellt werden.

- Kapitel 6.2.2 Verwendung eines Problemlösungsprozesses für Software für Rückmeldungen
- Kapitel 9 Problemlösungsprozess für Software
- Kapitel 9.1 Erstellen von Problemberichten
- Kapitel 9.2 Unterrichtung betroffener Kreise
- Kapitel 9.3 Untersuchung des Problems
- Kapitel 9.4 Bewertung der Relevanz des Problems hinsichtlich der Sicherheit
- Kapitel 9.5 Verfolgung in Bericht über den Zustand des Problembericht und zug-Änderungen
- Kapitel 9.7 Aufbewahrung von Aufzeichnungen über Problemberichte
- Kapitel 9.8 Analyse von Problemberichten hinsichtlich Trends
- Kapitel 9.9 Verifizierung der Lösung von Softwareproblemen

- [21CFR820]:
  - Kapitel 820.198 Führen einer Beanstandungsakte / Complaint files
- [FDA-Validation]:
  - Kapitel 5.2.7 Maintenance and Software Changes

Für identifizierte Probleme sind die folgenden Aktivitäten erforderlich:

- Sobald das Produkt freigegeben wurde, darf sich der Hersteller nicht darauf verlassen, dass aufgetretene Probleme an ihn weitergeleitet werden. Der Hersteller muss vielmehr aktiv nach Rückmeldungen über aufgetretene Probleme suchen, und zwar sowohl innerhalb seiner eigenen Organisation als auch bei Anwendern.
- Für jedes gemeldete Problem muss ein Problembericht erstellt werden. Problemberichte müssen nach Typ, Umfang und Kritikalität klassifiziert werden. Dies gilt auch für Anomalien, die während Verifikationsmaßnahmen wie Integrationstests gefunden wurden[406]. Problemberichte müssen wirkliche oder mögliche Schadensereignisse und wirkliche oder vermeintliche Abweichungen von Spezifikationen enthalten.
- Soweit es durch lokale Vorschriften gefordert ist, müssen Anwender und Regulatoren über Probleme in freigegebenen Software-Produkten und die Konsequenzen aus deren weiterer Verwendung ohne Änderungen informiert werden.

[406] [ISO prEN 62304], Kapitel 5.6.8.

- Jeder Problembericht muss bewertet werden, um festzustellen, ob ein wirkliches Problem besteht, in wieweit es die Sicherheit betrifft, und ob eine Änderung des Software-Produktes erforderlich ist, um das Problem zu adressieren.
- Jeder Problembericht muss hinsichtlich möglicher oder vorhandener Sicherheitsrisiken untersucht und beurteilt werden. Hierfür ist der Risikomanagementprozess zu verwenden.
- Das Problem muss untersucht werden und, soweit möglich, die Ursachen des Problems identifiziert werden. Danach muss entschieden werden, ob das Problem gelöst werden soll. Für die Ausführung der notwendigen Änderungen ist das definierte Änderungsverfahren (s. Kapitel 0) zu verwenden. Das Problemlösungsverfahren wird auch dann eingehalten, wenn – unter Berücksichtigung möglicher Sicherheitsbeeinträchtigungen – entschieden wird, dass das Problem nicht korrigiert wird.
- Der Hersteller muss den Zustand des Problemberichts, sowie ggf. die zugehörigen Änderungsspezifikationen verfolgen und dokumentieren.

Das untenstehende Aktivitätsdiagramm gibt einen Überblick über die Aktivitäten bei dem Problemlösungsverfahren:

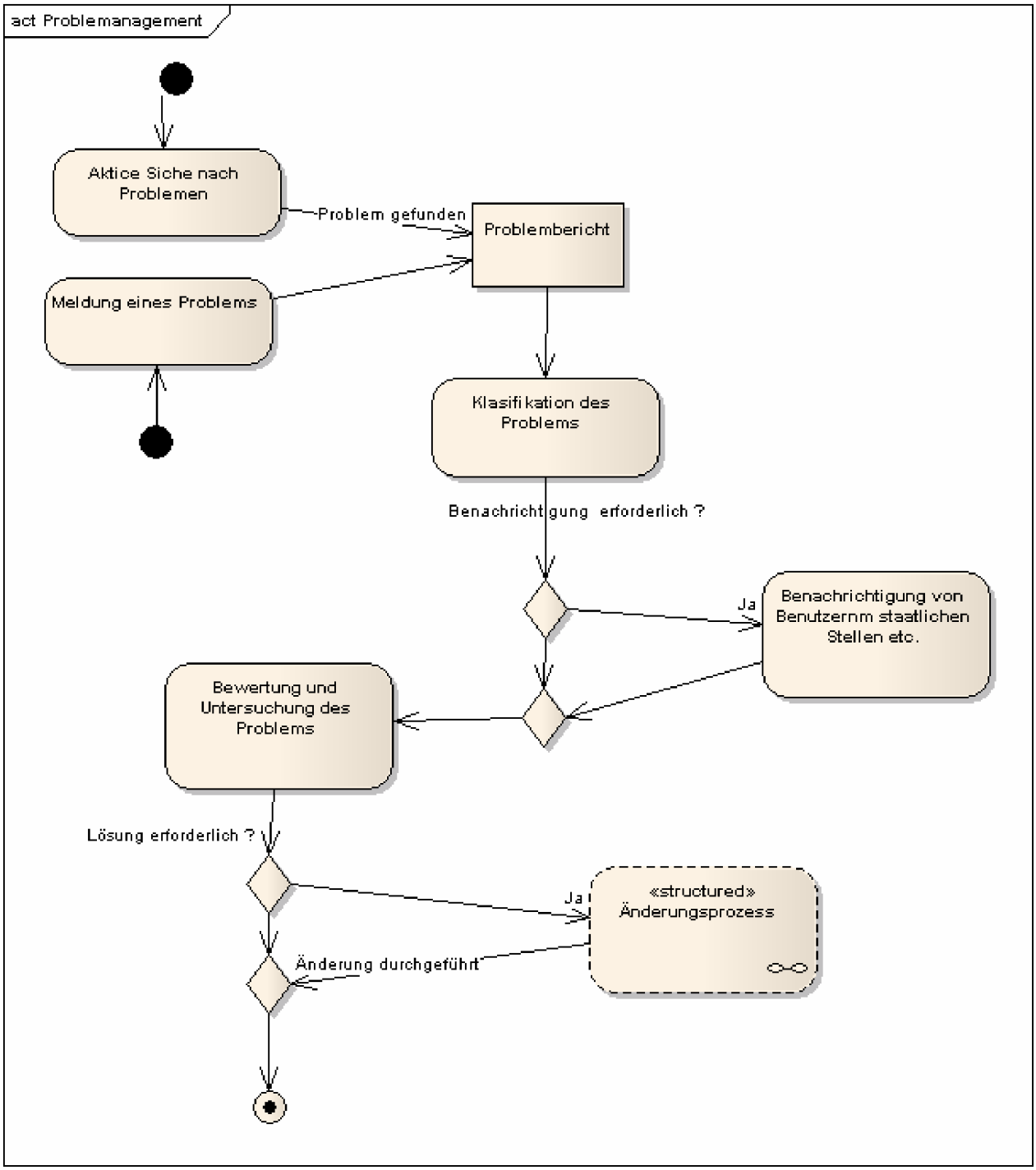

Abbildung 12: Problemlösungsverfahren

5.12 Konfigurationsmanagement

Der Hersteller muss während der Entwicklungsplanung das Konfigurationsmanagement planen und die getroffenen Festlegungen im Softwareentwicklungsplan dokumentieren oder referenzieren. Häufig wird das Konfigurationsmanagement in einem separaten KM-Plan definiert. Die folgende Liste listet alle Dokumente mit den Kapiteln auf, die wesentliche Vorgaben zum Konfigurationsmanagement enthalten.

- [ISO 13485]:
    - Kapitel 7.5.3.1 Identifikation
    - Kapitel 7.5.3.2 Rückverfolgbarkeit
- [ISO prEN 62304]:
    - Kapitel 5.1.10 Planung des Konfigurationsmanagements
    - Kapitel 5.1.11 Planung der Konfigurationskontrolle (vor der Verifizierung)
    - Kapitel 5.8.7 Archivierung der Software
    - Kapitel 8 Software-Konfigurationsmanagement-Prozess
    - Kapitel 8.1 Identifizierung der Konfiguration
    - Kapitel 8.1.1 Festlegung der Mittel zur Identifizierung von Konfigurationselementen
    - Kapitel 8.1.2 Identifizierung von SOUP-Elementen
    - Kapitel 8.1.3 Identifizierung der Dokumentation der Konfiguration
    - Kapitel 8.2.1 Konfigurationselemente dürfen nur als Reaktion auf geänderte Änderungsspezifikation geändert werden
    - Kapitel 8.3 Buchführung über den Status der Konfiguration
- [21CFR820]:
    - Kapitel 820.60 Identifikation
    - Kapitel 820.65 Rückverfolgbarkeit
- [FDA-Premarket]:
    - Revision Level History. S. 15

Danach sind für das Konfigurationsmanagement die folgenden Aktivitäten erforderlich:

- welche Arten von Komponenten unter Konfigurationskontrolle gestellt werden sollen, beispielsweise Bibliotheken mit ausführbaren Codes (Dll), ausführbare Programme, Konfigurationsdateien usw. und Listen von Komponenten, die tatsächlich unter Konfigurationskontrolle gestellt werden. Die Komponenten, die unter Konfigurationskontrolle stehen, werden meistens in einem separaten Konfigurationsidentifikationsdokument (KID) dokumentiert.
- die für das Konfigurationsmanagement erforderlichen Aktivitäten,

- die für die Durchführung des Konfigurationsmanagements verantwortlichen Organisationsteile und deren Beziehung zu anderen Organisationsteilen, wie Softwareentwicklung oder Wartung,
- wann die Komponenten unter Konfigurationskontrolle gestellt werden sollen[407].

5.13 Wartungsprozess

Die Wartung des Softwaresystems erfolgt nach der Freigabe, während das System in Betrieb ist. Damit gehört dieser Prozess nicht mehr eigentlich in den Bereich der Softwareentwicklung des Systems. Dennoch ist es wichtig, dass die für die Wartung erforderlichen Aktivitäten geplant und umgesetzt werden. Die folgende Liste listet alle Dokumente mit den Kapiteln auf, die wesentliche Vorgaben für den Wartungsprozess enthalten.

- [ISO 13485]:
    - Kapitel 7.2.3 (c) Kommunikation mit dem Kunden
    - Kapitel 8.2.1 Erfassung und Messung - Rückmeldungen
- [ISO prEN 62304]:
    - Kapitel 6 Software-Wartungs-Prozess
    - Kapitel 6.1 Festlegung eines Plans für die Softwarewartung
    - Kapitel 6.2.1 Aufzeichnung und Bewertung von Rückmeldungen
    - Kapitel 6.2.1.1 Suchen von Rückmeldungen
    - Kapitel 6.2.1.2 Aufzeichnung von Rückmeldungen
    - Kapitel 6.2.1.3 Bewertung von Rückmeldungen
    - Kapitel 6.2.1.4 Dokumentation der Rückmeldung
    - Kapitel 6.2.2 Verwendung eines Problemlösungsprozesses für Software für Rückmeldungen
- [ISO 14971]:
    - Kapitel 9 Informationen aus den der Produktion nachgelagerten Phasen
- [21CFR820]:
    - Kapitel 820.200 Wartung / Servicing

[407] [ISO prEN 62304], Kapitel 5.1.10 (e). Hinweis: Nach [ISO prEN 62304], Kapitel 5.1.11 müssen die Komponenten spätestens vor der Verifizierung unter Konfigurationskontrolle gestellt werden.

[Danach sind – außer der Planung der Wartungsaktivitäten - die folgenden Aktivitäten für die Wartung gefordert:

- Ein Verfahren für die Verarbeitung von Problemberichten und Änderungsanforderungen. Dieses Verfahren muss Kriterien festlegen, wann ein Problembericht oder eine Änderungsanforderung als Problem aufgefasst werden muss.
- Für die Adressierung von Gefährdungen ist der Risikomanagementprozess zu benutzen.
- Für die Handhabung von Problemen ist das Problemlösungsverfahren zu verwenden (s. Kapitel 5.11).
- Für die Handhabung von Änderungsanforderungen ist das Änderungsverfahren zu benutzen (s. Kapitel 5.10).
- Verwendung des Konfigurationsmanagements für die Verfolgung von Änderungen an einem System (s. Kapitel 5.12).
- Ein Verfahren, durch das festgelegt wird, wie Nachrüstungen, Fehlerkorrekturen und Programmkorrekturen an SOUP-Komponenten durchzuführen sind.

5.14 Risikomanagement

Durch die regulatorischen Vorgaben wird ein Prozess zum Management von Risiken gefordert. Die folgende Liste listet alle Dokumente mit den Kapiteln auf, die wesentliche Vorgaben zur Risikomanagement enthalten.

- [ISO 13485]:
    - Kapitel 7.3.3(d) Festlegung der Merkmale, die für den sicheren und bestimmungsgemäßen Gebrauch wesentlich sind
- [ISO 60601-1-4]:
    - Kapitel 52.202 Risikomanagementplan
    - Kapitel 52.202.1 Risikomanagementplan muss erstellt werden
    - Kapitel 52.203.2 Inhalt des Risikomanagementplans
    - Kapitel 52.202.3 Integraler Prozess für das Risikomanagement erforderlich
    - Kapitel 52.203.5 Risikomanagement muss sich über den gesamten Entwicklungslebenszyklus erstrecken
    - Kapitel 52.204.1 Risikomanagement muss Elemente zur Risikoanalyse und Risikobeherrschung enthalten

- Kapitel 52.204.3.1 Gefährdungsanalyse
- Kapitel 52.204.3.2 Risikoabschätzung
- Kapitel 52.204.4 Risiko-Beherrschung
- Kapitel 52.208.2 Dokumentation der Entwicklungsumgebung in der Risikomanagement-Dokumentation
- Kapitel 52.209.4 Verweis auf Verfahren, Techniken und Ergebnisse der Verifizierung in der RM-Dokumentation
- Kapitel 52.210.7 Verweis auf Verfahren und Ergebnisse der Validierung in der RM-Dokumentation
- Kapitel 52.212 Bewertung, ob das System nach den Vorgaben entwickelt wurde

- [ISO prEN 62304]:
  - Kapitel 4.2 Risikomanagement von Softwareänderungen
  - Kapitel 4.3 Software-Sicherheitsklassifizierung
  - Kapitel 5.1.8 Planung des Risikomanagements
  - Kapitel 5.2.4 Einschluss von Risikokontrollmaßnahmen in die Software-Anforderungen
  - Kapitel 5.2.5 Aktualisierung der Risikoanalyse bei der Festlegung von Software-Anforderungen
  - Kapitel 5.3.6 Festlegung der Aufteilung der Software-Komponenten, die für die Sicherheit erforderlich ist
  - Kapitel 7 Software-Risikomanagement-Prozess
  - Kapitel 7.1 Analyse von Software, die zu gefährlichen Situationen beiträgt
  - Kapitel 7.1.1 Identifikation von Komponenten, die zu einer gefährlichen Situation beitragen kann
  - Kapitel 7.1.2 Identifikation von möglichen Ursachen für den Beitrag zu einer gefährlichen Situation
  - Kapitel 7.1.3 Betrachtung spezieller möglicher Ursachen
  - Kapitel 7.1.4 Überprüfung veröffentlichter Listen mit Anomalien von SOUP
  - Kapitel 7.1.5 Dokumentation von Ursachen
  - Kapitel 7.1.6 Dokumentation von Folgen von Ereignissen
  - Kapitel 7.2 Risikokontroll-Maßnahmen

- Kapitel 7.2.1 Definition von Risikokontrollmaßnahmen
- Kapitel 7.2.2 Risikokontrollmaßnahmen, die in Software implementiert werden
- Kapitel 7.3 Verifizierung von Risikokontrollmaßnahmen
- Kapitel 7.3.2 Dokumentation neuer Folgen von Ereignissen
- Kapitel 7.3.3 Dokumentation der Rückverfolgbarkeit von Software-Gefährdungen
- Kapitel 7.4 Risikomanagement von Softwareänderungen
- Kapitel 7.4.1 Analyse von Änderungen in Hinblick auf Sicherheit
- Kapitel 7.4.2 Analyse von Änderungen in Hinblick auf bestehende Risikokontrollmaßnahmen
- Kapitel 7.4.3 Durchführung von Risikomanagementmaßnahmen
- Kapitel 9.4 Bewertung von Problemberichten hinsichtlich der Relevanz für die Sicherheit

- [ISO 60601-1-6]
  - Kapitel 46.201 Sicherheit für Patienten, Anwender (Benutzer) und andere Personen
- [ISO 14971]
  - Kapitel 3 Allgemeine Anforderungen an das Risikomanagement
  - Kapitel 3.2 Risikomanagement-Prozess
  - Kapitel 3.3 Verantwortlichkeit der Leitung
  - Kapitel 3.5 Risikomanagementplan
  - Kapitel 3.6 Risikomanagementakte
  - Kapitel 4 Risikoanalyse
  - Kapitel 4.1 Verfahren der Risikoanalyse
  - Kapitel 4.3 Feststellung bekannter oder vorhersehbarer Gefährdungen
  - Kapitel 4.4 Einschätzung der Risiken für jede Gefährdung
  - Kapitel 5 Risikobewertung
  - Kapitel 6 Risikokontrolle
  - Kapitel 6.1 Risikominderung
  - Kapitel 6.2 Analyse der Optionen
  - Kapitel 6.3 Umsetzung von Maßnahmen zur Risikokontrolle

- Kapitel 6.4 Bewertung der Restrisikos
- Kapitel 6.5 Risiko/Nutzen-Analyse
- Kapitel 6.6 Weitere verursachte Gefährdungen
- Kapitel 6.7 Vollständigkeit der Risikobewertung
- Kapitel 7 Gesamt-Restrisikobewertung
- Kapitel 8 Risikomanagement-Bericht

- [FDA-Premarket]:
  - Level of Concern. S. 5ff
  - Device Hazard Analysis, S. 11
- [FDA- UseSafety]:
  - Kapitel 1.1 Use-Related Risks
  - Kapitel 1.2 Use Scenarios Resulting in Risks
  - Kapitel 2.0 Risk Management
  - Kapitel 5.3 Apply Analytical and empirical Approaches to Identify and Understand use-Related risk
  - Kapitel 5.6 Prioritize and Assess Use-related Risks
  - Kapitel 5.7 Mitigate and Control Use-related Risks
  - Kapitel 6.0 Document Risk Management Activities for Device Use
- [FDA-OTS]
  - Kapitel 2.2 Hazard Analysis
  - Kapitel 2.3 Hazard Mitigation
  - Kapitel 2.4 Describe / Justify Residual Risk

Aus den verschiedenen Anforderungen kann man entnehmen, dass dieser Prozess dokumentiert werden und die folgenden Elemente beinhalten muss:

- Risikoanalyse
- Risikobewertung
- Risikokontrolle

Damit der Risikomanagementprozess angemessen durchgeführt werden kann, ist es erforderlich, dass die Organisation:

- Ihre Grundsätze zur Festlegung vertretbarer Risiken unter Berücksichtigung einschlägiger Normen und Vorschriften bestimmt,
- die Verfügbarkeit der benötigten Mittel sicherstellt,
- das erforderliche, ausgebildete Personal bereitstellt und
- die Ergebnisse der Risikomanagementaktivitäten in regelmäßigen Abständen überprüft, um die Wirksamkeit des Risikomanagementprozesses sicherzustellen.

Diese Festlegungen und die spezifische Umsetzung der drei Verfahren zur Risikoanalyse, Risikobewertung und Risikokontrolle werden üblicherweise während der Entwicklungsplanung festgelegt und in der Risikomanagementakte dokumentiert. An die drei aufgeführten Verfahren werden die folgenden Anforderungen gestellt:

- Risikoanalyse. Um mögliche Gefährdungen analysieren zu können, ist es zunächst erforderlich, den bestimmungsgemäßen Gebrauch und den vorhersehbaren Missbrauch zu ermitteln und zu dokumentieren. Basierend auf diesen Informationen wird eine Liste aller quantitativen und qualitativen Merkmale erarbeitet, die die Sicherheit des Medizinproduktes beeinflussen. Diese Daten sind in der Risikomanagementakte zu dokumentieren. Weiterhin müssen in der Risikoanalyse alle vernünftigerweise vorhersehbaren Umstände der Gefährdungen für Patienten, Anwender, Servicepersonal, Unbeteiligte sowie Umgebung und Umwelt ermittelt werden. Als Ursachen müssen sowohl menschliche Eigenschaften, Fehler sowie Umgebungsbedingungen als auslösende Ursachen betrachtet werden. Zudem müssen die vernünftigerweise vorhersehbaren Folgen von Ereignissen, die in einer Gefährdung resultieren, betrachtet werden. Die in der Risikoanalyse eingesetzten Verfahren werden in der Norm nicht festgelegt, jedoch müssen diese Verfahren in der Risikomanagementdokumentation enthalten oder referenziert werden.
- Risikobewertung. In dieser Aktivität werden die während der Risikoanalyse ermittelten möglichen Gefährdungen bewertet. Dazu wird für jede mögliche Gefährdung die Auftretenswahrscheinlichkeit und das Schadensausmaß ermittelt. Für jede Gefährdung muss sodann – unter Anwendung der im Risikomanagementplan festgelegten Kriterien – entschieden werden, ob das eingeschätzte Risiko so gering ist, dass eine Risikominderung nicht erforderlich ist, oder ob Maßnahmen zur Risikominderung festgelegt werden müssen. Die Risikobewertung ist in der Risikomanagementakte zu dokumentieren.
- Risikokontrolle. Wenn eine Risikominderung erforderlich ist, müssen Maßnahmen festgelegt werden, um das Risiko auf ein vertretbares Maß zu reduzieren. Eine Maßnahme kann dabei die Wahrscheinlichkeit des Auftretens oder den Schweregrad des möglichen Schadens verringern. Dazu muss zunächst versucht werden, das Risiko durch eine Änderung des Designs zu beseitigen oder zu verringern. Ist dies nicht möglich, sind Schutzvorrichtungen oder Schutzmaßnahmen vorzusehen. Ist auch dies nicht möglich,

sind Sicherheitsinformationen vorzusehen. Die ausgewählten Maßnahmen zur Risikokontrolle sind in der Risikomanagementakte zu dokumentieren. Jedes Restrisiko, das nach der Durchführung der Maßnahmen zur Risikokontrolle verbleibt, muss anhand der im Risikomanagementplan festgelegten Kriterien bewertet werden. Die Bewertung ist in der Risikomanagementakte zu dokumentieren. Ist das verbleibende Risiko nicht vertretbar, müssen weitere Maßnahmen zur Risikominderung festgelegt werden.

6 Referenzen

[21CFR814]	Code of Federal Regulations, Title 21 (CFR 21) Section 814, s. http://www.fda.gov/, letzter Zugriff 17.07.2007
[21CFR820]	Code of Federal Regulations, Title 21 (CFR 21) Section 820, s. http://www.fda.gov/, letzter Zugriff 17.07.2007
[21CFR860]	Code of Federal Regulations, Title 21 (CFR 21) Section 860, s. http://www.fda.gov/, letzter Zugriff 17.07.2007
[Balzert1]	Helmut Balzert – Lehrbuch der Software-Technik, Softwareentwicklung , Spektrum Akademischer Verlag, 1996
[Balzert2]	Helmut Balzert – Lehrbuch der Software-Technik, Software-Management, Software-Qualitätssicherung, Unternehmensmodellierung, Spektrum Akademischer Verlag, 1998
[Dröschel]	W. Dröschel, W. Heuser, R. Midderhoff, Inkrementelle und objektorientierte Vorgehensweisen mit dem V-Modell 07, R. Oldenbourg Verlag München Wien, 1998
[Ebert]	Christof Ebert - Systematisches Requirements Management, dpunkt Verlag, 2005
[FDA-Act]	Fedral Food, Drug, and Cosmetic Act, as amended through December 31, 2005 zugänglich über http://www.fda.gov/opacom/laws/fdcact/fdctoc.htm,, letzter Zugriff 17.08.2007
[FDA-Cybersecurity]	Guidance for Industry: Cybersecurity for Networked Medical Devices Conatining Off-The-Shelf (OTS) Software, http://www.fda.gov/cdrh/comp/guidance/1553.pdf, letzter Zugriff 17.07.2007
[FDA-DesignGuide]	Design Control Guidance for Medical Device Manufacturers, March 11, 1997, http://www.fda.gov/cdrh/comp/designgd.pdf, letzter Zugriff 17.07.2007.
[FDA-DoIt]	Dick Sawyer, Do it by Design – An Introduction to Human Factors in Medical Factors, December 1996, http://www.fda.Gov/cdrh/humfac/doitpdf.pdf, letzter Zugriff 17.07.2007.
[FDA-OTS]	Guidance for Industry, FDA Reviewers and Compliance on Off-The-Shelf-Software Use in Medical Devices, Document issued on: September 9,

	1999, http://www.fda.gov/cdrh/ode/guidance/585.pdf, letzter Zugriff, 17.07.2007.
[FDA-Premarket]	Guidance for FDA Reviewers and Industry: Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices; Document issued on: May 11, 2005, http://www.fda.gov/ cdrh/ode/ guidance/337.pdf, letzter Zugriff 17.07.2007.
[FDA-UseSafety]	Guidance for Industry and FDA Premarket and Design Control Reviewers: Medical Device Use-Safety: Incorporating Human Factors Engineering into Risk Management, Document issued on: July 18, 2000, http://www.fda.gov/cdrh/humfac/1497.pdf, letzter Zugriff 17.07.2007.
[FDA-Validation]	General Principles of Software Validation; Final Guidance for Industry and FDA Staff, Document issued on: January 11, 2002, http://www.fda.gov/cdrh/comp/guidance/938.pdf, letzter Zugriff 17.07.2007
[ISO 13495]	DIN EN ISO 13485:2003, erhältlich über den Beuth Verlag
[ISO 14971]	DIN EN ISO 14971 (ISO 14971:200) Anwendung des Risikomanagement auf Medizinprodukte, Deutsche Fassung EN ISO 14971:2001, erhältlich über den Beuth Verlag
[ISO 60601-1-4]	DIN EN ISO 60601-1-4:1996+A1:1999, erhältlich über den Beuth Verlag
[ISO 60601-1-6]	DIN EN 60601-1-6 (VDE 0750-1-6) Medizinische elektrische Geräte – Teil 1-6: Allgemeine Festlegung für die Sicherheit – Ergänzungsnorm: Gebrauchstauglichkeit (IEC 60601-1-6:2004), erhältlich über den Beuth Verlag
[ISO 9000]	DIN EN ISO 9000, Normen zum Qualitätsmanagement, Sonderdruck für Lehrveranstaltungen der DGQ, Beuth Verlag, 2003,
[ISO 9001]	DIN EN ISO 9001, Normen zum Qualitätsmanagement, Sonderdruck für Lehrveranstaltungen der DGQ, Beuth Verlag, 2003,
[ISO 9004]	DIN EN ISO 9004, Normen zum Qualitätsmanagement, Sonderdruck für Lehrveranstaltungen der DGQ, Beuth Verlag, 2003,
[ISO prEN 62304]	Medizingeräte-Software – Software-Lebenszyklus-Prozesse (IEC 62A / 474 /CDV:2004) Deutsche Fassung EN ISO prEN 62304:2004, Entwurf April 2005, erhältlich über den Beuth Verlag
[Kage]	Uwe Kage, Das Medizinproduktegesetz, Springer Verlag, 2005
[KOM(85)]	Weißbuch über die Vollendung des Binnenmarkts, KOM(85) 310 endg.

	vom 14.Juni 1985, erhältlich über http://europa.eu, letzter Zugriff 03.01.2007
[NB-MED-2.2/REC4]	http://www.team-nb.org/Documents/R2_2-4_rev5.pdf, letzter Zugriff 14.08.2007.
[Oestereich]	B. Oestereich, C. Schröder, M. Klink, G. Zockoll – OEP – oose Engineering Process, dpunkt Verlag, 2007
[Oestereich]	B. Oestereich, C. Schröder, M. Klink, G. Zockoll, OEP . OOSE Engineering Process, dpunkt.verlag, Heidelberg, 2007
[Partsch]	Helmuth Partsch - Requirements-Engineering systematisch, Springer Verlag, 1998
[Pomberger],	G. Pomberger, W. Pree, Software-Engeneering, Carl Hanser Verlag, München, Wien 2004
[Rupp]	Chris Rupp, Requirements-Engineering und –Management, 3. Auflage, Hanser Verlag, 2004
[Schorn]	Gert Schorn, MPG Medizinproduktegesetz, 3.Auflage, Stand:Dezember 2001, Wiss. Verl.-Ges., 2002
[SG1/N41R9]	SG1/N41R9:2005: Essential Principles of Safety & Performance of Medical Devices, http://www.ghtf.org/sg1/inventorysg1/sg1n41r92005.pdf, letzter Zugriff 14.08.2007. 2007
[SG3/N15R8]	SG3/N15R8:2005: Implementation of Risk Management Principles and Activities Within a Quality Management System, http://www.ghtf.org/sg3/inventorysg3/sg3n15r82005.pdf, letzter Zugriff 14.08.2007
[Versteegen1]	Gerhard Versteegen (Hrsg.) – Anforderungsmanagement, Springer Verlag, 2004
[Versteegen2]	Gerhard Versteegen – Projektmanagement mit dem Rational Unified Process, Springer Verlag, 2000
[Winter]	Methodische objektorientierte Softwareentwicklung, dpunkt.verlag, Heidelberg, 2005