SIEMENS

Georg Heidenreich, Gerd Neumann

Software für Medizingeräte

Die praktische Auslegung und Umsetzung
der gesetzlichen Standards für Entwicklungsleiter,
Qualitätsverantwortliche und Programmierer

Heidenreich / Neumann
Software für Medizingeräte

Dr. Georg Heidenreich
studierte Informatik an der Uni Erlangen-Nürnberg, promovierte 1996 in Ingenieurwissenschaften und ist seit 1998 Angestellter bei Siemens Healthcare. Seit 2005 ist er dort für Software-Regulierung zuständig.

Gerd Neumann
studierte Nachrichtentechnik und arbeitet seit 1975 in der Hardware- und Softwareentwicklung. Seit 2012 ist er bei Siemens Healthcare zuständig für Software-Prozessnormen und die Gremienarbeit in der IEC – besonders im Hinblick auf die Pflege der Norm IEC 62304.

Software für Medizingeräte

Die praktische Auslegung und Umsetzung der gesetzlichen Standards für Entwicklungsleiter, Qualitätsverantwortliche und Programmierer

von Georg Heidenreich
und Gerd Neumann

Die Deutsche Nationalbibliothek verzeichnet diese Publikation
in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten
sind im Internet über http://dnb.d-nb.de abrufbar.

www.publicis-books.de

Print ISBN 978-3-89578-442-2
ePDF ISBN 978-3-89578-930-4

Herausgeber: Siemens Aktiengesellschaft, Berlin und München
Verlag: Publicis Publishing, Erlangen

Printed in Germany

Inhalt

1 Worum es in diesem Buch geht ... 8

2 Warum das Einhalten von Standards so wichtig ist und was wir demnächst zu erwarten haben ... 10
2.1 Die Aktualisierung der IEC 62304 (Amendment 1) ... 12

3 Standards – ein Überblick ... 14
3.1 Wie sind Standards entstanden? ... 14
3.2 Vom Standard zur Norm ... 16

4 Produktentwicklung ... 17
4.1 Schritte im Lebenszyklus eines Produktes ... 17
4.2 Der Entwicklungsprozess ... 18

5 Anwendung von Normen ... 46
5.1 Warum ist Software anders? ... 46
5.2 Gültigkeitsbereich ... 48
5.3 Harmonisierung ... 55
5.4 Des Pudels Kern ... 56
5.5 Was in der Norm IEC 62304 seltsam ist ... 57

6 Die Anforderungen der Norm IEC 62304 ... 63
6.1 Sicherheitsstufen ... 63
6.2 Softwareprozesse ... 67
6.3 Entwicklungsplan ... 69
6.4 Konfigurationsverwaltung ... 70
6.5 Risikoanalyse ... 72
6.6 Risikokontrollmaßnahmen für Software ... 73
6.7 Rückverfolgbarkeit von Risikokontrolle: Traceability ... 74
6.8 Zuverlässigkeit ... 76
6.9 Lastenheft ... 77
6.10 Segregation ... 79
6.11 Architektur ... 81
6.12 Soup ... 82
6.13 Entwurf ... 84
6.14 Implementierung ... 85
6.15 Integration ... 86
6.16 Änderungskontrolle ... 89
6.17 Systemtest ... 90

6.18 Freigabe 93
6.19 Wartung 95
6.20 Risikomanagement für Änderungen 96
6.21 Problemlösung vor Freigabe 97
6.22 Problemlösung nach Freigabe 100
6.23 Sichere Bedienbarkeit 104

7 Risikomanagement 115
7.1 Grundlagen 116
7.2 Beispiel Risikomanagement beim Autofahren 118
7.3 Risikomanagement für Medizingeräte 126
7.4 Risikoanalyse in großen Systemen 129
7.5 ISO 14971 Risikomanagement für Medizingeräte 133

8 Segregation 139
8.1 Motivation 139
8.2 Defensiver Umgang mit Eingaben 140
8.3 Sequenz als Mittel zur Entkoppelung 141
8.4 Komponenten 142
8.5 Segregation durch Kapselung 144
8.6 Entkoppelung durch statische Ressourcenallokation 145
8.7 Entkoppelung durch Dependency Inversion 146
8.8 Entkoppelung durch exklusive Instanzen 147
8.9 Trennung durch asynchrone Abläufe 148
8.10 Zustandsfreie, referenzfreie Bibliotheken 150
8.11 Lange, optimistische Transaktionen 152
8.12 Berechtigungsprüfung 155
8.13 Segregation zwischen Prozessen des Betriebssystems 157
8.14 Trennung durch Hardware 159

9 Rückverfolgbarkeit (Traceability) 161
9.1 Einführung in Requirements Traceability 162
9.2 Ein allgemeines Traceability-Modell 164
9.3 Traceability in Standards 168
9.4 Regulatorische Anforderungen 170

10 Software als eigenes Produkt 173
10.1 Motivation für die Definition von Software als Produkt 173
10.2 Erweiterte Anwendbarkeit 173
10.3 Anforderungen an Health Software 174
10.4 Lebenszyklusprozesse für Software im Bereich Medizin und Gesundheit 179
10.5 Produktvalidierung für Health Software 181
10.6 Produktkennzeichnung und Begleitdokumente für Health Software 185
10.7 Post-Market-Anforderungen für Health Software 187

11 Vorhandene Software 189
11.1 Off-the-Shelf-Programme 189
11.2 Änderungen an vorhandener Software 190
11.3 Neue Verwendung für bestehende Software 191
11.4 Software-Plattformen für die Medizintechnik 192
11.5 Nachdokumentieren – aber richtig! 192

12 Effiziente Softwareentwicklung 195
12.1 Erfolgsfaktoren für Softwareprojekte 195
12.2 Agile Prozesse 200
12.3 Modellierung 211
12.4 Konfigurationsverwaltung 215

13 Stabile Programme 218
13.1 Quellcode 218
13.2 Entwurf 222

14 QM-System und Produkt-Anforderungen 226
14.1 Die Motivation für die Einführung eines QM-Systems 226
14.2 Aufbau der ISO 13485 228
14.3 Zusammenfassung der Anforderungen an ein QM-System 229
14.4 Beispielhafte Themen für ein QM-Handbuch für Medizingeräte-Software 235

15 Strukturierter Nachweis (Safety Assurance Case) 238
15.1 Motivation zur Erstellung strukturierter Nachweise 238
15.2 Geschichte 239
15.3 Das Prinzip des strukturierten Nachweises 240
15.4 Beispiel Generische Infusionspumpe (GIP) 240
15.5 Graphische Darstellung der strukturierten Nachweise 242
15.6 Erstellung eines strukturierten Nachweises 243
15.7 Reviews von strukturierten Nachweisen 250
15.8 Die Praxis des strukturierten Nachweises 251

16 Beispiel SONOPIX 254

17 Weiterführende Normen 260

18 Verweise 263

19 Abbildungs- und Tabellenverzeichnis 267

20 Index 269

1 Worum es in diesem Buch geht

Das Buch erläutert praktische Fragen für die Erstellung von Software für Medizingeräte in Europa. Die Autoren präsentieren eine genaue Entscheidungshilfe für die Anwendbarkeit der europäischen Medizinprodukterichtlinie sowie die etablierten Vorgehensweisen zur Einhaltung der regulatorischen Anforderungen an Software und sie erläutern die anwendbaren Standards, insbesondere die Norm IEC 62304 in der derzeitigen Version von 2006 – Hinweise zur Version in Kapitel 1. Die Anforderungen aus den vorgeschriebenen Sicherheits-Standards werden für typische Prozesse, Vorgehensweisen und Architekturen konkret angewendet. Ergänzend werden die Besonderheiten der anwendbaren Standards und die Unterschiede zu Software in anderen Branchen erläutert. Aufbauend auf einem umfangreichen Fragenkatalog diskutieren die Autoren auch spezielle Situationen und sie beantworten die entsprechenden Fragen mit Verweis auf die anwendbaren Normen. Spezialthemen werden in eigenen Kapiteln vertieft. Außerdem wird ein Überblick über die neuesten Trends in der Standardisierung sowie die Aussichten auf die neue Medizinprodukte-Regulierung im Hinblick auf Software gegeben.

Das große Ziel der IEC 62304 ist die Verringerung der Wahrscheinlichkeit oder der Schwere von Verletzungen und körperlichen Schäden beim Einsatz von Software in der Medizintechnik. Dabei liegt folgende medizinische Ethik zugrunde: Wenn die Risiken der Erkrankung viel größer sind als die Risiken der medizinischen Untersuchung und Behandlung, ist eine angemessene Körperverletzung des Patienten akzeptabel.

Hierin liegt der fundamentale Unterschied zwischen der IEC 62304 und allgemeinen Sicherheitsnormen, die das Lebensrisiko von mehr oder weniger Unbeteiligten allgemein reduzieren sollen: Die Risiken von Medizin im Allgemeinen und hier von Medizintechnik im Speziellen werden vom Hersteller dieser Technik minimiert. Allerdings sind die Akzeptanzschwellen deutlich höher, da die dokumentierten Restrisiken durch den *Arzt* gegen die Krankheitsrisiken bei Nichteinsatz dieser Technik abgewogen werden können. Genaugenommen gilt für das *Bedienpersonal* dann wieder das allgemeine, hohe Schutzziel, „keinerlei Gefährdung" hinzunehmen. Somit werden in der Medizintechnik zwei verschiedene Risikogruppen betrachtet.

Die Gesetzgebungen in der Welt sind sich bei Medizingeräten einig, dass die *informierte Bedienung des Medizingerätes durch den Mediziner kon-*

trollierte Risiken mit sich bringen darf, wenn sie angemessen in Bezug auf den Nutzen durch Diagnose oder Therapie sind. Risiken für das Bedienpersonal können jedoch nicht im gleichen Maße wie Risiken für den Patienten dem Nutzen für den Patienten gegenübergestellt werden.

Mit diesem Buch wird nicht der Anspruch erhoben, das gesamte Themengebiet vollständig abzudecken. Auch vertreten die Autoren bei den verschiedenen, mitunter sehr komplexen Themen ihre eigenen Betrachtungsweisen, die nicht unbedingt mit denen anderer Fachleute übereinstimmen müssen. Im konkreten Fall sollte man deshalb immer auch das Gespräch mit den benannten Stellen oder mit qualifizierten Beratungsbüros suchen.

Und noch ein Hinweis: Wir verweisen im Buch immer wieder auf Kapitel in der Norm; diese Stellen sind mit dem Piktogramm 🕮 gekennzeichnet. Querverweise im Buch heißen einfach „siehe …“. Und definierte Begriffe aus der Norm sind im Fließtext in Kapitälchen ausgezeichnet.

2 Warum das Einhalten von Standards so wichtig ist und was wir demnächst zu erwarten haben

Wenn wir uns mit Standardisierung beschäftigen, merken wir sehr schnell, dass bei Projektleitern und Entwicklern auf der einen Seite ein großes Interesse an Informationen über die einzuhaltenden Standards besteht, auf der anderen Seite aber die zur Verfügung stehenden Informationen meistens viel zu komplex und akademisch sind.

Daraus ergibt sich leider sehr oft eine Kombination aus mangelndem Wissen und Berührungsangst, was dazu führt, dass man sich eher gar nicht mit dem Thema beschäftigt oder sich auf andere verlässt.

Deswegen hatten wir die Idee, den Zugang zu diesem Thema zu erleichtern, indem wir versuchen, anhand von praxisnahen Beschreibungen und Beispielen den Bezug zur täglichen Arbeit herzustellen.

Natürlich ist es so, dass mit zunehmender Eindringtiefe in das Thema die Beschreibungen komplexer und technischer werden. Aber wir versuchen in diesem Buch, die detaillierten Erläuterungen in eigenen Kapiteln zusammenzufassen, auf die im laufenden Text verwiesen wird. Damit ist es möglich, eine verständliche, etwas allgemeine Erläuterung zu verfassen, die den Einstieg in das Thema deutlich erleichtert. Für jemanden, der bereits tiefergehendes Wissen zum Thema besitzt, kann die detaillierte Beschreibung als Nachschlagewerk dienen, wenn es darum geht, sich über konkrete Vorgaben der Norm zu informieren.

Wir beobachten auch, dass die Standardisierung im Lehrplan der Universitäten nicht oder unzureichend erwähnt wird.

Für jeden, der anfängt, sich mit Software, womöglich sogar im medizinischen Umfeld, zu beschäftigen, wird es aber irgendwann unumgänglich sein, sich mit den gesetzlichen Regeln und den damit verbundenen Standards auseinanderzusetzen.

Wenn sich Studenten im Rahmen ihres Studiums mit der Entwicklung von medizinischer Software beschäftigen, sollte man das Thema der Standardisierung auf keinen Fall ausklammern. Der gut gemeinte Vorsatz, nicht

von der eigentlichen Aufgabe der Softwareentwicklung und dem Erlernen verschiedenster Technologien und Methoden ablenken zu wollen, ist sehr zweifelhaft. Man lernt ja auch nicht das Autofahren, indem man zuerst einmal die anzuwendenden Verkehrsvorschriften außer Acht lässt.

Gerade in dieser Phase des Lernens sollte man das Thema nicht ausklammern, da ein direkter Bezug zwischen der momentanen Aufgabe und der damit verbunden Thematik „Qualität und Sicherheit" sehr einfach herzustellen ist. Wir sehen es als Vorteil an, wenn schon zu diesem Zeitpunkt vermittelt werden kann, wie es mit der persönlichen Verantwortung aussieht, wenn man ein Produkt auf den Markt bringt oder an der Entwicklung eines Produktes beteiligt ist.

Unser Ziel ist es, diesen „trockenen" Stoff etwas interessanter zu gestalten und es selbstverständlich werden zu lassen, sich mit den Anforderungen aus Standards in Bezug auf medizinische Software auseinanderzusetzen. Vollkommen wird das allerdings nie gelingen. Man kann es vergleichen mit der allgemeinen Gesetzgebung, die sich in Art und Form der Ausdrucksweise danach richtet, möglichst rechtssicher zu sein. Das hat dann zur Folge, dass es für die Anwendung und Auslegung von Gesetzen viele Kommentare gibt. Man sieht aber auch, dass es bei gleichem Sachverhalt mitunter gegensätzliche Urteile gibt, was zeigt, dass es immer einen Spielraum gibt, innerhalb dessen Gesetze – in unserem Fall Normen – ausgelegt werden können. Die Rechtsprechung kann also durchaus (negativ) anführen, dass bekannte, neue Technologien nicht eingesetzt wurden, obwohl diese ein erkennbares Risiko deutlich verringert hätten. Dabei ist es dann unerheblich, ob man die gültige Norm vollständig erfüllt hat. Ein Blick über den bekannten „Tellerrand" hinaus ist in jedem Fall zu empfehlen.

Ziel ist es, dass jedem Beteiligten klar wird, dass auch er eine Sorgfaltspflicht hat, die im Ernstfall zu einer Haftung führen kann. Allein schon das Risiko einer persönlichen Verantwortung, die vom Gesetzgeber gefordert wird, sollte dazu führen, sich mit Standardisierung auseinanderzusetzen.

Fast alle Länder verlangen per Gesetz, dass die Norm IEC 62304 „Software-Lebenszyklusprozesse" für Software in Medizinprodukten eingehalten wird. Einzelne Länder oder auch die Europäische Union haben auf Grundlage dieser Norm eigene Ausgaben herausgegeben, auf die per Gesetz hingewiesen wird.

Genauer gesagt: Werden diese Standards eingehalten, wird damit automatisch die Erfüllung gesetzlicher Anforderungen vermutet.

(siehe Abschnitt 5.3)

2.1 Die Aktualisierung der IEC 62304 (Amendment 1)

Die Norm IEC 62304 schreibt keine bestimmten Prozesse vor; sie verlangt lediglich, dass bestimme Aktivitäten durchgeführt und bestimmte Dokumente erstellt werden. Sie legt fest, wie der Hersteller von Software deren Gefährdungen dokumentiert und auch die Nachweise über die Reduktion der Risiken führt. Dazu beschreibt sie hauptsächlich die Anwendung der Risikomanagement-Norm ISO 14971 für Software.

Die Beziehung auf weiterführende Normen, wie zum Beispiel die Normenreihe IEC 61508-n „Funktionale Sicherheit", wird im Anhang dieses Buches beschrieben.

Seit 2012 wird an einer Fehlerkorrektur und Verbesserung der IEC 62304 gearbeitet. Wegen der vielen Initiativen und Ideen wird die eigentlich fällige Revision der IEC 62304 verzögert und zunächst einfach nur ein Zusatz mit Änderungen herausgebracht, der nicht den vollen Normtext, sondern lediglich Änderungsanweisungen enthält. Ein Dokument dieser Form mit „Deltas" ist das sogenannte Amendment . Es ist nicht gerade leicht lesbar, dennoch haben wir uns durch diese Änderungen schon einmal durchgearbeitet.

Die ersten Änderungen beziehen sich gleich auf die Verallgemeinerung der IEC 62304 im Hinblick auf „Software als Medizinprodukt" und die damit einhergehende Abgrenzung zur Produktsicherheit.

Als wichtigste Erweiterung wird der Umgang mit alter Software (Legacy), die bereits im Markt ist, geregelt, die jedoch vor der Publikation der IEC 62304 im Jahr 2005 entworfen wurde (für die Anwendbarkeit zählt das Jahr des Entwurfs, nicht das der Fertigstellung).

Ein weiterer wichtiger Punkt ist die Berücksichtigung von Wahrscheinlichkeiten bei der Festlegung der Sicherheitsstufe. Das wird jetzt jedoch mitnichten wie bei allen anderen Normen geregelt, die eben ganz durchgängig die Risikohöhe als Produkt von Wahrscheinlichkeit und Gefährdungshöhe betrachten, vielmehr werden die Wahrscheinlichkeiten nur für externe Maßnahmen berücksichtigt: Risikorelevante Maßnahmen außerhalb des Software-Systems gelten als „extern" und dürfen „normale" Risikohöhen anwenden. „Extern" heißen die Funktionen, die nicht im Software-Lastenheft desselben Produkts beschrieben werden.

Ein weiterer wichtiger Punkt ist die Berücksichtigung von Wahrscheinlichkeiten bei der Festlegung der Sicherheitsstufe. Das wird jetzt jedoch mitnichten wie bei allen anderen Normen geregelt, die eben ganz durchgängig die Risikohöhe als Produkt von Wahrscheinlichkeit und Gefährdungshöhe betrachten, vielmehr werden die Wahrscheinlichkeiten nur für externe Maßnahmen berücksichtigt: Risikorelevante Maßnahmen außerhalb des Software-Systems gelten als „extern" und dürfen „normale" Risikohöhen anwenden. „Extern" heißen die Funktionen, die nicht im Software-Lastenheft desselben Produkts beschrieben werden.

Außerdem werden die Hersteller im Amendment 1 verpflichtet, typische Programmierfehler, wie sie bei den verwendeten Programmiersprachen und -systemen auftreten, zu dokumentieren. Hintergrund dieser Forde-

rung ist, diese Fehler bei der Erstellung sicherheitsrelevanter Software zu vermeiden.

Dazu gibt es im Amendment 1 noch viele „Glättungen" und Korrekturen, die allerdings unsere Interpretation der IEC 62304 nicht verändern. An vielen Stellen wird auch explizit auf „Medical Device" verwiesen. Ebenso werden datierte Referenzen auf andere Normen eingeführt. Die IEC 62663 wird nun unter (Software-)Anforderungen und im Diagramm 🕮 C.1 erwähnt.

Mit der Veröffentlichung des Amendment 1 ist im Laufe des Jahres 2015 zu rechnen.

3 Standards – ein Überblick

3.1 Wie sind Standards entstanden?

Um Länder oder Territorien großer Ausdehnung verwalten zu können, war es schon immer notwendig, Dinge des täglichen Bedarfs zu vereinheitlichen. Die frühesten Standardisierungen dürften die Schrift und das Geld sein. Das sind sicher auch heute noch zwei der wichtigsten Gebiete der Standardisierung: Kommunikation und Handel. Ein weiterer Bereich, sowohl eigenständig als auch als Brücke zwischen den zuvor genannten, ist die Mobilität. Alle diese Bereiche haben natürlich auch eine starke Wechselwirkung untereinander. Die Mobilität und die Kommunikation unterstützen den Handel und sicher auch umgekehrt.

Einen Standard darf eigentlich jeder schreiben. Ob sich allerdings jemand dafür interessiert, das ist die Frage. Es gab schon Fälle, bei denen eine Firma sich einen eigenen Standard geschrieben hat und dieser dann irgendwann allgemein befolgt wurde, obwohl es dazu keine gesetzliche Regelung gab. Bekannt ist zum Beispiel die sog. „Centronics-Schnittstelle“ aus den 70er Jahren vom gleichnamigen Druckerhersteller, die als Quasistandard erst 1994 vom regulären Standard IEEE 1284 abgelöst wurde.

Damit ist bereits ein Grund für die Entwicklung von Standards genannt, nämlich, Handelshindernisse zu beseitigen. Zwar werden Standards jeweils von Experten eines Fachgebietes erstellt, der rechtliche Rahmen der Standardisierung ist jedoch meistens Wirtschaftspolitik ersten Ranges: So regeln die Verträge der Welthandelsorganisation WTO ganz genau die Regeln der Standardisierung in den WTO-Vertragsländern und nennen dabei allerdings gleich das Ziel: (Avoiding) „Technical Barriers To Trade“ [WTOTBT], also den Abbau von Handelshemmnissen, durch Verminderung der Vielfalt und verbesserte Rationalisierung, Verständigung und Kompatibilität.

Ein anderes großes Motiv der Standardisierung ist die Sicherheit von Diensten und Produkten – im Sinne von Gefährdungsfreiheit. Das Interesse an verbesserter Sicherheit ist zwar auch mit dem Ziel verbunden, Handelshindernisse zu beseitigen, hat seinen Ursprung jedoch im ethischen Verständnis, Menschen und Umwelt zu schützen. Die Unversehrtheit von Sachen ist dabei eher aus wirtschaftlicher Sicht zu betrachten.

Die erste „VDE-Vorschrift“ über Kabelschuhe und Klemmschrauben wurde bereits im Jahr 1896 herausgegeben. 1906 wurde die „Internationale Elektrotechnische Kommission“ (IEC, *International Electrotechnical Commission*) gegründet.

Standards lernt man erst schätzen, wenn sie fehlen oder nicht eingehalten werden.

> Albert Büttner entwickelte in Lauf bei Nürnberg 1926 den Schuko-Stecker, der heute als Standard CEE 7/4 weltweit in 39 Ländern eingesetzt wird. Wie wichtig dieser Standard ist, merken wir auf jeder Urlaubs- oder Dienstreise, und zwar besonders in den Ländern, die andere Stecker einsetzen.

Das Interesse von Staaten an einer Normung ist durch die zunehmende Industrialisierung und die damit verbundene Notwendigkeit zum Abbau von technischen Handelshemmnissen durch Vereinheitlichung (Standardisierung) gewachsen.

Die Festsetzung gemeinsamer Begrifflichkeiten und ihrer Bedeutung ist eine Grundvoraussetzung kultureller Interaktion. So war der Prozess der Normung seit jeher ein zentraler Bestandteil transnationalen und transkulturellen Austauschs. Im Europa des späten 18. Jahrhunderts wurde die Standardisierung jedoch erstmals von Grund auf systematisiert. Bemühungen, im großen Umfang Normen und Maßeinheiten festzusetzen, gewannen an Einfluss und stellten den Prozess der Standardisierung auf eine ganz neue Grundlage. Die gründliche Überarbeitung französischer Gewichts- und Längenmaße, die während einer historisch außergewöhnlichen Phase – der Französischen Revolution – begann, stellt den ersten Fall einer wissenschaftsbasierten und auf Konferenzen ausgehandelten Standardisierung dar. Dies wurde später die wichtigste Form, internationale Normen festzusetzen und aufrechtzuerhalten. Ein Artikel von Roland Wenzlhümer verfolgt die Standardisierung bis zu ihren Anfängen im Frankreich des 18. Jahrhunderts zurück und versucht zu erklären, warum gerade die Französische Revolution günstige Voraussetzungen für ein solches Vorhaben schuf. Dann werden die darauf folgenden, ersten Versuche einer internationalen Normung dargestellt. Schließlich erläutert er die Standardisierung im 19. Jahrhundert kurz an drei Beispielen, die aus den Bereichen der Telekommunikation, der Zeitmessung und der Währungen stammen und jeweils unterschiedlichen Wegen zur Standardisierung folgten. [WENZLH]

3.2 Vom Standard zur Norm

Ein Standard wird durch ein länderabhängiges Normierungsverfahren zu einer Norm, die als Basis den Standard enthält und eventuell noch Zusätze und Erläuterungen, um den nationalen Bedürfnissen und Vorschriften zu genügen.

Eine Norm ist ein von Experten erstelltes Dokument, das mit dem Ziel erstellt wird, gesetzliche Regelungen zu präzisieren.

Die Anwendung eines Standards ist zuerst einmal grundsätzlich freiwillig. Erst der Gesetzgeber macht dann aus dem Standard eine Norm, als verbindliche Vorschrift, nach der ein Produkt gefertigt werden muss, oder die festlegt, welche Eigenschaften es haben muss.

Natürlich braucht das alles seine Zeit: Die Erstellung eines Projektvorschlags dauert mit Abstimmung zur Annahme etwa ein Jahr, die anschließende technische Konsensbildung nochmals mindestens ein Jahr und die Zeit für Übersetzung und Publikation mindestens ein halbes Jahr. Somit kann man im Konsensfall in zweieinhalb Jahren einen Standard erstellen. Etwas ausführlicher ist dieser Prozess in Abbildung 1 dargestellt

Erst die Ergänzung sowie die Referenzierung in Gesetzeswerken macht daraus dann die Norm. Dazu gibt es etwa auf europäischer Ebene für jede Direktive (hier: die EU Medizingeräte-Direktive) spezielle Arbeitsgruppen (hier: MEDDEV), in denen Experten eine Beurteilung abgeben und Ergänzungen vorschlagen. Dieses Verfahren dauert selten weniger als zwei Jahre, bei vollkommen neuen Standards eher länger. Dabei spielen die Offenlegungszeiten für die Kommentierung sowie die Fristen für Übersetzungen eine große Rolle.

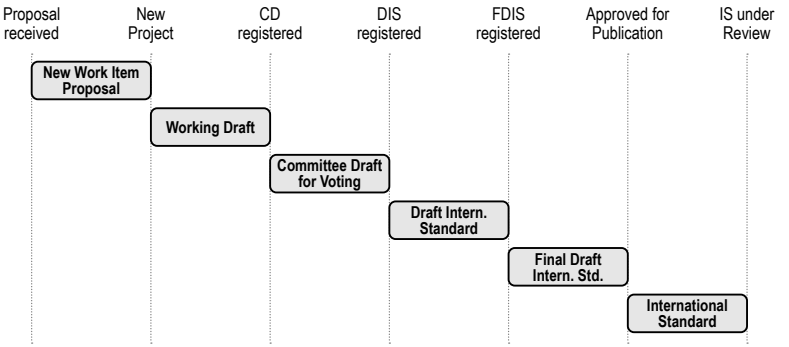

Abbildung 1 Entwicklungsstufen der Standardisierung

4 Produktentwicklung

Die folgenden Abschnitte beschreiben die Anwendung der IEC 62304 in den verschiedenen Schritten der Produktentwicklung. Die Norm enthält Anforderungen an den Prozess, also an alle Aktivitäten und Dokumente rund um den Produktlebenszyklus. Dazu gehören neben der Produktentwicklung noch weitere Schritte – wie etwa Wartung und Feldbeobachtung. Weitere Anforderungen auf Produktebene – also nicht für den Prozess – werden frühestens im Jahr 2016 in einem zukünftigen Standard „EN 82304“ publiziert. Wir beschreiben diese Anforderungen hier in einem eigenen Anhang, soweit sie uns bereits bekannt sind [82304].

Dem Entwicklungsprozess gehen Schritte voraus, die man als einleitenden Prozess bezeichnen kann. Dieser Prozess wird vor allem von geschäftlichen Interessen geleitet und kann an unterschiedlichsten Stellen abgebrochen werden, weil zum Beispiel das Produkt nicht wirtschaftlich herzustellen ist oder die Marktanalyse keinen nennenswerten Käuferkreis ermitteln konnte.

4.1 Schritte im Lebenszyklus eines Produktes

Produktidee – was soll der Kunde damit machen?

Produktbeschreibung – was soll das Produkt leisten?

Anforderungen – was sind genau die Merkmale des Produkts?

Pflichtenheft – wie erbringt das Produkt diese Leistungen?

Entwicklung – Erstellung aller Spezifikationen, inkl. Testen

Fertigung – Erstellung des Produkts (Kopien der Software)

Vertrieb – inklusive Werbung und vertragliche Aussagen

Beobachtung der Geräte im Feld und Sammlung von Beschwerden

Korrekturmaßnahmen und Benachrichtigungen

Wartung zur Verbesserung, Vorbeugung, Fehlerbehebung

Dekommissionierung bei Lebensende eines Produktes

Jedes Produkt hat während seines gesamten Lebenszyklus einen Besitzer, zum Beispiel den Produktmanager. Dieser ist für alles zuständig, was mit

der Entwicklung, der Herstellung, des Vertriebs und der Wartung dieses Produktes zu tun hat.

Der Produktidee folgt normalerweise eine Marktanalyse, ob dieses Produkt am Markt platziert werden kann. Anhand dieser Analyse wird der Produktmanager entscheiden, ob er die Entwicklung in Auftrag gibt.

Speziell wenn es bei einem Produkt um die Sicherheit im Sinne von gesundheitlicher Gefährdung geht, muss es für alle Phasen der Produktentwicklung einen Verantwortlichen geben.

Die allgemeinen gesetzlichen Vorschriften bezüglich der Produkthaftung müssen bei medizinischen Geräten besonders aufmerksam betrachtet werden (siehe Gesetz über die Haftung für fehlerhafte Produkte, das Produkthaftungsgesetz – ProdHaftG).

4.2 Der Entwicklungsprozess

Wenn wir uns die einzelnen Schritte eines Entwicklungsprozesses ansehen, können wir gut erkennen, dass es für jeden dieser Schritte Anforderungen gibt, die am Ende auch entsprechend überprüft werden müssen – daraus resultieren üblicherweise Dokumente, die als Ergebnis einer von der Norm geforderten Aktivität stehen.

Begleiten wir doch einfach einmal unseren Produktmanager Manni Ager und den Softwareentwickler Harry Hacker durch die gesamte Produktentwicklung. Die weiteren Mitarbeiter auf diesem Weg sind Mark Eting für die Marktforschung, Peter Seller für den Vertrieb, Kalli Brierer für den Service, und begleitet wird das alles von Konni Troller (genannt „Mr. Q“) für die Qualitätssicherung.

Der Produktmanager ist immer Auftraggeber. Alle anderen Abteilungen sind Lieferanten und Dienstleister.

Das gilt auch und ganz besonders für die Qualitätssicherung, wobei die Vorgaben dafür nicht vom Produktmanagement kommen, sondern vom Gesetzgeber oder vom Qualitätsmanagement einer Firma festgelegt werden.

Eine erste Betrachtung der zukünftigen Zielgruppe ist verbunden mit der Frage, welche gesetzlichen Vorgaben für dieses Produkt zu beachten sind. Abgesehen von allgemeinen Sicherheitsvorschriften kann ein Hersteller diese Frage nur genau beantworten, wenn er die **bestimmungsgemäße Verwendung** festlegt.

Mit dieser Definition kann ein Hersteller einigermaßen genau herausbekommen, welche gesetzlichen Vorgaben und damit verbundene Normen zu beachten sind. Umgekehrt stellt der Hersteller mit der Dokumentation der bestimmungsgemäßen Verwendung auch klar, für welche Anwendungen des Produkts er überhaupt Risiken betrachtet hat.

Produktidee

Manni Ager bekommt eine Zeitschrift auf den Tisch, die einen Artikel über moderne Spielekonsolen enthält und in dem beschrieben wird, wie ein sog. Datenhandschuh verwendet wird. Beim Lesen dieses Artikels erinnert er sich an eine länger zurückliegende Idee, die er eigentlich schon vergessen hatte, und macht sich dazu eine Notiz. Als er einige Tage später seine Notiz sieht, fällt ihm die Geschichte dazu wieder ein.

Vor vielen Jahren hatte sein Schwiegervater einen schweren Schlaganfall und war seitdem halbseitig gelähmt. Viele Bemühungen, mit Therapien eine Verbesserung herbeizuführen, zeigten nicht den erhofften Erfolg. Es gab aber zwei Ansätze, die zeigten, dass ein dauerhafter Fortschritt nur dann zu erzielen war, wenn ein ganz bestimmtes Ziel für den Patienten wichtig war oder wenn eine Aktion schnell einen für ihn erkennbaren Fortschritt brachte. Beide kann man zusammenfassen unter dem Begriff der positiven Rückkopplung.

Nachdem die Ärzte ihm eröffnet hatten, dass er die Klinik erst verlassen könne, wenn er in der Lage sei, Treppen zu steigen, übte er solange, bis ihm das tatsächlich gelang.

Therapien beim Krankengymnasten in den Jahren darauf erschienen ihm aber meistens lediglich dafür gut zu sein, die sadistischen Veranlagungen des Therapeuten zufriedenzustellen, da er für sich dabei keinerlei Erfolgserlebnis hatte.

Schon vor Jahren hatte Manni sich überlegt, ob es nicht möglich wäre, den Patienten mit Sensoren am Körper auszustatten, die sowohl Bewegungen als auch Hauttemperatur messen und diese Information in ein sichtbares Fernsehbild umwandeln. Dabei sollte es möglich sein, Veränderungen der Messsignale in Änderungen von Farbe, Größe und Position des Bildes umzusetzen.

Nach Gesprächen mit verschiedenen Ärzten hatte er dann diese Idee wieder begraben, da es keinerlei Zustimmung gab und man sich auch nicht vorstellen konnte, dass das zum Erfolg führen könnte.

Nun sieht er aber die Möglichkeit, durch Einsatz neuer Technologien diese Idee erneut aufzugreifen und vielleicht als Produkt anbieten zu können.

Seine ursprüngliche Idee der einfachen Rückkopplung erweitert er noch dahingehend, dass diese nicht nur rein visuell erfolgen soll, sondern gleichzeitig die betroffene Körperregion stimuliert wird. Dies könnte in Form einfacher elektrischer Impulse geschehen, die damit kleinste Muskelbewegungen „verstärken“ und dem Patien-

ten damit eine deutlichere Rückkopplung geben als nur die rein bildliche Darstellung.

Die Möglichkeiten der bildlichen Darstellung sind sehr vielfältig. Angefangen mit reinen Farbspielen bis hin zur genauen Abbildung der betroffenen Region, zum Beispiel einer Hand.

Er beschließt, das alles etwas genauer zu analysieren. Zuerst muss er aber herausfinden, ob dieses Produkt überhaupt in das Portfolio seiner Firma passt.

Nachdem klar ist, dass dieses Produkt für seine Firma von Interesse ist, beginnt er, eine genauere Produktbeschreibung anzufertigen.

In der Produktbeschreibung sollten alle Eigenschaften eines Produktes benannt werden.

Produktbeschreibung

Manni Ager kommt nach einiger Zeit nicht so richtig weiter. Ihm fehlen Informationen über die Zielgruppe und deren Anforderungen, auf die er keinen direkten Zugriff hat. Also ruft er seinen Kollegen Mark Eting an und bittet ihn, diese Informationen einzuholen. Dieser beginnt sofort, die wichtigsten Dinge zu untersuchen. Dabei stellt sich heraus, dass die wichtigste Zielgruppe im medizinischen Umfeld zu suchen ist. Marks Erfahrung sagt ihm, dass er sich auf alle Fälle mit Konni Troller zusammensetzen muss, um zu klären, ob hier eventuell spezielle Vorschriften oder die damit verbundenen Normen zu beachten sind.

Ergibt sich, dass die bestimmungsgemäße Verwendung im medizinischen Bereich liegt, dann sind ganz eigene gesetzliche Regelungen zu beachten, die sich auf speziell dafür entwickelte Standards und Normen beziehen.

Spätestens zu diesem Zeitpunkt ist klar, dass das bestehende Qualitätsmanagementsystem an diese speziellen gesetzlichen Vorgaben angepasst werden muss, falls bisher keine solchen Produkte entwickelt wurden.

Konni legt ihm alle möglichen infrage kommenden Normen vor, anhand derer sie prüfen wollen, in welchen Geltungsbereich das zukünftige Produkt fallen wird. Ihnen ist relativ klar, dass der Einsatz von Elektroimpulsen über die menschliche Haut einen erhöhten Sicherheitsaufwand bedeutet.

Jeder Standard legt seinen Geltungsbereich (Scope) fest. Dabei wird auch ganz klar die Abgrenzung beschrieben.

In den meisten Ländern wird für Medizingeräte die Beachtung der Normenfamilie IEC 60601 durch anwendbare Gesetze verlangt; das heißt: Es gilt dann die Konformitätsvermutung.

Die IEC 62304 gilt – laut anwendbarer Gesetzgebung – für die Inverkehrbringer und Ersteller von Software in Produkten mit medizinischer Zweckbestimmung.

Jede Software hat einen bestimmungsgemäßen Gebrauch (Zweckbestimmung, „Intended Use"), der vom Hersteller und nicht etwa vom Anwender oder einer benannten Stelle festgelegt wird. Diese Zweckbestimmung muss dem Anwender zugänglich sein und sie bestimmt auch die Gefährdungsszenarien, die in der Entwicklung berücksichtigt werden müssen. Als medizinische Zweckbestimmung gilt (laut deutschem Medizinproduktegesetz) alles, was am einzelnen (bekannten) menschlichen Patienten zur Erreichung von Diagnose oder Therapie eingesetzt wird.

Wenn ein Medizingerätehersteller die Entwicklung von Software an eine andere Organisation beauftragt („Outsourcing"), kennt der Auftragnehmer – als Hersteller der Software – die medizinische Zweckbestimmung und muss die IEC 62304 anwenden. Grundsätzlich ist aber weiterhin der Medizingerätehersteller für alles verantwortlich, auch für die Entwicklung des Produktes in der beauftragten Organisation (Lieferantenüberwachung).

Auf Werkzeuge, Plattformen und auch Software für „alte" Produkte wird die IEC 62304 sehr eingeschränkt angewendet.

Dokumente der Produktebene werden von der Norm IEC 62304 *nicht* erfasst – insbesondere nicht das Produktkonzept (Beschreibung, Zweckbestimmung) oder Klärungen zu externen Vorgaben (Gesetze, Marktanalysen, Studien zu Produkteigenschaften).

(siehe Abschnitt 5.2)

Nach Studie dieser Normen ist Manni klar, dass sein neues Produkt ein Medizinprodukt sein wird. Die Ausführung mit der elektrischen Stimulanz weist alle Merkmale für die Notwendigkeit eines Risikomanagements auf.

Da feststeht, dass es bestimmte Prozesse gibt, die speziell bei der Entwicklung medizinischer Geräte eingehalten werden müssen, geht es also zuerst einmal darum, zu prüfen, ob das bestehende Qualitätsmanagementsystem seiner Firma für die Entwicklung von Medizinprodukten geeignet ist.

Das vorhandene Qualitätssystem ist entsprechend der Norm ISO 9001 eingerichtet worden. Für die Medizintechnik ist dieses Qualitätssystem allerdings nicht ausreichend bzw. stellenweise zu weitreichend. Man wird also das Qualitätsmanagementsystem an die neuen Anforderungen anpassen und einen zweiten Prozess einrichten müssen.

Da die Notwendigkeit gesehen wurde, ein Qualitätssystem zu haben, das an die speziellen Bedürfnisse in der Medizintechnik angepasst ist, hat man einen eigenen Standard, ISO 13485, dafür entwickelt. Im Gegensatz zur ISO 9001, die hauptsächlich Anforderungen an die kontinuierliche Verbesserung des Produktes stellt, geht es in der ISO 13485 vornehmlich um die Produktsicherheit.

Die IEC 62304 schreibt allerdings kein spezielles Qualitätsmanagementsystem vor.

(siehe Kapitel 14)

Medizinprodukte haben besondere Anforderungen an die Sicherheit.

Anforderungen

Die Produktbeschreibung ist fertiggestellt und Mark Eting wird damit beauftragt, eine Marktanalyse durchzuführen, um festzustellen, wie die genauen Anforderungen an das Produkt aussehen sollen. Dabei geht es ja auch darum, der Konkurrenz gegenüber einen Vorsprung zu haben. Um den zu erreichen, muss das neue Produkt ganz klare (meist technische) Alleinstellungsmerkmale haben oder preislich besonders attraktiv sein.

Ein weiterer Wettbewerbsvorteil ist aber auch immer, wenn gewisse Qualitätsstandards eingehalten werden. Das erleichtert den Marktzugang und bietet die Möglichkeit, den Mitbewerbern voraus zu sein.

Das Einhalten von Qualitätsstandards bedeutet immer auch einen Wettbewerbsvorteil.

Auch muss Mark Eting an dieser Stelle genau prüfen, ob es patentrechtliche Bedenken gibt oder ob es nicht sinnvoll ist, eigene Patente anzumelden.

Alle denkbaren Anforderungen zu dem geplanten Produkt werden gesammelt und geordnet.

Im Normalfall kann man jede Anforderung definieren – typischerweise mit einem der Sätze:

- „Der Benutzer muss (Vorbedingung) (Aktion) können.“ Oder:
- „Das Produkt führt (Vorbedingung) (Zeitbedingung) (Aktion) selbsttätig aus.“

Die technische Beschreibung genau testbarer Anforderungen wird im Produkt-Lastenheft gesammelt. Jede Anforderung muss testbar sein (die genaue Beschreibung der Testfälle dazu gehören in die sog. Produkt-Testspezifikation) und jede Anforderung muss minimal sein, soll also keine zehn oder mehr unabhängigen Eigenschaften beschreiben.

Das Software-Lastenheft ist ein weiteres vorgeschriebenes Dokument nach IEC 62304 und gehört zum Software-Entwicklungsplan.

Das Software-Lastenheft muss die Anforderungen aus Produktsicht (also beim System aus Bedienersicht und beim Softwareprodukt aus Anwendungssicht) an die Software enthalten.

Software-Anforderungen sind abstrakt, dürfen also keine technischen Details enthalten. Das steht nicht deutlich in der IEC 62304 und ist mehr ein Thema der Projekt-/Entwicklungsleitung.

(siehe Abschnitte 6.3, 6.9)

Jede Anforderung muss testbar sein.

Softwareprozess

Man ist sich im Team sehr schnell einig, dass dieses neue Produkt nach dem Gesetz ein Medizinprodukt sein wird und die Entwicklung nach entsprechenden Normen durchgeführt werden muss. Für die Software wird hier der Standard IEC 62304 als die entscheidende Norm identifiziert.

Mit Beginn der Entwicklung wird der im Standard vorgeschriebene Entwicklungsprozess eingeleitet. Genaugenommen sind einige Aktivitäten und Dokumente vorgeschrieben, nicht die exakte Reihenfolge und Arbeitsaufteilung. Aus diesem Grund sind auch die einzelnen Schritte in dieser Phase nicht vollständig abzuschließen und immer offen für die Resultate von anderen Schritten. Einige vorgeschriebene „Infrastrukturprozesse“ (insbesondere Qualitätsmanagement, Änderungsprozess und Konfigurationsmanagement) werden nicht nur in der Entwicklung benötigt und sind deswegen in einem eigenen Kapitel der Norm zusammengefasst. Diese Prozesse müssen definitiv *vor* Beginn der Entwicklung bereitstehen, da sie sofort und vom ersten Dokument an benötigt werden.

Die IEC 62304 schreibt keine spezielle Reihenfolge der Prozessschritte vor.

Es wird beschlossen, ein Projektteam zu bilden und den gesamten Entwicklungsprozess zu beschreiben. Diesem Team gehören auch Harry Hacker als Verantwortlicher für die Softwareentwicklung und Kalli Brierer an, der die Anforderungen an das Produkt aus Sicht der Fertigung und des Service begleitet. Um sicher zu sein, dass alle Prozessschritte vollständig beschrieben werden, wendet man sich an eine externe Beraterfirma, die sich auf die Zulassung von Medizingeräten spezialisiert hat.

Einleitung

Unter Leitung der Qualitätsabteilung werden jetzt alle Maßnahmen getroffen, um die geforderten Dokumentationen zu verwalten. Dazu gehören auch so einfache Schritte wie das Beschriften von Ordnern mit entsprechenden Registern, die an den Entwicklungsprozess orientiert sind.

Konni Troller ist damit beschäftigt, das Qualitätshandbuch entsprechend zu überarbeiten und zu erweitern. Da man bereits Hard- und Software entwickelt und gefertigt hat und schon vor Jahren ein gut funktionierendes Qualitätssystem eingeführt hat, ist es nicht sehr schwierig, dieses an die neuen Anforderungen anzupassen. Ein wichtiger Unterschied ist die Pflicht zur „Feldbeobachtung", das heißt die ständige Kontrolle und Beantwortung aller einlaufenden Beschwerden.

Der Entwicklungsplan

Harry Hacker beginnt, mit seinem Softwareteam einen Entwicklungsplan aufzustellen und die Mitarbeiter mit den erweiterten Anforderungen vertraut zu machen. Er betont dabei noch einmal, dass es eine erhöhte Verantwortung gibt, die im Zweifelsfall, zum Beispiel wenn ein Personenschaden entstanden ist, dazu führen kann, dass die Einhaltung aller Anforderungen überprüft wird. Dabei ist es wichtig, dass nachgewiesen werden kann, dass vor allem jedes erkannte Risiko und alle sich daraus ergebenen Maßnahmen genau dokumentiert wurden.

Im Schadensfall ist es ausgesprochen wichtig, auch anhand der Dokumentation eventuelle Ereignisketten nachverfolgen zu können, um entsprechende Maßnahmen zu treffen.

Der Entwicklungsplan ist die aktuelle Zusammenfassung mit allen

- Prozessbeschreibungen
- Normen, Werkzeuge und Methoden
- Dokumentenplänen
- Software-Anforderungen
- Dokumenten für Rückverfolgbarkeit (TRACEABILITY)
- Akzeptanzkriterien.

(siehe Abschnitt 6.3)

Konfigurationsverwaltung

Da Manni Ager ein ehemaliger Hardwareentwickler ist, erklärt ihm Konni das Prinzip der Konfigurationsverwaltung, bezogen auf die Softwareentwicklung. Aus Erfahrung weiß Manni, dass bei Messaufbauten eine der wichtigsten Maßnahmen um die Messung reproduzierbar zu machen die ist, möglichst alle Informationen über den Messaufbau und den Messablauf genau zu erfassen. Dabei werden die verwendeten Messmittel genau dokumentiert.

Konni erklärt ihm, dass es bei der Softwareentwicklung letztlich um genau dasselbe geht: Unter welchen Bedingungen ist die Software entstanden? Außerdem ist es für die Nachverfolgbarkeit von Fehlern sehr wichtig, die Versionen einzelner Komponenten und auch der Gesamtsoftware festzuhalten sowie alle damit verbundenen Änderungen am Programmcode und der Entwicklungsumgebung aufzuzeichnen.

Konfigurationsverwaltung heißen die Verfahrung zur Identifikation, Archivierung und zum Rückspeichern einzelner Versionen von Dokumenten und Dateien, und zusätzlich auch alle Maßnahmen zur Kennzeichnung und Rekonstruktion von Konfigurationen, also die Zusammenstellung versionierter Dateien und Dokumente.

Dies sind die Folgen einer unzureichenden Konfigurationsverwaltung in großen Softwareprojekten:

- Es entsteht doppelte Arbeit durch nicht auffindbare oder überschriebene Textstellen.
- Immer wieder gibt es Überlappungen und Widersprüche zwischen verschiedenen Dateien.
- Software-Stände können nicht systematisch reproduziert werden.
- Laufende Arbeiten „stören" die letzte, stabile Version.

(siehe Abschnitt 6.4)

Klug ist nicht, wer keine Fehler macht.
Klug ist der, der es versteht, sie zu korrigieren.
Wladimir I. Lenin

Treten nach Auslieferung einer neuen Version vermehrt Fehlermeldungen auf, sollte man in der Lage sein, diese schon anhand der Versionskontrolle leichter zuordnen zu können und die betroffenen Komponenten zu identifizieren.

Durch das Konfigurationsmanagement muss sichergestellt werden, dass die auslieferbare Software-Version immer genau aus dem Quellcode erstellt werden kann. Hierzu ist es notwendig, wie bei einem Messaufbau, die verwendeten Werkzeuge genau zu erfassen.

Alle für die Erstellung einer gelieferten und in Betrieb befindlichen Version notwendigen Dateien und Werkzeuge müssen also unter einer Versionsnummer gespeichert und für die weitere Bearbeitung gesperrt (eingecheckt) werden.

Wird nun eine Änderung geplant, so werden die jeweils betroffenen Dateien zum Bearbeiten freigegeben (ausgecheckt) und jeder Änderungsschritt wird vom verwendeten System festgehalten. Nach Abschluss der Änderung (und aller damit verbundenen Tests) werden die betroffenen Dateien wieder gesperrt (eingecheckt) und mit einem neuen Versionsstempel versehen.

Auch die dann erstellte Gesamtsoftware erhält einen neuen Versionsstempel und der Erstellungsprozess (Build-Prozess) wird festgelegt.

Die für die Erstellung der Software und die Durchführung eventueller Tests verwendeten Geräte (Build-Rechner, Test-Rechner und sonstige Testumgebungen) müssen immer eine definierte Konstellation beinhalten.

Es ist grundsätzlich untersagt, abschließende Tests auf dem Entwicklungsrechner durchzuführen. Diese haben nie eine reproduzierbare Konstellation, allein schon durch die verwendete Entwicklungsumgebung werden im Normalfall entscheidende Eingriffe am Rechner vorgenommen.

(siehe Abschnitt 6.4)

Gefährdungsanalyse

Das Projektteam versucht zusammenzustellen, welche Ereignisse zu einem Fehlverhalten und damit zu einer Gefährdungssituation führen können. Dabei werden alle Programmteile identifiziert, die für die Ansteuerung der Hardware zuständig sind. Auch die Benutzerschnittstelle (User Interface) muss betrachtet werden, um zu verhindern, dass Fehlinterpretationen der angezeigten Informationen durch den Benutzer zu Fehlbedienungen führen können. Die Ergebnisse werden dann entsprechend im Lastenheft festgehalten.

Die Norm IEC 62304 verlangt, dass als Ergebnis einer Gefährdungsanalyse bzw. einer Gefährdungsbeurteilung die Software in Sicherheitsstufen (A, B, C) klassifiziert wird.

Dabei wird von der schwerwiegendsten Gefährdung aus Sicht von Patient und Bediener bei bestimmungsgemäßem Gebrauch des Medizingeräts ausgegangen.

Die Sicherheitsstufen können wie folgt beschrieben werden:

- A keine Verletzungen
- B leichte Verletzungen
- C Tod, schwere Verletzungen oder dauerhafte Einschränkungen

Das Lastenheft wird um die identifizierten Gefährdungsszenarien erweitert. Die Szenarien, die nicht durch die Software beinflussbar sind, müssen nicht eingetragen werden.

Aus der Sicherheitsstufe des „gefährlichsten“ Szenarios ergibt sich die Sicherheitsstufe der gesamten Software.

Risiko ist das Produkt aus Gefährdungshöhe und der Eintrittswahrscheinlichkeit. In der aktuellen Version der IEC 62304 wird also bei der Bewertung von Software nicht das Risiko, sondern nur die Gefährdungshöhe berücksichtigt. Ob zur Verringerung des Risikos die Wahrscheinlichkeit oder die Gefährdungshöhe verändert wird, ist freigestellt. Die Sicherheitsstufe bleibt dabei erhalten, denn es wird von den aus einer „Black-Box-Sicht“ denkbaren, ursprünglichen Gefährdungen ausgegangen!

Mit „Black Box“ ist hierbei die „Außenansicht“ des Verhaltens einer Software ohne Berücksichtigung der internen Datenflüsse oder programmtechnischer Lösungen gemeint.

Wird die Software durch die Architektur partitioniert, also in sog. Software Items zerlegt, und diese wiederum in weitere Software Items, dann wird die Sicherheitsstufe jeweils vererbt. Zeigt jedoch der Entwurf eines Software Items, dass diesem eine niedrigere Sicherheitsstufe zugewiesen werden kann, muss nachgewiesen werden, dass diese Software Items die höher eingestuften nicht in deren Funktion stören.

Diese Störungen können nur durch Abtrennung der Software Items voneinander vermieden werden; diese Abtrennung wird in der IEC 62304 SEGREGATION (von lateinisch segregare, ‚absondern‘, ‚trennen‘) genannt.

(siehe Abschnitt 6.10, 8)

Eine sinnvolle Softwarearchitektur reduziert die Abhängigkeiten derart, dass viele SOFTWARE ITEMS erkennbar von Risikobehandlungen getrennt werden können und eine niedrige Sicherheitsstufe haben.