

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                               |            |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | <b>DIN EN 62304<br/>(VDE 0750-101)</b>                                                                                                                                                                                                                                                                        | <b>DIN</b> |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Diese Norm ist zugleich eine <b>VDE-Bestimmung</b> im Sinne von VDE 0022. Sie ist nach Durchführung des vom VDE-Präsidium beschlossenen Genehmigungsverfahrens unter der oben angeführten Nummer in das VDE-Vorschriftenwerk aufgenommen und in der „etz Elektrotechnik + Automation“ bekannt gegeben worden. | <b>VDE</b> |
| <p>ICS 35.240.80</p> <p><b>Medizingeräte-Software –<br/>Software-Lebenszyklus-Prozesse<br/>(IEC 62304:2006);<br/>Deutsche Fassung EN 62304:2006</b></p> <p>Medical device software –<br/>Software life-cycle processes<br/>(IEC 62304:2006);<br/>German version EN 62304:2006</p> <p>Logiciels de dispositifs médicaux –<br/>Processus du cycle de vie du logiciel<br/>(CEI 62304:2006);<br/>Version allemande EN 62304:2006</p> <p>Gesamtumfang 83 Seiten</p> <p>DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE<br/>Normenausschuss Medizin (NAMed) im DIN<br/>Normenausschuss Rettungswesen und Krankenhaus (NARK) im DIN</p> |                                                                                                                                                                                                                                                                                                               |            |

## **Beginn der Gültigkeit**

Die von CENELEC am 2006-06-01 angenommene EN 62304 gilt als DIN-Norm ab 2007-03-01.

## **Nationales Vorwort**

*Vorausgegangener Norm-Entwurf: E DIN EN 62304 (VDE 0750-101):2005-04.*

Für diese Norm ist das nationale Arbeitsgremium UK 811.3 „Sicherheit von medizinisch genutzten Geräten/Systemen/Einrichtungen in der vernetzten Anwendung“ der DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE (<http://www.dke.de>) zuständig.

Die enthaltene IEC/ISO-Publikation wurde von der gemeinsamen Arbeitsgruppe JWG 3 „Medical device software“ des SC 62A „Common aspects of electrical equipment used in medical practice“ des Technischen Komitees TC 62 „Electrical equipment in medical practice“ der IEC (International Electrotechnical Committee) und dem Technischen Komitee TC 210 „Quality management and corresponding general aspects for medical devices“ der ISO (International Standardization Organization) erarbeitet.

Das IEC-Komitee hat entschieden, dass der Inhalt dieser Publikation bis zu dem auf der IEC-Website unter „<http://webstore.iec.ch>“ mit den Daten zu dieser Publikation angegebenen Datum (maintenance result date) unverändert bleiben soll. Zu diesem Zeitpunkt wird entsprechend der Entscheidung des Komitees die Publikation

- bestätigt,
- zurückgezogen,
- durch eine Folgeausgabe ersetzt oder
- geändert.

## **Nationaler Anhang NA** (informativ)

### **Zusammenhang mit Europäischen und Internationalen Normen**

Für den Fall einer undatierten Verweisung im normativen Text (Verweisung auf eine Norm ohne Angabe des Ausgabedatums und ohne Hinweis auf eine Abschnittsnummer, eine Tabelle, ein Bild usw.) bezieht sich die Verweisung auf die jeweils neueste gültige Ausgabe der in Bezug genommenen Norm.

Für den Fall einer datierten Verweisung im normativen Text bezieht sich die Verweisung immer auf die in Bezug genommene Ausgabe der Norm.

Eine Information über den Zusammenhang der zitierten Normen mit den entsprechenden Deutschen Normen ist in [Tabelle NA.1](#) wiedergegeben.

Tabelle NA.1

| Europäische Norm                    | Internationale Norm                          | Deutsche Norm                                                   | Klassifikation im VDE-Vorschriftenwerk |
|-------------------------------------|----------------------------------------------|-----------------------------------------------------------------|----------------------------------------|
| EN 60601-1:2006                     | IEC 60601-1:2005                             | DIN EN 60601-1<br>(VDE 0750-1):2007-XX                          | VDE 0750-1                             |
| EN 60601-1-4:1996<br>+ A1:1999      | IEC 60601-1-4:1996<br>+ A1:1999              | DIN EN 60601-1-4<br>(VDE 0750-1-4):2001-04                      | VDE 0750-1-4                           |
| EN 60601-1-6:2004                   | IEC 60601-1-6:2004                           | DIN EN 60601-1-6<br>(VDE 0750-1-6):2005-06                      | VDE 0750-1-6                           |
| EN 61010-1:2001                     | IEC 61010-1:2001                             | DIN EN 61010-1<br>(VDE 0411-1):2002-08                          | VDE 0411-1                             |
| –                                   | –                                            | DIN EN 61010-1 Berichtigung 1<br>(VDE 0411-1 Berichtigung 1)    | VDE 0411-1<br>Berichtigung 1           |
| –                                   | –                                            | DIN EN 61010-1 Berichtigung 2<br>(VDE 0411-1 Berichtigung 2)    | VDE 0411-1<br>Berichtigung 2           |
| –                                   | Vorgesehener Ersatz:<br>IEC 66/333A/CD:2003  | Vorgesehener Ersatz:<br>DIN IEC 61010-1<br>(VDE 0411-1):2004-03 | VDE 0411-1                             |
| EN 61508-3:2001                     | IEC 61508-3:1998<br>+ Corrigendum :1999      | DIN EN 61508-3<br>(VDE 0803-3):2002-12                          | VDE 0803-3                             |
| –                                   | Vorgesehener Ersatz:<br>IEC 65A/469/CD:2005  | Vorgesehener Ersatz:<br>DIN IEC 61508-3<br>(VDE 0803-3):2006-07 | VDE 0803-3                             |
| –                                   | ISO/IEC Guide 51:1999                        | DIN 820-120:2001-10                                             | –                                      |
| –                                   | ISO/IEC 90003:2004                           | –                                                               | –                                      |
| –                                   | ISO/IEC 14764:1999<br>(zurückgezogen)        | –                                                               | –                                      |
| –                                   | Nachfolger:<br>ISO/IEC 14764:2006            | –                                                               | –                                      |
| –                                   | ISO/IEC 12207:1995<br>+ A1:2002<br>+ A2:2004 | –                                                               | –                                      |
| EN ISO 13485:2003                   | ISO 13485:2003                               | DIN EN ISO 13485:2003-11                                        | –                                      |
| EN ISO 14971:2000<br>+ A1:2003      | ISO 14971:2000<br>+ A1:2003                  | DIN EN ISO 14971:2001-03<br>DIN EN ISO 14971/A1:2003-10         | –                                      |
| Nachfolger:<br>prEN ISO 14971:2005  | Nachfolger:<br>ISO/DIS 14971:2005            | Nachfolger:<br>E DIN EN ISO 14971:2005-11                       | –                                      |
| EN ISO 9000:2000<br>(zurückgezogen) | ISO 9000:2000<br>(zurückgezogen)             | DIN EN ISO 9000:2000-12<br>(zurückgezogen)                      | –                                      |
| EN ISO 9000:2005                    | ISO 9000:2005                                | DIN EN ISO 9000:2005-12                                         | –                                      |
| EN ISO 9001:2000                    | ISO 9001:2000                                | DIN EN ISO 9001:2000-12                                         | –                                      |
| –                                   | IEEE 1044:1993                               | –                                                               | –                                      |
| –                                   | IEEE 610.12:1990                             | –                                                               | –                                      |

## Nationaler Anhang NB (informativ)

### Literaturhinweise

DIN 820-120, *Normungsarbeit – Teil 120: Leitfaden für die Aufnahme von Sicherheitsaspekten in Normen (ISO/IEC-Guide 51:1999)*.

**DIN EN 60601-1 (VDE 0750-1)**, *Medizinische elektrische Geräte – Teil 1: Allgemeine Festlegungen für die Sicherheit einschließlich der wesentlichen Leistungsmerkmale*.

**DIN EN 60601-1-4 (VDE 0750-1-4)**, *Medizinische elektrische Geräte – Teil 1-4: Allgemeine Festlegungen für die Sicherheit – Ergänzungsnorm: Programmierbare elektrische medizinische Systeme (IEC 60601-1-4:1996 + A1:1999); Deutsche Fassung EN 60601-1-4:1996 + A1:1999*.

**DIN EN 60601-1-6 (VDE 0750-1-6)**, *Medizinische elektrische Geräte – Teil 1-6: Allgemeine Festlegungen für die Sicherheit – Ergänzungsnorm: Gebrauchstauglichkeit (IEC 60601-1-6:2004); Deutsche Fassung EN 60601-1-6:2004*.

**DIN EN 61010-1 (VDE 0411-1)**, *Sicherheitsbestimmungen für elektrische Mess-, Steuer-, Regel- und Laborgeräte – Teil 1: Allgemeine Anforderungen (IEC 61010-1:2001); Deutsche Fassung EN 61010-1:2001*.

**DIN EN 61010-1 Berichtigung 1 (VDE 0411-1 Berichtigung 1)**.

**DIN EN 61010-1 Berichtigung 2 (VDE 0411-1 Berichtigung 2)**.

**DIN EN 61508-3 (VDE 0803-3)**, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 3: Anforderungen an Software (IEC 61508-3:1998 + Corrigendum 1999); Deutsche Fassung EN 61508-3:2001*.

DIN EN ISO 9000, *Qualitätsmanagementsysteme – Grundlagen und Begriffe (ISO 9000:2005); Dreisprachige Fassung EN ISO 9000:2005*.

DIN EN ISO 9000, *Qualitätsmanagementsysteme – Grundlagen und Begriffe (ISO 9000:2000); Dreisprachige Fassung EN ISO 9000:2000 (zurückgezogen)*.

DIN EN ISO 9001, *Qualitätsmanagementsysteme – Anforderungen (ISO 9001:2000); Dreisprachige Fassung EN ISO 9001:2000*.

DIN EN ISO 13485, *Medizinprodukte – Qualitätsmanagementsysteme – Anforderungen für regulatorische Zwecke (ISO 13485:2003); Deutsche Fassung EN ISO 13485:2003*.

DIN EN ISO 14971, *Medizinprodukte – Anwendung des Risikomanagements auf Medizinprodukte (ISO 14971:2000); Deutsche Fassung EN ISO 14971:2000*.

DIN EN ISO 14971/A1, *Medizinprodukte – Anwendung des Risikomanagements auf Medizinprodukte – Änderung 1: Begründung der Anforderungen (ISO 14971:2000/AMD 1:2003); Deutsche Fassung EN ISO 14971:2001/A1:2003*.

E DIN EN ISO 14971, *Medizinprodukte – Anwendung des Risikomanagements auf Medizinprodukte (ISO/DIS 14971:2005); Deutsche Fassung prEN ISO 14971:2005*.

E DIN IEC 61010-1 (VDE 0411-1), *Sicherheitsbestimmungen für elektrische Mess-, Steuer-, Regel- und Laborgeräte – Teil 1: Allgemeine Anforderungen (IEC 66/333A/CD:2003)*.

E DIN IEC 61508-3 (VDE 0803-3), *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 3: Anforderungen an Software (IEC 65A/469/CD:2005)*.

**Medizingeräte-Software –  
Software-Lebenszyklus-Prozesse**  
(IEC 62304:2006)

Medical device software –  
Software life-cycle processes  
(IEC 62304:2006)

Logiciels de dispositifs médicaux –  
Processus du cycle de vie du logiciel  
(CEI 62304:2006)

Diese Europäische Norm wurde von CENELEC am 2006-06-01 angenommen. Die CENELEC-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist.

Auf dem letzten Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim Zentralsekretariat oder bei jedem CENELEC-Mitglied auf Anfrage erhältlich.

Diese Europäische Norm besteht in drei offiziellen Fassungen (Deutsch, Englisch, Französisch). Eine Fassung in einer anderen Sprache, die von einem CENELEC-Mitglied in eigener Verantwortung durch Übersetzung in seine Landessprache gemacht und dem Zentralsekretariat mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

CENELEC-Mitglieder sind die nationalen elektrotechnischen Komitees von Belgien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, der Schweiz, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, Ungarn, dem Vereinigten Königreich und Zypern.

## CENELEC

Europäisches Komitee für Elektrotechnische Normung  
European Committee for Electrotechnical Standardization  
Comité Européen de Normalisation Electrotechnique

**Zentralsekretariat: rue de Stassart 35, B-1050 Brüssel**

© 2006 CENELEC – Alle Rechte der Verwertung, gleich in welcher Form und in welchem Verfahren, sind weltweit den Mitgliedern von CENELEC vorbehalten.

Ref. Nr. EN 62304:2006 D

## Vorwort

Der Text des Schriftstücks 62A/523/FDIS, zukünftige 1. Ausgabe von IEC 62304, wurde von einer gemeinsamen Arbeitsgruppe zwischen SC 62A „Überarbeitung und Anpassung der allgemeinen Bestimmungen“ des IEC Technischen Komitees TC 62 „Allgemeine Bestimmungen für elektrische Einrichtungen in medizinischer Anwendung“ und dem ISO Technischen Komitee ISO TC 210 „Qualitätsmanagement und allgemeine Aspekte für Medizinprodukte“ ausgearbeitet. Dieser Text wurde der IEC-CENELEC Parallelen Abstimmung unterworfen und von CENELEC am 2006-06-01 als EN 62304 angenommen.

Nachstehende Daten wurden festgelegt:

- spätestes Datum, zu dem die EN auf nationaler Ebene durch Veröffentlichung einer identischen nationalen Norm oder durch Anerkennung übernommen werden muss (dop): 2007-03-01
- spätestes Datum, zu dem nationale Normen, die der EN entgegenstehen, zurückgezogen werden müssen (dow): 2009-06-01

In dieser Norm werden die folgenden Schriftarten verwendet:

- Festlegungen und Definitionen: Normalschrift;
- Informationen außerhalb von Tabellen, wie Anmerkungen und Referenzen, in Kleinschrift. Normativer Text von Tabellen: Kleinschrift;
- IN DIESER NORM BENUTZTE BEGRIFFE, DIE IN ABSCHNITT 3 DEFINIERT SIND UND IM VERZEICHNIS DER DEFINIERTEN BEGRIFFE ANGEZEIGT SIND: KAPITÄLCHEN.

Ein Stern (\*) am ersten Buchstaben einer Überschrift oder am Anfang eines Abschnittes bedeutet, dass erklärende Hinweise in Anhang B gegeben werden.

Tabelle C.5 wurde von ISO/IEC JTC 1/SC 7, Software und System-Engineering, erstellt.

Der Anhang ZA wurde von CENELEC hinzugefügt.

## Anerkennungsnotiz

Der Text der Internationalen Norm IEC 62304:2006 wurde von CENELEC ohne irgendeine Abänderung als Europäische Norm angenommen.

In der offiziellen Fassung sind unter „Literaturhinweise“ zu den aufgelisteten Normen die nachstehenden Anmerkungen einzutragen:

|                    |           |                                                                   |
|--------------------|-----------|-------------------------------------------------------------------|
| IEC 60601-1-4 + A1 | ANMERKUNG | Harmonisiert als EN 60601-1-4:1996 + A1:1999 (nicht modifiziert). |
| IEC 61508-3        | ANMERKUNG | Harmonisiert als EN 61508-3:2001 (nicht modifiziert).             |
| IEC 61010-1        | ANMERKUNG | Harmonisiert als EN 61010-1:2001 (nicht modifiziert).             |
| ISO 9000           | ANMERKUNG | Harmonisiert als EN ISO 9000:2005 (nicht modifiziert).            |
| ISO 9001           | ANMERKUNG | Harmonisiert als EN ISO 9001:2000 (nicht modifiziert).            |
| ISO 13485          | ANMERKUNG | Harmonisiert als EN ISO 13485:2003 (nicht modifiziert).           |
| IEC 60601-1-6      | ANMERKUNG | Harmonisiert als EN 60601-1-6:2004 (nicht modifiziert).           |

## Inhalt

|                                                                         | Seite |
|-------------------------------------------------------------------------|-------|
| Vorwort.....                                                            | 2     |
| Einführung.....                                                         | 5     |
| 1 Geltungsbereich .....                                                 | 9     |
| 1.1 *Zweck .....                                                        | 9     |
| 1.2 *Anwendungsbereich.....                                             | 9     |
| 1.3 Beziehung zu anderen Normen.....                                    | 9     |
| 1.4 Einhaltung.....                                                     | 9     |
| 2 *Normative Verweisungen .....                                         | 9     |
| 3 Begriffe .....                                                        | 10    |
| 4 *Allgemeine Anforderungen.....                                        | 15    |
| 4.1 *Qualitätsmanagement-System.....                                    | 15    |
| 4.2 *RISIKOMANAGEMENT .....                                             | 15    |
| 4.3 *Software-Sicherheitsklassifizierung .....                          | 15    |
| 5 Software-Entwicklungs-PROZESS.....                                    | 16    |
| 5.1 *Planung der Software-Entwicklung .....                             | 16    |
| 5.2 *Analyse der Software-Anforderungen.....                            | 19    |
| 5.3 *Design der Software-ARCHITEKTUR .....                              | 21    |
| 5.4 *Detailliertes Software-Design.....                                 | 22    |
| 5.5 *Implementierung und VERIFIZIERUNG der SOFTWARE-EINHEITEN .....     | 22    |
| 5.6 *Software-Integration und -Integrationsprüfung .....                | 23    |
| 5.7 *Prüfung des SOFTWARE-SYSTEMS .....                                 | 24    |
| 5.8 *Software-Freigabe.....                                             | 25    |
| 6 Software-Wartungs-PROZESS .....                                       | 26    |
| 6.1 *Festlegung eines Plans für die Software-Wartung .....              | 26    |
| 6.2 *Analyse von Problemen und Änderungen .....                         | 27    |
| 6.3 *Implementierung von Änderungen.....                                | 28    |
| 7 *Software-RISIKOMANAGEMENT-PROZESS .....                              | 28    |
| 7.1 *Analyse von Software, die zu Gefährdungssituationen beiträgt ..... | 28    |
| 7.2 RISIKOKONTROLL-Maßnahmen .....                                      | 29    |
| 7.3 VERIFIZIERUNG von RISIKOKONTROLL-Maßnahmen.....                     | 30    |
| 7.4 RISIKOMANAGEMENT von Software-Änderungen.....                       | 30    |
| 8 *Software-Konfigurationsmanagement-PROZESS .....                      | 31    |
| 8.1 *Identifizierung der Konfiguration .....                            | 31    |
| 8.2 *Änderungskontrolle .....                                           | 31    |
| 8.3 *Aufzeichnungen über den Status der Konfiguration .....             | 32    |
| 9 *Problemlösungs-PROZESS für Software .....                            | 32    |
| 9.1 Erstellen von PROBLEMBERICHTEN.....                                 | 32    |
| 9.2 Untersuchung des Problems .....                                     | 32    |

|                                                                                                                                          | Seite |
|------------------------------------------------------------------------------------------------------------------------------------------|-------|
| 9.3 Unterrichtung beteiligter Stellen.....                                                                                               | 33    |
| 9.4 Anwendung des Änderungskontroll-PROZESSES.....                                                                                       | 33    |
| 9.5 Aufbewahrung von Aufzeichnungen.....                                                                                                 | 33    |
| 9.6 Analyse von Problemen hinsichtlich Trends.....                                                                                       | 33    |
| 9.7 VERIFIZIERUNG der Lösung von Software-Problemen .....                                                                                | 33    |
| 9.8 Inhalt von Prüfungsdokumentation .....                                                                                               | 33    |
| Anhang A (informativ) Begründung für die Anforderungen dieser Norm .....                                                                 | 35    |
| Anhang B (informativ) Anleitung für die Bestimmungen dieser Norm .....                                                                   | 38    |
| Anhang C (informativ) Beziehung zu anderen Normen .....                                                                                  | 52    |
| Anhang D (informativ) Implementierung .....                                                                                              | 74    |
| Literaturhinweise .....                                                                                                                  | 76    |
| Stichwortverzeichnis der definierten Begriffe deutsch-englisch.....                                                                      | 77    |
| Stichwortverzeichnis der definierten Begriffe englisch-deutsch.....                                                                      | 78    |
| Anhang ZA (normativ) Normative Verweisungen auf internationale Publikationen mit ihren<br>entsprechenden europäischen Publikationen..... | 79    |
| <b>Bilder</b>                                                                                                                            |       |
| Bild 1 – Überblick über Software-Entwicklungs-PROZESSE und -AKTIVITÄTEN .....                                                            | 6     |
| Bild 2 – Überblick über Software-Wartungs-PROZESSE und -AKTIVITÄTEN .....                                                                | 7     |
| Bild B.1 – Beispiel einer Aufteilung von SOFTWARE-KOMPONENTEN .....                                                                      | 42    |
| Bild C.1 – Beziehung von wichtigen MEDIZINPRODUKTE-Normen zur IEC 62304.....                                                             | 53    |
| Bild C.2 – Software als Teil des V-Modells .....                                                                                         | 56    |
| Bild C.3 – Anwendung von IEC 62304 mit IEC 61010-1 .....                                                                                 | 66    |
| <b>Tabellen</b>                                                                                                                          |       |
| Tabelle A.1 – Zusammenfassung der Anforderungen nach Software-Sicherheitsklassen .....                                                   | 37    |
| Tabelle B.1 – Entwicklungs-(Modell-)Strategien wie in ISO/IEC 12207 definiert .....                                                      | 39    |
| Tabelle C.1 – Beziehung zu ISO 13485:2003.....                                                                                           | 53    |
| Tabelle C.2 – Beziehung zu ISO 14971:2000.....                                                                                           | 54    |
| Tabelle C.3 – Beziehung zur IEC 60601-1 .....                                                                                            | 57    |
| Tabelle C.4 – Beziehung zur IEC 60601-1-4 .....                                                                                          | 63    |
| Tabelle C.5 – Beziehung zu ISO/IEC 12207.....                                                                                            | 67    |
| Tabelle D.1 – Checkliste für kleine Firmen ohne zertifiziertes QM-SYSTEM .....                                                           | 75    |

## Einführung

Software ist oft ein integraler Bestandteil der MEDIZINPRODUKTE-Technik. Um die SICHERHEIT und Wirksamkeit eines MEDIZINPRODUKTS, das Software enthält, herzustellen, bedarf es der Kenntnis darüber, was die Software bewirken soll, und des Nachweises darüber, dass die Software diese Wirkung erzielt, ohne unvermeidbare RISIKEN zu verursachen.

Diese Norm stellt einen Rahmen von Lebenszyklus-PROZESSEN mit AKTIVITÄTEN und AUFGABEN bereit, der für den sicheren Entwurf und eine sichere Wartung von MEDIZINPRODUKTE-SOFTWARE erforderlich ist. Diese Norm stellt Anforderungen für jeden Lebenszyklus-PROZESS bereit. Jeder Lebenszyklus-PROZESS ist weiter unterteilt in einen Satz von AKTIVITÄTEN, wobei die meisten AKTIVITÄTEN weiter unterteilt sind in einen Satz von AUFGABEN.

Als Voraussetzung wird angenommen, dass MEDIZINPRODUKTE-SOFTWARE innerhalb eines Qualitätsmanagement-SYSTEMS (siehe [4.1](#)) und eines RISIKOMANAGEMENT-Systems (siehe [4.2](#)) entwickelt und gewartet wird. Der RISIKOMANAGEMENT-PROZESS ist bereits sehr gut durch die Internationale Norm ISO 14971 abgedeckt. Diesen Vorteil nutzt die IEC 62304, indem sie einen normativen Verweis auf die ISO 14971 verwendet. Einige zusätzliche RISIKOMANAGEMENT-Anforderungen werden für Software benötigt, insbesondere wenn es darum geht, Software-Faktoren zu identifizieren, die zu GEFÄHRDUNGEN beitragen können. Diese Anforderungen werden zusammengefasst und in [Abschnitt 7](#) als Software-RISIKOMANAGEMENT-PROZESS festgehalten.

Ob Software ein Faktor ist, der zu einer GEFÄHRDUNG beiträgt, wird durch die AKTIVITÄT der GEFÄHRDUNG-Identifikation innerhalb des RISIKOMANAGEMENT-PROZESSES ermittelt. GEFÄHRDUNGEN, die indirekt durch Software verursacht werden könnten (zum Beispiel durch Bereitstellung irreführender Informationen, die die Anwendung einer unangemessenen Behandlung verursachen könnte), müssen betrachtet werden, wenn ermittelt wird, ob die Software einen maßgeblichen Einfluss hat. Die Entscheidung, Software zur RISIKOBEHERRSCHUNG einzusetzen, wird während der AKTIVITÄT der RISIKOBEHERRSCHUNG innerhalb des RISIKOMANAGEMENT-PROZESSES getroffen. Der von dieser Norm geforderte Software-RISIKOMANAGEMENT-PROZESS muss in den Geräte-RISIKOMANAGEMENT-PROZESS nach ISO 14971 eingebunden sein.

Der Software-Entwicklungs-PROZESS besteht aus einer Anzahl von AKTIVITÄTEN. Diese AKTIVITÄTEN sind in [Bild 1](#) dargestellt und in [Abschnitt 5](#) beschrieben. Weil viele Vorkommnisse im Feld mit dem Service oder der Wartung von medizinischen SYSTEMEN im Zusammenhang stehen, einschließlich unsachgemäßer Software-Updates und Software-Upgrades, wird der Software-Wartungs-PROZESS als ebenso wichtig erachtet wie der Software-Entwicklungs-PROZESS. Der Software-Wartungs-PROZESS ist dem Software-Entwicklungs-PROZESS sehr ähnlich. Er ist in [Bild 2](#) dargestellt und in [Abschnitt 6](#) beschrieben.

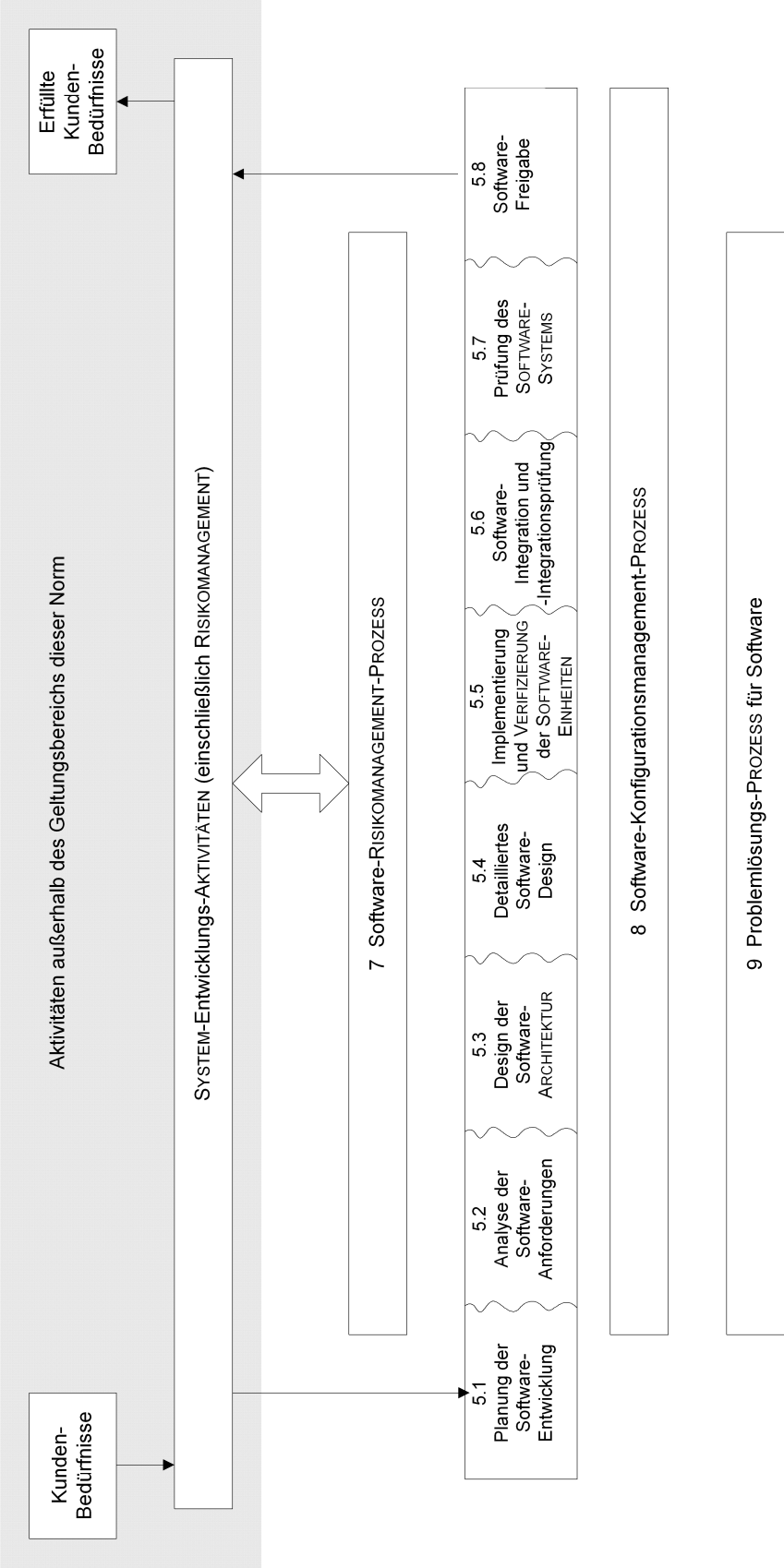


Bild 1 – Überblick über Software-Entwicklungs-Prozesse und -AKTIVITÄTEN

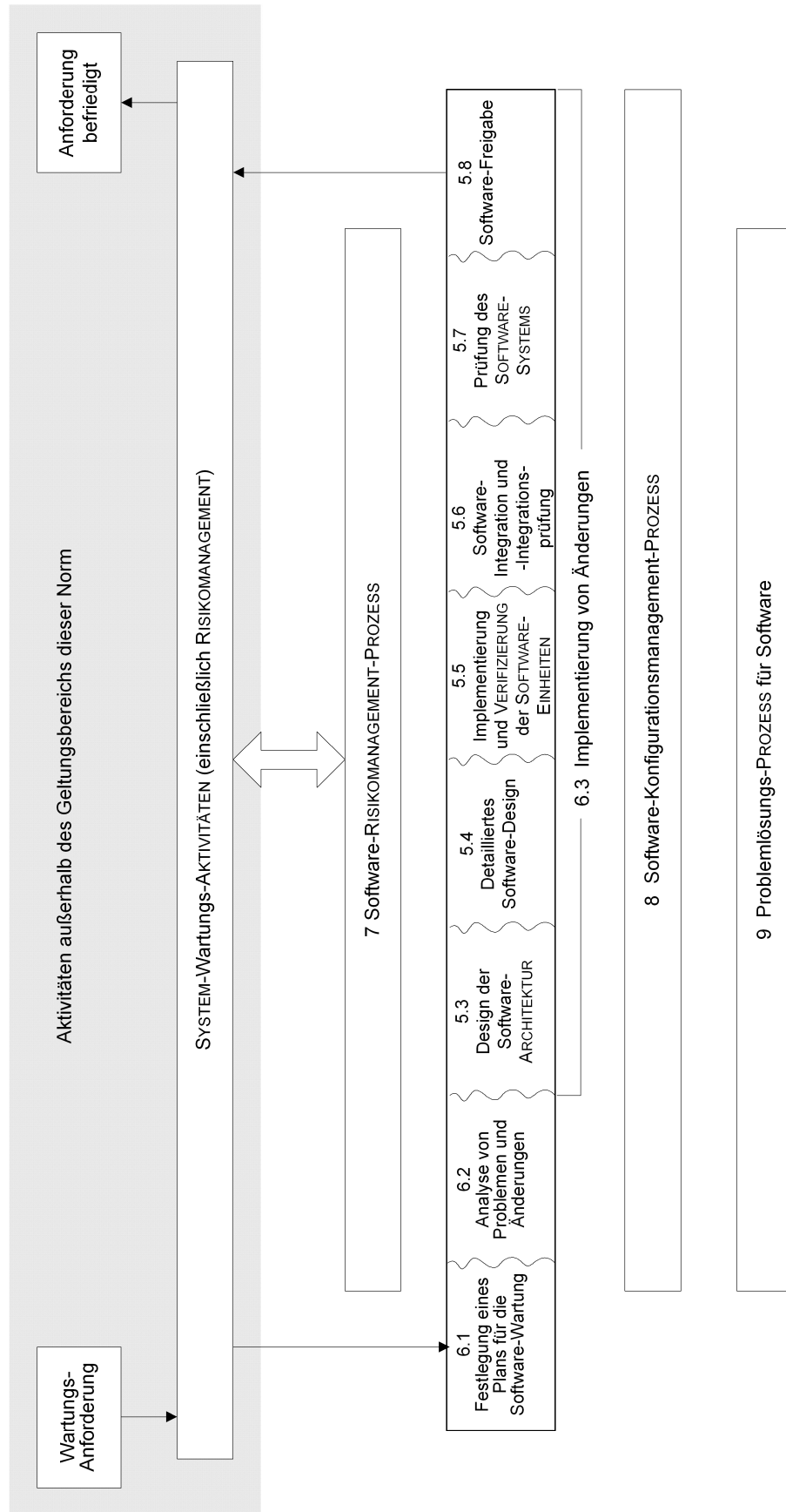


Bild 2 – Überblick über Software-Wartungs-Prozesse und -AKTIVITÄTEN

Die Norm identifiziert zwei zusätzliche PROZESSE, die für die Entwicklung von sicherer MEDIZINPRODUKTE-SOFTWARE als wesentlich betrachtet werden. Dies sind der Software-Konfigurations-Management-PROZESS ([Abschnitt 8](#)) und der Problemlösungs-PROZESS für Software ([Abschnitt 9](#)).

Diese Norm schreibt dem HERSTELLER keine Organisationsstruktur vor oder welcher Teil der Organisation welchen PROZESS, welche AKTIVITÄT oder welche AUFGABE durchführen soll. Diese Norm fordert nur, dass der PROZESS, die AKTIVITÄT oder die AUFGABE durchgeführt wird, um die Einhaltung dieser Norm nachzuweisen.

Diese Norm macht keine Vorgaben für die Bezeichnung, das Format oder den expliziten Inhalt der Dokumentation, die zu erstellen ist. Diese Norm erfordert eine Dokumentation der AUFGABEN, aber die Entscheidung, wie diese Dokumentation gestaltet wird, wird dem Benutzer der Norm überlassen.

Diese Norm schreibt kein spezifisches Lebenszyklus-Modell vor. Die Anwender dieser Norm sind verantwortlich für die Auswahl eines Lebenszyklus-Modells für das Software-Projekt und für das Abbilden der PROZESSE, AKTIVITÄTEN und AUFGABEN dieser Norm auf dieses Modell.

[Anhang A](#) enthält die Begründung für die Abschnitte dieser Norm, [Anhang B](#) eine Anleitung für die Umsetzung dieser Norm.

Für diese Norm gilt:

- „muss“ bedeutet, dass die Erfüllung einer Anforderung zwingend ist für die Einhaltung dieser Norm;
- „soll“ bedeutet, dass die Erfüllung einer Anforderung empfohlen wird, aber nicht zwingend ist für die Einhaltung dieser Norm;
- „kann“ wird benutzt, um einen möglichen Weg zu beschreiben, wie die Erfüllung einer Anforderung zu erreichen ist;
- „festlegen“ bedeutet: definieren, dokumentieren und implementieren.
- Wenn diese Norm den Begriff „soweit angemessen“ im Zusammenhang mit einem erforderlichen PROZESS, einer AKTIVITÄT, einer AUFGABE oder einem Ergebnis benutzt, dann bedeutet das, dass der HERSTELLER diesen PROZESS, diese AKTIVITÄT, diese AUFGABE oder dieses Ergebnis benutzen muss, es sei denn, der HERSTELLER kann eine Rechtfertigung dafür dokumentieren, warum er dies unterlässt.

# 1 Geltungsbereich

## 1.1 \*Zweck

Diese Norm definiert Anforderungen an den Lebenszyklus von MEDIZINPRODUKTE-SOFTWARE. Die Zusammenstellung von PROZESSEN, AKTIVITÄTEN und AUFGABEN, die in dieser Norm beschrieben werden, legt einen allgemeinen Rahmen für Lebenszyklus-PROZESSE von MEDIZINPRODUKTE-SOFTWARE fest.

## 1.2 \*Anwendungsbereich

Diese Norm gilt für die Entwicklung und Wartung von MEDIZINPRODUKTE-SOFTWARE.

Diese Norm gilt für die Entwicklung und Wartung von MEDIZINPRODUKTE-SOFTWARE, wenn die Software selbst ein MEDIZINPRODUKT ist oder wenn die Software ein eingebetteter oder integraler Bestandteil des fertigen MEDIZINPRODUKTS ist.

Diese Norm deckt nicht Validierung und abschließende Freigabe des MEDIZINPRODUKTS ab, auch dann nicht, wenn das MEDIZINPRODUKT gänzlich aus Software besteht.

## 1.3 Beziehung zu anderen Normen

Diese MEDIZINPRODUKTE-SOFTWARE-Lebenszyklus-Norm soll zusammen mit anderen geeigneten Normen benutzt werden, wenn ein MEDIZINPRODUKT entwickelt wird. [Anhang C](#) stellt die Beziehung zwischen dieser Norm und anderen relevanten Normen her.

## 1.4 Einhaltung

Die Einhaltung dieser Norm gilt als erfüllt, wenn alle PROZESSE, AKTIVITÄTEN und AUFGABEN, die in dieser Norm im Bezug auf die Software-Sicherheitsklasse festgelegt sind, implementiert wurden.

ANMERKUNG 1 Jeder Anforderung sind Software-Sicherheitsklassen zugeordnet. Die Angabe der Software-Sicherheitsklassen steht im normativen Abschnitt hinter der entsprechenden Anforderung.

Die Einhaltung wird durch das Besichtigen der gesamten Dokumentation festgestellt, die von dieser Norm gefordert wird, einschließlich der RISIKOMANAGEMENT-AKTE, und durch die Beurteilung der PROZESSE, AKTIVITÄTEN und AUFGABEN, die für die entsprechende Software-Sicherheitsklasse gefordert werden. Siehe [Anhang D](#).

ANMERKUNG 2 Diese Beurteilung kann durch ein internes oder externes Audit durchgeführt werden.

ANMERKUNG 3 Bei der Ausführung der festgelegten PROZESSE, AKTIVITÄTEN und AUFGABEN bestehen Freiheitsgrade in der Auswahl der Methoden zur Implementierung dieser PROZESSE und der Ausführung dieser AKTIVITÄTEN und AUFGABEN.

ANMERKUNG 4 Für diese Beurteilung ist an den Stellen, an denen bestimmte Anforderungen den Zusatz „soweit angemessen“ enthalten und nicht erfüllt werden, eine Begründung zu dokumentieren.

ANMERKUNG 5 An den Stellen, an denen die ISO/IEC 12207 den Begriff „Übereinstimmung“ verwendet, wird in dieser Norm der Begriff „Einhaltung“ verwendet.

# 2 \*Normative Verweisungen

Die folgenden zitierten Dokumente sind für die Anwendung dieses Dokuments erforderlich. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

ISO 14971, *Medical devices – Application of risk management to medical devices*

### 3 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

#### 3.1

##### **AKTIVITÄT**

Satz von einer oder mehreren aufeinander bezogenen oder sich gegenseitig beeinflussenden AUFGABEN

#### 3.2

##### **ANOMALIE**

jeglicher Zustand, der abweicht von dem, was auf Grund von Anforderungsspezifikationen, Entwicklungsdokumenten, Normen usw. oder von Wahrnehmungen oder Erfahrungen zu erwarten ist. ANOMALIEN können sich unter anderem beim Review, bei der Prüfung, der Analyse, der Kompilierung oder bei der Benutzung von SOFTWARE-PRODUKTEN oder zugehöriger Dokumentation finden.

[IEEE 1044:1993, Definition 3.1], [14]<sup>N1)</sup>

#### 3.3

##### **ARCHITEKTUR**

Organisationsstruktur eines SYSTEMS oder einer Komponente

[IEEE 610.12:1990], [13]<sup>N1)</sup>

#### 3.4

##### **ÄNDERUNGSANFORDERUNG**

dokumentierte Spezifikation einer Änderung, die an einem SOFTWARE-PRODUKT durchgeführt werden soll

#### 3.5

##### **KONFIGURATIONSELEMENT**

Einheit, die an einem gegebenen Referenzpunkt eindeutig identifiziert werden kann

ANMERKUNG Basierend auf ISO/IEC 12207:1995, Definition 3.6 [9]<sup>N1)</sup>.

#### 3.6

##### **ZU LIEFERNDEN ERGEBNIS**

gefordertes Resultat oder Ergebnis (einschließlich Dokumentation) einer AKTIVITÄT oder AUFGABE

#### 3.7

##### **EVALUATION**

systematische Bewertung oder Beurteilung, inwieweit eine Einheit ihre festgelegten Merkmale erfüllt.

[ISO/IEC 12207:1995, Definition 3.9], [9]<sup>N1)</sup>

#### 3.8

##### **SCHADEN**

physische Verletzung oder Schädigung der Gesundheit von Menschen oder Schädigung von Gütern oder der Umwelt

[ISO/IEC Guide 51:1999, Definition 3.3], [12]<sup>N1)</sup>

#### 3.9

##### **GEFÄHRDUNG**

potentielle Quelle eines SCHADENS

[ISO/IEC Guide 51:1999, Definition 3.5], [12]<sup>N1)</sup>

---

<sup>N1)</sup> Nationale Fußnote: Der Verweis zu den Literaturhinweisen fehlt in der Internationalen Norm.

### 3.10

#### HERSTELLER

natürliche oder juristische Person, die für die Auslegung, Herstellung, Verpackung oder Kennzeichnung eines MEDIZINPRODUKTS, für den Zusammenbau eines SYSTEMS oder für die Anpassung eines MEDIZINPRODUKTS vor dem Inverkehrbringen oder der Inbetriebnahme verantwortlich ist, unabhängig davon, ob diese Tätigkeiten von dieser Person selbst oder stellvertretend für diese von einer dritten Person ausgeführt werden

[ISO 14971:2000, Definition 2.6]

### 3.11

#### MEDIZINPRODUKT

alle einzeln oder miteinander verbunden verwendeten Instrumente, Apparate, Vorrichtungen, Stoffe oder anderen Gegenstände einschließlich der für ein einwandfreies Funktionieren des MEDIZINPRODUKTS eingesetzten Software, die vom HERSTELLER zur Anwendung für Menschen für folgende Zwecke bestimmt sind:

- Erkennung, Verhütung, Erfassen, Behandlung oder Linderung von Krankheiten,
- Erkennung, Erfassung, Behandlung, Linderung oder Kompensierung von Verletzungen oder Behinderungen,
- Untersuchung, Ersatz oder Veränderung des anatomischen Aufbaus oder eines physiologischen Vorgangs,
- Lebenserhaltung oder Lebensunterstützung,
- Empfängnisregelung,
- Desinfektion von MEDIZINPRODUKTEN,
- Bereitstellung von Informationen für medizinische Zwecke mittels In-vitro-Untersuchung von Probestücken des menschlichen Körpers,

und deren bestimmungsgemäße Hauptwirkung im oder am menschlichen Körper weder durch pharmakologische noch durch immunologische oder metabolische Mittel erreicht wird, deren Wirkungsweise aber durch solche Mittel unterstützt werden kann

ANMERKUNG 1 Diese Definition wurde durch die Global Harmonization Task Force (GHTF) entwickelt. Siehe Literaturhinweis [15] in ISO 13485:2003.

[ISO 13485:2003, Definition 3.7], [7]<sup>N2)</sup>

ANMERKUNG 2 In den Definitionen, wie sie in den nationalen Regularien des jeweiligen Landes verwendet werden, können Unterschiede auftreten.

### 3.12

#### MEDIZINPRODUKTE-SOFTWARE

ein SOFTWARE-SYSTEM, das entwickelt wurde, um in das in der Entwicklung befindliche MEDIZINPRODUKT integriert zu werden, oder das für die Benutzung als selbständiges MEDIZINPRODUKT vorgesehen ist

### 3.13

#### PROBLEMBERICHT

Aufzeichnung über ein tatsächliches oder mögliches Verhalten eines SOFTWARE-PRODUKTS, von dem ein Anwender oder eine andere beteiligte Person glaubt, dass es unsicher, ungeeignet für den bestimmungsgemäßen Gebrauch oder widersprüchlich zur Spezifikation sei

ANMERKUNG 1 Diese Norm fordert nicht, dass jeder PROBLEMBERICHT zu einer Änderung des SOFTWARE-PRODUKTS führt. Ein HERSTELLER kann einen PROBLEMBERICHT als Missverständnis, als Fehler oder als unbedeutendes Ereignis ablehnen.

<sup>N2)</sup> Nationale Fußnote: Der Verweis zu den Literaturhinweisen fehlt in der Internationalen Norm.

ANMERKUNG 2 Ein PROBLEMBERICHT kann sich auf ein freigegebenes SOFTWARE-PRODUKT oder auf ein noch in der Entwicklung befindliches SOFTWARE-PRODUKT beziehen.

ANMERKUNG 3 Diese Norm fordert vom HERSTELLER, dass er für einen PROBLEMBERICHT, der sich auf ein freigegebenes Produkt bezieht, besondere Entscheidungen trifft (siehe [Abschnitt 6](#)) um zu gewährleisten, dass regulatorische Maßnahmen identifiziert und implementiert werden.

### **3.14**

#### **PROZESS**

Satz von in Wechselbeziehung oder Wechselwirkung stehenden AKTIVITÄTEN, der Eingaben in Ergebnisse umwandelt  
[ISO 9000:2000, Definition 3.4.1]

ANMERKUNG Der Begriff „AKTIVITÄTEN“ beinhaltet den Gebrauch von Ressourcen.

### **3.15**

#### **REGRESSIONSPRÜFUNG**

Prüfung, die erforderlich ist um festzustellen, dass eine Änderung einer SYSTEM-Komponente deren Funktionalität, Zuverlässigkeit und Leistungsfähigkeit nicht beeinträchtigt und keine zusätzlichen Defekte verursacht hat

[ISO/IEC 90003:2004, Definition 3.11], [\[11\]](#)<sup>N3)</sup>

### **3.16**

#### **RISIKO**

Kombination der Wahrscheinlichkeit des Auftretens eines SCHADENS und des Schweregrades dieses SCHADENS

[ISO/IEC Guide 51:1999, Definition 3.2], [\[12\]](#)<sup>N3)</sup>

### **3.17**

#### **RISIKOANALYSE**

systematische Auswertung verfügbarer Informationen, um GEFÄHRDUNGEN zu identifizieren und RISIKEN abzuschätzen

[ISO/IEC Guide 51:1999, Definition 3.10], [\[12\]](#)<sup>N3)</sup>

### **3.18**

#### **RISIKOBEHERRSCHUNG**

PROZESS, in dem Entscheidungen getroffen und RISIKEN auf festgelegte Grenzen reduziert oder in diesen gehalten werden

[ISO 14971:2000, Definition 2.16, modifiziert]<sup>N4)</sup>

### **3.19**

#### **RISIKOMANAGEMENT**

systematische Anwendung von Managementgrundsätzen, Verfahren und Praktiken auf die Analyse, Bewertung und Kontrolle von RISIKEN

[ISO 14971:2000, Definition 2.18]

---

<sup>N3)</sup> Nationale Fußnote: Der Verweis zu den Literaturhinweisen fehlt in der Internationalen Norm.

<sup>N4)</sup> Nationale Fußnote: Der Begriff wurde zur besseren Verständlichkeit von „Risikokontrolle“ auf „Risikobeherrschung“ geändert. In der neuen Ausgabe von DIN EN ISO 14971:2006 wird dieser Begriff ebenfalls verwendet.

**3.20****RISIKOMANAGEMENT-AKTE**

Zusammenstellung von Aufzeichnungen und sonstigen Dokumenten, die durch den RISIKOMANAGEMENT-PROZESS erzeugt werden und nicht notwendigerweise an einer Stelle sein müssen

[ISO 14971:2000, Definition 2.19]

**3.21****SICHERHEIT**

Freiheit von unvertretbaren RISIKEN

[ISO/IEC Guide 51:1999, Definition 3.1], [12]<sup>N5)</sup>

**3.22****DATENSICHERHEIT**

Schutz von Informationen und Daten derart, dass nicht autorisierte Personen oder SYSTEME sie nicht lesen oder verändern können und dass autorisierten Personen und SYSTEMEN der Zugang zu ihnen nicht verweigert wird

[ISO/IEC 12207:1995, Definition 3.25], [9]<sup>N5)</sup>

**3.23****SCHWERE VERLETZUNG**

Verletzung oder Krankheit, die direkt oder indirekt

- a) lebensbedrohend ist,
- b) zu einer andauernden Beeinträchtigung einer Körperfunktion oder zu einer andauernden Schädigung des (menschlichen) Körpers führt oder
- c) ein medizinisches oder chirurgisches Eingreifen erfordert, um eine andauernde Beeinträchtigung einer Körperfunktion oder eine andauernde Schädigung des (menschlichen) Körpers zu verhindern

ANMERKUNG Andauernde Beeinträchtigung bedeutet eine unumkehrbare Beeinträchtigung oder Schädigung des (menschlichen) Körpers oder einer Körperfunktion und schließt geringfügige Beeinträchtigungen oder Schädigungen aus.

**3.24****LEBENSZYKLUS-MODELL DER SOFTWARE-ENTWICKLUNG**

konzeptionelle Struktur, welche die Lebenszeit der Software von der Anforderungsdefinition bis zur Freigabe für die Produktion umfasst und die

- die PROZESSE, AKTIVITÄTEN und AUFGABEN festlegt, die an der Entwicklung eines SOFTWARE-PRODUKTS beteiligt sind,
- die Reihenfolge und die Abhängigkeit von AKTIVITÄTEN und AUFGABEN beschreibt und
- die Meilensteine festlegt, bei denen die Vollständigkeit der festgelegten ZU LIEFERNDEN ERGEBNISSE verifiziert wird

ANMERKUNG Basierend auf ISO/IEC 12207:1995, Definition 3.11 [9]<sup>N5)</sup>

**3.25****SOFTWARE-KOMPONENTE**

jedes identifizierbare Teil eines Computerprogramms

[ISO/IEC 90003:2004, Definition 3.14], [11]<sup>N5)</sup>.

ANMERKUNG Drei Begriffe kennzeichnen die Zerlegung der Software in einzelne Bestandteile. Die oberste Ebene bildet das SOFTWARE-SYSTEM. Die niedrigste Ebene, die nicht weiter zerlegt wird, ist die SOFTWARE-EINHEIT. Alle Ebenen, die Bestandteile vereinen, einschließlich der höchsten und niedersten Ebene, können als SOFTWARE-KOMPONENTEN bezeichnet werden. Ein SOFTWARE-SYSTEM ist folglich zusammengesetzt aus einer oder mehreren SOFTWARE-KOMPONENTEN, und jede SOFTWARE-KOMPONENTE ist zusammengesetzt aus einer oder mehreren SOFTWARE-EINHEITEN

<sup>N5)</sup> Nationale Fußnote: Der Verweis zu den Literaturhinweisen fehlt in der Internationalen Norm.

oder zerlegbaren SOFTWARE-KOMPONENTEN. Es ist der Verantwortung des HERSTELLERS überlassen, die Definition und die Unterteilung der SOFTWARE-KOMPONENTEN und SOFTWARE-EINHEITEN festzulegen.

### 3.26

#### **SOFTWARE-PRODUKT**

Satz von Computerprogrammen, Prozeduren und möglicherweise zugeordneten Dokumentationen und Daten

[ISO/IEC 12207:1995, Definition 3.26], [9]<sup>N6)</sup>

### 3.27

#### **SOFTWARE-SYSTEM**

integrierte Sammlung von SOFTWARE-KOMPONENTEN, die so organisiert sind, dass eine spezifische Funktion oder ein Satz von Funktionen ausgeführt werden kann

### 3.28

#### **SOFTWARE-EINHEIT**

SOFTWARE-KOMPONENTE, die nicht in weitere Komponenten unterteilt ist

ANMERKUNG SOFTWARE-EINHEITEN können zum Zweck des Software-Konfigurations-Managements oder zum Prüfen benutzt werden.

### 3.29

#### **SOUP (en: SOFTWARE OF UNKNOWN PROVENANCE)**

##### **SOFTWARE UNBEKANNTER HERKUNFT**

SOFTWARE-KOMPONENTE, die bereits entwickelt und allgemein verfügbar ist und die nicht entwickelt wurde, um in das MEDIZINPRODUKT integriert zu werden (auch bekannt als „Off-The-Shelf Software“), oder bereits fertig entwickelte Software, für die angemessene Aufzeichnungen zum Entwicklungs-PROZESS nicht verfügbar sind

### 3.30

#### **SYSTEM**

integrierter Verbund, bestehend aus einem oder mehreren PROZESSEN, Hardware, Software, Einrichtungen und Personen, der eine Fähigkeit zur Verfügung stellt, um einen bestimmten Zweck oder ein bestimmtes Ziel zu erreichen

[ISO/IEC 12207:1995, Definition 3.31], [9]<sup>N6)</sup>

### 3.31

#### **AUFGABE**

eine Teilarbeit, die erledigt werden muss

### 3.32

#### **RÜCKVERFOLGBARKEIT**

die Möglichkeit, eine Beziehung zwischen zwei oder mehr Produkten des Entwicklungs-PROZESSES herstellen zu können

[IEEE 610.12:1990], [13]<sup>N6)</sup>

### 3.33

#### **VERIFIZIERUNG**

Bestätigung durch Bereitstellen eines objektiven Nachweises, dass festgelegte Anforderungen erfüllt worden sind

ANMERKUNG 1 Die Benennung „verifiziert“ wird zur Bezeichnung des entsprechenden Status verwendet.

[ISO 9000:2000, Definition 3.8.4]

---

<sup>N6)</sup> Nationale Fußnote: Der Verweis zu den Literaturhinweisen fehlt in der Internationalen Norm.

ANMERKUNG 2 Bei Design und Entwicklung beschäftigt sich die VERIFIZIERUNG mit dem PROZESS der EVALUATION des Ergebnisses einer gegebenen AKTIVITÄT um festzustellen, dass die für diese AKTIVITÄT aufgestellten Anforderungen eingehalten wurden.

### 3.34

#### VERSION

gekennzeichnete Ausgabe eines KONFIGURATIONSELEMENTES

ANMERKUNG 1 Die Änderung einer VERSION eines SOFTWARE-PRODUKTS, die in einer neuen VERSION resultiert, erfordert eine Konfigurations-Management-Aktion.

ANMERKUNG 2 Basierend auf ISO/IEC 12207:1995, Definition 3.37 [9]<sup>N7)</sup>.

## 4 \*Allgemeine Anforderungen

### 4.1 \*Qualitätsmanagement-System

Der HERSTELLER von MEDIZINPRODUKTE-SOFTWARE muss seine Fähigkeit, MEDIZINPRODUKTE-SOFTWARE zu erstellen, die Kundenanforderungen und anwendbare regulatorische Anforderungen dauerhaft erfüllt, nachweisen.

ANMERKUNG 1 Diese Fähigkeit kann durch die Anwendung eines Qualitätsmanagementsystems nachgewiesen werden, das

- ISO 13485 [7] oder
  - einer nationalen Norm für Qualitätsmanagement-SYSTEME oder
  - einem Qualitätsmanagement-System, das durch nationale Vorschriften gefordert wird,
- entspricht.

ANMERKUNG 2 Anleitung für die Anwendung von Anforderungen für Qualitätsmanagement-Systeme findet sich in ISO/IEC 90003 [11].

### 4.2 \*RISIKOMANAGEMENT

Der HERSTELLER muss einen RISIKOMANAGEMENT-PROZESS nach ISO 14971 anwenden.

### 4.3 \*Software-Sicherheitsklassifizierung

- a) Der HERSTELLER muss jedem SOFTWARE-SYSTEM eine Software-Sicherheitsklasse (A, B oder C) zuordnen, je nach den möglichen Auswirkungen einer Gefährdung auf den Patienten, den Anwender oder andere Personen, zu der das SOFTWARE-SYSTEM beitragen kann.

Die Software-Sicherheitsklassen müssen zu Beginn basierend auf dem Schweregrad wie folgt zugeordnet werden:

Klasse A: Keine Verletzung oder Schädigung der Gesundheit ist möglich.

Klasse B: Keine SCHWERE VERLETZUNG ist möglich.

Klasse C: Tod oder SCHWERE VERLETZUNG ist möglich.

Wenn die GEFÄHRDUNG davon herrühren könnte, dass das SOFTWARE-SYSTEM sich nicht entsprechend seiner Spezifikation verhält, muss die Wahrscheinlichkeit einer solchen Fehlfunktion als 100 Prozent angenommen werden.

Wenn das RISIKO des Todes oder einer SCHWEREN VERLETZUNG, das von einem Software-Fehler herrührt, anschließend durch eine Hardware-RISIKOKONTROLL-Maßnahme auf ein vertretbares Maß verringert wird (wie in ISO 14971 definiert), und zwar dadurch, dass die Folgen des Fehlers verringert werden oder dass die Wahrscheinlichkeit des Todes oder einer SCHWEREN VERLETZUNG, die von diesem Fehler herrührt, verringert wird, so kann die Software-Sicherheitsklasse von C auf B herabgesetzt

<sup>N7)</sup> Nationale Fußnote: Der Verweis zu den Literaturhinweisen fehlt in der Internationalen Norm.

werden, und wenn das RISIKO einer leichten Verletzung, das von einem Software-Fehler herrührt, in ähnlicher Weise durch eine Hardware-RISIKOKONTROLL-Maßnahme auf ein vertretbares Maß verringert wird, so kann die Software-Sicherheitsklasse von B auf A herabgesetzt werden.

- b) Der HERSTELLER muss jedem SOFTWARE-SYSTEM, das zur Implementierung einer RISIKOKONTROLL-Maßnahme beiträgt, eine Software-Sicherheitsklasse zuordnen. Sie basiert auf den möglichen Auswirkungen derjenigen GEFÄHRDUNG, die durch die RISIKOKONTROLL-Maßnahme kontrolliert wird.
- c) Der HERSTELLER muss die Software-Sicherheitsklasse, die jedem SOFTWARE-SYSTEM zugeordnet wurde, in der RISIKOMANAGEMENT-AKTE dokumentieren.
- d) Wenn ein SOFTWARE-SYSTEM in SOFTWARE-KOMPONENTEN zerlegt wird und wenn eine SOFTWARE-KOMPONENTE in weitere SOFTWARE-KOMPONENTEN zerlegt wird, so müssen diese SOFTWARE-KOMPONENTEN die Software-Sicherheitsklasse der ursprünglichen SOFTWARE-KOMPONENTE (oder des SOFTWARE-SYSTEMS) übernehmen, es sei denn, der HERSTELLER dokumentiert eine Begründung für die Klassifizierung in eine andere Software-Sicherheitsklasse. Eine solche Begründung muss darlegen, wie die neuen SOFTWARE-KOMPONENTEN so abgegrenzt sind, dass sie getrennt klassifiziert werden können.
- e) Der HERSTELLER muss die Software-Sicherheitsklasse jeder SOFTWARE-KOMPONENTE dokumentieren, wenn sich deren Klasse von der Klasse derjenigen SOFTWARE-KOMPONENTE, aus der sie durch Zerlegung entstanden ist, unterscheidet.
- f) Wenn ein PROZESS für SOFTWARE-KOMPONENTEN einer bestimmten Klasse gefordert wird und wenn dieser PROZESS notwendigerweise auf eine Gruppe von SOFTWARE-KOMPONENTEN angewandt wird, muss der HERSTELLER, um diese Norm einzuhalten, diejenigen PROZESSE und AUFGABEN verwenden, die durch die Klassifizierung der am höchsten klassifizierten SOFTWARE-KOMPONENTE in dieser Gruppe gefordert werden, es sei denn, der HERSTELLER dokumentiert eine Begründung für die Verwendung einer niedrigeren Klasse in der RISIKOMANAGEMENT-AKTE.
- g) Bis eine Software-Sicherheitsklasse zugeordnet ist, gelten für jedes SOFTWARE-SYSTEM die Anforderungen der Klasse C.

ANMERKUNG Bei den folgenden Anforderungen werden die Software-Sicherheitsklassen, für die diese Anforderung durchgeführt werden muss, in der Form [Klasse ...] festgelegt.

## 5 Software-Entwicklungs-PROZESS

### 5.1 \*Planung der Software-Entwicklung

#### 5.1.1 Software-Entwicklungsplan

Der HERSTELLER muss einen Software-Entwicklungsplan (oder -pläne) für die Durchführung der AKTIVITÄTEN des Software-Entwicklungs-PROZESSES erstellen. Dieser PROZESS muss dem Anwendungsbereich, dem Umfang und den Software-Sicherheitsklassen des zu entwickelnden SOFTWARE-SYSTEMS angemessen entsprechen. Das LEBENSZYKLUS-MODELL DER SOFTWARE-ENTWICKLUNG muss entweder vollständig definiert oder im Plan (oder Plänen) referenziert sein. Der Plan muss folgende Punkte umfassen:

- a) die PROZESSE, die bei der Entwicklung des SOFTWARE-SYSTEMS verwendet werden (siehe ANMERKUNG 4);
- b) die ZU LIEFERNDEN ERGEBNISSE (einschließlich der Dokumentation) der AKTIVITÄTEN und AUFGABEN;
- c) RÜCKVERFOLGBARKEIT zwischen SYSTEM-Anforderungen, Software-Anforderungen, SOFTWARE-SYSTEM-Prüfungen und RISIKOKONTROLL-Maßnahmen, die in Software implementiert werden;
- d) Software-Konfigurations- und Änderungsmanagement, einschließlich SOUP-KONFIGURATIONSELEMENTEN und Software, die zur Entwicklungsunterstützung verwendet wird, und
- e) Software-Problemlösung und Behandlung von Problemen, die bei SOFTWARE-PRODUKTEN, ZU LIEFERNDEN ERGEBNISSEN und AKTIVITÄTEN in jeder Phase des Lebenszyklus entdeckt werden.

[Klasse A, B, C]

ANMERKUNG 1 Das LEBENSZYKLUS-MODELL DER SOFTWAREENTWICKLUNG kann unterschiedliche Elemente (PROZESSE, AKTIVITÄTEN, AUFGABEN und ZU LIEFERNDE ERGEBNISSE) für unterschiedliche SOFTWARE-KOMPONENTEN entsprechend der Software-Sicherheitsklassifizierung für jede SOFTWARE-KOMPONENTE des SOFTWARE-SYSTEMS festlegen.

ANMERKUNG 2 Diese AKTIVITÄTEN und AUFGABEN können überlappend sein, können sich gegenseitig beeinflussen und können iterativ oder rekursiv durchgeführt werden. Es ist nicht die Absicht, die Anwendung eines bestimmten Lebenszyklus-Modells vorauszusetzen.

ANMERKUNG 3 Andere PROZESSE werden in dieser Norm getrennt vom Entwicklungs-PROZESS beschrieben. Dies bedeutet nicht, dass sie als getrennte AKTIVITÄTEN und AUFGABEN implementiert werden müssen. Die AKTIVITÄTEN und AUFGABEN der anderen PROZESSE können in den Entwicklungs-PROZESS integriert werden.

ANMERKUNG 4 Der Software-Entwicklungsplan kann auf bestehende PROZESSE verweisen oder neue definieren.

ANMERKUNG 5 Der Software-Entwicklungsplan kann in einen Gesamt-SYSTEM-Entwicklungsplan integriert sein

### 5.1.2 Aktualisierung des Software-Entwicklungsplans

Soweit angemessen, muss der HERSTELLER den Plan dem Entwicklungsfortschritt entsprechend aktualisieren. [Klasse A, B, C]

### 5.1.3 Referenz im Software-Entwicklungsplan auf SYSTEM-Design und -Entwicklung

- a) Der HERSTELLER muss SYSTEM-Anforderungen im Software-Entwicklungsplan als Vorgaben für die Software-Entwicklung referenzieren.
- b) Der HERSTELLER muss im Software-Entwicklungsplan Verfahren zur Koordination von Software-Entwicklung und Design- und Entwicklungs-Validierung einschließen oder referenzieren; dies ist für die Erfüllung von 4.1 erforderlich.

[Klasse A, B, C]

ANMERKUNG Es kann möglicherweise keinen Unterschied zwischen SOFTWARE-SYSTEM-Anforderungen und SYSTEM-Anforderungen geben, wenn das SOFTWARE-SYSTEM ein eigenständiges SYSTEM (eigenständiges Softwareprodukt) ist.

### 5.1.4 Planung von Normen, Methoden und Werkzeugen der Software-Entwicklung

Der HERSTELLER muss im Software-Entwicklungsplan einschließen oder referenzieren:

- a) Normen,
- b) Methoden und
- c) Werkzeuge,

die im Zusammenhang mit der Entwicklung von SOFTWARE-KOMPONENTEN der Klasse C stehen. [Klasse C]

### 5.1.5 Planung der Software-Integration und der Integrationsprüfung

Der HERSTELLER muss im Software-Entwicklungsplan einen Plan einschließen oder referenzieren, wie die SOFTWARE-KOMPONENTEN (einschließlich SOUP) integriert und wie während der Integration Prüfungen durchgeführt werden. [Klasse B, C]

ANMERKUNG Es ist vertretbar, die Integrationsprüfung und die SOFTWARE-SYSTEM-Prüfung in einem Plan und einem Satz von AKTIVITÄTEN zu kombinieren.

### 5.1.6 Planung der Software-VERIFIZIERUNG

Der HERSTELLER muss im Software-Entwicklungsplan folgende Informationen über die VERIFIZIERUNG einschließen oder referenzieren:

- a) ZU LIEFERNDE ERGEBNISSE, die eine VERIFIZIERUNG erfordern;
- b) die erforderlichen VERIFIZIERUNGS-AUFGABEN für jede AKTIVITÄT des Lebenszyklus,
- c) Meilensteine, bei denen die ZU LIEFERNDEN ERGEBNISSE VERIFIZIERT werden, und
- d) die Akzeptanzkriterien für die VERIFIZIERUNG der ZU LIEFERNDEN ERGEBNISSE.

[Klasse A, B, C]

#### 5.1.7 Planung des Software-RISIKOMANAGEMENTS

Der HERSTELLER muss im Software-Entwicklungsplan einen Plan einschließen oder referenzieren, wie die AKTIVITÄTEN und AUFGABEN des Software-RISIKOMANAGEMENTS durchgeführt werden, einschließlich des Managements von RISIKEN, die sich auf SOUP beziehen. [Klasse A, B, C]

ANMERKUNG Siehe [Abschnitt 7](#).

#### 5.1.8 Planung der Dokumentation

Der HERSTELLER muss Informationen über die Dokumente, die während des Software-Entwicklungszyklus erzeugt werden sollen, in den Software-Entwicklungsplan mit einschließen oder in diesem referenzieren. Für jedes identifizierte Dokument oder jede Art von Dokumenten müssen die folgenden Informationen enthalten sein oder referenziert werden:

- a) Titel, Benennung / Bezeichnung oder Konvention der Benennung;
- b) Zweck;
- c) vorgesehene Zielgruppe des Dokuments und
- d) Verfahren und Verantwortlichkeiten für Entwicklung, Überprüfung, Genehmigung und Änderung.

[Klasse A, B, C]

#### 5.1.9 Planung des Software-Konfigurationsmanagements

Der HERSTELLER muss im Software-Entwicklungsplan Informationen über das Software-Konfigurationsmanagement einschließen oder referenzieren. Die Information über das Software-Konfigurationsmanagement muss enthalten oder referenzieren:

- a) die Klassen, Arten, Kategorien oder Listen von Komponenten, die kontrolliert werden sollen;
- b) die AKTIVITÄTEN und AUFGABEN des Software-Konfigurationsmanagements;
- c) die Organisation(en), die für die Durchführung des Software-Konfigurationsmanagements und der AKTIVITÄTEN verantwortlich ist (sind);
- d) deren Beziehung zu anderen Organisationen, wie zum Beispiel der Software-Entwicklung oder -Wartung;
- e) wann die Komponenten unter Konfigurationskontrolle gestellt werden sollen und
- f) wann der Problemlösungs-PROZESS benutzt werden soll.

[Klasse A, B, C]

#### 5.1.10 Zu kontrollierende unterstützende Komponenten

Zu den zu kontrollierenden Komponenten gehören Werkzeuge, Elemente oder Einstellungen, die zur Entwicklung der MEDIZINPRODUKTE-SOFTWARE benötigt werden und die die MEDIZINPRODUKTE-SOFTWARE beeinflussen könnten. [Klasse B, C]

ANMERKUNG Beispiele für solche Komponenten sind Compiler-/Assembler-VERSIONEN, Make-Dateien, Batch-Dateien und spezifische Einstellungen der Entwicklungsumgebung.

#### 5.1.11 Kontrolle der Software-KONFIGURATIONSELEMENTE vor der Verifizierung

Der HERSTELLER muss planen, die KONFIGURATIONSELEMENTE unter eine dokumentierte Konfigurationsmanagement-Kontrolle zu stellen, bevor sie VERIFIZIERT werden. [Klasse B, C]

## 5.2 \*Analyse der Software-Anforderungen

### 5.2.1 Ableitung der Software-Anforderungen aus den SYSTEM-Anforderungen und Dokumentation

Für jedes SOFTWARE-SYSTEM des MEDIZINPRODUKTS muss der HERSTELLER die Anforderungen an das SOFTWARE-SYSTEM aus den Anforderungen an das Gesamt-SYSTEM ableiten und dokumentieren. [Klasse A, B, C]

ANMERKUNG Es kann möglicherweise keinen Unterschied zwischen SOFTWARE-SYSTEM-Anforderungen und SYSTEM-Anforderungen geben, wenn das SOFTWARE-SYSTEM ein eigenständiges SYSTEM (eigenständiges Softwareprodukt) ist.

### 5.2.2 Inhalt der Software-Anforderungen

Soweit angemessen muss der HERSTELLER in die Software-Anforderungen für die MEDIZINPRODUKTE-SOFTWARE Folgendes einschließen:

a) Anforderungen an die Funktionalität und die Leistungsfähigkeit;

ANMERKUNG 1 Beispiele sind:

- Leistungsmerkmale (z. B. Zweck der Software, Anforderungen bezüglich Zeitverhalten),
- physikalische Merkmale (z. B. Programmiersprache, Plattform, Betriebssystem),
- Rechnerumgebung (z. B. Hardware, Speichergröße, Prozessor, Zeitzone, Netzwerk-Infrastruktur), in der die Software laufen soll, und
- Notwendigkeit der Kompatibilität mit Nachrüstungen oder mit mehreren SOUP- oder anderen Geräte-VERSIONEN.

b) Ein- und Ausgaben des SOFTWARE-SYSTEMS;

ANMERKUNG 2 Beispiele sind:

- Merkmale von Daten (z. B. numerisch, alpha-numerisch, Format),
- Bereiche,
- Grenzen und
- Werte der Voreinstellungen.

c) Schnittstellen zwischen dem SOFTWARE-SYSTEM und anderen SYSTEMEN;

d) Software-gesteuerte Alarmer, Warnungen und Anwender-Meldungen;

e) Anforderungen für die DATENSICHERHEIT;

ANMERKUNG 3 Beispiele sind:

- Anforderungen im Zusammenhang mit der Beeinträchtigung vertraulicher Informationen,
- Authentifizierung,
- Autorisierung,
- Audio-Pfad,
- Integrität der Kommunikation.

f) Anforderungen an die Gebrauchstauglichkeit, die maßgeblich sind hinsichtlich menschlichem Versagen und Ausbildung;

ANMERKUNG 4 Beispiele sind solche in Bezug auf:

- Unterstützung für manuelle Tätigkeiten,
- Interaktionen zwischen Mensch und Gerät,
- Einschränkungen für das Personal und
- Bereiche, die eine konzentrierte menschliche Aufmerksamkeit erfordern.

ANMERKUNG 5 Informationen über Anforderungen hinsichtlich der Entwicklung von Gebrauchstauglichkeit finden sich in IEC 60601-1-6 [15].

g) Datendefinition und Datenbank-Anforderungen;

ANMERKUNG 6 Beispiele sind:

- Form,
- Eignung,
- Funktion.

h) Anforderungen für die Installation und Abnahme der gelieferten MEDIZINPRODUKTE-SOFTWARE am Standort/an den Standorten der Anwendung und Wartung;

i) Anforderungen hinsichtlich Methoden des Betriebs und der Wartung;

j) Anwender-Dokumentation, die entwickelt werden soll;

k) Anforderungen hinsichtlich der Wartung durch den Betreiber und

l) regulatorische Anforderungen.

[Klasse A, B, C]

ANMERKUNG 7 Möglicherweise sind nicht alle Anforderungen bei Beginn der Software-Entwicklung verfügbar.

ANMERKUNG 8 ISO/IEC 9126-1 [8] liefert Informationen über Qualitätsmerkmale, die bei der Festlegung von Software-Anforderungen nützlich sein könnten.

### 5.2.3 Einbeziehen von RISIKOKONTROLL-Maßnahmen in die Software-Anforderungen

Soweit es für die MEDIZINPRODUKTE-SOFTWARE angemessen ist, muss der HERSTELLER RISIKOKONTROLL-Maßnahmen für Hardware-Ausfälle und mögliche Software-Defekte in die Anforderungen aufnehmen. [Klasse B, C]

ANMERKUNG Möglicherweise sind diese Anforderungen bei Beginn der Software-Entwicklung nicht verfügbar, und sie können sich im Verlauf der Software-Entwicklung und der weiteren Definition von RISIKOKONTROLL-Maßnahmen ändern.

### 5.2.4 Erneute EVALUATION der RISIKOANALYSE

Wenn Software-Anforderungen festgelegt werden, muss der HERSTELLER die RISIKOANALYSE des MEDIZINPRODUKTS erneut EVALUIEREN und, soweit angemessen, aktualisieren. [Klasse A, B, C]

### 5.2.5 Aktualisierung von SYSTEM-Anforderungen

Der HERSTELLER muss sicherstellen, dass vorhandene Anforderungen, einschließlich der SYSTEM-Anforderungen, als Ergebnis der AKTIVITÄT der Analyse der Software-Anforderungen erneut EVALUIERT und, soweit angemessen, aktualisiert werden. [Klasse A, B, C]

### 5.2.6 VERIFIZIERUNG von Software-Anforderungen

Der HERSTELLER MUSS VERIFIZIEREN und dokumentieren, dass die Software-Anforderungen:

- a) die SYSTEM-Anforderungen einschließlich der Anforderungen für die RISIKOBEHERRSCHUNG implementieren;
- b) sich nicht gegenseitig widersprechen;
- c) so formuliert sind, dass Mehrdeutigkeit vermieden wird;
- d) so formuliert sind, dass sie die Festlegung von Prüfkriterien und die Durchführung von Prüfungen, die entscheiden, ob die Prüfkriterien erfüllt sind, ermöglichen;
- e) eindeutig identifiziert werden können;
- f) auf SYSTEM-Anforderungen oder andere Quellen zurückverfolgt werden können.

[Klasse A, B, C]

ANMERKUNG Diese Norm fordert nicht die Verwendung einer formalen Spezifikationssprache.

### 5.3 \*Design der Software-ARCHITEKTUR

#### 5.3.1 Umsetzung von Software-Anforderungen in eine ARCHITEKTUR

Der HERSTELLER muss die Anforderungen für die MEDIZINPRODUKTE-SOFTWARE in eine dokumentierte ARCHITEKTUR, die die Struktur der Software beschreibt und die die SOFTWARE-KOMPONENTEN identifiziert, umsetzen. [Klasse B, C]

#### 5.3.2 Entwicklung einer ARCHITEKTUR für die Schnittstellen zwischen SOFTWARE-KOMPONENTEN

Der HERSTELLER muss eine ARCHITEKTUR für die Schnittstellen zwischen den SOFTWARE-KOMPONENTEN und den Komponenten außerhalb der SOFTWARE-KOMPONENTEN (Software und Hardware) sowie zwischen den einzelnen SOFTWARE-KOMPONENTEN entwickeln und dokumentieren. [Klasse B, C]

#### 5.3.3 Spezifikation der Funktions- und Leistungsanforderungen für SOUP-Komponenten

Wenn eine SOFTWARE-KOMPONENTE als SOUP identifiziert ist, muss der HERSTELLER Funktions- und Leistungsanforderungen für die SOUP-Komponente festlegen, die für deren bestimmungsgemäßen Gebrauch notwendig sind. [Klasse B, C]

#### 5.3.4 Spezifikation der für die SOUP-Komponente erforderliche SYSTEM-Hardware und -Software

Wenn eine SOFTWARE-KOMPONENTE als SOUP identifiziert ist, muss der HERSTELLER die SYSTEM-Hardware und -Software spezifizieren, die erforderlich ist, um den ordnungsgemäßen Betrieb der SOUP-Komponente zu gewährleisten. [Klasse B, C]

ANMERKUNG Beispiele sind: Prozessortyp und -geschwindigkeit, Speichertyp und -größe, Typ der SYSTEM-Software, Anforderungen für Kommunikations- und Anzeigesoftware.

#### 5.3.5 Festlegung der für die RISIKOBEHERRSCHUNG erforderlichen Abgrenzung

Der HERSTELLER muss die Abgrenzung zwischen den SOFTWARE-KOMPONENTEN festlegen, die für die RISIKOBEHERRSCHUNG wesentlich ist, und muss zeigen, wie sichergestellt wird, dass die Abgrenzung wirksam ist. [Klasse C]

ANMERKUNG Ein Beispiel einer Abgrenzung ist, dass SOFTWARE-KOMPONENTEN auf verschiedenen Prozessoren ausgeführt werden. Die Wirksamkeit der Abgrenzung kann dadurch sichergestellt werden, dass keine gemeinsamen Ressourcen zwischen den Prozessoren bestehen.

#### 5.3.6 VERIFIZIERUNG der Software-ARCHITEKTUR

Der HERSTELLER muss VERIFIZIEREN und dokumentieren, dass:

- a) die Software-ARCHITEKTUR die SYSTEM- und Software-Anforderungen einschließlich derer, die sich auf die RISIKOBEHERRSCHUNG beziehen, implementiert;
- b) die Software-ARCHITEKTUR in der Lage ist, Schnittstellen zwischen den einzelnen SOFTWARE-KOMPONENTEN und zwischen SOFTWARE-KOMPONENTEN und Hardware zu unterstützen, und
- c) die ARCHITEKTUR des MEDIZINPRODUKTS den ordnungsgemäßen Betrieb aller SOUP-Komponenten unterstützt.

[Klasse B, C]