

Anwendungsbereich

Anwendungsbereich dieser Norm ist ...

Inhalt

	Seite
Einführung.....	13
1 Anwendungsbereich.....	16
1.1 *Zweck.....	16
1.2 *Anwendungsbereich.....	16
1.3 Beziehung zu anderen Normen.....	16
1.4 Einhaltung.....	16
2 *Normative Verweisungen.....	17
3 Begriffe.....	17
4 *Allgemeine Anforderungen.....	23
4.1 *Qualitätsmanagement-SYSTEM.....	23
4.2 *RISIKOMANAGEMENT.....	23
4.3 *Software-SICHERHEITSKlassifizierung.....	23
4.4 *Anwendung der IEC 62304 auf ALTSOFTWARE.....	24
5 Software-Entwicklungs-PROZESS.....	24
5.1 *Planung der Software-Entwicklung.....	24
5.1.1 Software-Entwicklungsplan.....	24
5.1.2 Aktualisierung des Software-Entwicklungsplans.....	25
5.1.3 Referenz im Software-Entwicklungsplan auf SYSTEM-Design und -Entwicklung.....	25
5.1.4 Planung von Normen, Methoden und Werkzeugen der Software-Entwicklung.....	25
5.1.5 Planung der Software-Integration und der Integrationsprüfung.....	26
5.1.6 Planung der Software-VERIFIZIERUNG.....	26
5.1.7 Identifizierung und Beseitigung üblicher Software Defekte.....	26
5.1.8 Planung des Software-RISIKOMANAGEMENTS.....	26
5.1.9 Planung der Dokumentation.....	26
5.1.10 Planung des Software-Konfigurationsmanagements.....	27
5.1.11 Zu kontrollierende unterstützende Komponenten.....	27
5.1.12 Kontrolle der Software-KONFIGURATIONSELEMENTE vor der VERIFIZIERUNG.....	27
5.2 *Analyse der Software-Anforderungen.....	27
5.2.1 Ableitung der Software-Anforderungen aus den SYSTEM-Anforderungen und Dokumentation.....	27
5.2.2 Inhalt der Software-Anforderungen.....	27
5.2.3 Einbeziehen von RISIKOBEHERRSCHUNGS-Maßnahmen in die Software-Anforderungen.....	29
5.2.4 Erneute EVALUATION der Risikoanalyse.....	29
5.2.5 Aktualisierung von Anforderungen.....	29
5.2.6 VERIFIZIERUNG von Software-Anforderungen.....	29
5.3 *Design der Software-ARCHITEKTUR.....	30

	Seite
5.3.1 Umsetzung von Software-Anforderungen in eine ARCHITEKTUR	30
5.3.2 Entwicklung einer ARCHITEKTUR für die Schnittstellen zwischen SOFTWARE-KOMPONENTEN	30
5.3.3 Spezifikation der Funktions- und Leistungsanforderungen für SOUP-Komponenten	30
5.3.4 Spezifikation der für die SOUP-Komponente erforderliche SYSTEM-Hardware und -Software	30
5.3.5 Festlegung der für die RISIKOBEHERRSCHUNG erforderlichen Abgrenzung	30
5.3.6 VERIFIZIERUNG der Software-ARCHITEKTUR	30
5.4 *Detailliertes Software-Design	31
5.4.1 Feinaufteilung der Software in SOFTWARE-EINHEITEN	31
5.4.2 Entwicklung eines detaillierten Designs für jede SOFTWARE-EINHEIT	31
5.4.3 Entwicklung eines detaillierten Designs für Schnittstellen	31
5.4.4 VERIFIZIERUNG des detaillierten Designs	31
5.5 *Implementierung und VERIFIZIERUNG der SOFTWARE-EINHEITEN	31
5.5.1 Implementierung jeder SOFTWARE-EINHEIT	31
5.5.2 Festlegung eines VERIFIZIERUNGSPROZESSES für SOFTWARE-EINHEITEN	31
5.5.3 Akzeptanzkriterien für SOFTWARE-EINHEITEN	31
5.5.4 Zusätzliche Akzeptanzkriterien für SOFTWARE-EINHEITEN	32
5.5.5 VERIFIZIERUNG der SOFTWARE-EINHEITEN	32
5.6 *Software-Integration und -Integrationsprüfung	32
5.6.1 Integration der SOFTWARE-EINHEITEN	32
5.6.2 VERIFIZIERUNG der Software-Integration	32
5.6.3 Prüfung der integrierten Software	32
5.6.4 Inhalt der Integrationsprüfung	32
5.6.5 EVALUATION der Integrationsprüfverfahren	33
5.6.6 Durchführung von REGRESSIONSPRÜFUNGEN	33
5.6.7 Inhalt von Aufzeichnungen über die Integrationsprüfung	33
5.6.8 Verwendung eines Problemlösungs-PROZESSES für Software	33
5.7 *Prüfung des SOFTWARE-SYSTEMS	33
5.7.1 Festlegung von Prüfungen für Software-Anforderungen	33
5.7.2 Verwendung eines Problemlösungs-PROZESSES für Software	34
5.7.3 Prüfungswiederholung nach Änderungen	34
5.7.4 VERIFIZIERUNG der SOFTWARE-SYSTEM-Prüfungen	34
5.7.5 Inhalte der Aufzeichnungen der SOFTWARE-SYSTEM-Prüfungen	34
5.8 *Software-Freigabe für die betriebliche Nutzung	35
5.8.1 Sicherstellen, dass die VERIFIZIERUNG der Software vollständig ist	35
5.8.2 Dokumentation bekannter restlicher ANOMALIEN	35
5.8.3 Bewertung bekannter restlicher ANOMALIEN	35
5.8.4 Dokumentation freigegebener VERSIONEN	35
5.8.5 Dokumentation, wie freigegebene Software erzeugt wurde	35
5.8.6 Sicherstellen, dass AKTIVITÄTEN und AUFGABEN abgeschlossen sind	35

	Seite
5.8.7 Archivierung der Software	35
5.8.8 Sicherstellen der Wiederholbarkeit der Software-Freigabe.....	35
6 Software-Wartungs-PROZESS	36
6.1 *Festlegung eines Plans für die Software-Wartung	36
6.2 *Analyse von Problemen und Änderungen	36
6.2.1 Dokumentation und EVALUATION von Rückmeldungen	36
6.2.1.1 Überwachung von Rückmeldungen	36
6.2.1.2 Dokumentation und EVALUATION von Rückmeldungen	36
6.2.1.3 EVALUATION von PROBLEMBERICHTEN auf Auswirkungen auf die SICHERHEIT	37
6.2.2 Verwendung des Problemlösungs-PROZESSES für Software.....	37
6.2.3 Analyse der Änderungsanforderungen.....	37
6.2.4 Genehmigung von Änderungsanforderungen	37
6.2.5 Kommunikation mit Anwendern und zuständigen Behörden	37
6.3 *Implementierung von Änderungen.....	37
6.3.1 Verwendung eines festgelegten PROZESSES für die Implementierung von Änderungen	37
6.3.2 Erneute Freigabe eines geänderten SOFTWARE-SYSTEMS	37
7 *Software-RISIKOMANAGEMENT-PROZESS	38
7.1 *Analyse von Software, die zu GEFÄHRDUNGSSITUATIONEN beiträgt	38
7.1.1 Identifikation von Software-Komponenten, die zu einer GEFÄHRDUNGSSITUATION beitragen könnten.....	38
7.1.2 Identifikation von möglichen Ursachen für den Beitrag zu einer GEFÄHRDUNGSSITUATION	38
7.1.3 EVALUATION veröffentlichter Listen mit ANOMALIEN der SOUP	38
7.1.4 Dokumentation möglicher Ursachen	38
7.1.5 Dokumentation von Folgen von Ereignissen.....	38
7.2 RISIKOBEHERRSCHUNGS-Maßnahmen	39
7.2.1 Definition von RISIKOBEHERRSCHUNGS-Maßnahmen	39
7.2.2 RISIKOBEHERRSCHUNGS-Maßnahmen, die in Software implementiert werden.....	39
7.3 VERIFIZIERUNG von RISIKOBEHERRSCHUNGS-Maßnahmen.....	39
7.3.1 VERIFIZIERUNG von RISIKOBEHERRSCHUNGS-Maßnahmen.....	39
7.3.2 Dokumentation neuer Folgen von Ereignissen	39
7.3.3 Dokumentation der RÜCKVERFOLGBARKEIT	39
7.4 RISIKOMANAGEMENT von Software-Änderungen.....	40
7.4.1 Analyse von Änderungen an MEDIZINPRODUKTE-SOFTWARE in Hinblick auf die SICHERHEIT	40
7.4.2 Analyse der Auswirkung von Software-Änderungen auf bestehende RISIKOBEHERRSCHUNGS-Maßnahmen	40
7.4.3 Durchführung von RISIKOMANAGEMENT-AKTIVITÄTEN basierend auf Analysen.....	40
8 *Software-Konfigurationsmanagement-PROZESS	40
8.1 *Identifizierung der Konfiguration	40
8.1.1 Festlegung von Mitteln zur Identifizierung von KONFIGURATIONSELEMENTEN.....	40
8.1.2 Identifizierung von SOUP.....	40

	Seite
8.1.3 Identifizierung der Dokumentation der SYSTEM-Konfiguration	40
8.2 *Änderungskontrolle	41
8.2.1 Genehmigung von Änderungsanforderungen	41
8.2.2 Implementierung von Änderungen	41
8.2.3 VERIFIZIERUNG von Änderungen	41
8.2.4 Bereitstellung von Mitteln für die RÜCKVERFOLGBARKEIT von Änderungen	41
8.3 *Aufzeichnungen über den Status der Konfiguration	41
9 *Problemlösungs-PROZESS für Software	42
9.1 Erstellen von PROBLEMBERICHTEN	42
9.2 Untersuchung des Problems	42
9.3 Unterrichtung beteiligter Stellen	42
9.4 Anwendung des Änderungskontroll-PROZESSES	42
9.5 Aufbewahrung von Aufzeichnungen	42
9.6 Analyse von Problemen hinsichtlich Trends	43
9.7 VERIFIZIERUNG der Lösung von Software-Problemen	43
9.8 Inhalt von Prüfungsdokumentation	43
Anhang A (informativ) Begründung für die Anforderungen dieser Norm	44
A.1 Begründung	44
A.2 Zusammenfassung der Anforderungen nach Klassen	45
Anhang B (informativ) Anleitung für die Bestimmungen dieser Norm	47
B.1 Anwendungsbereich	47
B.1.1 Zweck	47
B.1.2 Anwendungsbereich	48
B.2 Normative Verweisungen	49
B.3 Begriffe und Definitionen	49
B.4 Allgemeine Anforderungen	49
B.4.1 Qualitätsmanagement-SYSTEM	50
B.4.2 RISIKOMANAGEMENT	50
B.4.3 Software-SICHERHEITSKlassifizierung	50
B.5 Software-Entwicklungs-PROZESS	53
B.5.1 Planung der Software-Entwicklung	53
B.5.2 Analyse der Software-Anforderungen	54
B.5.3 Design der Software-ARCHITEKTUR	55
B.5.4 Detailliertes Design der Software	56
B.5.5 Implementierung und VERIFIZIERUNG von SOFTWARE-EINHEITEN	56
B.5.6 Software-Integration und Integrationsprüfung	57
B.5.7 Prüfung des SOFTWARE-SYSTEMS	58
B.5.8 Software-Freigabe für die betriebliche Nutzung	58
B.6 Software-Wartungs-PROZESS	59

	Seite
B.6.1 Festlegung eines Plans für die Software-Wartung.....	59
B.6.2 Analyse von Problemen und Änderungen.....	59
B.6.3 Implementierung von Änderungen	60
B.7 Software-RISIKOMANAGEMENT-PROZESS.....	60
B.7.1 Analyse von Software, die zu Gefährdungssituationen beiträgt.....	61
B.8 Software-Konfigurationsmanagement-PROZESS	61
B.8.1 Identifizierung der Konfiguration.....	61
B.8.2 Änderungskontrolle.....	61
B.8.3 Aufzeichnungen über den Status der Konfiguration.....	62
B.9 Problemlösungs-PROZESS für Software.....	62
Anhang C (informativ) Beziehung zu anderen Normen.....	63
C.1 Allgemeines	63
C.2 Beziehung zur ISO 13485	64
C.3 Beziehung zu ISO 14971.....	65
C.4 Beziehung zu PEMS – Anforderungen aus IEC 60601-1:2005	66
C.4.1 Allgemeines	66
C.4.2 Software-Beziehungen zur PEMS-Entwicklung	66
C.4.3 Entwicklungs-PROZESS	67
C.4.4 Wartungs-PROZESS.....	67
C.4.5 Andere PROZESSE.....	67
C.4.6 Abdeckung von PEMS-Anforderungen in IEC 60601-1	68
C.4.7 Beziehung zu den Anforderungen in IEC 60601-1-4	75
C.5 Beziehung zu IEC 61010-1	77
C.6 Beziehung zu ISO/IEC 12207	79
C.7 Beziehung zu IEC 61508.....	85
Anhang D (informativ) Implementierung.....	87
D.1 Einführung	87
D.2 Qualitätsmanagement-SYSTEM.....	87
D.3 EVALUATION von Qualitätsmanagement-PROZESSEN	87
D.4 Integration von Anforderungen dieser Norm in die QM-PROZESSE des HERSTELLERS.....	87
D.5 Checkliste für kleine HERSTELLER ohne zertifiziertes QM-SYSTEM	87
Anhang E (normativ) Anwendung des Software-Lebenszyklus-PROZESSES auf ALTSOFTWARE.....	89
E.1 Allgemeines	89
E.2 Erforderliche AKTIVITÄTEN für ALTSOFTWARE.....	89
E.2.1 Bestimmung notwendiger Aktionen.....	89
E.2.2 Durchführung der Lückenanalyse	89
E.2.3 EVALUATION der Informationen aus dem Feld.....	90
E.2.3.1 Der HERSTELLER muss Berichte aus dem Feld hinsichtlich Vorkommnissen/beinahe-Vorkommnissen oder Beanstandungen im Zusammenhang mit der ALTSOFTWARE überprüfen.....	90

	Seite
E.2.3.2 Benutzung von ALTSOFTWARE	90
E.2.4 Software SICHERHEITSKlassifizierung	90
E.2.5 Spezifikation der SYSTEManforderungen	91
E.2.5.1 Definition und Dokumentation der Software-Anforderungen	91
E.2.5.2 Inhalt der Software Anforderungen	91
E.2.5.3 Einbeziehen der RISIKOBEHERRSCHUNGS-Maßnahmen in die Software Anforderungen	91
E.2.6 PrüfSYSTEM für ALTSOFTWARE	91
E.2.6.1 Festlegung von Prüfungen der Software Anforderungen	91
E.2.6.2 Entscheidungen im Fall, dass Anomalien aufgedeckt werden	91
E.2.6.2.1 Anwendung von Änderungen	91
E.2.6.2.2 Wiederholung von Prüfungen	92
E.2.6.3 Benutzung des Software Problemlösungs-PROZESSES	92
E.2.7 RISIKOBEWERTUNG	92
E.2.8 Konfigurationsmanagement	92
E.2.8.1 Festlegung von Verfahren zur Identifizierung von KONFIGURATIONSELEMENTEN	92
E.2.8.2 Identifizierung der Konfigurations-Dokumentation für ALTSOFTWARE	93
E.2.8.3 Änderungskontrolle	93
E.2.8.4 Aufzeichnungen über den Konfigurations-Status	93
E.2.9 Software Wartungs-PROZESS (wie in Abschnitt 6 definiert)	93
E.2.9.1 Festlegung eines Software Wartungsplans	93
E.2.9.2 Problem- und Änderungsanalyse	93
E.2.9.3 Implementierung von Änderungen	93
E.2.9.3.1 Benutzung eines festgelegten PROZESSES, um Änderungen zu implementieren	93
E.2.9.3.2 Erneute Freigabe geänderter ALTSOFTWARE	93
Anhang F (informativ) PROZESS-Referenzmodell für MEDIZINPRODUKTE-SOFTWARE, das ISO/IEC 33004 (SPICE) einhält	94
F.1 Einführung	94
F.2 Anforderungen für PROZESS-Referenzmodelle	94
F.3 Anforderungen für PROZESS-Beschreibungen	95
F.4 Das PRM für MEDIZINPRODUKTE-SOFTWARE-PROZESSE und die Untermenge von PROZESSEN, die das IEC 62304 PRM darstellen	96
F.5 PROZESSE/AKTIVITÄTEN PRM DEFINITIONEN	97
Literaturhinweise	115
Verzeichnis der definierten Begriffe deutsch / englisch	117
Bilder	
Bild 1 – Überblick über Software-Entwicklungs-PROZESSE und –AKTIVITÄTEN	14
Bild 2 – Überblick über Software-Wartungs-PROZESSE und -AKTIVITÄTEN	14
Bild B.1 – Bildliche Darstellung des Zusammenhangs zwischen GEFÄHRDUNG, Abfolge von Ereignissen, GEFÄHRDUNGSSITUATION und SCHADEN – aus ISO 14971:2007 Anhang E	51
Bild B.2 – Beispiel einer Aufteilung von SOFTWARE-KOMPONENTEN	53

	Seite
Bild C.1 – Beziehung von wichtigen MEDIZINPRODUKTE-Normen zur IEC 62304	64
Bild C.2 – Software als Teil des V-Modells.....	67
Bild C.3 – Anwendung von IEC 62304 mit IEC 61010-1	78
Tabellen	
Tabelle A.1 – Zusammenfassung der Anforderungen nach Software-SICHERHEITSKlassen	45
Tabelle B.1 – Entwicklungs-(Modell-)Strategien wie in ISO/IEC 12207 definiert	48
Tabelle C.1 – Beziehung zu ISO 13485:2003	64
Tabelle C.2 – Beziehung zu ISO 14971:2000	65
Tabelle C.3 – Beziehung zur IEC 60601-1	68
Tabelle C.4 – Beziehung zur IEC 60601-1-4.....	75
Tabelle C.5 – Beziehung zu ISO/IEC 12207	79
Tabelle D.1 – Checkliste für kleine Firmen ohne zertifiziertes QM-SYSTEM	88
Tabelle F.1 – Individuelle PROZESSE/AKTIVITÄTEN im PRM – AKTIVITÄT 5.1	97
Tabelle F.2 – Individuelle PROZESSE/AKTIVITÄTEN im PRM – AKTIVITÄT 5.2	98
Tabelle F.3 – Individuelle PROZESSE/AKTIVITÄTEN im PRM – AKTIVITÄT 5.3	100
Tabelle F.4 – Individuelle PROZESSE/AKTIVITÄTEN im PRM – AKTIVITÄT 5.4	101
Tabelle F.5 – Individuelle PROZESSE/AKTIVITÄTEN im PRM – AKTIVITÄT 5.5	103
Tabelle F.6 – Individuelle PROZESSE/AKTIVITÄTEN im PRM – AKTIVITÄT 5.6	104
Tabelle F.7 – Individuelle PROZESSE/AKTIVITÄTEN im PRM – AKTIVITÄT 5.7	105
Tabelle F.8 – Individuelle PROZESSE/AKTIVITÄTEN im PRM – AKTIVITÄT 5.8	106
Tabelle F.9 – Individuelle PROZESSE/AKTIVITÄTEN im PRM – PROZESS 6	107
Tabelle F.10 – Individuelle PROZESSE/AKTIVITÄTEN im PRM – PROZESS 7	109
Tabelle F.11 – Individuelle PROZESSE/AKTIVITÄTEN im PRM – PROZESS 8	112
Tabelle F.12 – Individuelle PROZESSE/AKTIVITÄTEN im PRM – AKTIVITÄT 8.2	113
Tabelle F.13 – Individuelle PROZESSE/AKTIVITÄTEN im PRM – PROZESS 9	114