

Inhalt

	Seite
Vorwort	2
Europäisches Vorwort zu A1	3
Einleitung	10
1 Anwendungsbereich	14
1.1 *Zweck	14
1.2 *Anwendungsgebiet	14
1.3 Beziehung zu anderen Normen	14
1.4 Einhaltung	14
2 *Normative Verweisungen	15
3 *Begriffe	15
4 *Allgemeine Anforderungen	21
4.1 *Qualitätsmanagement-System	21
4.2 *RISIKOMANAGEMENT	22
4.3 *Software-Sicherheitsklassifizierung	22
4.4 *ÄLTERE SOFTWARE	23
4.4.1 Allgemeines	23
4.4.2 RISIKOMANAGEMENT-AKTIVITÄTEN	24
4.4.3 Lückenanalyse	24
4.4.4 Aktivitäten für das Schließen der Lücken	24
4.4.5 Begründung für die Benutzung der ÄLTEREN SOFTWARE	25
5 Software-Entwicklungs-PROZESS	25
5.1 *Planung der Software-Entwicklung	25
5.1.1 Software-Entwicklungsplan	25
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	26
5.1.5 Planung der Software-Integration und der Integrationsprüfung	26
5.1.6 Planung der Software-VERIFIZIERUNG	26
5.1.7 Planung des Software-RISIKOMANAGEMENTS	26
5.1.8 Planung der Dokumentation	26
5.1.9 Planung des Software-Konfigurationsmanagements	27
5.1.10 Zu kontrollierende unterstützende Komponenten	27
5.1.11 Kontrolle der Software-KONFIGURATIONSELEMENTE vor der VERIFIZIERUNG	27
5.1.12 Identifizierung und Vermeidung gemeinsamer Software-Fehler	27
5.2 *Analyse der Software-Anforderungen	28
5.2.1 Ableitung der Software-Anforderungen aus den SYSTEM-Anforderungen und Dokumentation	28
5.2.2 Inhalt der Software-Anforderungen	28

	Seite
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
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	Aufteilung 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 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..... 32
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 33
5.6.4	Inhalt der Software-Integrationsprüfung..... 33
5.6.5	EVALUIERUNG der Software-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 34
5.7.1	Festlegung von Prüfungen für Software-Anforderungen 34
5.7.2	Verwendung eines Problemlösungs-PROZESSES für Software..... 34
5.7.3	Prüfungswiederholung nach Änderungen 34
5.7.4	EVALUIERUNG der SOFTWARE-SYSTEM-Prüfungen..... 34
5.7.5	Inhalte der Aufzeichnungen der SOFTWARE-SYSTEM-Prüfungen..... 34
5.8	*Software-FREIGABE für die Benutzung auf einem SYSTEM-Niveau..... 35
5.8.1	Sicherstellen, dass die VERIFIZIERUNG der Software vollständig ist 35

	Seite
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
5.8.7	Archivierung der Software..... 35
5.8.8	Sicherstellen der zuverlässigen Auslieferung der freigegebenen Software 36
6	Software-Wartungs-PROZESS 36
6.1	*Festlegung eines Plans für die Software-Wartung 36
6.2	*Analyse von Problemen und Änderungen 37
6.2.1	Dokumentation und EVALUATION von Rückmeldungen 37
6.2.1.1	Überwachung von Rückmeldungen..... 37
6.2.1.2	Dokumentation und EVALUATION von Rückmeldungen..... 37
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 38
6.3.1	Verwendung eines festgelegten PROZESSES für die Implementierung von Änderungen..... 38
6.3.2	Erneute FREIGABE eines geänderten SOFTWARE-SYSTEMS 38
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..... 39
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	nicht benutzt..... 39
7.3.3	Dokumentation der RÜCKVERFOLGBARKEIT 39
7.4	RISIKOMANAGEMENT von Software-Änderungen 40
7.4.1	Analyse von Änderungen an MEDIZINPRODUKTE-SOFTWARE im Hinblick auf die SICHERHEIT 40
7.4.2	Analyse der Auswirkung von Software-Änderungen auf bestehende RISIKOBEHERRSCHUNGS-Maßnahmen 40

	Seite
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
8.1.3 Identifizierung der Dokumentation der SYSTEM-Konfiguration	41
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.....	42
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
Anhang B (informativ) Anleitung für die Bestimmungen dieser Norm	47
Anhang C (informativ) Beziehung zu anderen Normen.....	65
Anhang D (informativ) Implementierung.....	88
Literaturhinweise.....	90
Stichwortverzeichnis der definierten Begriffe deutsch – englisch	92
Stichwortverzeichnis der definierten Begriffe englisch – deutsch	94
Anhang ZA (normativ) Normative Verweisungen auf internationale Publikationen mit ihren entsprechenden europäischen Publikationen	96
Anhang ZZ (informativ) Zusammenhang mit grundlegenden Anforderungen von EG-Richtlinien	97
Bilder	
Bild 1 – Überblick über Software-Entwicklungs-PROZESSE und -AKTIVITÄTEN	11
Bild 2 – Überblick über Software-Wartungs-PROZESSE und -AKTIVITÄTEN.....	12
Bild 3 – Zuordnen einer Software-Sicherheitsklasse.....	22
Bild B.2 – Bildliche Darstellung der Beziehung zwischen GEFÄHRDUNG, Folge von Ereignissen, GEFÄHRDUNGSSITUATION und SCHADEN (ISO 14971:2007, Anhang E)	51
Bild B.1 – Beispiel einer Aufteilung von SOFTWARE-KOMPONENTEN.....	53
Bild C.1 – Beziehung von wichtigen MEDIZINPRODUKTE-Normen zur IEC 62304	66

	Seite
Bild C.2 – Software als Teil des V-Modells	70
Bild C.3 – Anwendung von IEC 62304 mit IEC 61010-1	79
Tabellen	
Tabelle A.1 – Zusammenfassung der Anforderungen nach Software-Sicherheitsklassen	46
Tabelle B.1 – Entwicklungs-(Modell-)Strategien wie in ISO/IEC 12207 definiert	48
Tabelle C.1 – Beziehung zu ISO 13485:2003	67
Tabelle C.2 – Beziehung zu ISO 14971:2007	68
Tabelle C.3 – Beziehung zur IEC 60601-1	72
Tabelle C.5 – Beziehung zu ISO/IEC 12207:2008	81
Tabelle D.1 – Checkliste für kleine Unternehmen ohne zertifiziertes QM-SYSTEM	89