

Inhalt

	Seite
Vorwort.....	2
Einleitung	8
1 Anwendungsbereich	9
2 Normative Verweisungen	10
3 Begriffe	10
4 Ziele und Konformität	13
5 Software-Dokumentation	13
5.1 Ziel	13
5.2 Anforderungen	13
6 Personal und Verantwortlichkeiten	14
6.1 Ziele	14
6.2 Anforderungen	14
7 Fragen des Lebenszyklus und Dokumentation	15
7.1 Ziele	15
7.2 Anforderungen	15
8 Software-Anforderungsspezifikation	17
8.1 Ziele	17
8.2 Eingangsdokumente	17
8.3 Ausgangsdokumente	18
8.4 Anforderungen	18
9 Software-Architektur	19
9.1 Ziele	19
9.2 Eingangsdokumente	19
9.3 Ausgangsdokumente	19
9.4 Anforderungen	19
10 Software-Entwurf und Implementierung	21
10.1 Ziele	21
10.2 Eingangsdokumente	21
10.3 Ausgangsdokumente	21
10.4 Anforderungen	21
11 Software-Verifikation und Testen	23
11.1 Ziele	23
11.2 Eingangsdokumente	23
11.3 Ausgangsdokumente	24
11.4 Anforderungen	24
12 Software/Hardware-Integration	26
12.1 Ziele	26
12.2 Eingangsdokumente	26

— Vornorm —

DIN V VDE V 0832-500 (VDE V 0832-500):2008-01

	Seite
12.3 Ausgangsdokumente	27
12.4 Anforderungen	27
13 Software-Validierung.....	28
13.1 Ziele	28
13.2 Eingangsdokumente	28
13.3 Ausgangsdokumente	28
13.4 Anforderungen	28
14 Software-Begutachtung	29
14.1 Ziele	29
14.2 Eingangsdokumente	29
14.3 Ausgangsdokumente	30
14.4 Anforderungen	30
15 Software-Qualitätssicherung.....	30
15.1 Ziele	30
15.2 Eingangsdokumente	30
15.3 Ausgangsdokumente	31
15.4 Anforderungen	31
16 Software-Wartung.....	33
16.1 Ziele	33
16.2 Eingangsdokumente	33
16.3 Ausgangsdokumente	33
16.4 Anforderungen	33
17 Anwendungsspezifisch konfigurierbare Systeme	34
17.1 Ziele	34
17.2 Eingangsdokumente	34
17.3 Ausgangsdokumente	35
17.4 Anforderungen	35
Anhang A (normativ) Kriterien für die Auswahl der Techniken und Maßnahmen.....	42
Anhang B (informativ) Verfahrensübersicht.....	53
B.1 KI (Künstliche-Intelligenz)-Fehlerkorrektur (en: AI Fault Correction) (zu Abschnitt 9)	53
B.2 Analysierbare Programme (zu Abschnitt 10).....	53
B.3 Avalanche-/Belastungstests (en: Avalanche/Stress Testing) (zu Tabelle A.17)	54
B.4 Grenzwertanalyse (en: Boundary Value Analysis) (zu den Tabellen A.13, A.14 und A.19).....	54
B.5 Rückwärts-Regeneration (en: Backward Recovery) (zu Abschnitt 9)	55
B.6 Ursache-Wirkungsdiagramme (en: Cause Consequence Diagrams) (zu Abschnitt 14 und Tabelle A.14).....	55
B.7 Zertifizierte Werkzeuge und zertifizierte Übersetzer (en: Certified Tools and certified Translators) (zu Abschnitt 10).....	56
B.8 Checklisten (en: Checklists) (zu Abschnitt 14 und Tabelle A.19).....	56
B.9 Steuerflussanalyse (en: Control Flow Analysis) (zu Tabelle A.19).....	57

	Seite
B.10 Analyse gemeinsamer Fehler (en: Common Cause Failure Analysis) (zu Abschnitt 14)	57
B.11 Datenflussanalyse (en: Data Flow Analysis) (zu Tabelle A.19)	58
B.12 Datenflussdiagramme (en: Data Flow Diagrams) (zu den Tabellen A.16 und A.18)	59
B.13 Datenaufzeichnung und -analyse (en: Data Recording and Analysis) (zu den Abschnitten 10 und 16)	59
B.14 Entscheidungstabellen (Wahrheitstabellen) (en: Decision Tables (Truth Tables)) (zu Abschnitt 14 und Tabelle A.18)	60
B.15 Defensive Programmierung (en: Defensive Programming) (zu Abschnitt 9)	60
B.16 Entwurfs- und Codierstandards (en: Design and Coding Standards) (zu Tabelle A.12).....	61
B.17 Diversitäre Programmierung (en: Diverse Programming) (zu Abschnitt 9).....	62
B.18 Dynamische Rekonfiguration (en: Dynamic Reconfiguration) (zu Abschnitt 9)	62
B.19 Tests auf Basis von Äquivalenzklassen und Eingangsdaten-Unterteilung (en: Equivalence Classes and Input Partitioning Testing) (zu den Tabellen A.13 und A.14)	63
B.20 Fehlererkennende und -korrigierende Codes (en: Error Detecting and Correcting Codes) (zu Abschnitt 9).....	63
B.21 Fehlererwartung (en: Error Guessing) (zu den Tabellen A.13 und A.19)	64
B.22 Fehlereinstreuung (en: Error Seeding) (zu Tabelle A.13)	64
B.23 Ereignisbaumanalyse (en: Event Tree Analysis) (zu Abschnitt 14)	65
B.24 Fagan-Inspektionen (en: Fagan Inspections) (zu Tabelle A.19)	65
B.25 Failure-Assertion-Programmierung (en: Failure Assertion Programming) (zu Abschnitt 9).....	65
B.26 SEEA – Softwarefehler-Auswirkungsanalyse (en: Software Error Effect Analysis) (zu den Abschnitten 9, 11 und 14)	66
B.27 Fehlererkennung und Diagnose (en: Fault Detection and Diagnosis) (zu Abschnitt 9)	67
B.28 Fehlerbaumanalyse (en: Fault Tree Analysis) (zu den Abschnitten 9 und 14)	67
B.29 Endliche Zustandsmaschinen (FSM)/Zustands-Übergangsdigramme (en: Finite State Machines/State Transition Diagrams) (zu den Tabellen A.16 und A.18)	68
B.30 Formale Verfahren (en: Formal Methods) (zu den Abschnitten 8 und 10 und Tabelle A.16)	69
B.30.1 CCS – Berechnung von Kommunikationssystemen (en: Calculus of Communicating Systems).....	69
B.30.2 CSP – Kommunikation in sequentiellen Prozessen (en: Communicating Sequential Processes).....	70
B.30.3 HOL – Logik höherer Ordnung (en: Higher Order Logic)	70
B.30.4 LOTOS (en: Language for Temporal Ordering Specification).....	70
B.30.5 OBJ.....	71
B.30.6 Zeitliche Logik (en: Temporal Logic)	71
B.30.7 VDM – Wiener Entwicklungsverfahren (en: Vienna Development Method).....	72
B.30.8 Z und B	73
B.31 Formaler Nachweis (en: Formal Proof) (zu Abschnitt 11)	73
B.32 Vorwärts-Regeneration (en: Forward Recovery) (zu Abschnitt 9)	74
B.33 Auswirkungsanalyse (en: Impact Analysis) (zu Abschnitt 16).....	74
B.34 Information-Hiding/Einkapselung (en: Information Hiding/Encapsulation) (zu Tabelle A.20)	74
B.35 Schnittstellentests (en: Interface Testing) (zu Abschnitt 10)	75

— Vornorm —

DIN V VDE V 0832-500 (VDE V 0832-500):2008-01

	Seite
B.36 Untermenge der Programmiersprache (en: Language Subset) (zu Abschnitt 10 und Tabelle A.15).....	75
B.37 Aufzeichnung ausgeführter Fälle (en: Memorising Executed Cases) (zu Abschnitt 9)	76
B.38 Bibliothek bewährter/verifizierter Module und Komponenten (en: Library of Trusted/Verified Modules and Components) (zu Abschnitt 10)	76
B.39 Markov-Modelle (zu Abschnitt 14)	77
B.40 Metriken (en: Metrics) (zu den Abschnitten 11 und 14).....	77
B.41 Modularer Ansatz (en: Modular Approach) (zu Tabelle A.20)	78
B.42 Leistungs-Modellierung (en: Performance Modelling) (zu den Tabellen A.13 und A.16).....	78
B.43 Leistungsanforderungen (en: Performance Requirements) (zu Tabelle A.17).....	79
B.44 Wahrscheinlichkeits-Tests (en: Probabilistic Testing) (zu den Abschnitten 11 und 13).....	80
B.45 Prozesssimulation (zu Tabelle A.14)	80
B.46 Prototyping/Animation (zu den Tabellen A.14 und A.16).....	81
B.47 Recovery Block (zu Abschnitt 9).....	81
B.48 Zuverlässigkeits-Blockdiagramme (en: Reliability Block Diagram) (zu Abschnitt 14)	82
B.49 Antwortzeiten und Speichergrenzen (en: Response Timing and Memory Constraints) (zu Tabelle A.17).....	82
B.50 Retry-Fault-Recovery-Mechanismen (zu Abschnitt 9).....	82
B.51 Externe Überwachungseinrichtung (en: Safety Bag) (zu Abschnitt 9)	83
B.52 Nebenpfadanalyse (en: Sneak Circuit Analysis) (zu Tabelle A.19).....	83
B.53 Software-Konfigurationsmanagement (en: Software Configuration Management) (zu Abschnitt 15).....	84
B.54 Streng typisierte Programmiersprache (en: Strongly Typed Programming Languages) (zu Abschnitt 10)	84
B.55 Strukturabhängige Tests (en: Structure Based Testing) (zu Tabelle A.13).....	85
B.56 Strukturdiagramme (en: Structure Diagrams) (zu Tabelle A.16)	86
B.57 Strukturierte Verfahrenslehren (en: Structured Methodology) (zu den Abschnitten 8 und 10)	86
B.57.1 Kontrollierte Anforderungsbeschreibung (CORE) (en: Controlled Requirements Expression)	87
B.57.2 JSD – Systementwicklung nach Jackson (en: Jackson System Development)	88
B.57.3 MASCOT (en: Modular Approach to Software Construction, Operation and Test).....	88
B.57.4 Echtzeit nach Yourdon (en: Real-time Yourdon)	89
B.57.5 SADT – Strukturierte Analyse und Entwurfstechnik (en: Structured Analysis and Design Technique)	89
B.58 Strukturierte Programmierung (en: Structured Programming) (Abschnitt 10)	90
B.59 Geeignete Programmiersprachen (en: Suitable Programming Languages) (zu Tabelle A.15).....	91
B.60 Symbolische Ausführung (en: Symbolic Execution) (zu Tabelle A.19)	92
B.61 Zeit-Petri-Netze (en: Time Petri Nets) (zu den Tabellen A.16 und A.18)	92
B.62 Betriebsbewährter Übersetzer (en: Translator Proven in Use) (zu Abschnitt 10)	93
B.63 Walkthroughs/Entwurfsüberprüfungen (en: Walkthroughs/Design Reviews) (zu Tabelle A.19).....	93
B.64 Fuzzy-Logik (en: Fuzzy Logic) (zu Abschnitt 10).....	94
B.65 Objektorientierte Programmierung (en: Object Oriented Programming) (zu Abschnitt 10).....	95
B.66 Verfolgbarkeit (en: Traceability) (zu Abschnitt 11).....	96

Bilder:

Bild 1 – Softwaresicherheit, Übersicht über das Vorgehen	37
Bild 2 – Entwicklungs-Lebenszyklus 1	38
Bild 3 – Entwicklungs-Lebenszyklus 2	39
Bild 4 – Unabhängigkeit bei der Software-Anforderungsstufe 3	40
Bild 5 – Beziehung zwischen der Entwicklung des generischen Systems und der Entwicklung der Anwendung.....	41
Tabelle 1 – Dokumenten-Cross-Referenz-Tabelle	17
Tabelle A.1 – Fragen des Lebenszyklus und Dokumentation (Abschnitt 7)	43
Tabelle A.2 – Software-Anforderungsspezifikation (Abschnitt 8)	43
Tabelle A.3 – Software-Architektur (Abschnitt 9)	44
Tabelle A.4 – Software-Entwurf und -Implementierung (Abschnitt 10)	45
Tabelle A.5 – Verifikation und Testen (Abschnitt 11)	46
Tabelle A.6 – Software/Hardware-Integration (Abschnitt 12)	46
Tabelle A.7 – Software-Validierung (Abschnitt 13)	46
Tabelle A.8 – Zu begutachtende Abschnitte	47
Tabelle A.9 – Software-Begutachtung (Abschnitt 14) – Techniken der Begutachtung	47
Tabelle A.10 – Software-Qualitätssicherung (Abschnitt 15)	48
Tabelle A.11 – Software-Wartung (Abschnitt 16)	48
Tabelle A.12 – Entwurfs- und Codierstandards (referenziert aus Abschnitt 10)	49
Tabelle A.13 – Dynamische Analyse und Testen (referenziert aus den Abschnitten 11 und 14)	49
Tabelle A.14 – Funktions-/Black-Box-Tests (referenziert aus den Abschnitten 10, 12, 13 und 14)	50
Tabelle A.15 – Programmiersprachen (referenziert aus Abschnitt 10)	50
Tabelle A.16 – Modellierung (referenziert aus Abschnitt 13)	51
Tabelle A.17 – Leistungstests (referenziert aus den Abschnitten 10, 12 und 13)	51
Tabelle A.18 – Formale Verfahren (referenziert aus den Abschnitten 8 und 10)	51
Tabelle A.19 – Statische Analyse (referenziert aus den Abschnitten 11 und 14)	52
Tabelle A.20 – Modulare Verfahren (referenziert aus Abschnitt 10)	52