

Inhalt

	Seite
Europäisches Vorwort.....	7
Einleitung	8
1 Anwendungsbereich.....	11
2 Normative Verweisungen	12
3 Begriffe und Abkürzungen.....	12
3.1 Begriffe	12
3.2 Abkürzungen	17
4 Ziele, Konformität und Software-Integritätslevel	17
5 Softwaremanagement und -organisation	18
5.1 Organisation, Rollen und Verantwortlichkeiten	18
5.2 Kompetenz der Mitarbeiter	22
5.3 Fragen des Lebenszyklus und Dokumentation	23
6 Software-Sicherung.....	26
6.1 Softwaretests.....	26
6.2 Software-Verifikation	27
6.3 Software-Validierung	29
6.4 Software-Begutachtung.....	31
6.5 Software-Qualitätssicherung	33
6.6 Änderungen und Änderungsmanagement	36
6.7 Unterstützende Werkzeuge und Sprachen	37
7 Entwicklung von Software	40
7.1 Lebenszyklus und Dokumentation für Software	40
7.2 Software-Anforderungen	41
7.3 Architektur und Entwurf.....	43
7.4 Komponentenentwurf	49
7.5 Implementierung und Test der Komponenten.....	51
7.6 Integration.....	53
7.7 Test der Gesamtsoftware/Abschließende Validierung	54
7.8 Entwicklung der Software, die durch Anwendungsdaten konfiguriert wird	57
8 Systeme, die durch Anwendungsdaten konfiguriert werden: Entwicklung von Anwendungsdaten.....	57
8.1 Ziele	57
8.2 Eingangsdokumente.....	58
8.3 Ausgangsdokumente.....	58
8.4 Anforderungen.....	58
9 Bereitstellung und Wartung der Software.....	62
9.1 Bereitstellung der Software	62

	Seite
9.2	Wartung der Software 64
Anhang A (normativ)	Kriterien für die Auswahl der Techniken und Maßnahmen 67
A.1	Tabellen zu den Abschnitten 68
A.2	Detaillierte Tabellen 74
Anhang B (normativ)	Software-Schlüsselrollen und Verantwortlichkeiten 79
Anhang C (informativ)	Zusammenfassung der Dokumentenkontrolle 87
Anhang D (informativ)	Verfahrensübersicht 89
D.1	KI(Künstliche-Intelligenz)-Fehlerkorrektur (en: AI Fault Correction) 89
D.2	Analysierbare Programme 89
D.3	Avalanche-/Belastungstests (en: Avalanche/Stress Testing) 90
D.4	Grenzwertanalyse (en: Boundary Value Analysis)..... 90
D.5	Rückwärts-Regeneration (en: Backward Recovery) 91
D.6	Ursache-Wirkungsdiagramme (en: Cause Consequence Diagrams)..... 91
D.7	Checklisten (en: Checklists)..... 91
D.8	Steuerflussanalyse (en: Control Flow Analysis)..... 92
D.9	Analyse gemeinsamer Fehler (en: Common Cause Failure Analysis) 92
D.10	Datenflussanalyse (en: Data Flow Analysis)..... 93
D.11	Datenflussdiagramme (en: Data Flow Diagrams)..... 93
D.12	Datenaufzeichnung und -analyse (en: Data Recording and Analysis) 94
D.13	Entscheidungstabellen (Wahrheitstabellen) (en: Decision Tables (Truth Tables))..... 94
D.14	Defensive Programmierung (en: Defensive Programming) 95
D.15	Codierstandards und Anleitung zum Programmierstil (en: Coding Standards and Style Guide)..... 96
D.16	Diversitäre Programmierung (en: Diverse Programming)..... 97
D.17	Dynamische Rekonfiguration (en: Dynamic Reconfiguration) 98
D.18	Tests auf Basis von Äquivalenzklassen und Eingangsdaten-Unterteilung (en: Equivalence Classes and Input Partitioning Testing) 98
D.19	Fehlererkennende und -korrigierende Codes (en: Error Detecting and Correcting Codes) 98
D.20	Fehlererwartung (en: Error Guessing) 99
D.21	Fehlereinstreuung (en: Error Seeding) 99
D.22	Ereignisbaumanalyse (en: Event Tree Analysis) 99
D.23	Fagan-Inspektionen (en: Fagan Inspections) 100
D.24	„Failure Assertion“-Programmierung (en: Failure Assertion Programming) 100
D.25	SEEA – Softwarefehler-Auswirkungsanalyse (en: Software Error Effect Analysis)..... 101
D.26	Fehlererkennung und Diagnose (en: Fault Detection and Diagnosis)..... 101
D.27	Finite-Zustandsmaschinen (FSM)/Zustands-Übergangsdigramme (en: Finite State Machines/State Transition Diagrams)..... 102
D.28	Formale Methoden (en: Formal Methods) 103
D.29	Formaler Beweis (en: Formal Proof)..... 108

	Seite
D.30 Vorwärts-Regeneration (en: Forward Recovery)	108
D.31 Abgestufte Funktionseinschränkungen (en: Graceful Degradation)	109
D.32 Auswirkungsanalyse (en: Impact Analysis)	109
D.33 Information-Hiding/Einkapselung (en: Information Hiding/Encapsulation)	109
D.34 Schnittstellentests (en: Interface Testing)	110
D.35 Untermenge der Programmiersprache (en: Language Subset)	110
D.36 Aufzeichnung ausgeführter Fälle (en: Memorising Executed Cases)	111
D.37 Metriken (en: Metrics)	111
D.38 Modularer Ansatz (en: Modular Approach)	111
D.39 Leistungs-Modellierung (en: Performance Modelling)	112
D.40 Leistungsanforderungen (en: Performance Requirements)	113
D.41 Wahrscheinlichkeits-Tests (en: Probabilistic Testing)	113
D.42 Prozesssimulation (en: Process Simulation)	114
D.43 Prototyping/Animation	114
D.44 Recovery Block	114
D.45 Antwortzeiten und Speichergrenzen (en: Response Timing and Memory Constraints)	115
D.46 „Re-Try Fault Recovery“-Mechanismen (en: Re-Try Fault Recovery Mechanisms)	115
D.47 Externe Überwachungseinrichtung (en: Safety Bag)	115
D.48 Software-Konfigurationsmanagement (en: Software Configuration Management)	116
D.49 Streng typisierte Programmiersprache (en: Strongly Typed Programming Languages)	116
D.50 Strukturabhängige Tests (en: Structure Based Testing)	116
D.51 Strukturdiagramme (en: Structure Diagrams)	117
D.52 Strukturierte Methodik (en: Structured Methodology)	118
D.53 Strukturierte Programmierung (en: Structured Programming)	118
D.54 Geeignete Programmiersprachen (en: Suitable Programming Languages)	119
D.55 Zeit-Petri-Netze (en: Time Petri Nets)	120
D.56 Walkthroughs/Entwurfsüberprüfungen (en: Walkthroughs/Design Reviews)	120
D.57 Objektorientierte Programmierung (en: Object Oriented Programming)	120
D.58 Rückverfolgbarkeit (en: Traceability)	121
D.59 Metaprogrammierung (en: Metaprogramming)	122
D.60 Prozedurale Programmierung (en: Procedural programming)	122
D.61 Absichtlich gestrichen	123
D.62 Absichtlich gestrichen	123
D.63 Absichtlich gestrichen	123
D.64 Absichtlich gestrichen	123
D.65 Datenmodellierung (en: Data modelling)	123
D.66 Kontrollflussdiagramm/Kontrollflussgraph (en: Control Flow Diagram/Control Flow Graph)	123
D.67 Ablaufdiagramm (en: Sequence diagram)	125

	Seite	
D.68	Tabellarische Spezifikationsverfahren (en: Tabular Specification Methods).....	125
D.69	Anwendungsspezifische Sprache (en: Application specific language).....	125
D.70	UML (Unified Modelling Language)	125
D.71	Domänenspezifische Sprachen (en: Domain specific languages).....	126
D.72	Trennung.....	127
Anhang ZY (informativ) Änderungen in dieser Europäischen Norm im Vergleich zu EN 50128:2011		129
Literaturhinweise		134
Bilder		
Bild 1 – Software, Übersicht über das Vorgehen		10
Bild 2 – Darstellung der bevorzugten Organisationsstruktur.....		20
Bild 3 – Beispielhafter Entwicklungs-Lebenszyklus 1		25
Bild 4 – Beispielhafter Entwicklungs-Lebenszyklus 2		26
Tabellen		
Tabelle 1 – Beziehung zwischen Werkzeugklasse und anwendbarem Abschnitt		40
Tabelle A.1 – Fragen des Lebenszyklus und der Dokumentation (5.3)		68
Tabelle A.2 – Software-Anforderungsspezifikation (7.2).....		70
Tabelle A.3 – Software-Architektur (7.3)		70
Tabelle A.4 – Software-Entwurf und -Implementierung (7.4).....		71
Tabelle A.5 – Verifikation und Testen (6.2 und 7.3).....		72
Tabelle A.6 – Integration (7.6).....		72
Tabelle A.7 – Testen der Gesamtsoftware (6.2 und 7.7)		73
Tabelle A.8 – Software-Analysetechniken (6.3)		73
Tabelle A.9 – Software-Qualitätssicherung (6.5)		73
Tabelle A.10 – Software-Wartung (9.2).....		74
Tabelle A.11 – Techniken für die Datengenerierung (8.4)		74
Tabelle A.12 – Codierstandards.....		74
Tabelle A.13 – Dynamische Analyse und Testen		75
Tabelle A.14 – Funktions-/Black-Box-Tests		75
Tabelle A.15 – Absichtlich gestrichen		75
Tabelle A.16 – Absichtlich gestrichen		75
Tabelle A.17 – Modellierung.....		76
Tabelle A.18 – Leistungstests		76
Tabelle A.19 – Statische Analyse.....		76
Tabelle A.20 – Komponenten.....		77
Tabelle A.21 – Testabdeckung für Code.....		77
Tabelle A.22 – Objektorientierte Software-Architektur		78
Tabelle A.23 – Objektorientierter detaillierter Entwurf.....		78
Tabelle B.1 – Spezifikation der Rolle des Anforderungsmanagers.....		79

	Seite
Tabelle B.2 – Spezifikation der Rolle des Entwerfers.....	80
Tabelle B.3 – Spezifikation der Rolle des Implementierers.....	80
Tabelle B.4 – Spezifikation der Rolle des Testers.....	81
Tabelle B.5 – Spezifikation der Rolle des Verifizierers.....	82
Tabelle B.6 – Spezifikation der Rolle des Integrators.....	83
Tabelle B.7 – Spezifikation der Rolle des Validierers.....	84
Tabelle B.8 – Spezifikation der Rolle des Gutachters.....	85
Tabelle B.9 – Spezifikation der Rolle des Projektmanagers.....	86
Tabelle B.10 – Spezifikation der Rolle des Konfigurationsmanagers.....	86
Tabelle C.1 – Zusammenfassung der Dokumentenkontrolle.....	87
Tabelle ZY.1 – Zusammenhang zwischen dieser Europäischen Norm und EN 50128:2011.....	129