

	Kernkraftwerke Leittechnik für Systeme mit sicherheitstechnischer Bedeutung Allgemeine Systemanforderungen (IEC 61513:2001)	DIN IEC 61513
VDE	Diese Norm ist zugleich eine VDE-Bestimmung im Sinne von VDE 0022. Sie ist nach Durchführung des vom VDE-Vorstand beschlossenen Genehmigungsverfahrens unter nebenstehenden Nummern in das VDE-Vorschriftenwerk aufgenommen und in der etz Elektrotechnische Zeitschrift bekannt gegeben worden.	Klassifikation VDE 0491 Teil 2
ICS 27.120.20 Nuclear power plants Instrumentation and control for systems important to safety General requirements for systems (IEC 61513:2001) Centrales nucléaires Instrumentation et contrôle commande des systèmes importants pour la sûreté Prescriptions générales pour les systèmes (CEI 61513:2001) Die Internationale Norm IEC 61513:2001 „Nuclear power plants – Instrumentation and control for systems important to safety – General requirements for systems“ ist unverändert in diese Deutsche Norm übernommen worden. Beginn der Gültigkeit Diese Norm gilt ab 01. Oktober 2002 Nationales Vorwort Für die vorliegende Norm ist das nationale Arbeitsgremium GUK 967.1 „Reaktorinstrumentierung“ der DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE zuständig. Bei Fragen der Interpretation von Aussagen wird empfohlen, ergänzend auf die zugrunde liegende, in englischer und französischer Sprache erschienene IEC-Publikation zurückzugreifen. Norm-Inhalt war veröffentlicht als E DIN IEC 61513:2000-01. Die Internationale Norm wurde vom SC 45A „Reactor instrumentation“ des TC 45 „Nuclear instrumentation“ der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet. Diese Norm, deren Anwendung international empfohlen wird, gibt das höchstmögliche Maß internationaler Übereinstimmung für das behandelte Sachgebiet wieder. Die Auslegung kerntechnischer Anlagen in Deutschland wird wesentlich durch die Strahlenschutzverordnung, die BMI-Kriterien, die KTA-Regeln und die RSK-Leitlinien bestimmt. Fortsetzung Seite 2 bis 94 DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE		

In der Reihe VDE 0491 sind erschienen:

- **DIN IEC 61226 (VDE 0491 Teil 1)**, *Kernkraftwerke – Sicherheitsleittechnik – Kategorisierung* (IEC 61226:1993)
- **DIN IEC 61513 (VDE 0491 Teil 2)**, *Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Allgemeine Systemanforderungen* (IEC 61513:2001)
- **DIN IEC 60880-2 (VDE 0491 Teil 3-2)**, *Kernkraftwerke – Software für Rechner mit sicherheitstechnischer Bedeutung – Teil 2: Vorkehrungen gegen Versagen aufgrund von Softwarefehlern, Verwendung von Software-Werkzeugen und von vorgefertigter Software* (IEC 60880-2:2000)
- **DIN IEC 62117 (VDE 0491 Teil 4)**, *Kernkraftwerke – Druckwasserreaktoren – Überwachung ausreichender Kühlung des Kerns im abgeschalteten Zustand des Reaktors* (IEC 62117:1999)
- **DIN IEC 61839 (VDE 0491 Teil 5)**, *Kernkraftwerke – Auslegung von Warten – Analyse und Zuordnung der Funktionen* (IEC 61839:2000)

Als weitere Teile der Reihe VDE 0491 sind derzeit vorgesehen:

- **DIN IEC 60880 (VDE 0491 Teil 3-1)**, *Kernkraftwerke – Software für Rechner mit sicherheitstechnischer Bedeutung – Anforderungen an Software für Funktionen der Kategorie A* (IEC 60880:xxxx)
- **DIN IEC 62138 (VDE 0491 Teil 3-3)**, *Kernkraftwerke – Software für Rechner mit sicherheitstechnischer Bedeutung – Anforderungen an Software für Funktionen der Kategorien B und C* (IEC 62138:xxxx)

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.

Der Zusammenhang der zitierten Normen mit den entsprechenden Deutschen Normen ist nachstehend wiedergegeben. Zum Zeitpunkt der Veröffentlichung dieser Norm waren die angegebenen Ausgaben gültig.

IEC hat 1997 die Benummerung der IEC-Publikationen geändert. Zu den bisher verwendeten Normnummern wird jeweils 60000 addiert. So ist zum Beispiel aus IEC 68 nun IEC 60068 geworden.

Tabelle NA.1

Europäische Norm	Internationale Norm	Deutsche Norm	Klassifikation im VDE-Vorschriftenwerk
–	IEC 60709:1981	–	–
–	IEC 60780:1998	DIN IEC 60780:2000-12	–
–	IEC 60880:1986	DIN IEC 60880:1987-08	–
–	IEC 60880-2:2000	DIN IEC 60880-2 (VDE 0491 Teil 3-2):2001-12	VDE 0491 Teil 3-2
EN 61000-4-1:2000	IEC 61000-4-1:2000	DIN EN 61000-4-1 (VDE 0847 Teil 4-1):2001-06	VDE 0847 Teil 4-1
EN 61000-4-2:1995 EN 61000-4-2/A1:1998	IEC 61000-4-2:1995 A1:1998	DIN EN 61000-4-2 (VDE 0847 Teil 4-2):2001-12	VDE 0847 Teil 4-2
EN 61000-4-3:1996 EN 61000-4-3/A1:1998 EN 61000-4-3/A2:2001	IEC 61000-4-3:1995 A1:1998 A2:2000	DIN EN 61000-4-3 (VDE 0847 Teil 4-3):2001-12	VDE 0847 Teil 4-3
EN 61000-4-4:1995 EN 61000-4-4/A1:2001 EN 61000-4-4/A2:2001	IEC 61000-4-4:1995 A1:2000 A2:2001	DIN EN 61000-4-4 (VDE 0847 Teil 4-4):2001-12	VDE 0847 Teil 4-4
EN 61000-4-5:1995 EN 61000-4-5/A1:2001	IEC 61000-4-5:1995 A1:2000	DIN EN 61000-4-5 (VDE 0847 Teil 4-5):2001-12	VDE 0847 Teil 4-5
EN 61000-4-6:1996 EN 61000-4-6/A1:2001	IEC 61000-4-6:1996 A1:2000	DIN EN 61000-4-6 (VDE 0847 Teil 4-6):2001-12	VDE 0847 Teil 4-6
EN 61069-1:1993	IEC 61069-1:1991	DIN EN 61069-1:1994-08	–
–	IEC 61226:1993	DIN IEC 61226 (VDE 0491 Teil 1):1997-07	VDE 0491 Teil 1
–	IEC 61500:1996	–	–
EN 61508-1:2001	IEC 61508-1:1998	DIN EN 61508-1 (VDE 0803 Teil 1):2002-.... *)	VDE 0803 Teil 1
EN 61508-2:2001	IEC 61508-2:1998	DIN EN 61508-2 (VDE 0803 Teil 2):2002-.... *)	VDE 0803 Teil 2
EN 61508-4:2001	IEC 61508-4:1998	DIN EN 61508-4 (VDE 0803 Teil 4):2002-.... *)	VDE 0803 Teil 4
–	ISO/IEC 12207:1995	–	–
EN ISO 9000:2000	ISO 9000:2000	DIN EN ISO 9000:2000-12	–
EN ISO 9000-3:1997	ISO 9000-3:1997	DIN EN ISO 9000-3:1998-08	–
EN ISO 9001:2000	ISO 9001:2000	DIN EN ISO 9001:2000-12	–

*) In Vorbereitung

Nationaler Anhang NB (informativ) Literaturhinweise

DIN EN 61000-4-1 (VDE 0847 Teil 4-1), *Elektromagnetische Verträglichkeit (EMV) – Teil 4-1: Prüf- und Messverfahren; Übersicht über die Reihe IEC 61000-4 (IEC 61000-4-1:2000); Deutsche Fassung EN 61000-4-1:2000.*

DIN EN 61000-4-2 (VDE 0847 Teil 4-2), *Elektromagnetische Verträglichkeit (EMV) – Teil 4-2: Prüf- und Messverfahren; Prüfung der Störfestigkeit gegen die Entladung statischer Elektrizität (IEC 61000-4-2:1995 + A1:1998 + A2:2000); Deutsche Fassung EN 61000-4-2:1995 + A1:1998 + A2:2001.*

DIN EN 61000-4-3 (VDE 0847 Teil 4-3), *Elektromagnetische Verträglichkeit (EMV) – Teil 4-3: Prüf- und Messverfahren; Prüfung der Störfestigkeit gegen hochfrequente elektromagnetische Felder (IEC 61000-4-3:1995 + A1:1998 + A2:2000); Deutsche Fassung EN 61000-4-3:1996 + A1:1998 + A2:2001.*

DIN EN 61000-4-4 (VDE 0847 Teil 4-4), *Elektromagnetische Verträglichkeit (EMV) – Teil 4-4: Prüf- und Messverfahren; Prüfung der Störfestigkeit gegen schnelle transiente elektrische Störgrößen/Burst (IEC 61000-4-4:1995 + A1:2000); Deutsche Fassung EN 61000-4-4:1995 + A1:2001.*

DIN EN 61000-4-5 (VDE 0847 Teil 4-5), *Elektromagnetische Verträglichkeit (EMV) – Teil 4-5: Prüf- und Messverfahren; Prüfung der Störfestigkeit gegen Stoßspannungen (IEC 61000-4-5:1995 + A1:2000); Deutsche Fassung EN 61000-4-5:1995 + A1:2001.*

DIN EN 61000-4-6 (VDE 0847 Teil 4-6), *Elektromagnetische Verträglichkeit (EMV) – Teil 4-6: Prüf- und Messverfahren; Störfestigkeit gegen leitungsgeführte Störgrößen, induziert durch hochfrequente Felder (IEC 61000-4-6:1996 + A1:2000); Deutsche Fassung EN 61000-4-6:1996 + A1:2001.*

DIN EN 61069-1, *Leittechnik für industrielle Prozesse – Ermittlung der Systemeigenschaften zum Zweck der Eignungsbeurteilung eines Systems – Teil 1: Allgemeine Überlegungen und Methodik (IEC 61069-1:1991); Deutsche Fassung EN 61069-1:1993.*

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

DIN EN ISO 9000-3, *Normen zum Qualitätsmanagement und zur Qualitätssicherung/QM-Darlegung – Teil 3: Leitfaden für die Anwendung von ISO 9001:1994 auf Entwicklung, Lieferung, Installation und Wartung von Computer-Software (ISO 9000-3:1997); Zweisprachige Fassung EN ISO 9000-3:1997.*

DIN EN ISO 9001, *Qualitätsmanagementsysteme – Anforderungen (ISO 9001:2000-09); Dreisprachige Fassung EN ISO 9001:2000.*

DIN IEC 60780, *Kernkraftwerke – Elektrisches Gerät des Sicherheitssystems – Qualifizierung (IEC 60780:1998).*

DIN IEC 60880, *Software für Rechner im Sicherheitssystem von Kernkraftwerken; Identisch mit IEC 60880, Ausgabe 1986.*

DIN IEC 60880-2 (VDE 0491 Teil 3-2), *Kernkraftwerke – Software für Rechner mit sicherheitstechnischer Bedeutung – Teil 2: Vorkehrungen gegen Versagen aufgrund von Softwarefehlern, Verwendung von Software-Werkzeugen und von vorgefertigter Software (IEC 60880-2:2000).*

DIN IEC 61226 (VDE 0491 Teil 1), *Kernkraftwerke – Sicherheitsleittechnik – Kategorisierung (IEC 61226:1993).*

Nationaler Anhang NC (informativ) Verzeichnis der verwendeten Begriffe

deutsch	englisch	siehe Abschnitt
Abweichung	error	3.19
Anwendungsfunktion	application function	3.1
Anwendungssoftware	application software	3.2
Anwendungssoftware, Bibliothek der	application software library	3.3
anzunehmendes Versagen auslösendes Ereignis (AVE)	postulated initiating event (PIE)	3.41
Architektur, leittechnische	I&C architecture	3.31
Ausfall/Versagen	failure	3.21
bereits verfügbare(s) Software/Hardware/System	pre-existing software/hardware/system	3.65
Bewertung (einer Systemeigenschaft)	evaluation (of a system property)	3.20
Bibliothek der Anwendungssoftware	application software library	3.3
CCF (Versagen aufgrund gemeinsamer Ursache)	common cause failure (CCF)	3.7
Daten	data	3.13
deterministisches Verfahren	deterministic method	3.15
Diversität	diversity	3.16
Einzelversagen/Einzelausfall	single failure	3.55
Einzelversagens-/Einzelausfall-Kriterium	single-failure criterion	3.56
Fehlabschaltung	spurious scram	3.66
Fehler	fault	3.22
Fehlverhalten, menschliches (Irrtum)	human error (mistake)	3.28
FSE	FSE	3.34
Funktion, leittechnische	I&C function	3.32
Funktion, sicherheitstechnisch wichtige	function important to safety	3.26
funktionale Diversität	functional diversity	3.23
funktionale Validierung	functional validation	3.24
Funktionalität	functionality	3.25
Gefährdung	hazard	3.27
Gerät	equipment	3.17
Gerät, unabhängiges	independent equipment	3.29
Gerätefamilie	equipment family	3.18
gesamter Sicherheitslebenszyklus der Leittechnik	overall safety life cycle of the I&C	3.39
Inbetriebnahme des Kernkraftwerks	commissioning of the NPP	3.11
Instandhaltbarkeit	maintainability	3.38
Interrupt	interrupt	3.30
Kanal	channel	3.5
Kategorie einer leittechnischen Funktion	category of an I&C function	3.4
Klasse eines leittechnischen Systems	class of an I&C system	3.6
Komplexität	complexity	3.8
Komponente	component	3.9
Konfigurationsmanagement	configuration management	3.12
Konzept gestufter Maßnahmen	defence-in-depth concept	3.14
Leittechnik, gesamter Sicherheitslebenszyklus der	overall safety life cycle of the I&C	3.39
leittechnische Architektur	I&C architecture	3.31
leittechnische Funktion	I&C function	3.32
leittechnische Funktion, Kategorie einer	category of an I&C function	3.4

deutsch	englisch	siehe Abschnitt
leittechnische Funktionen und zugehörige Systeme und Einrichtungen (FSE)	I&C functions, and the associated systems and equipment (FSE)	3.34
leittechnische Systemarchitektur	I&C system architecture	3.36
leittechnische Teilfunktion	I&C subfunction	3.33
leittechnisches System	I&C system	3.35
leittechnisches System, Klasse eines	class of an I&C system	3.6
Maßnahmen, Konzept gestufter	defence-in-depth concept	3.14
Maßnahmen, sicherheitstechnisch wichtige	items important to safety	3.37
menschliches Fehlverhalten (Irrtum)	human error (mistake)	3.28
probabilistisches Verfahren	probabilistic method	3.43
Projektorganisation	project organisation	3.44
Qualifizierung	qualification	3.45
Qualität	quality	3.46
Qualitätssicherung	quality assurance	3.47
Qualitätssicherungsplan	quality plan	3.48
rechnerbasiertes System	computer based system	3.10
Redundanz	redundancy	3.49
Sicherheitsanalyse der Anlage	plant safety analysis	3.40
Sicherheitsgruppe	safety group	3.52
Sicherheitslebenszyklus der Leittechnik, gesamter	overall safety life cycle of the I&C	3.39
Sicherheitssysteme	safety systems	3.53
sicherheitstechnisch wichtige Funktion	function important to safety	3.26
sicherheitstechnisch wichtige Maßnahmen	items important to safety	3.37
Software, vorgefertigte (VGS)	pre-developed software (PDS)	3.42
Software, wiederverwendbare	reusable software	3.51
Software/Hardware/System, bereits verfügbare(s)	pre-existing software/hardware/system	3.65
Softwarefehler	software fault	3.58
Softwareversagen	software failure	3.57
Softwarezuverlässigkeit	software reliability	3.59
Spezifikation	specification	3.60
System	system	3.62
System, leittechnisches	I&C system	3.35
System, rechnerbasiertes	computer based system	3.10
Systemarchitektur, leittechnische	I&C system architecture	3.36
systematisches Versagen	systematic failure	3.62
System-Sicherheitslebenszyklus	system safety life cycle	3.63
Systemsoftware	system software	3.64
Teilfunktion, leittechnische	I&C subfunction	3.33
unabhängiges Gerät	independent equipment	3.29
Versagen/Ausfall	failure	3.21
Versagen aufgrund gemeinsamer Ursache (CCF)	common cause failure (CCF)	3.7
vorgefertigte Software (VGS)	pre-developed software (PDS)	3.42
wiederverwendbare Software	reusable software	3.51
Zugriffschutz	security	3.54
Zuverlässigkeit	reliability	3.50

Deutsche Übersetzung

Kernkraftwerke
Leittechnik für Systeme mit sicherheitstechnischer Bedeutung
Allgemeine Systemanforderungen

Inhalt

	Seite
Vorwort.....	9
Einleitung.....	10
Zusammenhang mit anderen Normen	10
1 Anwendungsbereich	10
1.1 Allgemeines.....	10
1.2 Anwendung auf neue und in Betrieb befindliche Anlagen	11
1.3 Rahmen.....	11
2 Normative Verweisungen.....	13
3 Begriffe.....	14
4 Formelzeichen und Abkürzungen	27
5 Gesamter Sicherheitslebenszyklus der Leittechnik	28
5.1 Ableitung der Anforderungen an die Leittechnik aus der sicherheitstechnischen Auslegungsgrundlage der Anlage.....	31
5.2 Dokumentation	33
5.3 Auslegung der leittechnischen Gesamtarchitektur und Zuordnung der leittechnischen Funktionen	34
5.4 Gesamtplanung.....	40
5.5 Dokumentation.....	44
6 System-Sicherheitslebenszyklus	44
6.1 Anforderungen	47
6.2 Systemplanung	59
6.3 Dokumentation.....	63
6.4 Systemqualifizierung.....	68
6.5 Zusammenstellung der wesentlichen Anforderungen für verschiedene Klassen und Kategorien.....	72
7 Gesamtintegration und Inbetriebsetzung.....	73
7.1 Anforderungen an die zu erreichenden Ziele.....	73
7.2 Dokumentation	73
8 Gesamtbetrieb und Instandhaltung.....	73
8.1 Anforderungen an die zu erreichenden Ziele.....	73
8.2 Dokumentation	74
 Anhang A (informativ) Grundsätzliche Sachverhalte zur Sicherheit von Kernkraftwerken.....	 75
A.1 Sicherheitsziele der Anlage	75
A.2 Sicherheitsanalyse der Anlage	75
A.2.1 Analyse der Ereignisabläufe	76
A.2.2 Beurteilung der Auslegungsgrundlagen: deterministische/probabilistische Verfahren.....	76
A.3 Gestufte Maßnahmen (Defence in Depth).....	76

	Seite
Anhang B (informativ) Kategorisierung von Funktionen und Klassifizierung von Systemen	78
B.1 Hintergrund des Kategorisierungs-/Klassifizierungsschemas.....	78
B.2 Prinzipien der in dieser Norm angewendeten Kategorisierung und Klassifizierung	78
B.2.1 Verfahrenstechnische Auslegung des Kernkraftwerks	79
B.2.2 Leittechnische Auslegung des Kernkraftwerks	80
B.3 Kategorisierung der sicherheitstechnisch wichtigen leittechnischen Funktionen	81
B.4 Klassifizierung der leittechnischen Systeme	81
Anhang C (informativ) Qualitativer Ansatz zur Vorsorge gegen CCF	83
C.1 Beispiel der Zuordnung von Funktionen einer Sicherheitsgruppe zu Systemen	83
C.2 Beispiele für die CCF-Empfindlichkeit in Sicherheitsgruppen.....	84
Anhang D (informativ) Beziehungen zwischen IEC 61508 und IEC 61513 einschließlich Normen im Bereich nuklearer Anwendungen	87
D.1 Anwendungsbereiche und Konzepte	87
D.2 Zusammenhang zwischen IEC 61508-1 und dieser Norm	89
D.3 Zusammenhang zwischen IEC 61508-2 und dieser Norm	91
D.4 Zusammenhang zwischen einigen wichtigen Begriffen von IEC 61508-4 und Definitionen in dieser Norm sowie im Bereich nuklearer Anwendungen	92
Literaturhinweise	94
Bild 1 – Gesamtrahmen dieser Norm	12
Bild 2 – Typische Zusammenhänge von Hardware und Software in einem rechnerbasierten System	26
Bild 3 – Zusammenhänge zwischen Versagen des Systems, zufälligem Ausfall und systematischem Fehler	27
Bild 4 – Zusammenhänge zwischen dem gesamten Sicherheitslebenszyklus der Leittechnik und den Sicherheitslebenszyklen der einzelnen leittechnischen Systeme	30
Bild 5 – Sicherheitslebenszyklus des Systems	47
Bild 6 – Im System-Qualifizierungsplan anzusprechende Themen.....	71
Bild B.1 – Zusammenhänge zwischen leittechnischen Funktionen und leittechnischen Systemen	79
Bild C.1 – Beispiele der Zuordnung von Funktionen einer Sicherheitsgruppe zu leittechnischen Systemen	83
Tabelle 1 – Übersicht über den gesamten Sicherheitslebenszyklus der Leittechnik	29
Tabelle 2 – Beziehung zwischen Klassen leittechnischer Systeme und Kategorien leittechnischer FSE	34
Tabelle 3 – Übersicht über den Sicherheitslebenszyklus des Systems	46
Tabelle 4 – Anforderungen an Auslegung und Qualifizierung von leittechnischen Systemen und Geräten	72
Tabelle 5 – Anforderungen an die Spezifikation und Realisierung der FSE	72
Tabelle B.1 – Typische Klassifizierung leittechnischer Systeme	82

Vorwort

- 1) Die IEC (Internationale Elektrotechnische Kommission) ist eine weltweite Normungsorganisation, die alle Nationalen Elektrotechnischen Komitees (Nationale Komitees der IEC) umfasst. Die IEC hat das Ziel, die internationale Zusammenarbeit in allen Fragen der Normung auf dem Gebiet der Elektrotechnik und Elektronik zu fördern. Zu diesem Zweck und neben anderen Aktivitäten veröffentlicht die IEC Internationale Normen. Mit der Vorbereitung sind die Technischen Komitees beauftragt. Jedes Nationale Komitee der IEC, das an dem behandelten Thema interessiert ist, darf an dieser Vorbereitungsarbeit teilnehmen. Internationale Organisationen, Regierungs- und Nichtregierungsstellen, die mit der IEC in Verbindung stehen, nehmen ebenfalls an diesen Vorbereitungsarbeiten teil. Die IEC arbeitet eng mit der Internationalen Organisation für Normung (ISO) nach den in der Vereinbarung zwischen beiden Organisationen festgelegten Bedingungen zusammen.
- 2) Die offiziellen Beschlüsse oder Vereinbarungen der IEC über technische Fragen, die in Technischen Komitees von Vertretern aller an dem behandelten Thema besonders interessierten Nationalen Komitees erarbeitet werden, bringen das höchstmögliche Maß internationaler Übereinstimmung für das behandelte Sachgebiet zum Ausdruck.
- 3) Sie stellen Empfehlungen zur internationalen Anwendung dar, die als Normen, Fachberichte oder Leitlinien veröffentlicht werden und als solche von den Nationalen Komitees angenommen sind.
- 4) Um die internationale Vereinheitlichung zu fördern, verpflichten sich die Nationalen Komitees der IEC, Internationale Normen der IEC so durchschaubar wie möglich in ihren nationalen und regionalen Normen anzuwenden. Jede Abweichung zwischen der IEC-Norm und der entsprechenden nationalen oder regionalen Norm muss in dieser deutlich gekennzeichnet werden.
- 5) Die IEC hat kein Verfahren für die Kennzeichnung der Konformität festgelegt und übernimmt keine Verantwortung, wenn ein Gegenstand als konform mit einer ihrer Normen erklärt wird.
- 6) Es besteht die Möglichkeit, dass Bestandteile dieser Internationalen Norm Gegenstand von Patentrechten sind. Die IEC hat nicht die Verantwortung, das Vorhandensein solcher Patentrechte festzustellen und auf deren Existenz hinzuweisen.

Die Internationale Norm IEC 61513 wurde vom Technischen Unterkomitee 45A „Reactor instrumentation“ des Technischen Komitees 45 „Nuclear instrumentation“ der IEC ausgearbeitet.

Dieser Text basiert auf den folgenden Dokumenten:

Internationaler Norm-Entwurf	Abstimmungsbericht
45A/405/FDIS	45A/418/RVD

Ausführliche Auskunft über die Abstimmung zur Genehmigung dieser Norm gibt der in obiger Tabelle zitierte Abstimmungsbericht.

Die Anhänge A, B, C und D dienen nur zur Information.

Diese Norm wurde entsprechend ISO/IEC Directives, Teil 3 ausgearbeitet.

Das Komitee hat entschieden, dass diese Publikation bis 2006 unverändert gültig sein soll. Dann wird die Publikation entsprechend der Entscheidung des Komitees

- bestätigt,
- zurückgezogen,
- durch eine überarbeitete Ausgabe ersetzt oder
- geändert.

Einleitung

Diese Norm enthält Anforderungen an die Leittechnik (Systeme und Geräte), die für die Durchführung sicherheitstechnisch wichtiger Funktionen in Kernkraftwerken verwendet wird.

Diese Norm befasst sich insbesondere mit den Zusammenhängen zwischen:

- den Sicherheitszielen des Kernkraftwerks und den Anforderungen an die Architektur der sicherheitstechnisch wichtigen Leittechnik;
- der Gesamtarchitektur der Leittechnik und den Anforderungen an die einzelnen sicherheitstechnisch wichtigen Systeme.

Zusammenhang mit anderen Normen

Bei der Erarbeitung dieser Norm wurden die Internationalen Normen von IEC und ISO, die Schriften der IAEA-Sicherheitsserie und weitere Dokumente, die den technischen Konsens repräsentieren, verwendet; insbesondere:

a) IEC-Normen für den nuklearen Bereich

Diese Norm nimmt auf andere nukleare Normen der IEC Bezug, insbesondere in Hinblick auf Themen wie Qualifizierung, Wartenauslegung, Kategorisierung von Funktionen und Klassifizierung von Systemen (siehe 3.4 und 3.6) sowie Multiplexing.

Wenn rechnerbasierte Systeme der Klasse 1 angesprochen werden (siehe 5.1.2.1 und Anhang B), ist diese Norm zusammen mit IEC 60880, IEC 60880-2 und IEC 60987 anzuwenden, um die Vollständigkeit der Systemanforderungen an Software und Hardware sicherzustellen.

b) Andere Internationale Normen

Für die Aussagen dieser Norm wurde eine Form ähnlich der in IEC 61508 gewählt, entsprechend werden ein gesamter Sicherheitslebenszyklus und ein Sicherheitslebenszyklus der Systeme festgelegt. In dieser Norm wird außerdem eine Interpretation der allgemeinen Anforderungen von IEC 61508-1, -2 und -4 für den nuklearen Anwendungsbereich bereitgestellt. Übereinstimmung mit vorliegender Norm erleichtert die Konsistenz mit den Anforderungen von IEC 61508, da diese hierin bereits bezüglich ihrer Anwendung in der nuklearen Industrie interpretiert wurden.

Hinsichtlich der Qualitätssicherung bezieht sich vorliegende Norm auf ISO.

c) Schriften der IAEA-Sicherheitsserie

Bei der Erarbeitung dieser Norm wurde auf Übereinstimmung mit den Prinzipien und grundsätzlichen Sicherheitsaspekten für Kernkraftwerke des „IAEA Code of Safety“ und den „IAEA Safety Guides“ geachtet. Tatsächlich sind die genannten IAEA-Dokumente auf alle die Leittechnik betreffenden Normen von IEC/TC 45 anwendbar. Die Terminologie dieser Norm sowie die verwendeten Definitionen sind mit denen von IAEA konsistent (siehe Anmerkung).

ANMERKUNG Entsprechend dem „Agreement of co-operation on matters of common interest“ vom Mai 1981.

Hinsichtlich der Qualitätssicherung bezieht sich vorliegende Norm auf IAEA 50-C-QA (Rev 1).

1 Anwendungsbereich

1.1 Allgemeines

Sicherheitstechnisch wichtige leittechnische Systeme können realisiert werden, indem konventionelles festverdrahtetes Gerät, rechnerbasiertes Gerät oder eine Kombination beider Gerätetypen verwendet wird. Diese Norm enthält Anforderungen und Empfehlungen (siehe Anmerkung) für die gesamte leittechnische Architektur, die auf einer der beiden oder beiden Technologien beruhen kann.

ANMERKUNG Im Folgenden wird „Anforderungen“ als umfassender Begriff für Anforderungen und Empfehlungen verwendet. Die Unterscheidung wird in den Teilen der Norm getroffen, in denen Anforderungen durch „muss“ oder „ist zu“ (en: shall) gekennzeichnet sind, Empfehlungen durch „sollte“ (en: should).

In dieser Norm wird besonders auf komplette und präzise, von den Sicherheitszielen der Anlage abgeleitete Anforderungen Wert gelegt, da dies die erforderliche Voraussetzung zur Festlegung umfassender Anforderungen an die gesamte leittechnische Architektur und folglich an die einzelnen sicherheitstechnisch wichtigen leittechnischen Systeme ist.

In dieser Norm werden die Konzepte des Sicherheitslebenszyklus für die gesamte leittechnische Architektur und des Sicherheitslebenszyklus für die einzelnen Systeme eingeführt. Die Lebenszyklen, die in dieser Norm beschrieben und verfolgt werden, sind nicht die einzig möglichen; andere Lebenszyklen dürfen ebenso genutzt werden, vorausgesetzt, sie genügen den in dieser Norm festgelegten Zielen.

1.2 Anwendung auf neue und in Betrieb befindliche Anlagen

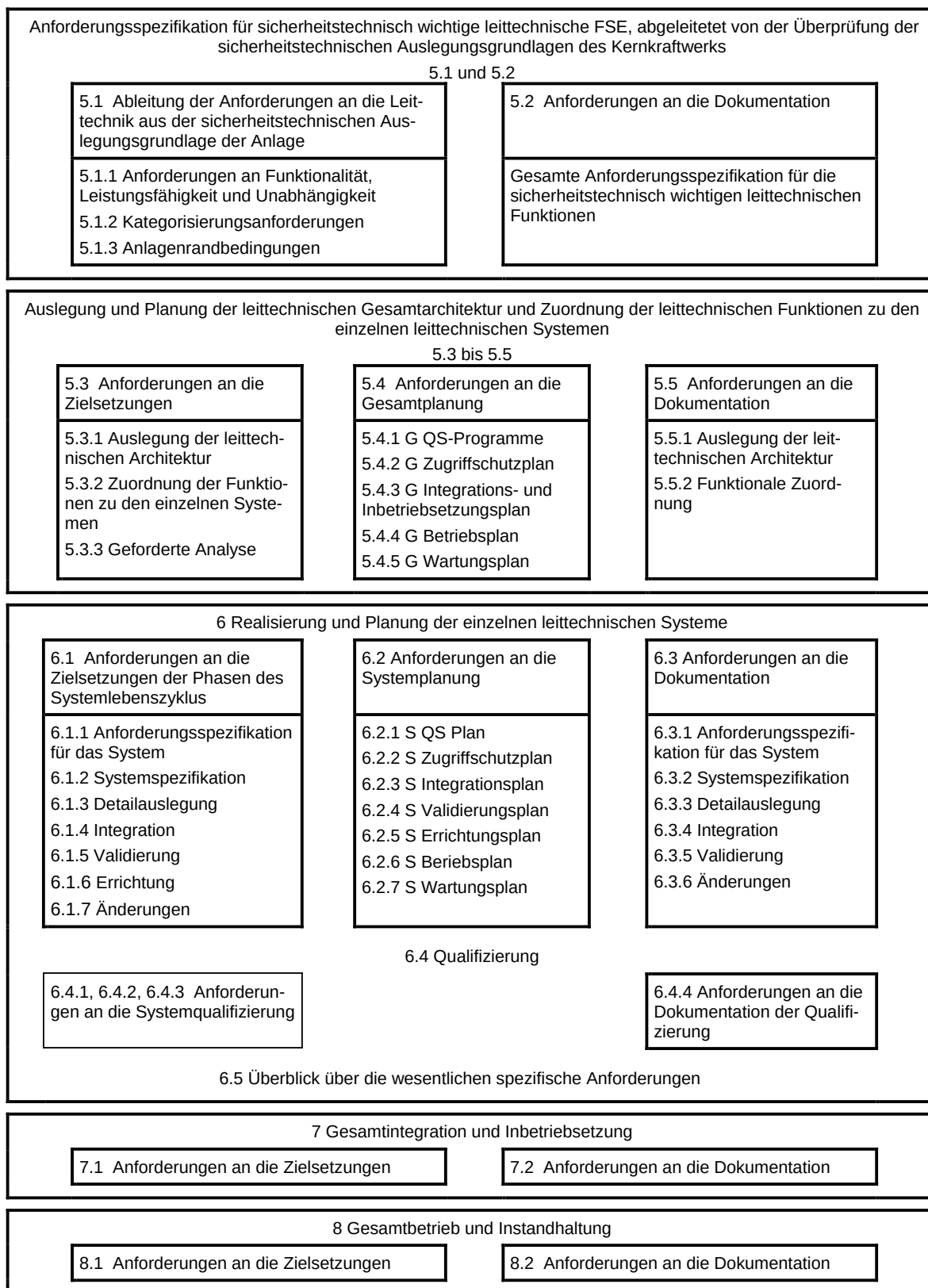
Diese Norm gilt für die Leittechnik neuer Kernkraftwerke und für die Erneuerung oder Verbesserung der Leittechnik in Betrieb befindlicher Anlagen.

Für in Betrieb befindliche Anlagen ist nur eine Teilmenge der Anforderungen zutreffend. Diese Teilmenge ist zu Beginn jedes Projekts zu ermitteln.

1.3 Rahmen

Bild 1 zeigt den Gesamtrahmen dieser Norm, mit seinen normative Aussagen enthaltenden Abschnitten.

- **Abschnitt 5** spricht die Gesamtarchitektur der sicherheitstechnisch wichtigen leittechnischen Systeme an:
 - Definition der Anforderungen an die leittechnischen Funktionen und zugehörigen Systeme und Geräte, abgeleitet von der Sicherheitsanalyse der Anlage, der Kategorisierung der leittechnischen Funktionen sowie der Anlagenauslegung und den betrieblichen Zusammenhängen;
 - Strukturierung der Gesamtarchitektur der Leittechnik, Einteilung in Systeme und Zuordnung der leittechnischen Funktionen zu den Systemen. Auslegungskriterien werden festgelegt, einschließlich jenen zur Erzielung eines DiD-Konzepts (en: defence-in-depth concept) und zur Minimierung des Potenzials von Versagen aufgrund gemeinsamer Ursache (CCF);
 - Planung der Gesamtarchitektur der Leittechnik.
- **Abschnitt 6** beinhaltet die Anforderungen an einzelne sicherheitstechnisch wichtige leittechnische Systeme, insbesondere die Anforderungen an rechnerbasierte Systeme;
- **Abschnitte 7 und 8** enthalten die Gesamtintegration, Inbetriebnahme, Betrieb und Wartung der leittechnischen Systeme;
- **Anhang A** enthält die Zusammenhänge zwischen IAEA-Anforderungen und den grundsätzlichen Sicherheitskonzepten, die in dieser Norm angewendet werden;
- **Anhang B** informiert über Kategorisierungs-/Klassifizierungsprinzipien;
- **Anhang C** zeigt Beispiele von gegenüber CCF empfindlicher Leittechnik;
- **Anhang D** enthält Anleitungen zur Erleichterung des Vergleichs dieser Norm mit **IEC 61508-1, -2 und -4**. Er gibt einen Überblick über die wichtigen Anforderungen der IEC 61508, um sicherzustellen, dass die sicherheitstechnisch relevanten Gesichtspunkte hinreichend berücksichtigt wurden; weiterhin wird auf die Verwendung einer gemeinsamen Terminologie geachtet und es werden die Gründe erläutert, wenn unterschiedliche oder ergänzende Techniken oder Begriffe verwendet werden.



Legende. QS: Qualitätssicherung; G: Gesamt; S: System

Bild 1 – Gesamtrahmen dieser Norm

2 Normative Verweisungen

Die folgenden normativen Dokumente enthalten Festlegungen, die durch Verweisung in diesem Text Bestandteil dieser Internationalen Norm sind. Bei datierten Verweisungen gelten spätere Änderungen oder Überarbeitungen dieser Publikationen nicht. Anwender dieser Internationalen Norm werden jedoch gebeten, die Möglichkeit zu prüfen, die jeweils neuesten Ausgaben der nachfolgend angegebenen normativen Dokumente anzuwenden. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen normativen Dokuments ^{N1)}. Mitglieder von ISO und IEC führen Verzeichnisse der gültigen Internationalen Normen.

IEC 60709:1981, *Separation within the reactor protection system.*

IEC 60780:1998, *Nuclear power plants – Electrical equipment of the safety system – Qualification.*

IEC 60880:1986, *Software for computers in the safety systems of nuclear power stations.*

IEC 60880-2:2000, *Software for computers important to safety for nuclear power plants – Part 2: Software aspects of defence against common cause failures, use of software tools and of pre-developed software.*

IEC 60964:1989, *Design for control rooms of nuclear power plants.*

IEC 60965:1989, *Supplementary control points for reactor shutdown without access to the main control room.*

IEC 60987:1989, *Programmed digital computers important to safety for nuclear power stations.*

IEC 61000-4-1:2000, *Electromagnetic compatibility (EMC) – Part 4-1: Testing and measurement techniques – Overview of IEC 61000-4 series.*

IEC 61000-4-2:1995, *Electromagnetic compatibility (EMC) – Part 4: Testing and measurement techniques – Section 2: Electrostatic discharge immunity test. Basic EMC Publication.*

IEC 61000-4-3:1995, *Electromagnetic compatibility (EMC) – Part 4: Testing and measurement techniques – Section 3: Radiated, radio-frequency, electromagnetic field immunity test.*

IEC 61000-4-4:1995, *Electromagnetic compatibility (EMC) – Part 4: Testing and measurement techniques – Section 4: Electrical fast transient/burst immunity test. Basic EMC Publication.*

IEC 61000-4-5:1995, *Electromagnetic compatibility (EMC) – Part 4: Testing and measurement techniques – Section 5: Surge immunity test.*

IEC 61000-4-6:1996, *Electromagnetic compatibility (EMC) – Part 4: Testing and measurement techniques – Section 6: Immunity to conducted disturbances, induced by radio-frequency fields.*

IEC 61069-1:1991, *Industrial-process measurement and control – Evaluation of system properties for the purpose of system assessment – Part 1: General considerations and methodology.*

IEC 61226:1993, *Nuclear power plants – Instrumentation and control systems important for safety – Classification.*

IEC 61500:1996, *Nuclear power plants – Instrumentation and control systems important for safety – Functional requirements for multiplexed data transmission.*

^{N1)} Nationale Fußnote: Die Verweisungen im Text der Norm sind zwar undatiert, beziehen sich aber immer auf die hier angegebene Ausgabe des Dokuments. Sollen spätere Ausgaben angewendet werden, ist in jedem Einzelfall deren Eignung für die jeweils betroffene Anforderung zu prüfen.

DIN IEC 61513 (VDE 0491 Teil 2):2002-10

IEC 61508-1:1998, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements.*

IEC 61508-2:2000, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems.*

IEC 61508-4:1998, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations.*

ISO/IEC 12207:1995, *Information technology – Software life cycle processes.*

ISO 8402:1994, *Quality management and quality assurance – Vocabulary.* ^{N2)}

ISO 9000-3:1997, *Quality management and quality assurance standards – Part 3: Guidelines for the application of ISO 9001:1994 to the development, supply, installation and maintenance of computer software.*

ISO 9001:1994, *Quality systems – Model for quality assurance in design, development, production, installation and servicing.*

IAEA Safety Series No. 50-C-D (Rev. 1):1988, *Code on the Safety of NPPs: Design.*

IAEA Safety Series No. 50-C-QA (Rev. 1):1988, *Code on the Safety of NPPs: Quality assurance.*

IAEA Safety Series No. 50-SG-D1:1979, *Safety functions and Component Classification for BWR, PWR and PTR – A Safety Guide.*

IAEA Safety Series No. 50-SG-D3:1980, *Protection system and related features in NPPs – A Safety Guide.*

IAEA Safety Series No. 50-SG-D8:1984, *Safety-Related Instrumentation and Control Systems for NPPs – A Safety Guide.*

IAEA Safety Series No. 50-SG-D11:1986, *General Design Safety Principles for NPPs – A Safety Guide.*

IAEA Safety series 75-INSAG-3:1988, *Basic Safety Principles for NPPs.*

3 Begriffe

Für die Anwendung dieser Norm gelten die folgenden Begriffe:

3.1

Anwendungsfunktion

(en: application function)

Funktion eines leittechnischen Systems, die eine Aufgabe in Verbindung mit dem Prozess und nicht mit dem Funktionieren des Systems selbst erfüllt

[2.1 von IEC 60880, modifiziert]

ANMERKUNG 1 Siehe auch „leittechnische Funktion“, „leittechnisches System“, „Anwendungssoftware“.

ANMERKUNG 2 Eine Anwenderfunktion ist üblicherweise eine Teilfunktion einer leittechnischen Funktion.

3.2

Anwendungssoftware

(en: application software)

Teil der Software eines leittechnischen Systems, durch den Anwendungsfunktionen realisiert werden

Siehe [Bild 2](#).

ANMERKUNG 1 Siehe auch „Anwendungsfunktion“, „Bibliothek der Anwendungssoftware“, „Systemsoftware“.

^{N2)} Nationale Fußnote: ISO 8402:1994 ist ersetzt durch ISO 9000:2000.

ANMERKUNG 2 Anwendungssoftware ist nicht Systemsoftware.

3.3

Bibliothek der Anwendungssoftware

(en: application software library)

Sammlung von Softwaremodulen, mit denen typische Anwendungsfunktionen realisiert werden

Siehe [Bild 2](#).

ANMERKUNG Wenn bereits vorhandenes Gerät eingesetzt werden soll, ist eine derartige Bibliothek als Teil der Systemsoftware zu betrachten und als solche zu qualifizieren.

3.4

Kategorie einer leittechnischen Funktion

(en: category of an I&C function)

eine von drei möglichen Sicherheitszuordnungen (A, B, C) von leittechnischen Funktionen, die aus der Sicherheitsrelevanz der durchzuführenden Funktionen resultieren. Wenn die Funktion für die Sicherheit nicht signifikant ist, erfolgt keine Sicherheitszuordnung (Kategorisierung)

ANMERKUNG 1 Siehe auch „Klasse eines leittechnischen Systems“, „leittechnische Funktion“.

ANMERKUNG 2 In [IEC 61226](#) werden leittechnische FSE festgelegt (Functions and associated Systems and Equipment; siehe [3.34](#)). Zu jeder Kategorie gehört ein Satz von Anforderungen, und zwar sowohl für die leittechnische Funktion (bezüglich Spezifikation, Auslegung, Realisierung, Verifizierung und Validierung) als auch für die ganze Kette von Maßnahmen, die für die Realisierung der Funktion erforderlich sind (bezüglich deren Eigenschaften und Qualifizierung), unabhängig davon, wie diese Maßnahmen auf mehrere miteinander verbundene leittechnische Systeme verteilt sind.

3.5

Kanal

(en: channel)

Anordnung von Komponenten in einem System, das ein einziges Ausgangssignal erzeugt. Ein Kanal endet an der Stelle, an der einzelne Ausgangssignale mit Signalen anderer Kanäle verknüpft werden, z. B. einem Überwachungskanal oder einem Kanal zur Auslösung von Sicherheitsaktionen ^{N3)}

[IAEA 50-SG-D8]

3.6

Klasse eines leittechnischen Systems

(en: class of an I&C system)

eine von drei möglichen Zuordnungen (1, 2, 3) sicherheitstechnisch wichtiger leittechnischer Systeme, entsprechend der Anforderung, leittechnische Funktionen unterschiedlicher Sicherheitsrelevanz zu realisieren

ANMERKUNG Siehe auch „Kategorie einer leittechnischen Funktion“, „sicherheitstechnisch wichtige Maßnahmen“, „Sicherheitssysteme“.

3.7

Versagen aufgrund gemeinsamer Ursache ^{N4)}

(CCF)

(en: common cause failure; CCF)

Versagen infolge eines oder mehrerer Ereignisse, das/die ein koinzidentes Versagen in zwei oder mehreren eigenständigen Kanälen eines mehrkanaligen Systems oder in verschiedenen Systemen verursacht/verursachen, sodass es zu einem Versagen des Systems/der Systeme kommt

[3.6.10 von IEC 61508, modifiziert]

ANMERKUNG Abhängig von den Umständen kann CCF auf Systemebene oder auf der Ebene von Systemen betrachtet werden, die eine Sicherheitsgruppe darstellen.

^{N3)} Nationale Fußnote: In IEC 60880-2 ist eine vereinfachte Definition enthalten, die jedoch in der vorliegenden Norm durch die ausführlichere IAEA-Definition ersetzt wurde.

^{N4)} Nationale Fußnote: Im Folgenden wird für das Versagen aufgrund gemeinsamer Ursache die Abkürzung CCF verwendet. Durch Softwarefehler verursachtes CCF wird kurz Software-CCF genannt.

3.8

Komplexität

(en: complexity)

Schwierigkeitsgrad der Verständlichkeit und Verifizierbarkeit eines Systems oder einer Komponente aufgrund von Auslegung, Realisierung oder Verhalten

[IEEE 610 [1]¹⁾, modifiziert]

3.9

Komponente

(en: component)

einer der Teile, aus dem ein System besteht. Eine Komponente kann auch aus Hardware oder Software bestehen und in weitere Komponenten unterteilt werden

[IEEE 610 [1]]

ANMERKUNG 1 Siehe auch „leittechnisches System“, „Gerät“.

ANMERKUNG 2 Die Begriffe „Gerät“, „Komponente“, „Modul“ sind in ihrer derzeitigen Benutzung austauschbar. Unterschiede und Zusammenhang dieser Begriffe sind bislang in keiner Norm verbindlich festgelegt.

3.10

rechnerbasiertes System

(en: computer based system)

leittechnisches System, dessen Funktionen zum größten Teil oder auch vollständig von Mikroprozessoren, programmierbarem elektronischen Gerät oder Rechnern abhängen bzw. durchgeführt werden

Siehe [Bild 2](#).

ANMERKUNG Siehe auch „leittechnisches System“.

3.11

Inbetriebnahme des Kernkraftwerks

(en: commissioning of the NPP)

Verfahren, im Verlauf dessen Komponenten und Systeme des Kernkraftwerks nach ihrem Bau in Betrieb gesetzt und verifiziert werden, um die Übereinstimmung mit den Annahmen der Auslegung sowie die Einhaltung ihrer Leistungsmerkmale festzustellen; dieses umfasst konventionelle und nukleare Prüfungen

[IAEA 50-C-D]

3.12

Konfigurationsmanagement

(en: configuration management)

Disziplin, in der technische und administrative Anleitungen und Kontrollmaßnahmen angewendet werden, um die funktionalen und physikalischen Eigenschaften einer Konfigurationskomponente festzustellen und zu dokumentieren, Änderungen solcher Eigenschaften zu überwachen, Änderungsprozesse und Implementierungsstatus zu dokumentieren und die Übereinstimmung mit den spezifizierten Anforderungen zu verifizieren

[IEEE 610 [1]]

3.13

Daten

(en: data)

Darstellung von Information oder Anweisungen in einer für die Übertragung, Auswertung oder Verarbeitung mittels Rechner geeigneten Weise

[IEEE 610 [1], modifiziert]

Siehe [Bild 2](#).

¹⁾ Zahlen in eckigen Klammern verweisen auf Angaben in den Literaturhinweisen.

3.14**Konzept gestufter Maßnahmen** ^{N5)}

(en: defence-in-depth concept)

siehe [A.3](#)**3.15****deterministisches Verfahren**

(en: deterministic method)

siehe [A.2.2](#)**3.16****Diversität**

(en: diversity)

Vorhandensein von zwei oder mehr unterschiedlichen Verfahren oder Mitteln, um ein bestimmtes Ziel zu erreichen. Diversität ist als Schutzmaßnahme gegen CCF besonders geeignet. Sie kann erreicht werden, indem physikalisch unterschiedliche Systeme eingesetzt werden, oder durch funktionale Diversität, bei der gleichartige Systeme ein bestimmtes Ziel über unterschiedliche Verfahren erreichen

[\[3.6 von IEC 60880-2\]](#)

ANMERKUNG 1 Siehe auch „funktionale Diversität“.

ANMERKUNG 2 Diese Definition ist allgemeiner als die von IAEA 50-C-D, die wie folgt lautet: „das Vorhandensein von redundanten Komponenten oder Systemen, um eine bestimmte Funktion auszuführen, wobei diese Komponenten oder Systeme jeweils kollektiv ein oder mehrere unterschiedliche Attribute aufweisen. Beispiele dafür sind unterschiedliche Betriebsbedingungen, unterschiedliche Gerätegrößen, unterschiedliche Hersteller, unterschiedliche Arbeitsweisen sowie Gerätetypen, die auf unterschiedlichen physikalischen Verfahren beruhen“.

3.17**Gerät**

(en: equipment)

ein oder mehrere Teile eines Systems. Ein Gerät ist ein einzelnes, definierbares (und üblicherweise ausbaubares) Teil eines Systems

[\[IEC 61226, modifiziert\]](#)

ANMERKUNG 1 Siehe auch „Komponente“, „leitechnisches System“.

ANMERKUNG 2 Gerät kann Software einschließen.

ANMERKUNG 3 Die Begriffe „Gerät“, „Komponente“, „Modul“ sind in ihrer derzeitigen Benutzung austauschbar. Unterschiede und Zusammenhang dieser Begriffe sind bislang in keiner Norm verbindlich festgelegt.

3.18**Gerätefamilie**

(en: equipment family)

Satz von Hardware- und Softwarekomponenten, die in einer oder mehreren Architekturen (Konfigurationen) zusammenarbeiten können. Die Entwicklung von anlagenspezifischen Konfigurationen und der zugehörigen Anwendungssoftware kann durch Software-Werkzeuge unterstützt werden. Eine Gerätefamilie stellt üblicherweise eine Anzahl von Standardfunktionen zur Verfügung, die zur Erzeugung spezifischer Anwendungssoftware miteinander kombiniert werden können

ANMERKUNG 1 Siehe auch „Funktionalität“, „Anwendungssoftware“, „Bibliothek der Anwendungssoftware“.

ANMERKUNG 2 Eine Gerätefamilie kann das Produkt eines speziellen Herstellers oder ein Satz von Produkten sein, die vom Lieferanten zusammengestellt und adaptiert sind.

^{N5)} Nationale Fußnote: Für dieses Auslegungsprinzip hat sich inzwischen die englische Bezeichnung „Defence-in-Depth (DiD)“ etabliert. Im Folgenden wird die Abkürzung DiD verwendet. Das DiD-Konzept ist durch die Anwendung gestufter Maßnahmen gegen die Auswirkung Versagen auslösender Ereignisse gekennzeichnet. In IAEA 50-C-D sind vier Stufen definiert, die von Maßnahmen bei der Abweichung vom Normalbetrieb (Stufe 1) bis zur Verminderung der Konsequenzen schwerer Störfälle (Stufe 4) reichen. Je nach Anforderung können innerhalb einer Maßnahmenstufe redundante oder auch diversitäre Maßnahmen getroffen werden.

DIN IEC 61513 (VDE 0491 Teil 2):2002-10

ANMERKUNG 3: Die Bezeichnung „equipment platform“ wird gelegentlich gleichbedeutend mit „equipment family“ verwendet

3.19

Abweichung

(en: error)

Diskrepanz zwischen berechneten, beobachteten oder gemessenen Werten oder Bedingungen und den tatsächlichen, spezifizierten oder theoretischen Werten oder Bedingungen

Siehe [Bild 3](#).

3.20

Bewertung (einer Systemeigenschaft)

(en: evaluation (of a system property))

Zuordnung eines qualitativen oder quantitativen Werts zu einer Systemeigenschaft

[2.2.2 von IEC 61069-1]

3.21

Versagen

Ausfall^{N6)}

(en: failure)

Abweichung der ausgeführten Funktion von der vorgesehenen Funktion

[3.8 von IEC 60880-2]

Siehe [Bild 3](#).

ANMERKUNG 1 Ein Versagen ist das Ergebnis eines Hardwarefehlers, eines Softwarefehlers, eines System-Fehlers oder von Fehlverhalten bei Bedienung oder Wartung, und einer damit verbundenen Signaltrajektorie, die zu dem Versagen führt.^{N7)}

ANMERKUNG 2 Siehe auch „Fehler“, „Softwareversagen“.

3.22

Fehler

(en: fault)

Mangel an einer Hardware-, Software- oder Systemkomponente

Siehe [Bild 3](#).

ANMERKUNG 1 Fehler können Zufallsfehler sein, z. B. bei Hardware, oder systematische Fehler, z. B. Softwarefehler, die auf Auslegungsmängel zurückgehen.

ANMERKUNG 2 Ein Fehler (insbesondere ein Auslegungsfehler) kann in einem System unentdeckt bleiben, bis besondere Bedingungen auf dieses System so einwirken, dass die resultierende Funktion nicht mit der vorgesehenen Funktion übereinstimmt, d. h. ein Versagen eintritt.

ANMERKUNG 3 Siehe auch „Softwarefehler“.

3.23

funktionale Diversität

(en: functional diversity)

Anwendung der Diversität auf der Funktionsebene (z. B. Ableitung eines Abschaltkriteriums sowohl aus Druck- als auch Temperaturgrenzwerten)

[3.10 von IEC 60880-2]

ANMERKUNG Siehe auch „Diversität“.

^{N6)} Nationale Fußnote: Wenn Hardware oder Teilsysteme (z. B. ein Strang eines redundanten Systems) betroffen sind, wird „failure“ mit „Ausfall“ übersetzt.

^{N7)} Nationale Fußnote: Bei Hardware kann der Ausfall allein aufgrund der Alterungseffekte einer Komponente erfolgen.

3.24**funktionale Validierung**

(en: functional validation)

Prüfung der Übereinstimmung von Spezifikationen der Anwendungsfunktionen mit den originären funktionalen und Leistungsfähigkeitsanforderungen der Anlage. Die funktionale Validierung ist als Ergänzung zur Systemvalidierung zu sehen, bei der die Übereinstimmung des Systems mit den Spezifikationen der Anwendungsfunktionen geprüft wird

3.25**Funktionalität**

(en: functionality)

Eigenschaft einer Funktion, die Operationen charakterisiert, durch die Eingangsinformation in Ausgangsinformation umgesetzt wird

ANMERKUNG Funktionalität der Anwendungsfunktionen beeinflusst im Allgemeinen den Anlagenbetrieb. Eingangsinformation kann von Messfühlern, Operateuren, anderen Geräten oder anderer Software bezogen werden. Ausgänge können auf Stellglieder, Operateure, andere Geräte oder andere Software gerichtet sein (siehe [4]).

3.26

sicherheitstechnisch wichtige Funktion

(en: function important to safety)

auf eine bestimmte Aufgabe ausgerichtete Funktion, die aus Sicherheitsgründen auszuführen ist

[IAEA 50-SG-D3 und IEC 61226, modifiziert]

ANMERKUNG Siehe auch „leittechnische Funktion“, „leittechnische Teilfunktion“, „Anwendungsfunktion“.

3.27**Gefährdung**

(en: hazard)

Ereignis mit dem Potenzial, schwere Schäden an Personal, Gerät, Komponenten oder Strukturen zu verursachen. Solche Vorfälle werden in interne und externe unterteilt

ANMERKUNG 1 Interne Gefährdungen sind z. B. Feuer oder Überflutung. Sie können die Folge eines AVE sein, z. B. Kühlmittelverlust-Störfall oder Dampfrohrbruch.

ANMERKUNG 2 Externe Gefährdungen sind z. B. Erdbeben oder Blitzschlag.

3.28**menschliches Fehlverhalten (Irrtum)**

(en: human error (mistake))

Handlung oder Vorgehensweise eines Menschen, die eine unbeabsichtigte Folge hat

[3.12 von IEC 60880-2]

3.29**unabhängiges Gerät**

(en: independent equipment)

unabhängiges Gerät besitzt folgende Eigenschaften:

- a) seine Funktionsfähigkeit wird vom Betrieb oder Versagen anderer Geräte nicht beeinträchtigt;
- b) seine Funktionsfähigkeit wird durch die Effekte eines AVE, für die es ausgelegt ist, nicht beeinträchtigt.

[IAEA 50-SG-D8]

ANMERKUNG Mittel zur Erzielung der Unabhängigkeit bei der Auslegung sind elektrische Trennung (in IAEA-Dokumenten auch funktionale Trennung genannt), physikalische Trennung und unabhängige Kommunikation.

3.30**Interrupt**

(en: interrupt)

Stoppen eines Prozesses, wie z. B. die Ausführung eines Rechenprogramms, durch ein Ereignis außerhalb dieses Prozesses

[IEEE 610]

3.31

leittechnische Architektur

(en: I&C architecture)

organisatorische Struktur der leittechnischen Systeme der Anlage, die sicherheitstechnische Bedeutung haben

ANMERKUNG 1 Siehe auch „leittechnische Systemarchitektur“, „leittechnisches System“.

ANMERKUNG 2 Durch die organisatorische Struktur werden vor allem die Hauptfunktionen, Klasse und Abgrenzung jedes Systems, Verbindungen und Grad der Unabhängigkeit von Systemen, Priorität und Abstimmung bei mehreren gleichzeitig auftretenden Signalen, die Mensch-Maschine-Kommunikation festgelegt.

ANMERKUNG 3 In dieser Norm bezeichnet der Begriff „leittechnische Architektur“ nur die sicherheitstechnisch bedeutende Teilmenge der gesamten leittechnischen Architektur der Anlage. Letztere umfasst auch die nicht klassifizierten Geräte und Systeme.

3.32

leittechnische Funktion

(en: I&C function)

Funktion, um einen bestimmten Teilprozess zu betreiben, zu steuern und/oder zu überwachen

ANMERKUNG 1 Siehe auch „leittechnische Teilfunktion“, „leittechnische FSE“, „Anwendungsfunktion“.

ANMERKUNG 2 Der Begriff „leittechnische Funktion“ wird von Verfahrenstechnikern verwendet, um die funktionalen Anforderungen an die Leittechnik zu strukturieren. Eine „leittechnische Funktion“ ist so definiert, dass

- ihr funktionaler Zweck vollständig dargestellt wird,
- sie entsprechend ihrer Bedeutung für die Sicherheit kategorisiert werden kann,
- sie die zur Erfüllung ihres funktionalen Zwecks erforderliche kleinste Einheit umfasst (vom Messfühler bis zum Betätigungsbaustein).

ANMERKUNG 3 Eine „leittechnische Funktion“ kann in eine Anzahl von Teilfunktionen (z. B. Messfunktion, Steuerungsfunktion, Betätigungsfunktion) untergliedert werden, um die Zuordnung zu leittechnischen Systemen durchzuführen.

3.33

leittechnische Teilfunktion

(en: I&C subfunction)

Unterteilung einer „leittechnischen Funktion“, die einem leittechnischen System oder Teilsystem zugeordnet wird

ANMERKUNG 1 Siehe auch „leittechnische Funktion“, „Anwendungsfunktion“.

ANMERKUNG 2 Der Begriff „Funktion“ wird oft auch für „Teilfunktion“ verwendet, wenn es in diesem Zusammenhang nicht zweideutig ist.

3.34

leittechnische Funktionen und zugehörige Systeme und Einrichtungen (FSE)

(en: functions, and the associated systems and equipment; FSE)

leittechnische Funktionen werden zu einem bestimmten Zweck ausgeführt oder um ein Ziel zu erreichen. Die zugehörigen Systeme und Einrichtungen sind die Komponentengruppen und die Komponenten selbst, die eingesetzt werden, um die Funktionen zu realisieren

[IEC 61226, modifiziert]

ANMERKUNG Siehe auch „leittechnische Funktion“, „leittechnisches System“.

3.35

leittechnisches System

(en: I&C system)

auf elektrischer und/oder elektronischer und/oder programmierbar elektronischer Technologie beruhendes System (E/E/PES), das sowohl leittechnische Funktionen als auch auf sich selbst bezogene Dienstleistungs- und Überwachungsfunktionen ausführt

Der Begriff wird allgemein verwendet und umfasst alle Elemente des Systems wie interne Energieversorgung, Messfühler und andere Eingangsgерäte, Datenbusse und andere Kommunikationspfade, Schnittstellen zu den Betätigungsgliedern und anderen Ausgangsgерäten (siehe Anmerkung 2). Die verschiedenen Funktionen in einem System können strikt zugeordnete oder gemeinsame Ressourcen verwenden.

[3.3.2 von IEC 61508-4, modifiziert]

ANMERKUNG 1 Siehe auch „System“, leittechnische Funktion“.

ANMERKUNG 2 Die zu einem spezifischen leittechnischen System gehörenden Elemente sind durch die Spezifikation der Systemgrenzen definiert.

ANMERKUNG 3 Entsprechend ihrer typischen Funktionalität unterscheidet IAEA zwischen Automatisierungs- und Steuerungs-/Regelsystemen, MMK-Systemen, Verriegelungssystemen und Schutzsystemen (siehe [B.4](#)).

3.36

leittechnische Systemarchitektur

(en: I&C system architecture)

Organisationsstruktur eines leittechnischen Systems

ANMERKUNG Siehe auch „leittechnische Architektur“.

3.37

sicherheitstechnisch wichtige Maßnahmen

(en: items important to safety)

diese Maßnahmen umfassen:

- a) Strukturen, Systeme und Komponenten, deren Fehlverhalten oder Versagen zu einer unzulässigen Strahlungsbelastung des Anlagenpersonals oder von Personen in der Öffentlichkeit führt;
- b) Strukturen, Systeme und Komponenten, die verhindern, dass anzunehmende betriebliche Ereignisse zu Störfallsituationen führen;
- c) Vorkehrungen, die zur Verringerung der Konsequenzen des Fehlverhaltens oder Versagens von Strukturen, Systemen oder Komponenten dienen.

[IAEA 50-SG-D3]

ANMERKUNG 1 Siehe auch „Sicherheitssysteme“, „Klasse eines leittechnischen Systems“.

ANMERKUNG 2 In dieser Norm werden die sicherheitstechnisch wichtigen leittechnischen Systeme in die Klassen 1, 2, 3 unterteilt.

ANMERKUNG 3 In IAEA 50-SG-D8 werden die sicherheitstechnisch wichtigen Systeme in „Sicherheitssysteme“ und „sicherheitsrelevante Systeme“ unterteilt.

3.38

Instandhaltbarkeit

(en: maintainability)

Wahrscheinlichkeit, dass eine vorgegebene Instandhaltungsmaßnahme an einem unter bestimmten Betriebsbedingungen arbeitenden Teil in einer bestimmten Zeitspanne ausgeführt werden kann, wenn die Instandhaltungsmaßnahme unter bestimmten Betriebsbedingungen und unter Nutzung festgelegter Prozeduren und Ressourcen erfolgt

[2.10 von IEC 60987]

3.39

gesamter Sicherheitslebenszyklus der Leittechnik

(en: overall safety life cycle of the I&C)

erforderliche Aktivitäten bei der Realisierung der sicherheitstechnisch wichtigen Systeme und Geräte der leittechnischen Architektur, beginnend mit der Herleitung der Anforderungen an die Leittechnik von der sicherheitstechnischen Auslegungsgrundlage der Anlage bis zu dem Zeitpunkt, zu dem keines der leittechnischen Systeme für die Nutzung zur Verfügung steht

[3.7.1 von IEC 61508-4, modifiziert]

ANMERKUNG 1 Der gesamte Sicherheitslebenszyklus der Leittechnik ist auf die individuellen System-Sicherheitslebenszyklen zurückzuführen.

ANMERKUNG 2 Siehe auch „System-Sicherheitslebenszyklus“.

3.40

Sicherheitsanalyse der Anlage

(en: plant safety analysis)

siehe [A.2](#)

3.41

anzunehmendes Versagen auslösendes Ereignis

(AVE)

(en: postulated initiating event; PIE)

identifizierte Ereignisse, die zu den zu betrachtenden betrieblichen Störungen oder Störfallbedingungen und deren Folgewirkungen führen

[IAEA 50-C-D]

ANMERKUNG 1 Zu betrachtende betriebliche Störungen sind alle vom Normalbetrieb abweichenden Vorkommnisse, die erwartungsgemäß ein oder mehrere Male während der betrieblichen Lebenszeit der Anlage auftreten und die im Hinblick auf geeignete Auslegungsmaßnahmen keine signifikanten Auswirkungen auf sicherheitstechnisch wichtige Einrichtungen haben oder zu Störfallbedingungen führen.

ANMERKUNG 2 Die primären Ursachen von AVE können plausible Geräteausfälle und Operateurfehler sein (beide sowohl innerhalb als auch außerhalb der Anlage), vom Menschen verursachte Ereignisse oder Naturereignisse. Die Spezifikation der AVE muss für die Genehmigungsbehörde der Anlage akzeptierbar sein.

3.42

vorgefertigte Software

(VGS)

(en: pre-developed software; PDS)

Software, die bereits vorgefertigt, als kommerzielles oder proprietäres Produkt verfügbar und für den Einsatz in einem rechnerbasierten System vorgesehen ist (siehe auch „bereits vorhandene Software“)

[3.17 von IEC 60880-2]

ANMERKUNG Vorgefertigte Software (VGS) kann eingeteilt werden in allgemeine VGS, die nicht für eine spezielle Hardwareumgebung entwickelt wurde, und in Hardwarekomponenten integrierte VGS, die zusammen mit dieser Hardware zu verwenden ist.

3.43

probabilistisches Verfahren

(en: probabilistic method)

siehe [A.2.2](#)

3.44

Projektorganisation

(en: project organisation)

Organisation(en) oder Einzelpersonen, die in den Phasen des gesamten Sicherheitslebenszyklus der Leittechnik und/oder in den Phasen der Sicherheitslebenszyklen der leittechnischen Systeme die Verantwortung dafür tragen, die organisatorischen und technischen Aktivitäten bezüglich sicherheitstechnisch wichtiger leittechnischer Funktionen, Systemen und Einrichtungen zu definieren und auszuführen

ANMERKUNG Dieser Begriff ist im Unterschied zu „Betriebsorganisation“ zu sehen.

3.45

Qualifizierung

(en: qualification)

Vorgang, im Rahmen dessen die Eignung eines Systems oder einer Komponente für den betrieblichen Gebrauch bestimmt wird. Die Qualifizierung wird im Zusammenhang mit einer bestimmten Klasse des leittechnischen Systems und einem entsprechenden Satz von Qualifizierungsanforderungen durchgeführt

3.46

Qualität

(en: quality)

Gesamtheit aller Eigenschaften eines Produkts oder einer Dienstleistung, die dazu beitragen, angegebene und implizierte Erfordernisse zu erfüllen

[2.1 von ISO 8402]

3.47**Qualitätssicherung**

(en: quality assurance)

alle geplanten und systematischen Aktionen, die erforderlich sind, um ein angemessenes Vertrauen zu schaffen, dass ein Produkt oder eine Dienstleistung die gestellten Qualitätsanforderungen erfüllt

[3.5 von ISO 8402, modifiziert]^{N2)}

3.48**Qualitätssicherungsplan**

(en: quality plan)

Dokument, in dem die spezifischen Praktiken der Qualitätssicherung sowie Hilfsmittel und Reihenfolge der Aktivitäten festgelegt werden, die für das entsprechende Produkt, Projekt oder den Kontrakt relevant sind

3.49**Redundanz**

(en: redundancy)

Vorsehen alternativer (identischer oder unterschiedlicher) Elemente oder Systeme, sodass jedes, unabhängig vom Betriebszustand oder Versagen irgend eines anderen, die geforderte Funktion erfüllen kann

[IAEA 50-SG-D8]

3.50**Zuverlässigkeit**

(en: reliability)

Wahrscheinlichkeit, dass ein Gerät, System oder eine Einrichtung seine beabsichtigte Funktion für eine spezifizierte Zeit unter festgelegten Betriebsbedingungen zufrieden stellend ausführt

[IAEA 50-SG-D8]

ANMERKUNG Die Zuverlässigkeit eines rechnerbasierten Systems umfasst die Zuverlässigkeit seiner Hardware, die üblicherweise quantifiziert ist, und die Zuverlässigkeit seiner Software, die üblicherweise ein qualitatives Maß darstellt, weil es im Allgemeinen keine anerkannten Mittel für eine Quantifizierung gibt.

3.51**wiederverwendbare Software**

(en: reusable software)

Softwaremodul, das in mehr als einem Rechnerprogramm oder Softwaresystem verwendet werden kann

[IEEE 610 [1], modifiziert]

3.52**Sicherheitsgruppe**

(en: safety group)

Anordnung von Gerät, die dazu bestimmt ist, alle erforderlichen Aktionen auszuführen, um sicherzustellen, dass für ein bestimmtes AVE die in der Auslegungsgrundlage der Anlage festgelegten Grenzwerte nicht überschritten werden

[IAEA 50-SG-D3]

ANMERKUNG Die leittechnischen Funktionen in einer Sicherheitsgruppe können verschiedenen Kategorien zugeordnet sein.

3.53**Sicherheitssysteme**

(en: safety systems)

sicherheitstechnisch wichtige Systeme, die dazu dienen, unter allen Umständen die sichere Abschaltung des Reaktors und die Wärmeabfuhr aus dem Reaktorkern sicherzustellen, und/oder die Konsequenzen von anzunehmenden betrieblichen Störungen sowie von Störfallbedingungen zu begrenzen

[IAEA 50-SG-D8]

^{N2)} Siehe Seite 14.

DIN IEC 61513 (VDE 0491 Teil 2):2002-10

ANMERKUNG 1 Siehe auch „sicherheitstechnisch wichtiges System“, „Klasse eine leittechnischen Systems“.

ANMERKUNG 2 Das von IAEA definierte Sicherheitssystem entspricht im Allgemeinen den Systemen der Klasse 1 dieser Norm.

3.54

Zugriffsschutz

(en: security)

Fähigkeit des rechnerbasierten Systems, Informationen und Daten so zu schützen, dass nicht autorisierte Personen oder Systeme sie nicht lesen oder ändern können, und autorisierten Personen oder Systemen der Zugriff nicht verwehrt wird

[3.25 von ISO/IEC 12207, modifiziert]

3.55

Einzelausfall ^{N8)}

Einzelfersagen

(en: single failure)

zufälliger Ausfall mit dem Ergebnis, dass eine Komponente oder ein System die geplanten Funktionen nicht ausführen kann. Folgeausfälle, die aus einem angenommenen Einzelausfall resultieren, werden als Teil des Einzelausfalls betrachtet

[IAEA 50-SG-D8, modifiziert]

ANMERKUNG 1 Siehe auch „Einzelfersagens-Kriterium“.

ANMERKUNG 2 Einzelfersagen kann die Folge einer anlageninternen oder -externen Gefährdung sein.

3.56

Einzelfersagens-Kriterium

Einzelausfall-Kriterium

(en: single-failure criterion)

Kriterium für eine Anordnung von Geräten, das bedeutet, dass diese ihre Aufgabe trotz eines angenommenen zufälligen Einzelausfalls an irgendeiner Stelle der Anordnung durchführen kann. Dabei sind Folgeausfälle, die aus dem angenommenen Einzelausfall resultieren, als integraler Bestandteil des Einzelausfalls zu betrachten

[IAEA 50-C-D]

ANMERKUNG 1 Siehe auch „Einzelfersagen“, „Softwareversagen“.

ANMERKUNG 2 Softwareversagen ist systematisch und kein Zufallsversagen.

3.57

Softwareversagen

(en: software failure)

Systemversagen infolge der Aktivierung eines Auslegungsfehlers in einer Softwarekomponente

ANMERKUNG 1 Jedes Softwareversagen hat seine Ursache in Auslegungsfehlern, weil Software sich nicht abnützt oder von physikalischen Ausfällen abhängt. Die Aktivierung von Auslegungsfehlern der Software während des Betriebs erfolgt zufällig, daher tritt auch Softwareversagen zufällig ein.

ANMERKUNG 2 Siehe auch „Versagen“, „Fehler“, „Softwarefehler“.

3.58

Softwarefehler

(en: software fault)

Auslegungsfehler in einer Softwarekomponente

ANMERKUNG Siehe auch „Fehler“.

^{N8)} Nationale Fußnote: siehe auch [3.21](#) „Versagen“, „Ausfall“.

3.59**Softwarezuverlässigkeit**

(en: software reliability)

Teil der Systemzuverlässigkeit, der von Softwareversagen abhängig ist

3.60**Spezifikation**

(en: specification)

Dokument, in dem Anforderungen, Auslegung, Funktionsweisen oder andere Eigenschaften eines Systems oder einer Komponente, oft auch die Verfahren zur Überprüfung der Einhaltung dieser Angaben, in kompletter, präziser und verifizierbarer Weise angegeben sind

[3.21 von IEC 60880-2 und IEEE 610 [1]]

3.61**System**

(en: system)

Satz von Komponenten, die laut Auslegung zusammenarbeiten, wobei ein Element des Systems ein weiteres System, genannt Teilsystem, sein kann

[3.3.1 von IEC 61508-4, modifiziert]

ANMERKUNG 1 Siehe auch „leittechnisches System“.

ANMERKUNG 2 Leittechnische Systeme stellen neben den mechanischen und elektrischen Systemen der Anlage eine separate Systemgruppe dar.

3.62**systematisches Versagen**

(en: systematic failure)

Versagen, das deterministisch auf eine Ursache zurückgeführt werden kann und das nur durch eine Änderung der Auslegung oder des Produktionsprozesses, der Bedienungsanleitungen, Dokumentation oder anderer relevanter Faktoren zu beheben ist

[3.6.6 von IEC 61508-4]

3.63**System-Sicherheitslebenszyklus**

(en: system safety life cycle)

erforderliche Aktivitäten in Zusammenhang mit der Realisierung eines sicherheitstechnisch wichtigen leittechnischen Systems in einer Zeitspanne beginnend mit den Systemanforderungen in der Konzeptphase bis zu dem Zeitpunkt, in dem das leittechnische System nicht mehr für die Nutzung zur Verfügung steht

ANMERKUNG 1 Der System-Sicherheitslebenszyklus lässt sich auf die Aktivitäten im Rahmen des gesamten Sicherheitslebenszyklus zurückführen.

ANMERKUNG 2 Siehe auch „gesamter Sicherheitslebenszyklus der Leittechnik“.

3.64**Systemsoftware**

(en: system software)

Software, die für ein bestimmtes Rechnersystem oder eine Rechnerfamilie erstellt wurde, um den Betrieb und die Instandhaltung/Pflege des Rechnersystems und zugehöriger Programme zu erleichtern, z. B. Betriebssysteme, Compiler, Dienstprogramme. Systemsoftware besteht üblicherweise aus Betriebssoftware und Hilfssoftware

[3.24 von IEC 60880-2]

Siehe Bild 2.

ANMERKUNG 1 Systemsoftware: Software, die während des Systembetriebs auf dem Zielprozessor läuft, wie etwa Betriebssystem, Ein-/Ausgangstreiber, Behandlung von Ausnahmen, Kommunikationssoftware, Anwendersoftware-Bibliotheken, Online-Diagnose, Redundanz und Management der kontrollierten Reduzierung.

ANMERKUNG 2 Hilfssoftware: Software, die bei Entwicklung, Test, oder Pflege anderer Software und des Systems unterstützt, wie z. B. Compiler, Codegeneratoren, graphische Editoren, Offline-Diagnose, Verifizierungs- und Validierungswerkzeuge.

ANMERKUNG 3 Siehe auch „Anwendungssoftware“.

3.65 ^{N9)}

bereits verfügbare(s) Software/Hardware/System

(en: pre-existing software/hardware/system)

bei der Planung oder Auslegung bereits verfügbare(s) und kommerziell genutzte(s) Software/Hardware/System

ANMERKUNG In dieser Übersetzung wird grundsätzlich „bereits verfügbar“ verwendet, auch an Stelle von „vorgefertigt“.

3.66 ^{N9)}

Fehlabschaltung

(en: spurious scram)

zufälliges Versagen eines Abschaltsystems, das zu einer fälschlichen (d. h. aufgrund des Anlagenzustandes nicht erforderlichen) Auslösung der Abschaltfunktion führt, z. B. beim Reaktorschutz zur Abschaltung des Reaktors

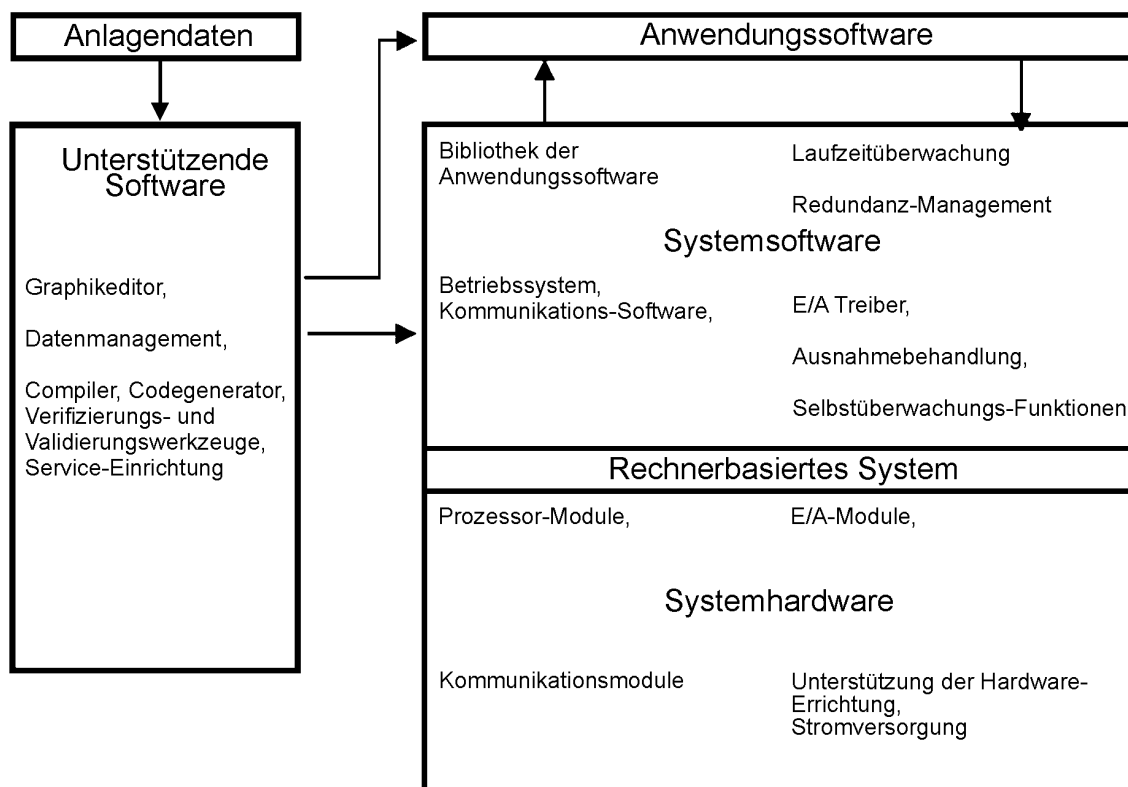


Bild 2 – Typische Zusammenhänge von Hardware und Software in einem rechnerbasierten System

^{N9)} Nationale Fußnote: Im IEC-Original nicht enthalten; zum besseren Verständnis der Übersetzung hier national ergänzt.

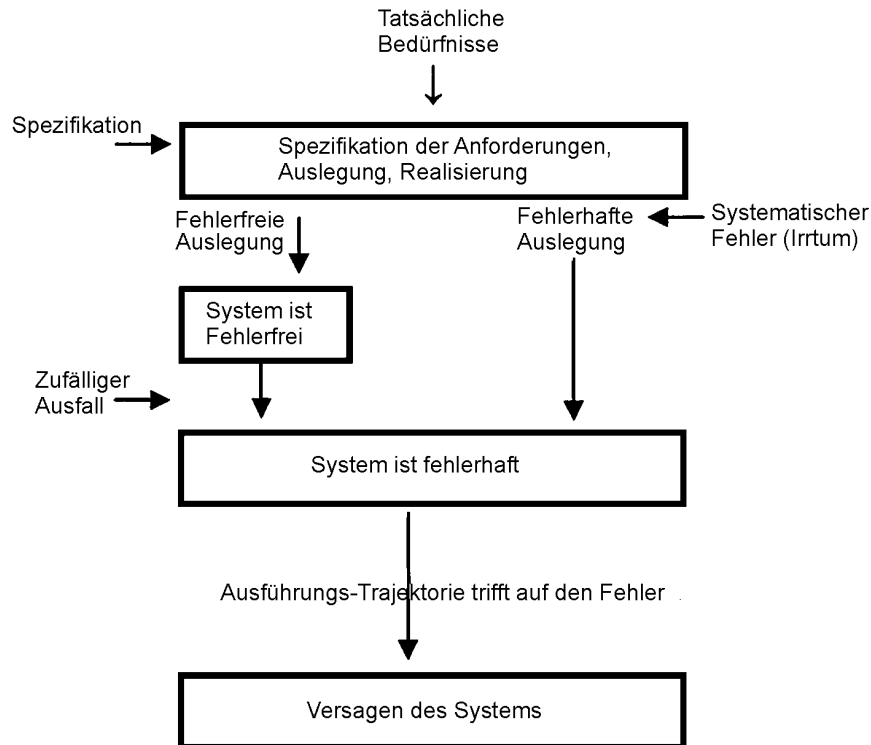


Bild 3 – Zusammenhänge zwischen Versagen des Systems, zufälligem Ausfall und systematischem Fehler

4 Formelzeichen und Abkürzungen

englisch		deutsch	
CB	computer-based	RB	rechnerbasiert/rechnergestützt
CCF	common cause failure	CCF	Versagen aufgrund gemeinsamer Ursache
COTS	commercial off-the shelf	COTS	kommerziell verfügbare Software, vorgefertigte Software
EMI	electromagnetic interference	EMB	elektromagnetische Beeinflussung
EUC	equipment under command		Betriebseinrichtung
FSE	functions, and associated systems and equipment	FSE	Funktionen und zugehörige Systeme und Geräte
HMI	human machine interface	MMK	Mensch-Maschine-Kommunikation
I&C	instrumentation and control	LT	Leittechnik
I/O	input/output	E/A	Eingang/Ausgang
LOCA	loss of coolant accident	KMV	Kühlmittelverlust-Störfall
NPP	nuclear power plant	KKW	Kernkraftwerk
PDS	pre-developed software	VGS	vorgefertigte Software
PIE	postulated initiating event	AVE	anzunehmendes Versagen auslösendes Ereignis
PSA	probabilistic safety assessment	PSA	probabilistische Sicherheitsanalyse
QA	quality assurance	QS	Qualitätssicherung
SIL	safety integrity level		Sicherheitsniveau
E/E/PES	electrical/electronic/programmable electronic system	E/E/PES	elektrisches/elektronisches/programmierbares elektronisches System

5 Gesamter Sicherheitslebenszyklus der Leittechnik

Der Zweck dieses Abschnitts ist festzustellen,

- wie die gesamten Anforderungen an die sicherheitstechnisch wichtigen leittechnischen FSE aus der sicherheitstechnischen Auslegungsgrundlage der Anlage abzuleiten sind (siehe [A.1](#) und [A.2](#)),
- wie die Anforderungen an die Architektur der sicherheitstechnisch wichtigen leittechnischen Systeme von den Gesamtanforderungen der leittechnischen FSE abzuleiten sind,
- wie das Zusammenwirken zwischen den Anforderungen an die leittechnische Architektur und den Anforderungen an die einzelnen sicherheitstechnisch wichtigen leittechnischen Systeme festzulegen ist.

Um sicherzustellen, dass alle Sicherheitsanforderungen der Anlage, die von der Leittechnik zu erfüllen sind, berücksichtigt, realisiert und aufrechterhalten werden, ist ein systematisches Vorgehen erforderlich. Dies wird erreicht, indem die Aktivitäten in Zusammenhang mit Entwicklung, Realisierung und Betrieb der Leittechnik in den Rahmen des gesamten Sicherheitslebenszyklus der Leittechnik eingebunden werden. Dieser Lebenszyklus wiederum bezieht sich auf die Sicherheitslebenszyklen der einzelnen leittechnischen Systeme (siehe [Abschnitt 6](#)).

Die Phasen eines typischen gesamten Sicherheitslebenszyklus der Leittechnik umfassen:

- a) Überprüfung der sicherheitstechnischen Auslegungsgrundlage der Anlage, einschließlich (siehe [5.1](#)):
 - Anforderungen hinsichtlich Funktion, Leistungsfähigkeit und Unabhängigkeit,
 - Kategorisierung der Funktionen,
 - Einschränkungen aufgrund der Randbedingungen der Anlage.
- b) Festlegung der gesamten Anforderungsspezifikation der sicherheitstechnisch wichtigen leittechnischen FSE (siehe [5.2](#)),
- c) Auslegung der gesamten leittechnischen Architektur und Zuordnung der leittechnischen Funktionen zu den einzelnen Systemen und Geräten,
- d) Festlegung der Gesamtplanung (siehe [5.4](#)),
- e) Realisierung der einzelnen Systeme (siehe [Abschnitt 6](#)),
- f) Gesamtintegration und Inbetriebnahme der Systeme (siehe [Abschnitt 7](#)),
- g) Gesamtbetrieb und Instandhaltung (siehe [Abschnitt 8](#)).

Die Ziffern in Klammern beziehen sich auf diejenigen Abschnitte dieser Norm, in denen die jeweilige Phase angesprochen wird; Ziel der Aktivitäten, Eingangsinformation und Ergebnis sowie Anwendungsbereich jeder Phase sind in [Tabelle 1](#) dargestellt.

Die Verbindung zwischen diesem Lebenszyklus und den Sicherheitslebenszyklen der einzelnen leittechnischen Systeme ist in vereinfachter Form in [Bild 4](#) gezeigt:

- a) Der gesamte Sicherheitslebenszyklus der Leittechnik stellt einen iterativen Prozess dar, in dem die Konsistenz der Ergebnisse jeder Phase mit den Eingangsinformationen für die vorangegangenen Aktivitäten verifiziert wird. Eine Phase kann auch dann beginnen, wenn die Aktivitäten der vorangegangenen Phase nicht abgeschlossen sind, vorausgesetzt, geeignete Konfigurationskontrollen wurden eingesetzt, um die Gesamtkonsistenz des Entwicklungsprozesses sicherzustellen.
- b) Eine Phase darf nur dann beendet werden, wenn die vorangegangenen Phasen komplett abgeschlossen sind.

ANMERKUNG Die Verantwortung für die Sicherheit eines Kernkraftwerks liegt beim Betreiber und kann in keinem Fall durch Delegation von Verantwortlichkeiten an Hersteller, Lieferanten, Konstrukteure oder Genehmigungsbehörden verwässert werden, die in verschiedenen Tätigkeiten im Zusammenhang mit der Anlage involviert sind (siehe 3.1.2 von IAEA 75-INSAG-3).

Tabelle 1 – Übersicht über den gesamten Sicherheitslebenszyklus der Leittechnik

Abschnitt	Eingangs- information	Ziel der Aktivitäten	Anwendungs- bereich	Ergebnis
5	Anforderungen an den gesamten Sicherheitslebenszyklus und seine Beziehung zu den Lebenszyklen der Systeme			
5.1	Ableitung der Leittechnikanforderungen von der sicherheitstechnischen Auslegungsgrundlage der Gesamtanlage			
5.1.1 Überprüfung der Anforderungen an Funktionalität, Leistungsfähigkeit und Unabhängigkeit	Dokumente zur sicherheitstechnischen Auslegungsgrundlage der Anlage Prinzipien des Anlagenbetriebs	Identifizierung von – Gesamtanforderungen an Funktion und Leistungsfähigkeit der sicherheitstechnisch wichtigen leittechnischen FSE, – Unabhängigkeitsanforderungen an die leittechnischen FSE aufgrund des DiD-Konzepts der Anlage, – automatisierte Funktionen und Operateuraufgaben	Anlagensysteme und zugehörige sicherheitstechnisch wichtige leittechnische FSE	Ermittlung von Eingangsanforderungen für 5.2
5.1.2 Überprüfung der Kategorisierung der leittechnischen FSE	Kategorisierung der Sicherheitsfunktionen der Anlage	Festlegung der Kategorisierung von FSE Verifizierung auf Vollständigkeit und Verifizierung auf Brauchbarkeit für komplexe Anforderungen	Sicherheitstechnisch wichtige leittechnische FSE	Identifizierung von Eingangsanforderungen für 5.2
5.1.3 Überprüfung der Anlagen-Randbedingungen	Dokumente zur Anlagenanordnung und Auslegungsgrundlage	Identifizierung von – Grenzen der Anlagen- und leittechnischen Systeme – Randbedingungen von Versorgungssystemen, Anlagenanordnung und Umgebungsbedingungen – Quellen möglicher interner und externer Gefährdungen, – Prinzipien des Anlagenbetriebs und der Instandhaltung	Anlagenanordnung Anlagensysteme Leittechnische Systeme	Identifizierung von Randbedingungen für die Auslegung der leittechnischen Architektur (5.3) und für die Anforderungsspezifikation der leittechnischen Einzelsysteme (6.1)
5.2 Dokumentation	Ergebnisse von 5.1	Entwicklung der gesamten Anforderungsspezifikation für die sicherheitstechnisch wichtigen leittechnischen FSE in Bezug auf Funktion, Leistungsfähigkeit, Unabhängigkeit und Kategorisierungsanforderungen	Leittechnische FSE	Gesamte Anforderungsspezifikation für die leittechnischen FSE in Hinblick auf 5.3
5.3	Auslegung der leittechnischen Gesamtarchitektur und Zuordnung der leittechnischen Funktionen			
5.3.1 Auslegung der leittechnischen Architektur	Ergebnisse von 5.2	Entwicklung der Auslegung der Architektur der leittechnischen Systeme, sodass sie für die Realisierung der gesamten Anforderungsspezifikation der sicherheitstechnisch wichtigen leittechnischen FSE geeignet ist Vorsehen angemessene Maßnahmen in Bezug auf das CCF-Potenzial	Leittechnische Funktionen und leittechnische Systeme	Detailauslegung der Architektur der Sicherheitsleittechnik in Bezug auf automatische Systeme, Mensch-Maschine-Kommunikation, Verbindungen, Werkzeuge (siehe 5.5.1)
5.3.2 Funktionale Zuordnung	Ergebnisse von 5.3.1 und 5.4 (Iteration mit den Ergebnissen von 6.3)	Zuordnung der leittechnischen Funktionen zu den einzelnen leittechnischen Systemen und Einrichtungen Erstellung von Anforderungen (Grenzen, Klassifizierung, Funktionalität, Zuverlässigkeit und andere geforderten Eigenschaften) für die einzelnen leittechnischen Systeme	Leittechnische FSE und leittechnische Systeme	Anforderungen an die Anwendungsfunktionen der Systeme und Mensch-Maschine-Kommunikation, die Auslegung der leittechnischen Systeme und die Werkzeuge (siehe 5.5.2)
5.3.3 Geforderte Analyse	Ergebnisse von 5.3.1 ; 5.3.2	Beurteilung der Zuverlässigkeit und Vorsorge gegen CCF Beurteilung menschlicher Faktoren.	Leittechnische Funktionen und leittechnische Systeme	Beurteilung der Zuverlässigkeit und der Vorsorge gegen CCF (5.3.3.1) Beurteilung menschlicher Faktoren (5.3.3.2)
5.4 Gesamtplanung	Ergebnisse von 5.3	Entwicklung von Plänen für QS, Zugriffsschutz, Integration, Inbetriebsetzung, Betrieb und Instandhaltung der Systeme	Zusammenwirkende leittechnische Systeme	Planung der erforderlichen Aktivitäten