

	DIN IEC 61226 (VDE 0491-1)	DIN
	Diese Norm ist zugleich eine VDE-Bestimmung im Sinne von VDE 0022. Sie ist nach Durchführung des vom VDE-Präsidium beschlossenen Genehmigungsverfahrens unter der oben angeführten Nummer in das VDE-Vorschriftenwerk aufgenommen und in der „etz Elektrotechnik + Automation“ bekannt gegeben worden.	VDE
ICS 27.120.20 Einsprüche bis 2008-12-30 Vorgesehen als Ersatz für DIN IEC 61226 (VDE 0491-1):2005-09 Entwurf Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Kategorisierung leittechnischer Funktionen (IEC 45A/705/CDV:2008) Nuclear power plants – Instrumentation and control important to safety – Classification of instrumentation and control functions (IEC 45A/705/CDV:2008) Centrales nucléaires de puissance – Instrumentation et contrôle commande importants pour la sûreté – Classement des fonctions d'instrumentation et de contrôle-commande (CEI 45A/705/CDV:2008) Anwendungswarnvermerk Dieser Norm-Entwurf mit Erscheinungsdatum 2008-10-07 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt. Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfes besonders zu vereinbaren. Stellungnahmen werden erbeten – vorzugsweise als Datei per E-Mail an dke@vde.com in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.dke.de/stellungnahme abgerufen werden – oder in Papierform an die DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE, Stresemannallee 15, 60596 Frankfurt am Main. Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevante Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen. Gesamtumfang 63 Seiten DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE		

Beginn der Gültigkeit

Diese Norm gilt ab 2008-10-01.

Nationales Vorwort

Das internationale Dokument IEC 45A/705/CDV:2008 „Nuclear power plants – Instrumentation and control important to safety – Classification of instrumentation and control functions“ (CDV, en: Committee Draft for Vote) ist unverändert in diesen Norm-Entwurf übernommen worden. Dieser Norm-Entwurf enthält eine noch nicht autorisierte deutsche Übersetzung.

Um Zweifelsfälle in der Übersetzung auszuschließen, ist die englische Originalfassung des CDV entsprechend der diesbezüglich durch die IEC erteilten Erlaubnis beigefügt. Die Nutzungsbedingungen für den deutschen Teil des Norm-Entwurfes gelten gleichermaßen auch für den englischen IEC-Text.

Das internationale Dokument wurde vom SC 45A „Instrumentation and control of nuclear facilities“ der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet und den nationalen Komitees zur Stellungnahme und Abstimmung vorgelegt. Es wird jedoch nicht zeitgleich (parallel) bei IEC und CENELEC zur Umfrage gestellt. Derzeit ist also nicht vorgesehen, dieses Dokument als Europäische Norm zu übernehmen.

Da der Abstimmungszeitraum für einen FDIS (en: Final Draft International Standard) nur 2 Monate beträgt, und dann keine sachlichen Stellungnahmen mehr abgegeben werden können, sondern nur noch eine „JA/NEIN“-Entscheidung möglich ist, wobei eine „NEIN“-Entscheidung fundiert begründet werden muss, wird bereits der CDV als DIN-Norm-Entwurf veröffentlicht, um die Stellungnahmen aus der Öffentlichkeit noch vor der Abstimmung berücksichtigen zu können.

Für diesen Norm-Entwurf ist das nationale Arbeitsgremium UK 967.1 „Leittechnik für kerntechnische Anlagen“ der DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE (www.dke.de) zuständig.

In der Reihe VDE 0491 sind als Normen erschienen:

- DIN IEC 61226 (VDE 0491-1):2005-09, *Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Kategorisierung leittechnischer Funktionen (IEC 61226:2005)*
- DIN IEC 61513 (VDE 0491-2):2002-10, *Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Allgemeine Systemanforderungen (IEC 61513:2001)*
- DIN IEC 61513/A100 (VDE 0491-2/A100):2005-02, *Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Allgemeine Systemanforderungen – Nationaler Anhang ND (informativ): Mitgeltende Festlegungen aus anderen IEC-Normen*
- DIN IEC 60987 (VDE 0491-3-1):2008-04, *Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Anforderungen an die Hardwareauslegung rechnerbasierter Systeme (IEC 60987:2007)*
- DIN IEC 60880 (VDE 0491-3-2):2007-08, *Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Softwareaspekte für rechnerbasierte Systeme zur Realisierung von Funktionen der Kategorie A (IEC 60880:2006)*
- DIN IEC 62138 (VDE 0491-3-3):2004-09, *Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Softwareaspekte für rechnerbasierte Systeme zur Realisierung von Funktionen der Kategorien B oder C (IEC 62138:2004)*
- DIN IEC 62117 (VDE 0491-4):2001-10, *Kernkraftwerke – Druckwasserreaktoren – Überwachung ausreichender Kühlung des Kerns im abgeschalteten Zustand des Reaktors (IEC 62117:1999)*
- DIN IEC 61839 (VDE 0491-5):2002-09, *Kernkraftwerke – Auslegung von Warten – Analyse und Zuordnung der Funktionen (IEC 61839:2000)*
- DIN IEC 62241 (VDE 0491-5-2):2006-05, *Kernkraftwerke – Hauptwarte – Funktionen zur Meldung und Anzeige von Störungen (IEC 62241:2004)*
- DIN IEC 61227 (VDE 0491-5-3):200...-..., *Kernkraftwerke – Warten – Handbedienungen (IEC 61227:2008) – zurzeit in Druck*

- DIN IEC 60568 (VDE 0491-6):2006-11, *Kernkraftwerke – Instrumentierung mit sicherheitstechnischer Bedeutung – Kerninstrumentierung zur Messung der Neutronenflussdichte in Leistungsreaktoren (IEC 60568:2006)*
- DIN IEC 60709 (VDE 0491-7):2006-05, *Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Physikalische und elektrische Trennung (IEC 60709:2004)*
- DIN IEC 62340 (VDE 0491-10):200...-..., *Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Anforderungen zur Beherrschung von Versagen aufgrund gemeinsamer Ursache (CCF) (IEC 62340:2007) – zurzeit in Vorbereitung*
- DIN IEC 60671 (VDE 0491-100):2007-12, *Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Prüfungen zur Sicherstellung der Funktionsfähigkeit (IEC 60671:2007)*
mit Berichtigung 1:2008-08

Als weitere Norm-Entwürfe liegen vor:

- E DIN IEC 60964 (VDE 0491-5-1):2007-11, *Kernkraftwerke – Warten – Auslegung (IEC 45A/652/CDV:2007)*
- E DIN IEC 61772 (VDE 0491-5-4):2008-05, *Kernkraftwerke – Warten – Anwendung von Sichtgeräten (IEC 45A/681/CDV:2007)*

Änderungen

Gegenüber DIN IEC 61226 (VDE 0491-1):2005-09 wurden folgende Änderungen vorgenommen:

- a) Aufnahme einer Definition des sicheren stabilen Zustands (en: non-hazardous stable state, siehe 3.22);
- b) Verdeutlichung der Abgrenzungen zwischen den Kategorien (siehe Änderungsstriche am linken Rand);
- c) Verdeutlichung von Anforderungen für Einrichtungen zur Beherrschung auslegungsüberschreitender Ereignisse (siehe Änderungsstriche am linken Rand).

Die zum Vorwort des IEC-Entwurfs angegebene Fußnote 1) ist mit jenem Vorwort nicht Teil dieser deutschen Übersetzung. Aus Gründen der Übereinstimmung mit dem IEC-Bezugsdokument beginnen daher die Fußnoten mit Nummer 2.

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.

Eine Information über den Zusammenhang der zitierten Normen mit den entsprechenden Deutschen Normen ist in Tabelle NA.1 wiedergegeben.

Tabelle NA.1

Europäische Norm	Internationale Norm	Deutsche Norm	Klassifikation im VDE-Vorschriftenwerk
–	IEC 60709:2004	DIN IEC 60709 (VDE 0491-7):2006-05	VDE 0491-7
–	IEC 60780:1998	DIN IEC 60780:2000-12	–
EN 60812:2006	IEC 60812:2006	DIN EN 60812:2006-11	–
–	IEC 60880:2006	DIN IEC 60880 (VDE 0491-3-2):2007-08	VDE 0491-3-2
–	IEC 60964:20... (zurzeit Entwurf)	E DIN IEC 60964 (VDE 0491-5-1):2007-11	VDE 0491-5-1
–	IEC 60965	–	–
–	IEC 60980	–	–
–	IEC 60987:2007	DIN IEC 60987 (VDE 0491-3-1):2008-04	VDE 0491-3-1
Normen der Reihe EN 61000-4	Normen der Reihe IEC 61000-4	Normen der Reihe DIN EN 61000-4 (VDE 0847-4)	VDE 0847-4
EN 61000-6-2	IEC 61000-6-2:2005	DIN EN 61000-6-2 (VDE 0839-6-2):2006-03	VDE 0839-6-2
EN 61508-1:2001	IEC 61508-1:1998 + Corr.:1999	DIN EN 61508-1 (VDE 0803-1):2002-11	VDE 0803-1
EN 61508-2:2001	IEC 61508-2:2000	DIN EN 61508-2 (VDE 0803-2):2002-12	VDE 0803-2
EN 61508-3:2001	IEC 61508-3:1998 + Corr.:1999	DIN EN 61508-3 (VDE 0803-3):2002-12	VDE 0803-3
EN 61508-4:2001	IEC 61508-4:1998 + Corr.:1999	DIN EN 61508-4 (VDE 0803-4):2002-11	VDE 0803-4
–	IEC 61513:2001	DIN IEC 61513 (VDE 0491-2):2002-10 und DIN IEC 61513/A100 (VDE 0491-2/A100):2005-02	VDE 0491-2 VDE 0491-2/A100
–	IEC 61771:1995	–	–
–	IEC 61772:20... (zurzeit Entwurf)	E DIN IEC 61772 (VDE 0491-5-4):2008-05	VDE 0491-5-4
–	IEC 61839:2000	DIN IEC 61839 (VDE 0491-5):2002-09	VDE 0491-5
–	IEC 62138:2004	DIN IEC 62138 (VDE 0491-3-3):2004-09	VDE 0491-3-3
–	IAEA NS-R-1:2000	–	–
–	IAEA 50-C/SG-Q:2001	–	–
–	IAEA NS-G-1.3:2002	–	–

Nationaler Anhang NB (informativ)

Literaturhinweise

DIN EN 60812:2006-11, *Analysetechniken für die Funktionsfähigkeit von Systemen – Verfahren für die Fehlzustandsart- und -auswirkungsanalyse (FMEA) (IEC 60812:2006); Deutsche Fassung EN 60812:2006*

Normen der Reihe

DIN EN 61000-4 (VDE 0847-4), *Elektromagnetische Verträglichkeit (EMV) – Teil 4: Prüf- und Messverfahren*

DIN EN 61000-6-2 (VDE 0839-6-2):2006-03, *Elektromagnetische Verträglichkeit (EMV) – Teil 6-2: Fachgrundnormen – Störfestigkeit für Industriebereiche (IEC 61000-6-2:2005); Deutsche Fassung EN 61000-6-2:2005*

DIN EN 61508-1 (VDE 0803-1):2002-11, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 1: Allgemeine Anforderungen (IEC 61508-1:1998 + Corrigendum 1999); Deutsche Fassung EN 61508-1:2001*

DIN EN 61508-2 (VDE 0803-2):2002-12, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 2: Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme (IEC 61508-2:2000); Deutsche Fassung EN 61508-2:2001*

DIN EN 61508-3 (VDE 0803-3):2002-12, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 3: Anforderungen an Software; (IEC 61508-3:1998 + Corrigendum 1999); Deutsche Fassung EN 61508-3:2001*

DIN EN 61508-4 (VDE 0803-4):2002-11, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 4: Begriffe und Abkürzungen (IEC 61508-4:1998 + Corrigendum 1999); Deutsche Fassung EN 61508-4:2001*

DIN IEC 60709 (VDE 0491-7):2006-05, *Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Physikalische und elektrische Trennung (IEC 60709:2004)*

DIN IEC 60780:2000-12, *Kernkraftwerke – Elektrisches Gerät des Sicherheitssystems – Qualifizierung (IEC 60780:1998)*

DIN IEC 60880 (VDE 0491-3-2):2007-08, *Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Softwareaspekte für rechnerbasierte Systeme zur Realisierung von Funktionen der Kategorie A (IEC 60880:2006)*

E DIN IEC 60964 (VDE 0491-5-1):2007-11, *Kernkraftwerke - Warten – Auslegung (IEC 45A/652/CDV:2007)*

DIN IEC 60987 (VDE 0491-3-1):2008-04, *Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Anforderungen an die Hardwareauslegung rechnerbasierter Systeme (IEC 60987:2007)*

DIN IEC 61513 (VDE 0491-2):2002-10, *Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Allgemeine Systemanforderungen (IEC 61513:2001)*

DIN IEC 61513/A100 (VDE 0491-2/A100):2005-02, *Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Allgemeine Systemanforderungen – Nationaler Anhang ND (informativ): Mitgeltende Festlegungen aus anderen IEC-Normen*

E DIN IEC 61772 (VDE 0491-5-4):2008-05, *Kernkraftwerke – Warten – Anwendung von Sichtgeräten (IEC 45A/681/CDV:2007)*

DIN IEC 61839 (VDE 0491-5):2002-09, *Kernkraftwerke – Auslegung von Warten – Analyse und Zuordnung der Funktionen (IEC 61839:2000)*

DIN IEC 62138 (VDE 0491-3-3):2004-09, *Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Softwareaspekte für rechnerbasierte Systeme zur Realisierung von Funktionen der Kategorien B oder C (IEC 62138:2004)*

**Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung –
Kategorisierung leittechnischer Funktionen**

Inhalt

	Seite
Einleitung.....	6
1 Anwendungsbereich	10
2 Normative Verweisungen.....	10
3 Begriffe.....	11
4 Abkürzungen.....	15
5 Kategorisierungsschema	15
5.1 Einleitung	15
5.2 Hintergrund	15
5.3 Beschreibung der Kategorien	16
5.3.1 Allgemeines	16
5.3.2 Kategorie A	17
5.3.3 Kategorie B	17
5.3.4 Kategorie C	17
5.4 Zuordnungskriterien	18
5.4.1 Kategorie A	18
5.4.2 Kategorie B	18
5.4.3 Kategorie C	19
6 Vorgehensweise bei der Kategorisierung	20
6.1 Ermittlung der Auslegungsgrundlage.....	20
6.2 Festlegung und Kategorisierung der Funktionen.....	20
7 Zuordnung der technischen Anforderungen zu Kategorien.....	22
7.1 Allgemeine Anforderungen	22
7.2 Anforderungen betreffend Funktionen	22
7.2.1 Grundsätzliche Anforderungen	22
7.2.2 Spezielle Anforderungen	23
7.3 Anforderungen betreffend leittechnische Systeme.....	23
7.3.1 Grundsätzliche Anforderungen	23
7.3.2 Spezielle Anforderungen	24
7.4 Anforderungen betreffend Gerät.....	26
7.4.1 Grundsätzliche Anforderungen	26
7.4.2 Spezielle Anforderungen	26
7.5 Anforderungen betreffend Qualitätsgesichtspunkte	27
7.5.1 Grundsätzliche Anforderungen	27
7.5.2 Spezielle Anforderungen	27

	Seite
Anhang A (informativ) Beispiele zu Kategorien	30
A.1 Kategorie A.....	30
A.1.1 Typische Funktionen	30
A.1.2 Typische leittechnische Systeme	30
A.2 Kategorie B.....	30
A.2.1 Typische Funktionen	30
A.2.2 Typische leittechnische Systeme	30
A.3 Kategorie C.....	31
A.3.1 Typische Funktionen	31
A.3.2 Typische leittechnische Systeme	31
 Bild 1 – Vorgehensweise bei der Kategorisierung.....	 21
 Tabelle 1 – Zusammenhang zwischen Kategorien und anderen IEC Normen	 29

Einleitung

Hintergrund, hauptsächliche Inhalte und Organisation der Norm

Mit dieser Internationalen Norm wird eine Forderung der IAEA umgesetzt²⁾, die leittechnischen Systeme von Kernkraftwerken gemäß ihrer sicherheitstechnischen Bedeutung zu klassifizieren. Bei den rechnerbasierten leittechnischen Systemen, die heute in Kernkraftwerken eingesetzt werden, sind die sicherheitstechnisch wichtigen Funktionen über mehrere Systeme und Teilsysteme verteilt. Daher wird mit dieser Norm beachtet,

- die sicherheitstechnisch wichtigen leittechnischen Funktionen in Kategorien einzuteilen, abhängig von ihrem Beitrag zur Verhinderung oder Abschwächung von anzunehmenden Versagen auslösenden Ereignissen (AVE), und Anforderungen zu entwickeln, die der sicherheitstechnischen Bedeutung jeder Kategorie entsprechen;
- den leittechnischen Systemen und Geräten, welche die kategorisierten Funktionen ausführen, die entsprechenden Anforderungen zuzuordnen.

Gemäß Empfehlung der IAEA³⁾ beruhen die Methoden der Klassifizierung grundsätzlich auf der deterministischen Sicherheitsanalyse und sollten, wo angemessen, durch probabilistische Methoden ergänzt werden. Mehrere mögliche Vorgehensweisen für die Anwendung probabilistischer Sicherheitsanalysen zur Klassifizierung sind in IEC 61838:2001 beschrieben.

Die vorliegende Neuauflage der IEC 61226 ermöglicht die teilweise Berücksichtigung quantitativer Beurteilungen.

Einordnung der vorliegenden Norm in die Struktur der Normen des IEC/SC 45A

Auf vorliegende Norm wird in IEC 61513 direkt Bezug genommen. Sie stellt ein Dokument der zweiten Ebene der Normen des IEC/SC 45A dar und befasst sich mit der Kategorisierung von Funktionen und der Klassifizierung von Systemen.

Näheres zur Struktur der Normen des IEC/SC 45A ist am Ende dieser Einleitung zu finden.

Empfehlungen und Einschränkungen bei Anwendung der Norm

Die richtige Kategorisierung von Funktionen führt zu einem der sicherheitstechnischen Bedeutung der Funktionen angemessenen Aufwand der Anlagenplaner, Betreiber und Genehmigungsbehörden hinsichtlich Spezifikation, Auslegung, Qualifizierung, Qualitätssicherung, Fertigung, Inbetriebnahme, Instandhaltung und Prüfung der Systeme, welche die Funktionen ausführen.

Diese Norm legt die Kriterien und Vorgehensweisen fest, die anzuwenden sind, um die leittechnischen Funktionen einer der drei Kategorien A, B und C entsprechend ihrer sicherheitstechnischen Bedeutung und einer Kategorie „nicht kategorisiert“ für Funktionen ohne sicherheitstechnische Bedeutung zuzuordnen. Es werden allgemeine Anforderungen für jede Kategorie beschrieben und grundlegende technische Anforderungen für Bereiche wie Qualitätssicherung, Zuverlässigkeit, Prüfung und Instandhaltung angegeben.

²⁾ 5.1 von IAEA NS-R-1.

³⁾ In 5.2 von IAEA NS-R-1 wird gefordert, dass die Vorgehensweise zur Klassifizierung der sicherheitstechnischen Bedeutung einer Struktur, eines Systems oder einer Komponente grundsätzlich auf deterministischen Methoden beruhen muss, wo angemessen ergänzt durch probabilistische Methoden und ingenieurmäßige Beurteilungen, wobei Faktoren zu berücksichtigen sind wie

- a) die durchzuführenden Sicherheitsfunktionen;
- b) die Folgen des Versagens einer Funktion;
- c) die Wahrscheinlichkeit, dass es (das leittechnische System) zur Durchführung einer Sicherheitsfunktion angefordert wird;
- d) die Zeit nach einem AVE oder die Zeitspanne, für die der Betrieb (des leittechnischen Systems) gefordert wird.

Die Kategorie, der eine Funktion zugeordnet wird, bestimmt allgemeine und spezifische technische Anforderungen. Allgemeine Anforderungen haben zum Ziel, für jede Funktion in angemessenem Ausmaß sicherzustellen, dass sie im Anforderungsfall die erforderliche Leistungsfähigkeit und Zuverlässigkeit aufweist. Dies betrifft Gesichtspunkte der Funktionalität, Zuverlässigkeit, Leistungsfähigkeit, Beständigkeit gegen Umgebungseinflüsse und Qualitätssicherung. Der Grad der Sicherstellung, mit dem diese Gesichtspunkte zu belegen sind, muss der sicherheitstechnischen Bedeutung der Funktion entsprechen.

- a) Die Sicherstellung der Funktionalität wird durch Erstellung einer vollständigen und umfassenden Anforderungsspezifikation sowie der Anwendung geeigneter Normen und Regeln erreicht.
- b) Die Sicherstellung der Zuverlässigkeit wird durch Auswahl geeigneter Komponenten, Strukturen und dem Grad an Redundanz und Diversität in Zusammenhang mit physikalischer Trennung und/oder physikalischen Barrieren, elektrischer Isolation sowie wiederkehrenden Prüfungen während des Betriebs erreicht.
- c) Die Sicherstellung der Leistungsfähigkeit wird durch Erstellen von Spezifikationen unter Angabe der erforderlichen Leistungsfähigkeit, der Anwendung von Vorgehensweisen zur Qualitätssteuerung, durch Verifizierung und Validierung während Auslegung, Entwicklung und Fertigung, durch Prüfung der einzelnen und integrierten Systeme und Geräte vor Inbetriebnahme sowie durch Prüfungen während des Betriebs erreicht.
- d) Die Sicherstellung der Beständigkeit gegen Umwelteinflüsse wird durch Programme zur Qualifizierung von Geräten erreicht. Dadurch wird sichergestellt, dass Alterungseffekte und Umweltbedingungen, die während der geforderten Betriebszeit auftreten können, die Leistungsfähigkeit der Geräte nicht unzulässig vermindern.
- e) Die Sicherstellung, dass die Gesichtspunkte der Funktionalität, der Leistungsfähigkeit, der Beständigkeit gegen Umwelteinflüsse und der Zuverlässigkeit in jeder Phase der Konzeption, Planung, Auslegung, Entwicklung, Fertigung, Prüfung, Erstellung und Inbetriebnahme in einwandfreier Weise in Betracht gezogen wurden, wird erreicht, indem jede Projektphase nach einem angemessenen Qualifizierungsprogramm abgewickelt wird.

In der gesamten Norm bezeichnet „muss“ Anforderungen, deren Erfüllung zur Einhaltung dieser Norm zwingend ist; „sollte“ bezeichnet Anforderungen, deren Erfüllung zur Einhaltung dieser Norm zwar nicht zwingend ist, die aber dringend empfohlen werden; „darf“ bezeichnet optionale Anforderungen.

Beschreibung der Struktur der Normen des IEC/SC 45A und deren Beziehungen zu anderen Dokumenten einschließlich der Dokumente anderer Organisationen (IAEA, ISO)

Das Dokument der höchsten Ebene unter den Normen des IEC/SC 45A stellt die Norm IEC 61513 dar. Diese enthält allgemeine Anforderungen an die leittechnischen Systeme und Geräte, die zur Ausführung sicherheitstechnisch wichtiger Funktionen in Kernkraftwerken genutzt werden. Durch die IEC 61513 werden die Normen des IEC/SC 45A strukturiert.

In IEC 61513 wird direkt auf andere Normen des IEC/SC 45A verwiesen, die allgemeine Themen wie die Kategorisierung von Funktionen und die Klassifizierung von Systemen, Qualifizierung, Trennung von Systemen, Maßnahmen gegen Versagen aufgrund gemeinsamer Ursache, Software-Aspekte rechnerbasierter Systeme, Hardware-Aspekte rechnerbasierte Systeme und Auslegung von Warten behandeln. Die Normen, auf die direkt verwiesen wird, bilden die zweite Ebene und sollten zusammen mit IEC 61513 als ein in sich konsistenter Satz von Dokumenten betrachtet werden.

Die dritte Ebene bilden Normen des IEC/SC 45A, auf die in IEC 61513 nicht direkt verwiesen wird. Diese Normen behandeln spezielles Gerät, technische Methoden oder spezifische Aktivitäten. Sie beziehen sich hinsichtlich der allgemeinen Themen auf die Dokumente der zweiten Ebene, können jedoch im Allgemeinen für sich allein benutzt werden.

Eine vierte Ebene erweitert die Normen des IEC/SC 45A mit Technischen Berichten, die nicht normativ sind.

Für IEC 61513 wird ein Darstellungsformat verwendet, das dem der grundsätzlichen Sicherheitsnorm IEC 61508 ähnlich ist, mit einem Sicherheits-Lebenszyklus als Gesamtrahmen und einem System-Lebenszyklus als weiteren wichtigen Rahmen. Mit IEC 61513 werden die allgemeinen Anforderungen (für Sicherheitssysteme unterschiedlicher industrieller Anwendungen) von IEC 61508-1, -2 und -4 für die Anwendung auf nuklearem Sektor umgesetzt. Die Einhaltung der IEC 61513 erleichtert somit die Übereinstimmung mit der Norm IEC 61508, weil deren allgemeine Anforderungen für die nukleare Industrie berücksichtigt wurden. In diesem Rahmen entsprechen IEC 60880 und IEC 62138 für den nuklearen Sektor der Norm IEC 61508-3.

IEC 61513 stützt sich für Themen der Qualitätssicherung sowohl auf ISO als auch auf IAEA 50-C-QA ab.

In den Normen des IEC/SC 45A werden die Prinzipien und grundsätzlichen Sicherheitsaspekte des „IAEA Code for the safety of nuclear power plants“ und der „IAEA safety series“, insbesondere der Anforderungen des NS-R-1 „Safety of Nuclear Power Plants: Design“ und des Safety Guide NS-G-1.3 „Instrumentation and control systems important to safety in Nuclear Power Plants“, umgesetzt. Terminologie und Definitionen in den Normen des IEC/SC 45A sind mit den von der IAEA verwendeten konsistent.

1 Anwendungsbereich

Diese Internationale Norm legt ein Verfahren fest, das die Einteilung der Informations- und Steuerungsfunktionen für Kernkraftwerke und der leittechnischen Systeme, welche diese Funktionen ausführen, in Kategorien erlaubt, die maßgebend für die sicherheitstechnische Bedeutung der Funktionen sind. Die sich daraus ergebende Kategorisierung bestimmt die anzuwendenden Auslegungskriterien.

Die Auslegungskriterien sind die Qualitätsmaßstäbe, über die die Angemessenheit jeder Funktion in Bezug auf ihre Bedeutung für die Sicherheit der Anlage sichergestellt wird. In dieser Norm beziehen sich die Auslegungskriterien auf Funktionalität, Zuverlässigkeit, Leistungsfähigkeit, Beständigkeit gegen Umwelteinflüsse und Qualitätssicherung.

Diese Norm gilt für alle Informations-, Steuerungs- und Regelungsfunktionen sowie die leittechnischen Systeme und Geräte, die diese Funktionen ausführen. Die betrachteten Funktionen, Systeme und Geräte führen automatische Schutzfunktionen sowie Funktionen der Prozesssteuerung und -regelung aus und stellen Informationen für das Betriebspersonal zur Verfügung. Sie halten die Betriebsparameter des Kernkraftwerks innerhalb der Grenzen für den sicheren Anlagenbetrieb, stellen automatische Maßnahmen zur Verfügung oder ermöglichen Handmaßnahmen, die Störfälle vermeiden oder minimieren oder die Abgabe radioaktiver Stoffe in die Anlage oder in die Umwelt vermeiden oder minimieren. Die leittechnischen Funktionen, die diese Aufgaben erfüllen, schützen die Gesundheit und stellen die Sicherheit des Kraftwerkspersonals und der Öffentlichkeit sicher.

Diese Norm folgt den allgemeinen Prinzipien nach IAEA NS-R-1 und NS-G-1.3 und beinhaltet ein strukturiertes Verfahren zur Anwendung der darin enthaltenen Leitlinien auf leittechnische Systeme, die sicherheitstechnisch wichtige Funktionen in Kernkraftwerken ausführen. Diese Norm sollte in Verbindung mit den IAEA-Sicherheitsanforderungen und -Leitlinien sowie IEC 61513 unter Umsetzung der Anforderungen von IEC 61508 benutzt werden.

2 Normative Verweisungen

Die folgenden zitierten Dokumente sind für die Anwendung dieses Dokuments erforderlich. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

IEC 60709, *Nuclear power plants – Instrumentation and control systems important to safety – Separation*

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

IEC 60812, *Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)*

IEC 60880, *Nuclear power plants – I&C systems important to safety – Software aspects for computer-based systems performing category A functions*

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

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

IEC 60980, *Recommended practices for seismic qualification of electrical equipment of the safety system for nuclear generating stations*

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

IEC 61000-4 (alle Teile), *Electromagnetic compatibility (EMC) – Testing and measurement techniques*

IEC 61000-6-2, *Electromagnetic compatibility (EMC) – Part 6-2: Generic standards – Immunity for industrial environments*

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

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

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

IEC 61513, *Nuclear power plant – Instrumentation and control for systems important to safety – General requirements for systems*

IEC 61771, *Nuclear power plants – Main control room – Verification and validation of design*

IEC 61772, *Nuclear power plants – Main control room – Application of visual display units (VDU)*

IEC 61839, *Nuclear power plants – Design of control rooms – Functional analysis and assignment*

IEC 62138, *Nuclear power plants – Instrumentation and control important for safety – Software aspects for computer-based systems performing category B or C functions*

IAEA Safety Standard Series Requirements NS-R-1:2000, *Safety of Nuclear Power Plants: Design*

IAEA Code 50-C/SG-Q:2001, *Quality Assurance for Safety in Nuclear Power Plants and other Nuclear Installations*

IAEA Safety Guide NS-G-1.3:2002, *Instrumentation and Control Systems Important to Safety in Nuclear Power Plants*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe. Sie sind mit jenen Definitionen konsistent oder, wenn möglich, identisch, die in anderen aktuellen Normen oder Leitlinien von IEC oder IAEA verwendet werden.

3.1

anzunehmende betriebliche Vorkommnisse

(en: anticipated operational occurrences)

alle betrieblichen Vorgänge, die vom Normalbetrieb abweichen und erfahrungsgemäß einmal oder mehrere Male während der Lebenszeit der Anlage auftreten und die wegen entsprechender Auslegungsmaßnahmen weder signifikante Auswirkungen auf sicherheitstechnisch wichtige Einrichtungen haben noch zu Störfällen führen

3.2

Versagen aufgrund gemeinsamer Ursache

(en: common cause failure)

Versagen von zwei oder mehreren Strukturen, Systemen oder Komponenten infolge eines einzelnen spezifischen Ereignisses oder einer spezifischen Ursache

3.3

Auslegungsstörfall

(en: design basis accident)

Störfallbedingungen, für die das Kernkraftwerk gemäß den vorgegebenen Auslegungskriterien konstruiert ist und bei denen eine Beschädigung der Brennelemente sowie die Abgabe radioaktiver Stoffe innerhalb genehmigter Grenzen liegen

3.4

Auslegungsereignis

(en: design basis event)

Sammelbegriff zur Bezeichnung der Auslegungsstörfälle und der anzunehmenden betrieblichen Vorkommnisse

3.5

Diversität

(en: diversity)

Vorhandensein von zwei oder mehreren unterschiedlichen Verfahren oder Mitteln, um ein bestimmtes Ziel zu erreichen. Diversität ist besonders geeignet als Schutzmaßnahme gegen Versagen aufgrund gemeinsamer Ursache (CCF). 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.

ANMERKUNG Diese Definition (nach IEC 60880) ist umfassender als die in IAEA NS-G-1.3, die lautet:

„Vorhandensein von zwei oder mehreren Systemen oder Komponenten zur Ausführung identischer Funktionen, wobei die verschiedenen Systeme oder Komponenten unterschiedliche Eigenschaften aufweisen, und zwar derart, dass die Möglichkeit von Versagen aufgrund gemeinsamer Ursache verringert wird.“

3.6

Gerät

Einrichtung

(en: equipment)

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

3.7

Funktion

(en: function)

dient einem bestimmten zu erreichenden Zweck oder Ziel, das spezifiziert oder beschrieben werden kann; auf die zum Erreichen des Ziels erforderlichen physikalischen Mittel wird nicht näher eingegangen

3.8

Funktionalität

(en: functionality)

Attribut einer Funktion, das die Operationen zur Umwandlung der Eingangsinformationen in die Ausgangsinformationen definiert

3.9

HF-Engineering-Programm

Human-Factor-Engineering-Programm

(en: human factor engineering programme)

Programm, das wenigstens die HF-Organisation, die Rolle und Aufgabe der HF-Spezialisten, die HF-Aktivitäten und ihre Einbindung in die Auslegungs- und Validierungsvorgänge beschreibt und eine Liste der in jedem Schritt des Programms zu erledigenden Aufgaben umfasst

3.10

leittechnische Systeme mit sicherheitstechnischer Bedeutung

sicherheitstechnisch wichtige leittechnische Systeme

(en: I&C systems important to safety)

die leittechnischen Systeme, deren Fehlfunktion oder Versagen zu unzulässiger Strahlenbelastung des Anlagenpersonals oder der Öffentlichkeit führen könnte, und solche leittechnischen Systeme, die verhindern, dass anzunehmende betriebliche Vorkommnisse zu unzulässigen Folgen führen

3.11

Anlagenzustände

(en: plant states)

Betriebszustände		Störfallbedingungen			
Normalbetrieb	Auslegungsereignisse			Auslegungsüberschreitende Störfälle	
	Anzunehmende betriebliche Vorkommnisse	a)	Auslegungsstörfälle	b)	Schwere Störfälle
–	–			Störfall-Management	
a) Störfallbedingungen, die nicht explizit als Auslegungsstörfälle betrachtet werden, aber die von den Auslegungsstörfällen mit eingeschlossen werden.					
b) Auslegungsüberschreitende Störfälle ohne signifikante Schädigung des Kerns.					

3.12

Leistungsfähigkeit

(en: performance)

Effizienz, mit der eine gewünschte Funktion ausgeführt wird (z. B. Antwortzeit, Genauigkeit, Empfindlichkeit gegenüber Parameteränderungen)

3.13

anzunehmende Versagen auslösende Ereignisse

(en: postulated initiating events)

Ereignisse, die zu den anzunehmenden betrieblichen Vorkommnissen oder Störfallbedingungen führen ^{N1)}

3.14

Redundanz

(en: redundancy)

Vorsehen alternativer (identischer oder unterschiedlicher) Strukturen, Systeme oder Komponenten, so dass das Versagen einer Einheit davon nicht zum Versagen der ganzen Funktion führt

3.15

Sicherheitsgruppe

(en: safety group)

Anordnung von Geräten, die dazu bestimmt ist, alle erforderlichen Aktionen durchzuführen, um sicherzustellen, dass für ein bestimmtes, anzunehmendes Versagen auslösendes Ereignis die in der Auslegungsgrundlage der Anlage für Auslegungsereignisse festgelegten Grenzwerte nicht überschritten werden

3.16

Sicherheitssysteme

(en: safety systems)

sicherheitstechnisch wichtige Systeme, die dazu dienen, die sichere Abschaltung des Reaktors und die Wärmeabfuhr aus dem Reaktorkern sicherzustellen oder die Konsequenzen von anzunehmenden betrieblichen Vorkommnissen und Auslegungsstörfällen zu begrenzen

3.17

sicherheitsrelevante leittechnische Systeme

(en: safety related I&C systems)

jene sicherheitstechnisch wichtigen leittechnischen Systeme, die nicht zu den Sicherheitssystemen gehören

^{N1)} Nationale Fußnote: Siehe auch 3.11.

3.18

Einzelausfall

Einzelversagen ^{N2)}

(en: single failure)

ein Ausfall mit dem Ergebnis, dass eine Komponente die geplanten Funktionen nicht ausführen kann, und alle daraus resultierenden Folgeausfälle

3.19

System

(en: system)

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

3.20

Typprüfung

(en: type testing)

Nachweis der Fähigkeit eines Gerätetyps, die spezifizierten Anforderungen zu erfüllen, indem ein repräsentatives Gerät diese Typs oder eine Anzahl solcher Geräte einer bestimmten Reihe physikalischer, chemischer, Umgebungs- oder betrieblicher Bedingungen ausgesetzt wird

3.21

unzulässige Folgen

(en: unacceptable consequences)

Folgen eines Betriebszustands oder eines AVE, bei denen für die entsprechenden Anlagenzustände spezifizierte Grenzen hinsichtlich radioaktiver Freisetzungen auf der Anlage oder in die weitere Umgebung überschritten werden

ANMERKUNG Zusätzliche Grenzen wie unzulässige Brennelementschäden oder Schäden an anderen wichtigen Komponenten können auf nationaler Ebene spezifiziert werden. Dies kann entweder eine massive, unkontrollierte Freisetzung sein, verursacht durch Ereignisse mit einer Häufigkeit, die über die Auslegungsgrundlagen hinausgeht, oder es können Ereignisse mit einer Häufigkeit sein, die zwar im Rahmen der Auslegungsgrundlagen liegt, bei denen aber die Größe der Freisetzung den spezifizierten Grenzwert überschreitet. Zusätzliche Grenzen wie unzulässige Beschädigung von Brennelementen können ebenso spezifiziert werden. Das kann eine Beschädigung der Brennstoffhülle sein, die zu einem unzulässigen Anstieg der Aktivität im Primärkühlmittel führt, oder eine Beschädigung der Brennelementstruktur, die eine Beeinträchtigung der Kühlfähigkeit verursacht. Beschädigung der anderen Barrieren kann ebenfalls als unzulässige Folge betrachtet werden.

3.22

sicherer stabiler Zustand

(en: non-hazardous stable state)

Anlagenzustand, in dem die Stabilisierung einer Transiente erreicht worden ist, der Reaktor unterkritisch ist, ausreichende Wärmeabfuhr sichergestellt ist und radioaktive Freisetzungen begrenzt sind

ANMERKUNG Eine Transiente gilt als stabilisiert, wenn für alle sicherheitstechnisch signifikanten Parameter die Sicherheitsabstände (z. B. zwischen Wärmeabfuhr und Wärmeerzeugung) entweder stabil sind oder anwachsen, oder ein ausreichender Sicherheitsabstand verbleibt, um alle zu erwartenden physikalischen Vorgänge abzudecken.

^{N2)} Nationale Fußnote: Wenn Hardware oder Teilsysteme (z. B. ein Strang eines redundanten Systems) betroffen sind, wird „failure“ mit „Ausfall“ übersetzt.

4 Abkürzungen

Deutsch	Englisch
ALARA so gering wie mit vertretbarem Aufwand erreichbar	ALARA as low as reasonably achievable
DBA Auslegungstörfall	DBA design basis accident
DBE Auslegungsereignis	DBE design basis event
WAP Werksabnahmeprüfung	FAT factory acceptance test
FMEA Fehlermöglichkeits- und -einflussanalyse	FMEA Failure Modes and Effects Analysis
MMK Mensch-Maschine-Kommunikation	HMI human machine interface
I&C Instrumentation and control	LT Leittechnik
IAEA Internationale Atomenergie-Behörde	IAEA International Atomic Energy Agency
KKW Kernkraftwerk	NPP Nuclear power plant
AVE anzunehmendes Versagen auslösendes Ereignis	PIE postulated initiating event
PRA probabilistische Risikobewertung	PRA probabilistic risk assessment
QS Qualitätssicherung	QA quality assurance
SAT Abnahmeprüfung auf der Anlage	SAT site acceptance test

5 Kategorisierungsschema

5.1 Einleitung

Durch leittechnische Systeme ausgeführte Funktionen müssen entsprechend ihrer sicherheitstechnischen Bedeutung in Kategorien eingeteilt werden. Für die sicherheitstechnische Bedeutung einer Funktion sind die Folgen ihres Versagens bei Anforderung und ihrer Fehlauflösung ohne Anforderung maßgebend. Die Kategorie bestimmt die Auslegungs- und Qualitätsanforderungen für leittechnische Systeme und Geräte. Diese Anforderungen müssen unabhängig von der Technologie der eingesetzten Geräte festgelegt werden. 5.2 erläutert den Hintergrund des Kategorisierungsschemas.

5.3 beschreibt die drei Kategorien, die zur Einteilung der Funktionen benutzt werden. Die Kategorien beruhen auf den ursprünglich in der 1. Ausgabe der IEC 61226 (1993) definierten.

5.4 enthält die Zuordnungskriterien für die jeweiligen Kategorien.

Abschnitt 6 gibt eine Anleitung für den Kategorisierungsvorgang.

Abschnitt 7 beschreibt die technischen Anforderungen für jede der drei Kategorien. Die meisten dieser Anforderungen beziehen sich auf die Systeme und Geräte, welche die Funktionen ausführen, aber einige betreffen nur die Funktionen.

Anhang A enthält typische Beispiele für die Kategorisierung leittechnischer Funktionen von Kernkraftwerken. Wegen möglicher Abhängigkeit vom jeweiligen Reaktortyp dienen die Ausführungen nur zur Information.

5.2 Hintergrund

Das Konzept der gestuften Maßnahmen (defence-in-depth, DiD) ist in der Auslegungsgrundlage von Kernkraftwerken fest verankert^{N3)}. Die grundlegende Idee besteht in der Einrichtung mehrerer Maßnahmenstufen zur Vermeidung unsicherer Anlagenzustände, wobei die Verhinderung unsicherer Anlagenzustände der Abschwächung von Folgen unsicherer Anlagenzustände vorzuziehen ist. Wegen der Vielzahl von Funktionen, die für Betrieb und Sicherheit der Anlage benötigt wird und die mit dem Einsatz von DiD zunimmt, ist es wichtig, die sicherheitstechnische Bedeutung jeder Funktion zu kennen.

^{N3)} Nationale Fußnote: Siehe A.3 von DIN IEC 61513 (VDE 0491-2):2002-10.

In IAEA NS-R-1 wird die Idee der Klassifizierung von KKW-Systemen entsprechend ihrer sicherheitstechnischen Bedeutung aufgegriffen und es werden Beispiele für die Klassifizierung von wichtigen Systemen mehrerer KKW-Typen angeführt. Alle Strukturen, Systeme und Komponenten (einschließlich Software für die Leittechnik), die sicherheitstechnisch wichtig sind, müssen zuerst ermittelt und dann auf der Basis ihrer Funktion und ihrer sicherheitstechnischen Bedeutung klassifiziert werden. Sie müssen so ausgelegt, hergestellt und gewartet werden, dass ihre Qualität und Zuverlässigkeit mit dieser Klassifizierung in Einklang steht.

IAEA NS-G-1.3 gibt Anleitung zur Klassifizierung von Systemen entsprechend der sicherheitstechnischen Bedeutung der Funktionen, die sie ausführen. Sie enthält Überlegungen zum Zeitablauf, wie

- die Dauer, in der das leittechnische System nach seiner Anforderung benötigt wird;
- die für alternative Maßnahmen zur Verfügung stehende Zeit;
- die Rechtzeitigkeit der Entdeckung und Beseitigung unentdeckter Ausfälle.

In dieser Norm wird die Klassifizierungsstrategie von IAEA NS-G-1.3 erweitert, und es werden die Kriterien und Methoden für die Einordnung leittechnischer Funktionen von Kernkraftwerken zur Verfügung gestellt, die je nach sicherheitstechnischer Bedeutung in eine der drei Kategorien A, B, C oder eine weitere Kategorie für Funktionen mit keiner direkten sicherheitstechnischen Rolle erfolgt. Leittechnische Funktionen, die nach IAEA-Definition zum Sicherheitssystem gehören, werden im Allgemeinen den Kategorien A oder B zugeordnet; die nach IAEA als sicherheitsrelevant eingestuften Funktionen werden im Allgemeinen den Kategorien B oder C zugeordnet.

Die jeweilige sicherheitstechnische Bedeutung und die damit verbundenen Anforderungen an Teile des Sicherheitssystems und der sicherheitsrelevanten Leittechnik unterscheiden sich, so dass es angemessen ist, sie verschiedenen Sicherheitsklassen zuzuweisen. Einige leittechnische Systeme können wesentliche Auswirkungen auf die Sicherheit haben und bedürfen daher angemessener Aufmerksamkeit. Andere leittechnische Systeme haben mittlere, geringe oder keine Bedeutung für die Sicherheit. An sie sind vergleichsweise weniger strenge Anforderungen hinsichtlich Sicherstellung der Leistungsfähigkeit und zu erbringender Sicherheitsnachweise zu stellen; für sie gelten andere technische Anforderungen.

Bei der nationalen Anwendung der Prinzipien und Kriterien dieser Norm mag eine andere Nomenklatur bezüglich der Kategorien A, B und C verwendet werden. Jedoch müssen bei der Anwendung im nationalen Bereich die Prinzipien, Kriterien und zugehörigen Anforderungen dieser Norm beachtet werden. Dabei ist für Darstellung und Dokumentation eine angemessene Entsprechung zu den hier definierten Kategorien zu berücksichtigen.

5.3 Beschreibung der Kategorien

5.3.1 Allgemeines

Leittechnische Systeme in Kernkraftwerken führen Funktionen unterschiedlicher Bedeutung für die Sicherheit aus. Die sicherheitstechnische Bedeutung jeder leittechnischen Funktion hängt von der Rolle ab, die sie spielt, um Sicherheit zu erreichen und beizubehalten, von den möglichen Folgen des Versagens einer erforderlichen Funktion und der Wahrscheinlichkeit dieser Folgen. Daher wird vor Kategorisierung der leittechnischen Funktionen der Abschluss einer ersten Sicherheitsanalyse der jeweiligen Auslegung des Kernkraftwerks gefordert. Das Ausmaß der möglichen Folgen eines angenommenen Versagens einer leittechnischen Funktion definiert den Grad der Sicherstellung der Eigenschaften der verschiedenen Systeme und Geräte, die diese Funktion ausführen, insbesondere hinsichtlich der Funktionalität, Leistungsfähigkeit und Zuverlässigkeit.

Für die Auslegungs-, Bewertungs- und Genehmigungsvorgänge werden die Sicherheitskategorien A, B und C definiert, mit den zugehörigen technischen und qualitativen Anforderungen, die für Auslegung und Realisierung der sicherheitstechnisch wichtigen leittechnischen Systeme und Geräte anzuwenden sind.

5.3.2 Kategorie A

In Kategorie A werden die Funktionen eingestuft, die eine grundsätzliche Rolle für die Erreichung und Beibehaltung der Sicherheit des Kernkraftwerks spielen, weil sie verhindern, dass Auslegungsereignisse (DBE) zu unzulässigen Folgen führen. Diese Rolle ist zu Beginn der Transiente besonders wichtig, weil da keine alternativen Maßnahmen ergriffen werden können, selbst wenn es möglich wäre, bisher verborgene Fehler zu entdecken. Diese Funktionen spielen für das Erreichen oder Erhalten des sicheren stabilen Zustands eine grundsätzliche Rolle ⁴⁾. Wenn spezifizierte Handmaßnahmen vorgesehen sind, um den sicheren stabilen Zustand zu erreichen, müssen Faktoren beachtet werden wie die Verfügbarkeit redundanter validierter Informationsquellen, genügend Zeit für den Operateur zur Hinzuziehung alternativer Informationen und Überlegungen, ob Handmaßnahmen bei den vorliegenden Ereignisabläufen die einzige Möglichkeit zur Erhaltung der Anlagensicherheit sind.

Kategorie A umfasst auch Funktionen, deren Versagen direkt zu Störfallbedingungen mit unzulässigen Folgen führen könnten, wenn sie nicht durch andere Funktionen der Kategorie A abgeschwächt werden. Funktionen der Kategorie A haben hohe Zuverlässigkeitsanforderungen. Folglich kann es erforderlich sein, ihre Funktionalität und Komplexität einzuschränken.

5.3.3 Kategorie B

In Kategorie B werden Funktionen eingestuft, die für das Erreichen und Erhalten der erforderlichen Sicherheit des Kernkraftwerks eine ergänzende Rolle zu den Funktionen der Kategorie A spielen. Dazu gehören insbesondere die nach Erreichen des sicheren stabilen Zustands erforderlichen Funktionen, um unzulässige Folgen von Auslegungsereignissen (DBE) zu verhindern oder DBE-Folgen abzuschwächen. Wenn eine Funktion der Kategorie B wirksam ist, kann die Notwendigkeit entfallen, eine Funktion der Kategorie A anzuzeigen. Funktionen der Kategorie B können die Ausführung einer Funktion der Kategorie A hinsichtlich der Abschwächung von Konsequenzen eines DBE verbessern oder ergänzen, so dass Beschädigung von Gerät der Anlage oder Freisetzung von Radioaktivität vermieden oder minimiert wird.

Kategorie B enthält auch Funktionen, deren Versagen DBE auslösen oder das Ausmaß eines DBE erhöhen könnte. Wegen des Vorhandenseins von Funktionen der Kategorie A, die die ultimative Schwelle zur Verhinderung oder Abschwächung der Konsequenzen eines DBE darstellen, müssen die Sicherheitsanforderungen für Funktionen der Kategorie B jedoch nicht so hoch sein wie die für Funktionen der Kategorie A. Das erlaubt es, wenn erforderlich, Funktionen der Kategorie B mit einer höheren Funktionalität auszustatten als Funktionen der Kategorie A, etwa hinsichtlich der Methode, die Notwendigkeit des Ansprechens zu erkennen, oder in der Durchführung der automatischen Maßnahmen.

5.3.4 Kategorie C

In Kategorie C werden Funktionen eingestuft, die eine unterstützende oder indirekte Rolle bei der Erreichung und Erhaltung der erforderlichen Sicherheit des Kernkraftwerks spielen. Kategorie C umfasst Funktionen, die eine gewisse sicherheitstechnische Bedeutung haben, aber nicht in Kategorie A oder Kategorie B einzuordnen sind. Sie können Teil der Gesamtmaßnahmen bei Auftreten von DBA sein, sind aber nicht direkt an der Abschwächung der physikalischen Folgen des Störfalls beteiligt; oder es handelt sich um erforderliche Funktionen bei auslegungsüberschreitenden Störfällen.

⁴⁾ Um schnelle Transienten beherrschen zu können, wird die Anlage während dieser Phase durch automatische Maßnahmen gesteuert. Für langsamere Transienten kann der stabile sichere Zustand durch Handmaßnahmen erreicht werden, vorausgesetzt solche Maßnahmen werden erst nach einer bestimmten Zeitspanne in Betracht gezogen. Dieses Zeitkriterium stellt eine Auslegungsanforderung für die Anlage dar und berücksichtigt den Zeitaufwand für Diagnose und Maßnahmen auf der Grundlage von HF-Überlegungen. Es bedeutet also nicht, dass während dieser Zeitspanne keine Handmaßnahmen durchgeführt werden dürfen. In einigen Ländern und für ältere Anlagen kann die Grenze der Kategorie A durch dieses Zeitkriterium anstatt durch den stabilen sicheren Zustand bestimmt sein.

5.4 Zuordnungskriterien

Im Folgenden sind die Kriterien für die Einordnung von Funktionen in die Kategorien A, B und C beschrieben.

Wenn für eine Funktion keines der unten genannten Kriterien zutrifft, dann ist sie als „nicht kategorisiert“ (NK) einzustufen.

Im Fall von Mehrfachzuordnungen muss die endgültige Einordnung dieser Funktion in die höchste relevante Kategorie erfolgen.

Die endgültige Zuordnung der Funktion kann durch Anwendung probabilistischer Methoden in Übereinstimmung mit den in 6.2 ausgeführten Prinzipien erfolgen.

5.4.1 Kategorie A

Eine leittechnische Funktion muss in Kategorie A eingeordnet werden, wenn eines der folgenden Kriterien zutrifft:

- a) Funktionen, die zur Erreichung des sicheren stabilen Zustands benötigt werden, um zu verhindern, dass ein DBE zu unzulässigen Folgen führt, oder um die Folgen abzuschwächen;
- b) Funktionen, deren Versagen oder Fehlauslösung zu unzulässigen Folgen führen würde und für die keine andere Funktion der Kategorie A vorhanden ist, die unzulässige Folgen verhindert ^{N4)};
- c) Funktionen, die Informations- oder Steuerungsmöglichkeiten für spezifizierte Handmaßnahmen bereitstellen, die erforderlich sind, um den sicheren stabilen Zustand zu erreichen.

5.4.2 Kategorie B

Eine leittechnische Funktion muss in Kategorie B eingeordnet werden, wenn eines der folgenden Kriterien zutrifft und sie nicht schon aus anderen Gründen in Kategorie A eingeordnet ist:

- a) Funktionen, die bei einem DBE nach Erreichen des sicheren stabilen Zustands erforderlich sind, um zu verhindern, dass es zu unzulässigen Folgen kommt, oder um die Folgen abzuschwächen;
- b) Funktionen, die Informations- oder Steuerungsmöglichkeiten für spezifizierte Handmaßnahmen bereitstellen, die nach Erreichen des sicheren stabilen Zustands erforderlich sind, um zu verhindern, dass ein DBE zu unzulässigen Folgen führt, oder um die Folgen abzuschwächen;
- c) Funktionen, deren Versagen während des Normalbetriebs eine Funktion der Kategorie A erfordern würde, um einen Störfall zu verhindern, dessen Berücksichtigung in der Sicherheitsanalyse verlangt wird;
- d) Funktionen, durch die die Häufigkeit eines DBE verringert wird, so wie dies in der Sicherheitsanalyse angenommen ist;
- e) Steuerungsfunktionen für die verfahrenstechnischen Prozesse in der Anlage, durch die wichtige Prozessvariable innerhalb der in der Sicherheitsanalyse angenommenen Grenzen gehalten werden, wenn diese Steuerungsfunktionen das einzige Mittel zur Beeinflussung der genannten Prozessvariablen sind ^{N5)}. Sind weitere Mittel vorgesehen, kann Absatz 5.4.3 a) zutreffen.
- f) Funktionen, die zur Vermeidung oder Minderung einer radioaktiven Freisetzung oder einer Beschädigung der Brennelemente dienen, welche über die in der Sicherheitsanalyse definierten Grenzen und Bedingungen des Normalbetriebs hinausgeht.

ANMERKUNG Das bezieht sich auf Funktionen, die nicht bereits aufgrund der DBE-Analyse in Kategorie A eingeordnet wurden.

^{N4)} Nationale Fußnote: In Deutschland sind in diesem Fall Funktionen zu verwenden, die den Störfalleintritt verhindern.

^{N5)} Nationale Fußnote: In Deutschland werden hierunter Begrenzungsschaltungen verstanden.

- g) Funktionen, die eine kontinuierliche oder wiederkehrende Prüfung oder Überwachung von Kategorie A – Funktionen bereitstellen, um ihre ständige Verfügbarkeit anzuzeigen und das Wartpersonal bei Versagen zu informieren, wenn keine alternativen Mittel (z. B. wiederkehrende Prüfungen) vorgesehen sind, um ihre Verfügbarkeit festzustellen⁵⁾.

ANMERKUNG Wenn die Überwachungsfunktion das einzige Mittel darstellt, anderenfalls unentdeckt bleibende Ausfälle zu finden, dann stellt die Einordnung dieser Funktion in Kategorie B sicher, dass die für die Ausführung dieser Funktion verantwortlichen Geräte hinreichend qualifiziert sind.

5.4.3 Kategorie C

Eine leittechnische Funktion muss in Kategorie C eingeordnet werden, wenn eines der folgenden Kriterien zutrifft und sie nicht schon aus anderen Gründen in Kategorie A oder Kategorie B eingeordnet ist:

- a) Nicht durch Absatz 5.4.2 e) abgedeckte Steuerungsfunktionen für die verfahrenstechnischen Prozesse in der Anlage, durch die Prozessvariable innerhalb der in der Sicherheitsanalyse angenommenen Grenzen gehalten werden. Wenn eine Kombination von Funktionen der Kategorie C verwendet wird, muss gerechtfertigt werden, dass dies ausreicht^{N6)};
- b) Funktionen zur Verhinderung oder Abschwächung einer kleineren radioaktiven Freisetzung oder einer kleineren Beschädigung der Brennelemente, also Vorgängen, die im Rahmen der Auslegungsgrundlage liegen;

ANMERKUNG Eine kleinere Freisetzung oder eine kleinere Beschädigung der Brennelemente liegt vor, wenn sie innerhalb der normalen Grenzen und Bedingungen des Betriebs liegt (z. B. Grenzen beim Ablassen von Flüssigkeiten).

- c) Funktionen, die eine kontinuierliche oder periodische Prüfung oder Überwachung von Funktionen der Kategorie A und B bereitstellen oder diese Funktionen überwachen, um ihre ständige Verfügbarkeit anzuzeigen und das Wartpersonal bei Versagen zu informieren, und nicht nach 5.4.2 g) in Kategorie B eingeordnet sind;
- d) Funktionen, die zum Erreichen der probabilistischen Sicherheitsziele sowie zur Minderung der Häufigkeit von DBE erforderlich sind;
- e) Funktionen, die Anforderungen von Funktionen der Kategorie A verringern, entsprechend den Annahmen in der Sicherheitsanalyse;
- f) Funktionen, die nach anlageninternen Störfällen im Rahmen der Auslegungsgrundlage des KKW (z. B. Brand, Überflutung) die Überwachung und die erforderlichen Gegenmaßnahmen ermöglichen;
- g) Funktionen zur Warnung des Personals oder zur Sicherstellung der Sicherheit des Personals während oder nach Ereignissen, die mit der Freisetzung von Radioaktivität in der Anlage oder dem Risiko radioaktiver Belastung einhergehen;
- h) Funktionen, die nach natürlichen Ereignissen (z. B. Erdbeben, extremen Windverhältnissen) die Überwachung und die erforderlichen Gegenmaßnahmen ermöglichen;
- i) Funktionen für die Strategie des Störfall-Managements, um für auslegungsüberschreitende Störfälle einen sicheren Zustand erreichen und erhalten zu können;
- j) Funktionen zur Minimierung der Folgen schwerer Störfälle;
- k) Funktionen zur Zugangskontrolle für das Kernkraftwerk.

⁵⁾ IEC 60671 (Abschnitt 4.2.6) enthält weitere Anleitungen über die Geräteklasse zur Realisierung solcher Funktionen, insbesondere die Anmerkung „wenn Prüffunktionen sich in ungeeigneter Weise auf den Betrieb eines Systems oder Geräts, das eine sicherheitstechnisch wichtige Funktion ausführt, auswirken könnten, müssen sie in die selbe Kategorie eingeordnet werden“.

^{N6)} Nationale Fußnote: Gemeint ist eine Kombination von Funktionen der Kategorie C zur Erzielung einer Funktion der Kategorie B.