

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 2015-09-24

Vorgesehen als Ersatz für
 DIN EN 61226
 (VDE 0491-1):2010-08

Entwurf

**Kernkraftwerke –
 Leittechnische und elektrische Systeme mit sicherheitstechnischer
 Bedeutung –
 Kategorisierung von Funktionen und Klassifizierung von Systemen
 (IEC 45A/1018/CD:2015)**

Nuclear power plants –
 Instrumentation, control and electrical systems important to safety –
 Categorization of functions and classification of systems
 (IEC 45A/1018/CD:2015)

Centrales nucléaires de puissance –
 Systèmes d'instrumentation, de contrôle-commande et électriques importants pour la sûreté –
 Catégorisation des fonctions et classement des systèmes
 (CEI 45A/1018/CD:2015)

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2015-07-24 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfs besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal des DIN unter www.entwuerfe.din.de bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an dke@vde.com möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/stellungnahme oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an die DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE, Stresemannallee 15, 60596 Frankfurt am Main.

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 69 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE

Anwendungsbeginn

Anwendungsbeginn dieser Norm ist

Inhalt	Seite
Nationales Vorwort.....	3
Nationaler Anhang NA (informativ) Zusammenhang mit Europäischen und Internationalen Dokumenten	5
Nationaler Anhang NB (informativ) Literaturhinweise.....	7
Einleitung	8
1 Anwendungsbereich	11
2 Normative Verweisungen	11
3 Begriffe	12
4 Abkürzungen	16
5 Kategorisierungsschema	17
5.1 Allgemeines	17
5.2 Hintergrund	17
5.3 Beschreibung der Kategorien	18
5.4 Zuordnungskriterien	20
6 Vorgehensweise bei der Kategorisierung und Klassifizierung	22
6.1 Allgemeines	22
6.2 Ermittlung der Auslegungsergebnisse und Auslegungserweiterungs-Bedingungen	22
6.3 Festlegung und Kategorisierung der Funktionen	23
6.4 Klassifizierung der Systeme und Komponenten	24
7 Zuordnung der technischen Anforderungen zu Kategorien und Klassen	25
Anhang A (normativ) Zuordnung technischer Anforderungen zu Kategorien und Klassen.....	26
A.1 Anforderungen betreffend Funktionen.....	26
A.2 Anforderungen betreffend leittechnische Systeme	27
A.3 Anforderungen betreffend Gerät	29
A.4 Anforderungen betreffend Qualitätsgesichtspunkte	30
Anhang B (informativ) Beispiele zu Kategorien	34
B.1 Allgemeines	34
B.2 Kategorie A.....	34
B.3 Kategorie B.....	34
B.4 Kategorie C.....	35
Literaturhinweise.....	36
Bild 1 – Vorgehensweise bei der Kategorisierung der Funktionen.....	22
Tabelle 1 – Korrelation zwischen System-Klassen und Funktions-Kategorien	24
Tabelle 2 – Zusammenhang zwischen Kategorien und anderen IEC-Normen	33

Nationales Vorwort

Das internationale Dokument IEC 45A/1018/CD:2015 „Nuclear power plants – Instrumentation, control and electrical systems important to safety – Categorization of functions and classification of systems“ (CD, en: Committee Draft) 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 CD entsprechend der diesbezüglich durch die IEC erteilten Erlaubnis beigelegt. Die Nutzungsbedingungen für den deutschen Text des Norm-Entwurfes gelten gleichermaßen auch für den englischen IEC-Text.

Das internationale Dokument wurde vom SC 45A „Instrumentation, control and electrical systems of nuclear facilities“ der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet und den nationalen Komitees zur Stellungnahme vorgelegt.

Da der Abstimmungszeitraum für einen FDIS bzw. Schluss-Entwurf prEN 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 CD als DIN-Norm-Entwurf veröffentlicht, um die Stellungnahmen aus der Öffentlichkeit frühzeitig berücksichtigen zu können.

Für dieses Dokument ist das nationale Arbeitsgremium UK 967.1 „Elektro- und Leittechnik für kerntechnische Anlagen“ der DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE (www.dke.de) zuständig.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. ISO [und/oder] IEC sind nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

In der Reihe VDE 0491 sind als Normen erschienen:

- DIN EN 61226 (VDE 0491-1):2010-08, *Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Kategorisierung leittechnischer Funktionen (IEC 61226:2009); Deutsche Fassung EN 61226:2010*
- DIN EN 61513 (VDE 0491-2):2013-09, *Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Allgemeine Systemanforderungen (IEC 61513:2011); Deutsche Fassung EN 61513:2013*
- DIN EN 60987 (VDE 0491-3-1):2015-06, *Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Anforderungen an die Hardwareauslegung rechnerbasierter Systeme (IEC 60987:2007 + A1:2013); Deutsche Fassung EN 60987:2015*
- DIN EN 60880 (VDE 0491-3-2):2010-03, *Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Softwareaspekte für rechnerbasierte Systeme zur Realisierung von Funktionen der Kategorie A (IEC 60880:2006); Deutsche Fassung EN 60880:2009*
- DIN EN 62138 (VDE 0491-3-3):2010-03, *Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Softwareaspekte für rechnerbasierte Systeme zur Realisierung von Funktionen der Kategorien B oder C (IEC 62138:2004); Deutsche Fassung EN 62138:2009*
- DIN EN 61500 (VDE 0491-3-4):2011-12, *Kernkraftwerke – Leittechnik mit sicherheitstechnischer Bedeutung – Datenkommunikation (IEC 61500:2009); Deutsche Fassung EN 61500:2011*
- DIN EN 62566 (VDE 0491-3-5):2015-02, *Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Entwicklung HDL-programmierter integrierter Schaltkreise für Systeme, die Funktionen der Kategorie A ausführen (IEC 62566:2012); Deutsche Fassung EN 62566:2014*
- DIN IEC 62117 (VDE 0491-4):2001-10, *Kernkraftwerke – Druckwasserreaktoren – Überwachung ausreichender Kühlung des Kerns im abgeschalteten Zustand des Reaktors (IEC 62117:1999)*
- DIN EN 61839 (VDE 0491-5):2015-01, *Kernkraftwerke – Auslegung von Warten – Analyse und Zuordnung der Funktionen (IEC 61839:2000); Deutsche Fassung EN 61839:2014*
- DIN EN 60964 (VDE 0491-5-1):2010-08, *Kernkraftwerke – Warten – Auslegung (IEC 60964:2009); Deutsche Fassung EN 60964:2010*

E DIN IEC 61226 (VDE 0491-1):2015-08

- DIN EN 62241 (VDE 0491-5-2):2015-06, *Kernkraftwerke – Warte – Funktionen zur Meldung und Anzeige von Störungen (IEC 62241:2004); Deutsche Fassung EN 62241:2015*
- DIN IEC 61227 (VDE 0491-5-3):2009-01, *Kernkraftwerke – Warten – Handbedienungen (IEC 61227:2008)*
- DIN EN 61772 (VDE 0491-5-4):2013-09, *Kernkraftwerke – Warten – Anwendung von Sichtgeräten (IEC 61772:2009); Deutsche Fassung EN 61772:2013*
- DIN EN 60965 (VDE 0491-5-5):2011-12, *Kernkraftwerke – Warten – Notsteuerstellen für das Abfahren des Reaktors ohne Verbindung zur Hauptwarte (IEC 60965:2009); Deutsche Fassung EN 60965:2011*
- DIN IEC 60568 (VDE 0491-6):2006-11, *Kernkraftwerke – Instrumentierung mit sicherheitstechnischer Bedeutung – Kerninstrumentierung zur Messung der Neutronenflussdichte in Leistungsreaktoren (IEC 60568:2006)*
- DIN EN 60709 (VDE 0491-7):2010-12, *Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Physikalische und elektrische Trennung (IEC 60709:2004); Deutsche Fassung EN 60709:2010*
- DIN EN 62340 (VDE 0491-10):2010-12, *Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Anforderungen zur Beherrschung von Versagen aufgrund gemeinsamer Ursache (IEC 62340:2007); Deutsche Fassung EN 62340:2010*
- DIN EN 60671 (VDE 0491-100):2011-12, *Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Prüfungen zur Sicherstellung der Funktionsfähigkeit (IEC 60671:2007); Deutsche Fassung EN 60671:2011*

Als Norm-Entwürfe liegen vor:

- E DIN IEC 61226 (VDE 0491-1):2015-08, *Kernkraftwerke – Leittechnische und elektrische Systeme mit sicherheitstechnischer Bedeutung – Kategorisierung von Funktionen und Klassifizierung von Systemen (IEC 45A/1018/CD::2015)*
- E DIN IEC 62138 (VDE 0491-3-3):2015-01, *Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Softwareaspekte für rechnerbasierte Systeme zur Realisierung von Funktionen der Kategorien B oder C (IEC 45A/962/CD:2014)*
- E DIN IEC 62645 (VDE 0491-3-7):2013-04, *Kernkraftwerke – Leittechnische Systeme – Anforderungen an die IT-Sicherheitsplanung für rechnerbasierte Systeme (IEC 45A/890/CDV:2012)*
- E DIN IEC 60965 (VDE 0491-5-5):2014-11, *Kernkraftwerke – Warten – Notsteuerstellen für das Abfahren des Reaktors ohne Verbindung zur Hauptwarte (IEC 45A/952/CD:2014)*
- E DIN IEC 62646 (VDE 0491-5-6):2011-09, *Kernkraftwerke – Warten – Rechnerunterstützte Prozeduren (IEC 45A/839/CDV:2011)*
- E DIN IEC 61225 (VDE 0491-8):2012-06, *Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Anforderungen an die elektrische Energieversorgung (IEC 61225:2005)*
- E DIN IEC 62855 (VDE 0491-8-1):2014-11, *Kernkraftwerke – Elektrische Systeme – Analyse der Stromversorgung (IEC 45A/964/CD:2014)*
- E DIN IEC 60772 (VDE 0491-9-1):2014-11, *Kernkraftwerke – Sicherheitswichtige Instrumentierung – Elektrische Durchführungen für Sicherheitsbehälter (IEC 45A/966/CD:2014)*
- E DIN IEC 60744 (VDE 0491-9-2):2014-11, *Kernkraftwerke – Leittechnik mit sicherheitstechnischer Bedeutung – Sicherheitslogikanordnungen: Merkmale und Testverfahren (IEC 45A/946/CD:2014)*
- E DIN IEC 62705 (VDE 0491-15):2015-02, *Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Strahlungsüberwachungssysteme: Eigenschaften und Lebenszyklus (IEC 62705:2014)*
- E DIN IEC 62342 (VDE 0491-20-1):2012-02, *Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Alterungsmanagement (IEC 62342:2007)*
- E DIN IEC/IEEE 62582-1 (VDE 0491-21-1):2015-06, *Kernkraftwerke – Leittechnik mit sicherheitstechnischer Bedeutung – Zustandsüberwachung elektrischer Geräte – Teil 1: Allgemeines (IEC/IEEE 62582-1:2011)*
- E DIN IEC/IEEE 62582-2 (VDE 0491-21-2):2015-08, *Kernkraftwerke – Leittechnik mit sicherheitstechnischer Bedeutung – Zustandsüberwachung elektrischer Geräte – Teil 2: Eindringprüfung (IEC/IEEE 62582-2:2011)*

- E DIN IEC/IEEE 62582-3 (VDE 0491-21-3):2015-07, *Kernkraftwerke – Leittechnik mit sicherheitstechnischer Bedeutung – Zustandsüberwachung elektrischer Geräte – Teil 3: Reißdehnung* (IEC/IEEE 62582-3:2012)
- E DIN IEC 62765-1 (VDE 0491-22-1):2015-06, *Kernkraftwerke – Leittechnik mit sicherheitstechnischer Bedeutung – Alterungsmanagement von Sensoren und Transmittern – Teil 1: Drucktransmitter* (IEC 45A/1001/FDIS:2015)
- E DIN IEC 60780-323 (VDE 0491-80):2014-03, *Kerntechnische Anlagen – Elektrisches Gerät mit sicherheitstechnischer Bedeutung – Qualifizierung* (IEC 45A/940/CD:2013)

Änderungen

Gegenüber DIN EN 61226 (VDE 0491-1):2010-08 wurden folgende Änderungen vorgenommen:

- Ergänzung der Kategorisierung leittechnischer Funktionen um die Klassifizierung der diese realisierenden Geräte und Systeme;
- Ausdehnung der Kategorisierung und Klassifizierung auf alle elektrischen Geräte und Systeme der Anlage;
- Anpassung an neuere Anforderungen und Empfehlungen der IAEA (insbesondere Ersatz des IAEA NS-R-1 durch IAEA SSR 2/1 und die Veröffentlichung der IAEA SSG 30);
- redaktionelle Überarbeitung der Texte.

Nationaler Anhang NA (informativ)

Zusammenhang mit Europäischen und Internationalen Dokumenten

Für den Fall einer undatierten Verweisung im normativen Text (Verweisung auf ein Dokument ohne Angabe des Ausgabedatums und ohne Hinweis auf eine Abschnittsnummer, eine Tabelle, ein Bild usw.) bezieht sich die Verweisung auf die jeweils aktuellste Ausgabe des in Bezug genommenen Dokuments.

Für den Fall einer datierten Verweisung im normativen Text bezieht sich die Verweisung immer auf die in Bezug genommene Ausgabe des Dokuments.

Eine Information über den Zusammenhang der zitierten Dokumente mit den entsprechenden Deutschen Dokumenten ist nachstehend wiedergegeben.

Tabelle NA.1 (1 von 2)

Europäisches Dokument	Internationales Dokument	Deutsches Dokument	Klassifikation im VDE-Vorschriftenwerk
EN 60671:2011	IEC 60671:2007	DIN EN 60671 (VDE 0491-100):2011-12	VDE 0491-100
EN 60709:2010	IEC 60709:2004	DIN EN 60709 (VDE 0491-7):2010-12	VDE 0491-7
–	IEC 60780:1998 z.Z. in Überarbeitung, siehe 45A/991/CDV ^a	DIN IEC 60780:2000-12	–

Tabelle NA.1 (2 von 2)

Europäisches Dokument	Internationales Dokument	Deutsches Dokument	Klassifikation im VDE-Vorschriftenwerk
–	IEC 60812	–	–
EN 60880:2009	IEC 60880:2006	DIN EN 60880 (VDE 0491-3-2):2010-03	VDE 0491-3-2
EN 60964:2010	IEC 60964:2009	DIN EN 60964 (VDE 0491-5-1):2010-08	VDE 0491-5-1
EN 60965:2011	IEC 60965:2009	DIN EN 60965 (VDE 0491-5-5):2011-12	VDE 0491-5-5
–	IEC 60980	–	–
EN 60987:2015	IEC 60987:2007 + A1:2013	DIN EN 60987 (VDE 0491-3-1):2015-06	VDE 0491-3-1
EN 61000-4 (alle Teile)	IEC 61000-4 (alle Teile)	DIN EN 61000-4 (VDE 0847-4) (alle Teile)	VDE 0847-4
EN 61000-6-2:2005	IEC 61000-6-2:2005	DIN EN 61000-6-2 (VDE 0839-6-2):2006-03	VDE 0839-6-2
EN 61508-1	IEC 61508-1	DIN EN 61508-1 (VDE 0803-1)	VDE 0803-1
EN 61508-2	IEC 61508-2	DIN EN 61508-2 (VDE 0803-2)	VDE 0803-2
EN 61508-3	IEC 61508-3	DIN EN 61508-3 (VDE 0803-3)	VDE 0803-3
EN 61508-4	IEC 61508-4	DIN EN 61508-4 (VDE 0803-4)	VDE 0803-4
EN 61513:2013	IEC 61513:2011	DIN EN 61513 (VDE 0491-2):2013-09	VDE 0491-2
–	IEC 61771	–	–
EN 61772:2013	IEC 61772:2009	DIN EN 61772 (VDE 0491-5-4):2013-09	VDE 0491-5-4
EN 61839:2014	IEC 61839:2000	DIN EN 61839 (VDE 0491-5):2015-01	VDE 0491-5
EN 62138:2009	IEC 62138:2004	DIN EN 62138 (VDE 0491-3-3):2010-03	VDE 0491-3-3
–	IAEA SSR-2/1:2011	–	–
–	IAEA GS-R-3:2006	–	–
–	IAEA SSG-30:2014	–	–
–	IAEA SSG 39	–	–
–	IAEA DS 462	–	–
^a Zu beziehen über DKE-Schriftstückservice, Stresemannallee 15, 60596 Frankfurt am Main.			

Nationaler Anhang NB (informativ)

Literaturhinweise

DIN EN 60671 (VDE 0491-100):2011-12, *Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Prüfungen zur Sicherstellung der Funktionsfähigkeit (IEC 60671:2007); Deutsche Fassung EN 60671:2011*

DIN EN 60709 (VDE 0491-7):2010-12, *Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Physikalische und elektrische Trennung (IEC 60709:2004); Deutsche Fassung EN 60709:2010*

DIN EN 60880 (VDE 0491-3-2):2010-03, *Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Softwareaspekte für rechnerbasierte Systeme zur Realisierung von Funktionen der Kategorie A (IEC 60880:2006); Deutsche Fassung EN 60880:2009*

DIN EN 60964 (VDE 0491-5-1):2010-08, *Kernkraftwerke – Warten – Auslegung (IEC 60964:2009); Deutsche Fassung EN 60964:2010*

DIN EN 60965 (VDE 0491-5-5):2011-12, *Kernkraftwerke – Warten – Notsteuerstellen für das Abfahren des Reaktors ohne Verbindung zur Hauptwarte (IEC 60965:2009); Deutsche Fassung EN 60965:2011*

DIN EN 60987 (VDE 0491-3-1):2015-06, *Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Anforderungen an die Hardwareauslegung rechnerbasierter Systeme (IEC 60987:2007 + A1:2013); Deutsche Fassung EN 60987:2015*

DIN EN 61000-4 (VDE 0847-4) (Reihe); *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), *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 1: Allgemeine Anforderungen*

DIN EN 61508-2 (VDE 0803-2), *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 2: Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme*

DIN EN 61508-3 (VDE 0803-3), *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 3: Anforderungen an Software*

DIN EN 61508-4 (VDE 0803-4), *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 4: Begriffe und Abkürzungen*

DIN EN 61513 (VDE 0491-2):2013-09, *Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Allgemeine Systemanforderungen (IEC 61513:2011); Deutsche Fassung EN 61513:2013*

DIN EN 61772 (VDE 0491-5-4):2013-09, *Kernkraftwerke – Warten – Anwendung von Sichtgeräten (IEC 61772:2009); Deutsche Fassung EN 61772:2013*

DIN EN 61839 (VDE 0491-5):2015-01, *Kernkraftwerke – Auslegung von Warten – Analyse und Zuordnung der Funktionen (IEC 61839:2000); Deutsche Fassung EN 61839:2014*

DIN EN 62138 (VDE 0491-3-3):2010-03, *Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Softwareaspekte für rechnerbasierte Systeme zur Realisierung von Funktionen der Kategorien B oder C (IEC 62138:2004); Deutsche Fassung EN 62138:2009*

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

Kernkraftwerke – Leittechnische und elektrische Systeme mit sicherheitstechnischer Bedeutung – Kategorisierung von Funktionen und Klassifizierung von Systemen

Einleitung

a) Technischer Hintergrund, hauptsächliche Inhalte und Organisation der Norm

Mit dieser Internationalen Norm wird eine Forderung der IAEA umgesetzt¹⁾, sicherheitstechnisch wichtige Einheiten von Kernkraftwerken festzustellen und basierend auf ihrer Funktion und 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 beabsichtigt,

- die mit sicherheitstechnisch wichtigen leittechnischen und elektrischen Systemen realisierten Funktionen zu ermitteln und 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;
- die leittechnischen und elektrischen Systeme und Geräte, die diese Funktionen ausführen, entsprechend zu klassifizieren und ihnen Spezifikationen und Auslegungs-Anforderungen zuzuordnen.

Nach Empfehlung der IAEA²⁾ 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/TR 61838 beschrieben.

b) 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.

Näheres zur Struktur der Normen des IEC/SC 45A ist in d) dieser Einleitung zu finden.

c) 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 durch leittechnische und elektrische Systeme eines Kernkraftwerks ausgeführten Funktionen einer der drei Kategorien A, B oder 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.

¹⁾ IAEA SSR-2/1, Anforderung 22, unter Berücksichtigung auch der Anforderungen 4, 18 und 27.

²⁾ In SSR-2/1, 5.34, wird gefordert, dass die Vorgehensweise zur Klassifizierung der sicherheitstechnischen Bedeutung einer Einheit grundsätzlich auf deterministischen Methoden beruhen muss, wo angemessen ergänzt durch probabilistische Methoden, wobei Faktoren zu berücksichtigen sind wie

- a) die von der Einheit auszuführenden Sicherheitsfunktionen;
- b) die Folgen des Versagens einer Sicherheitsfunktion;
- c) die Häufigkeit, mit der die Einheit zur Ausführung einer Sicherheitsfunktion angefordert wird;
- d) die Zeit nach einem AVE oder die Zeitspanne, für welche die Einheit zur Durchführung einer Sicherheitsfunktion angefordert 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.

- i) Die Sicherstellung der Funktionalität wird durch Erstellung einer vollständigen und umfassenden Anforderungsspezifikation sowie der Anwendung geeigneter Normen und Regeln erreicht.
- ii) 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, galvanischer Trennung sowie wiederkehrenden Prüfungen während des Betriebs erreicht.
- iii) Die Sicherstellung der Leistungsfähigkeit wird durch Erstellen von Spezifikationen unter Angabe der erforderlichen Leistungsfähigkeit, der Anwendung von Vorgehensweisen zur Qualitätssicherung, 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.
- iv) 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.
- v) 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“ bzw. „kann“ bezeichnet optionale Anforderungen.

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

Das Eingangsdokument der 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 GS-R-3 ab.

In den Normen des IEC/SC 45A werden die Prinzipien und grundsätzlichen Sicherheitsaspekte des „IAEA code safety fundamentals“ und der „IAEA safety series“ konsistent realisiert, insbesondere die Sicherheitsanforderungen von SSR-2/1 über die Auslegung von Kernkraftwerken und die Sicherheitsrichtlinien SSG-30 über Klassifizierung, SSG-34 über sicherheitstechnisch wichtige Leittechnik in Kernkraftwerken und SSG-39 über elektrische Systeme. 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 für Kernkraftwerke fest, das die Einteilung der Anlagenfunktionen in Kategorien erlaubt, welche die sicherheitstechnische Bedeutung der Funktionen definieren. Es gilt speziell für jene Anlagenfunktionen, die auf leittechnischen oder elektrischen Systemen und Geräten aufbauen. Die anschließende Klassifizierung von Systemen und Geräten basiert auf der jeweils zugeordneten Kategorie und bestimmt dann die zutreffenden Auslegungskriterien.

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

Diese Norm gilt für alle Anlagenfunktionen und leittechnischen und elektrischen Systeme und Geräte, die eine Realisierung dieser Funktionen ermöglichen. 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 den Sicherheitsanforderungen IAEA SSR-2/1 und den Sicherheitsrichtlinien SSG-30, SSG-34 und SSG-39, und beinhaltet ein strukturiertes Verfahren zur Anwendung der in diesen Codes enthaltenen Anleitungen auf leittechnische und elektrische 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 Dokumente, die in diesem Dokument teilweise oder als Ganzes zitiert werden, 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 60671:2007, *Nuclear power plants – Instrumentation and control systems important to safety – Surveillance testing*

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, *Nuclear power plants – Control rooms – Design*

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, *Nuclear power plants – Instrumentation and control important to safety – Hardware design requirements for computer-based systems*

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

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

IEC 61513, *Nuclear power plants – 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 SSR-2/1:2011, *Safety of Nuclear Power Plants: Design*

IAEA GS-R-3:2006, *The management system for facilities and activities (Under revision DS 484)*

IAEA SSG-30:2014, *Safety classification of structures, systems and components in nuclear power plants*

IAEA SSG 39, *Design of Instrumentation and Control Systems for Nuclear Power Plants (Under Revision DS 431, step 14 established as an IAEA Safety Standard by the Publications Committee)*

IAEA DS 462 (draft step 14) addendum to SSR 2/1, GSR part 1, GSR part 4, and NSR-3

3 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

3.1

anzunehmendes betriebliches Vorkommnis

(en: anticipated operational occurrence)

betrieblicher Vorgang, der vom Normalbetrieb abweicht und erfahrungsgemäß wenigstens einmal während der Lebenszeit der Anlage auftritt, und der wegen entsprechender Auslegungsmaßnahmen weder signifikante Auswirkungen auf sicherheitstechnisch wichtige Einheiten hat noch zu Störfallbedingungen führt

[IAEA Safety Glossary 2007]

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

[IAEA Safety Glossary 2007]

3.3

Auslegungsstörfall

(en: design basis accident)

Störfallbedingungen, für die eine Anlage gemäß anerkannter Auslegungskriterien und konservativer Methodik konstruiert ist und bei denen die Abgabe radioaktiver Stoffe innerhalb genehmigter Grenzen liegt

[IAEA SSR-2/1]

3.4

Auslegungsereignis

(en: design basis event)

Sammelbegriff zur Bezeichnung der Auslegungsstörfälle und der anzunehmenden betrieblichen Vorkommnisse

Anmerkung zum Begriff: Siehe auch 3.13.

3.5

Auslegungserweiterungs-Bedingungen

(en: design extension conditions)

Angenommene Störfallbedingungen, die für Auslegungsstörfälle nicht berücksichtigt werden, jedoch im Auslegungsprozess der Anlage nach der Best-Estimate-Methode in Betracht gezogen werden, und für die sich Freisetzen von radioaktiven Stoffen innerhalb akzeptabler Grenzen halten. Auslegungserweiterungs-Bedingungen können Bedingungen von Ereignissen ohne signifikanten Brennstoffschaden und Bedingungen mit Kernschmelzen umfassen.

[IAEA SSR-2/1 und Addendum DS 462]

3.6

Diversität

(en: diversity)

Vorhandensein von zwei oder mehreren redundanten Systemen oder Komponenten zur Ausführung einer bestimmten Funktionen, wobei die verschiedenen Systeme oder Komponenten unterschiedliche Eigenschaften aufweisen, und zwar derart, dass die Möglichkeit von Versagen aufgrund gemeinsamer Ursache verringert wird, einschließlich „common mode“-Versagen^{N1)}

[IAEA Safety Glossary 2007]

Anmerkung zum Begriff: Nach IEC 60880, 3.14, ist Diversität folgend definiert: *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.* Die beiden Definitionen sind konsistent.

3.7

Gerät

Einrichtung

(en: equipment)

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

[IEC 61513, 3.17, modifiziert]

3.8

Funktion

(en: function)

dient einem bestimmten zu erreichenden Zweck oder Ziel, der/das ohne Hinweis auf die dafür erforderlichen physikalischen Mittel spezifiziert oder beschrieben werden kann

3.9

Funktionalität

(en: functionality)

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

[IEC 61513, 3.25]

3.10

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

^{N1)} Nationale Fußnote: In Deutschland wird ein Versagen gemeinsamer Art (common mode failure) nicht separat betrachtet; diese Versagensart ist im Versagen gemeinsamer Ursache (CCF) integriert.

3.11

sicherheitstechnisch wichtige Gegebenheit/Maßnahme

(en: item important to safety)

Gegebenheit/Maßnahme, die Teil einer Sicherheitsgruppe ist und/oder deren Fehlfunktion oder Versagen zur Strahlenbelastung des Anlagenpersonals oder der Öffentlichkeit führen könnte.

Sicherheitstechnisch wichtige Gegebenheiten/Maßnahmen umfassen:

- a) Strukturen, Systeme und Komponenten, deren Fehlfunktion oder Versagen zu unzulässiger Strahlenbelastung des Anlagenpersonals oder der Öffentlichkeit führen könnte;
- b) Strukturen, Systeme und Komponenten, die verhindern, dass anzunehmende betriebliche Vorkommnisse zu Störfallbedingungen führen;
- c) Merkmale, die dazu dienen, die Folgen von Fehlfunktion oder Versagen der Strukturen, Systeme oder Komponenten abzuschwächen

[IAEA Safety Glossary 2007]

Anmerkung zum Begriff: Die Betrachtungen in dieser Norm beziehen sich hauptsächlich auf sicherheitstechnisch wichtige leittechnische und elektrische Systeme und Geräte.

3.12

kontrollierter Zustand

(en: controlled state)

Anlagenzustand nach einem angenommenen betrieblichen Vorkommnis oder einem Auslegungsstörfall, in dem die fundamentalen Sicherheitsfunktionen sichergestellt werden können und der für eine genügend lange Zeit beibehalten werden kann, um einen sicheren Zustand zu erreichen

[IAEA SSR-2/1]

3.13

Leistungsfähigkeit

(en: performance)

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

3.14

Anlagenzustände^{N2)}

(en: plant states)

Betriebszustände		Störfallbedingungen		
Normalbetrieb	Auslegungsereignisse			Auslegungserweiterungs-Bedingungen
	Anzunehmende betriebliche Vorkommnisse		Auslegungsstörfälle	a) Mit Kernschmelzen

a) Ohne signifikanten Brennstoffschaden.

Anmerkung zum Begriff: Diese Definition ist mit der in IAEA SSR-2/1 und dem Addendum DS 462 konsistent; sie zeigt lediglich die Stellung des „Konzepts der Auslegungsstörfälle“ im Vergleich zu anderen Konzepten.

^{N2)} Nationale Fußnote: Diese Graphik zeigt einen Überblick und die Zusammenhänge der im Normtext genannten Anlagenzustände.

3.15

anzunehmendes Versagen auslösendes Ereignis

(en: postulated initiating events)

im Zuge der Auslegung ermitteltes Ereignis, das zu den anzunehmenden betrieblichen Vorkommnissen oder Störfallbedingungen führen kann^{N3)}

[IAEA Safety Glossary 2007]

3.16

Redundanz

(en: redundancy)

Einsatz mehrerer (identischer oder unterschiedlicher) Strukturen, Systeme oder Komponenten, so dass jede Einheit (Struktur, System oder Komponente) unabhängig vom Betriebszustand oder Versagen irgend einer anderen Einheit die geforderte Funktion ausführen kann.

[IAEA Safety Glossary 2007]

3.17

sicherer Zustand

(en: safe state)

Anlagenzustand nach einem anzunehmenden betrieblichen Vorkommnis oder einer Störfallbedingung, in welcher der Reaktor unterkritisch ist und die fundamentalen Sicherheitsfunktionen für eine lange Zeit sichergestellt und beibehalten werden können

[IAEA SSR-2/1]

3.18

Sicherheitsmerkmal für Auslegungserweiterungs-Bedingungen

(en: safety feature for design extension conditions))

Auslegungs-Gegebenheit/Maßnahme, die unter Auslegungserweiterungs-Bedingungen eine Sicherheitsfunktion aufweist oder für die Durchführung einer Sicherheitsfunktion konzipiert wird

[IAEA SSR-2/1]

3.19

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 anzunehmende betriebliche Vorkommnisse und Auslegungsstörfälle festgelegten Grenzwerte nicht überschritten werden.

[IAEA Safety Glossary 2007]

3.20

sicherheitsrelevantes leittechnisches System

(en: safety related I&C system)

sicherheitstechnisch wichtiges leittechnisches System, das nicht Teil eines Sicherheitssystems ist

[IAEA Safety Glossary 2007]

3.21

Sicherheitssystem

(en: safety system)

sicherheitstechnisch wichtiges System, das dazu dient, die sichere Abschaltung des Reaktors und die Wärmeabfuhr aus dem Reaktorkern sicherzustellen, oder die Konsequenzen von anzunehmenden betrieblichen Vorkommnissen und Auslegungsstörfällen zu begrenzen

[IAEA Safety Glossary 2007]

^{N3)} Nationale Fußnote: Siehe auch 3.14.

3.22

Einzelausfall

Einzelversagen^{N4)}

(en: single failure)

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

[IAEA Safety Glossary 2007]

3.23

System

(en: system)

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

[IEC 61513]

3.24

Typprüfung

(en: type testing)

Konformitätsprüfung, die an einem oder mehreren für die Produktion repräsentativen Stücken durchgeführt wird^{N5)}

[IEV 394-40-02]

4 Abkürzungen

Deutsch	Englisch
ALARA so gering wie möglich	ALARA as low as reasonably achievable
DBA Auslegungsstörfall	DBA design basis accident
DBE Auslegungsereignis	DBE design basis event
DEC Auslegungserweiterungs-Bedingung	DEC design extension condition
DEC-A Auslegungserweiterungs-Bedingung ohne signifikanten Brennelements Schaden	DEC-A design extension condition without significant fuel degradation
WAP Werksabnahmeprüfung	FAT factory acceptance test
FMEA Fehlermöglichkeits- und -einflussanalyse	FMEA failure modes and effects analysis
MMK Mensch-Maschine-Kommunikation	HMI human machine interface
IAEA Internationale Atomenergie-Behörde	IAEA International Atomic Energy Agency
LT Leittechnik	I&C instrumentation and control
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
— —	SSC structures, systems and components

^{N4)} Nationale Fußnote: Wenn Hardware oder Teilsysteme (z. B. ein Strang eines redundanten Systems) betroffen sind, wird „failure“ mit „Ausfall“ übersetzt.

^{N5)} Nationale Fußnote: Bei Typprüfungen nach KTA 3503 und KTA 3505 sind mindestens drei repräsentative Stücke vorgesehen.

5 Kategorisierungsschema

5.1 Allgemeines

Durch leittechnische Systeme ausgeführte oder unterstützte 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 Fehlauslösung ohne Anforderung während normalen Anlagenbetrieb in Betracht zu ziehen. Die Kategorie bestimmt die Auslegungs- und Qualitätsanforderungen für leittechnische und elektrische 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. Diese beruhen auf den ursprünglich in der 1. Ausgabe der IEC 61226 (1993) festgelegten Kategorien und stimmen mit den in IAEA SSG-30 definierten Kategorien überein.

5.4 enthält die Zuordnungskriterien für die jeweiligen Kategorien.

Abschnitt 6 gibt eine Anleitung für den Kategorisierungsvorgang bis hin zur Festlegung der korrespondierenden Kategorien und Klassen.

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^{N6)}.

Anhang B 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 (en: defence-in-depth, DiD) ist in der Auslegungsgrundlage von Kernkraftwerken fest verankert^{N7)}. 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. Die auf den verschiedenen Maßnahmenstufen ausgeführten Funktionen werden berücksichtigt.

In IAEA Sicherheitsstandard SSR-2/1 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.

Die IAEA Sicherheitsrichtlinie SSG-30 gibt Anleitung zur Kategorisierung von Funktionen und zur Klassifizierung von SSC entsprechend ihrer sicherheitstechnischen Bedeutung. Hinsichtlich der sicherheitstechnischen Bedeutung einer als Maßnahme gegen AVE ausgelegten Funktion muss folgendes berücksichtigt werden:

- die Folgen des Ausfalls der Funktion;
- die Eintrittshäufigkeit des AVE, bei dem die Funktion angefordert wird;

^{N6)} Nationale Fußnote: Für den zweiten Satz wurde in der Übersetzung die Formulierung der bestehenden Norm belassen, da die im IEC-Entwurf vorgeschlagene neue Formulierung eher verwirrend wirkt. Ein entsprechender deutscher Kommentar zum IEC-Entwurf wurde abgegeben.

^{N7)} Nationale Fußnote: Siehe DIN IEC 61513 (VDE 0491-2):2002-10, Abschnitt A.3.

- die Bedeutung des Beitrags der Funktion zum Erreichen entweder eines kontrollierten Zustands oder eines sicheren Zustands.

In SSG-30 werden auch die zu kategorisierenden Funktionen identifiziert, einschließlich jener, die zu den verschiedenen Maßnahmenstufen der DiD-Auslegung gehören. Basierend auf der Schwere der Folgen, die bei Nichtausführung der Funktion entstehen könnten, werden drei Ebenen definiert:

- „Hohe Schwere der Folgen“, wenn das Versagen der Funktion schlimmstenfalls zu einer Freisetzung von radioaktiven Stoffen führen könnte, durch die von der Genehmigungsbehörde für Auslegungsstörfälle akzeptierten Grenzen überschritten werden; oder das Versagen verursacht, dass die Werte physikalischer Schlüsselparameter die Akzeptanzkriterien für Auslegungsstörfälle überschreiten.
- „Mittlere Schwere der Folgen“, wenn das Versagen der Funktion schlimmstenfalls zu einer Freisetzung von radioaktiven Stoffen führen könnte, wodurch die festgelegten Grenzen für anzunehmende betriebliche Vorkommnisse überschritten werden; oder verursacht, dass die Werte physikalischer Schlüsselparameter die Auslegungsgrenzen für anzunehmende betriebliche Vorkommnisse überschreiten.
- „Niedrige Schwere der Folgen“, wenn das Versagen der Funktion schlimmstenfalls zu einer Strahlungsdosis des Personals oberhalb der autorisierten Grenzen führen könnte.

In dieser Norm wird die Klassifizierungsstrategie von IAEA SSG-30 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.

IAEA SSG 39, Abschnitt 5 bezüglich Klassifizierung von leittechnischen Funktionen und IAEA SSG 34, Abschnitt 3 bezüglich Klassifizierung von elektrischen Leistungssystemen beziehen sich direkt auf SSR 2/1 und SSG-30 und stimmen mit den Prinzipien dieser Norm überein.

Die jeweilige sicherheitstechnische Bedeutung und die damit verbundenen Anforderungen an Teile der sicherheitstechnisch wichtigen Leittechnik und elektrischen Systeme unterscheiden sich, so dass es angemessen ist, sie verschiedenen Sicherheitsklassen zuzuweisen. Einige leittechnische und elektrische Systeme können wesentliche Auswirkungen auf die Sicherheit haben und bedürfen daher angemessener Aufmerksamkeit. Andere 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 muss eine angemessene Entsprechung zu den in dieser Norm definierten Kategorien erreicht und dokumentiert werden.

5.3 Beschreibung der Kategorien

5.3.1 Allgemeines

Leittechnische und elektrische Systeme in Kernkraftwerken führen Funktionen unterschiedlicher Bedeutung für die Sicherheit aus. Die sicherheitstechnische Bedeutung jeder 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 Häufigkeit dieser Folgen. Sie hängt auch ab von den Folgen einer fälschlichen Auslösung bei Normalbetrieb. Daher wird vor Kategorisierung der Funktionen der Abschluss einer ersten Sicherheitsanalyse der jeweiligen Auslegung des Kernkraftwerks gefordert. Die sicherheitstechnische Bedeutung einer 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 Kategorien A, B und C definiert, mit den zugehörigen technischen und qualitativen Anforderungen, die für Auslegung und Realisierung der sicherheitstechnisch wichtigen leittechnischen und elektrischen 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 einer hohen Schwere der 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 kontrollierten Zustands eine grundsätzliche Rolle³⁾. Wenn spezifizierte Handmaßnahmen vorgesehen sind, um den kontrollierten 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 hoher Schwere der 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 kontrollierten Zustands erforderlichen Funktionen, um Auslegungsereignisse (DBE) mit mittlerer Schwere der Folgen zu verhindern. Wenn eine Funktion der Kategorie B wirksam ist, kann die Notwendigkeit entfallen, eine Funktion der Kategorie A anzuregen. Funktionen der Kategorie B können die Ausführung einer Funktion der Kategorie A verbessern oder eine Backup-Funktion bilden, indem die Folgen einer DEC ohne Kernschmelzen abgeschwächt werden, so dass Beschädigung von Anlage oder Gerät oder Freisetzung von Radioaktivität vermieden oder minimiert wird.

Kategorie B enthält auch Funktionen, deren Versagen Auslegungsereignisse auslösen oder die Schwere der Folgen eines Auslegungsereignisses erhöhen könnte. Wegen des Vorhandenseins von Funktionen der Kategorie A, die die ultimative Schwelle zur Verhinderung oder Abschwächung der Konsequenzen eines Auslegungsereignisses 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 Eingreifens zu erkennen, oder in der Durchführung nachfolgender 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 Auslegungsstörfällen sein, sind aber nicht direkt an der Vermeidung einer hohen Schwere der Folgen eines Störfalls beteiligt; oder es handelt sich um erforderliche Funktionen bei DEC oder Gefährdungen.

³⁾ 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

5.4.1 Allgemeines

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 6.3 ausgeführten Prinzipien erfolgen.

5.4.2 Kategorie A

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

- a) Funktionen, die zur Erreichung des kontrollierten Zustands benötigt werden, um zu verhindern, dass ein Auslegungsereignis zu einer hohen Schwere der Folgen führt;
- b) Funktionen, deren Versagen oder Fehlauslösung zu einer hohen Schwere der Folgen führen würde und für die keine andere Funktion der Kategorie A vorhanden ist, welche die hohe Schwere der Folgen verhindert^{N8)};
- c) Funktionen, die Informations- oder Steuerungsmöglichkeiten für spezifizierte Handmaßnahmen bereitstellen, die zum Erreichen des kontrollierten Zustands erforderlich sind, um eine hohe Schwere der Folgen zu verhindern.

5.4.3 Kategorie B

Eine 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 Auslegungsereignis nach Erreichen des kontrollierten Zustands erforderlich sind, um zu verhindern, dass es zu einer hohen Schwere der Folge kommt;
- b) Funktionen, die Informations- oder Steuerungsmöglichkeiten für spezifizierte Handmaßnahmen bereitstellen, die nach Erreichen des kontrollierten Zustands erforderlich sind, um ein Auslegungsereignis mit hoher Schwere der Folgen zu verhindern;
- c) Funktionen, die als Backup für eine Funktion der Kategorie A ausgelegt sind, um eine DCE-A mit hoher Schwere der Folgen zu verhindern;
- d) Funktionen, deren Versagen oder Fehlauslösung bei Normalbetrieb zu einer mittleren Schwere der Folgen führen würde und für die keine andere Funktion der Kategorie A oder B vorhanden ist, welche die mittlere Schwere der Folgen verhindert;
- e) Funktionen zur deutlichen Reduktion der Häufigkeit von Auslegungsereignissen, entsprechend den Ausführungen in der Sicherheitsanalyse (*in Deutschland Begrenzungsschaltungen genannt*);
- f) Funktionen, die zum Erreichen des kontrollierten Zustands erforderlich sind, um ein Auslegungsereignis mit mittlerer Schwere der Folgen zu verhindern;
- 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 festzustellen⁴⁾.

^{N8)} Nationale Fußnote: In Deutschland sind in diesem Fall Funktionen zu verwenden, die den Störfalleintritt verhindern.

⁴⁾ IEC 60671, 4.2.6 enthält weitere Anleitungen über die Geräteklasse zur Realisierung solcher Funktionen; insbesondere wird dort angemerkt: „Wenn Prüffunktionen sich in ungeeigneter Weise auf den Betrieb eines Systems oder Geräts,

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

5.4.4 Kategorie C

Eine 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) Steuerungsfunktionen für die verfahrenstechnischen Prozesse in der Anlage, durch die wichtige Prozessvariable innerhalb der in der Sicherheitsanalyse angenommenen Grenzen gehalten werden.
- b) Bei einem Auslegungsereignis aktivierte Funktionen, deren Ausfall in einer niedrigen Schwere der Folgen resultieren würde.
- c) Funktionen, die zum Erreichen und für lange Zeit zum Erhalten eines sicheren Zustands erforderlich sind, und deren Ausfall bei Anforderung in einer mittleren Schwere der Folgen resultieren würde.
- d) Funktionen, die eine kontinuierliche oder periodische Prüfung oder Überwachung von Funktionen der Kategorien A und B bereitstellen oder diese Funktionen überwachen, um ihre ständige Verfügbarkeit anzuzeigen und bei Versagen das Wartepersonal zu informieren, und nicht nach 5.4.3 g) in Kategorie B eingeordnet sind;
- e) Funktionen zur Reduzierung der Auslösungshäufigkeit von Reaktorabschaltung oder verfahrenstechnischen Sicherheitsmaßnahmen.
- f) Funktionen, die nach anlageninternen Gefährdungen im Rahmen der Auslegungsgrundlage des Kernkraftwerks (z. B. Brand, Überflutung) die Überwachung und die erforderlichen Gegenmaßnahmen vornehmen;
- g) Funktionen, deren Ausfall bei Normalbetrieb zu einer niedrigen Schwere der Folgen führen würde;
- h) 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;
- i) Funktionen zur Bereitstellung der notwendigen Information, um im Störfall Größe und Verteilung des freigesetzten radioaktiven Materials feststellen zu können;
- j) Funktionen, die es ermöglichen, auf natürlichen Ereignisse (z. B. Erdbeben, hoher Wasserstand, extreme Windverhältnisse, Blitzschlag) aufmerksam zu machen und angemessene präventive Maßnahmen zu ergreifen, oder nach solchen Ereignissen eine Überwachung und mildernde Gegenmaßnahmen durchzuführen;
- k) Funktion zur Milderung der Folgen von DEC, wenn nicht schon eine Einstufung in Kategorie B gefordert wurde, einschließlich notwendige leittechnische Einrichtungen zur Realisierung von Richtlinien zum Management schwerer Störfälle, und deren Ausfall bei Anforderung in einer hohen Schwere der Folgen resultieren würde;
- l) Funktionen zur Zugangskontrolle für Personalschutz;
- m) Kommunikationsfunktionen, die Anlagenpersonal und Notfalldienste außerhalb der Anlage mit hinreichender und zuverlässiger Information versorgen (bei einem Störfall im Rahmen des Notfallplans).

das eine sicherheitstechnisch wichtige Funktion ausführt, auswirken könnten, müssen sie in dieselbe Kategorie eingeordnet werden“.