

	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 Ersatz für DIN IEC 61226 (VDE 0491-1):1997-07 Siehe jedoch Beginn der Gültigkeit Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Kategorisierung leittechnischer Funktionen (IEC 61226:2005) Nuclear power plants – Instrumentation and control systems important to safety – Classification of instrumentation and control functions (IEC 61226:2005) Centrales nucléaires de puissance – Systèmes d' instrumentation et de contrôle commande importants pour la sûreté – Classement des fonctions d' instrumentation et de contrôle commande (CEI 61226:2005) Gesamtumfang 31 Seiten DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE		

Beginn der Gültigkeit

Diese Norm gilt ab 2005-09-01.

Daneben darf **DIN IEC 61226 (VDE 0491-1):1997-07** noch bis 2007-12-31 angewendet werden.

Nationales Vorwort

Vorausgegangener Norm-Entwurf: E DIN IEC 61226 (VDE 0491-1):2003-07.

Für die vorliegende Norm ist das nationale Arbeitsgremium GUK 967.1 „Leittechnik für kerntechnische Anlagen“ und dessen Arbeitskreis AK 967.1.10 „Sicherheitsleittechnik“ der DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE zuständig. Bei Fragen der Interpretation von Aussagen wird empfohlen, ergänzend auf die zugrunde liegende, in englischer und französischer Sprache erschienene IEC-Publikation zurückzugreifen.

Die Internationale Norm wurde vom SC 45A „Instrumentation and control of nuclear facilities“ der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet. Diese Norm, deren Anwendung international empfohlen wird, gibt das höchstmögliche Maß internationaler Übereinstimmung für das behandelte Sachgebiet wieder. Die Auslegung kerntechnischer Anlagen in Deutschland wird wesentlich durch die Strahlenschutzverordnung, die BMI-Kriterien, die KTA-Regeln und die RSK-Leitlinien bestimmt.

Hinweis zur Übertragung in die deutsche Sprache: „Gerät“ ist in der vorliegenden Norm als Ober- bzw. Sammelbegriff im Sinne von Gerätschaft, Einrichtung verwendet, wie auch in DIN IEC 60780. Im aktuellen Fall kann „Gerät“ ein Einzelgerät sein oder aus einer kleineren oder größeren Zahl von zusammengeschalteten Einzelgeräten mit verschiedener Funktion bestehen.

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 60880-2 (VDE 0491-3-2):2001-12**, *Kernkraftwerke – Software für Rechner mit sicherheitstechnischer Bedeutung – Teil 2: Vorkehrungen gegen Versagen aufgrund von Softwarefehlern, Verwendung von Software-Werkzeugen und von vorgefertigter Software (IEC 60880-2:2000).*
- **DIN IEC 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).*

Als Norm-Entwürfe liegen vor:

- E DIN IEC 60880 (VDE 0491-3-2):2004-07, *Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Softwareaspekte für rechnerbasierte Systeme zur Realisierung von Funktionen der Kategorie A (IEC 45A/523/CD:2003).*
- E DIN IEC 62241 (VDE 0491-5-2):2005-06, *Kernkraftwerke – Hauptwarte – Funktionen zur Meldung und Anzeige von Störungen (IEC 62241:2004).*
- E DIN IEC 60568 (VDE 0491-6):2003-11, *Kernkraftwerke – Kern-Instrumentierung zur Messung der Neutronenflussdichte (IEC 45A/480/CD:2003).*

Änderungen

Gegenüber **DIN IEC 61226 (VDE 0491-1):1997-07** wurden folgende Änderungen vorgenommen:

- a) Klarstellung, dass Funktionen kategorisiert werden, technische Anforderungen jedoch vor allem die zugehörigen Systeme und Geräte betreffen, mit denen diese Funktionen realisiert werden;
- b) im Gegensatz zu FSE (Funktionen und zugehörige Systeme und Geräte) in der 1. Ausgabe der Norm beruht nunmehr die Kategorisierung allein auf der sicherheitstechnischen Bedeutung der Funktionen;
- c) deutlichere Formulierung der Zuordnungskriterien für die Kategorien;
- d) Berücksichtigung der überarbeiteten IAEA-Dokumente NS-R-1 und NS-G-1.3;
- e) so weit wie möglich Ersatz ausformulierter Anforderungen durch Verweisungen auf relevante andere Normen, insbesondere auf IEC 61513 und andere seit 1993 erschienene Normen;
- f) Anforderungen zur Mensch-Maschine-Schnittstelle und zur Elektromagnetischen Verträglichkeit aufgenommen;
- g) Erlaubnis zur Verwendung der Ergebnisse probabilistischer Beurteilungen entsprechend IEC/TR 61838 bei der Kategorisierung aufgenommen;
- h) redaktionelle Überarbeitung.

Frühere Ausgaben

DIN IEC 61226 (VDE 0491-1):1997-07

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 nachstehend wiedergegeben.

Tabelle NA.1

Europäische Norm	Internationale Norm	Deutsche Norm	Klassifikation im VDE-Vorschriftenwerk
–	IEC 60709:2004	vorgesehen als DIN IEC 60709 (VDE 0491-7); Entwurf zurzeit in Vorbereitung	VDE 0491-7
–	IEC 60780:1998	DIN IEC 60780:2000-12	–
–	IEC 60812:1985	–	–
–	IEC 60880:200x	vorgesehen als DIN IEC 60880 (VDE 0491-3-2); zurzeit Entwurf E DIN IEC 60880 (VDE 0491-3-2):2004:07, vorgesehen als Ersatz für DIN IEC 60880:1987-08 und DIN IEC 60880-2 (VDE 0491-3-2):2001-12	VDE 0491-3-2
–	IEC 60964:1989	–	–
–	IEC 60965:1989	–	–
–	IEC 60980:1989	–	–
–	IEC 60987:1989	–	–
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 61000-6-2:2001	IEC 61000-6-2:1999, mod.	DIN EN 61000-6-2 (VDE 0839-6-2):2002-08	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	DIN EN 61508-2 (VDE 0803-2):2002-12	VDE 0803-2
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
–	IEC 61771:1995	–	–
–	IEC 61772:1995	–	–
–	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-G-1.3:2002	–	–
–	IAEA NS-R-1:2000	–	–
–	IAEA 50-C/SG-Q:2001	–	–

Nationaler Anhang NB (informativ)

Literaturhinweise

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), *Elektromagnetische Verträglichkeit (EMV) – Teil 6-2: Fachgrundnormen; Störfestigkeit für Industriebereich (IEC 61000-6-2:1999, modifiziert); Deutsche Fassung EN 61000-6-2:2001*.

DIN EN 61508-1 (VDE 0803-1), *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), *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 61508-4 (VDE 0803-4), *Funktionale Sicherheit elektrischer/elektronischer/programmierbarer elektronischer sicherheitsbezogener Systeme – Teil 4: Begriffe und Abkürzungen (IEC 61508-4:1998 + Corrigendum 1999); Deutsche Fassung EN 61508-4:2001*.

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

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

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

E DIN IEC 60880 (VDE 0491-3-2), *Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Softwareaspekte für rechnerbasierte Systeme zur Realisierung von Funktionen der Kategorie A (IEC 45A/523/CD:2003)*.

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

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

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

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

Inhalt

	Seite
Vorwort.....	7
Einleitung.....	8
1 Anwendungsbereich	11
2 Normative Verweisungen.....	11
3 Begriffe.....	12
4 Abkürzungen.....	15
5 Kategorisierungsschema	16
5.1 Einleitung	16
5.2 Hintergrund	16
5.3 Beschreibung der Kategorien	17
5.3.1 Allgemeines	17
5.3.2 Kategorie A	17
5.3.3 Kategorie B	18
5.3.4 Kategorie C	18
5.4 Zuordnungskriterien	18
5.4.1 Kategorie A	18
5.4.2 Kategorie B	19
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
Anhang A (informativ) Beispiele zu Kategorien	30
Bild 1 – Vorgehensweise bei der Kategorisierung	21
Tabelle 1 – Zusammenhang zwischen Kategorien und anderen IEC Normen.....	29

Vorwort

- 1) Die IEC (Internationale Elektrotechnische Kommission) ist eine weltweite Normungsorganisation, die alle Nationalen Elektrotechnischen Komitees (Nationale Komitees der IEC) umfasst. Die IEC hat das Ziel, die internationale Zusammenarbeit in allen Fragen der Normung auf dem Gebiet der Elektrotechnik und Elektronik zu fördern. Zu diesem Zweck und neben anderen Aktivitäten veröffentlicht die IEC Internationale Normen, technische Spezifikationen, technische Berichte, öffentlich verfügbare Spezifikationen (PAS) und Leitfäden (im Folgenden als „Publikation(en) der IEC“ bezeichnet). Mit der Vorbereitung sind die Technischen Komitees beauftragt. Jedes Nationale Komitee der IEC, das an dem behandelten Thema interessiert ist, darf an dieser Vorbereitungsarbeit teilnehmen. Internationale, staatliche und nicht-staatliche Organisationen, die mit der IEC in Verbindung stehen, nehmen ebenfalls an diesen Vorbereitungsarbeiten teil. Die IEC arbeitet eng mit der Internationalen Organisation für Normung (ISO) nach den in der Vereinbarung zwischen beiden Organisationen festgelegten Bedingungen zusammen.
- 2) Die offiziellen Beschlüsse oder Vereinbarungen der IEC über technische Fragen, die in Technischen Komitees von Vertretern aller an dem behandelten Thema besonders interessierten Nationalen Komitees erarbeitet werden, bringen das höchstmögliche Maß internationaler Übereinstimmung für das behandelte Sachgebiet zum Ausdruck.
- 3) Publikationen der IEC haben die Form von Empfehlungen zur internationalen Anwendung und werden von den Nationalen Komitees der IEC in diesem Sinne anerkannt. Obwohl alle möglichen Anstrengungen unternommen werden, um sicherzustellen, dass der fachliche Inhalt ihrer Publikationen korrekt ist, kann die IEC nicht für deren Art der Anwendung oder für eventuelle Fehlinterpretationen durch den Anwender verantwortlich gemacht werden.
- 4) Um die internationale Vereinheitlichung zu fördern, verpflichten sich die Nationalen Komitees der IEC, Publikationen der IEC möglichst unverändert in ihren nationalen und regionalen Normen anzuwenden. Jede Abweichung zwischen der Publikation der IEC und der entsprechenden nationalen oder regionalen Norm muss in dieser deutlich gekennzeichnet werden.
- 5) Die IEC hat kein Verfahren für die Kennzeichnung der Konformität festgelegt und übernimmt keine Verantwortung, wenn ein Gegenstand als konform mit einer ihrer Publikationen erklärt wird.
- 6) Alle Anwender sollten sicherstellen, dass sie über die neueste Ausgabe dieser Publikation verfügen.
- 7) Weder die IEC, deren Geschäftsführung, Angestellte oder sonstige Beteiligte oder Beauftragte der IEC noch einzelne Fachleute oder Mitglieder ihrer Technischen Komitees und Nationalen Komitees der IEC dürfen für Schäden an Personen, Sachen oder sonstige Schäden beliebiger Art, sei es direkt oder indirekt, oder für Kosten (einschließlich Gerichtskosten) oder Ausgaben, die sich aus der Veröffentlichung, Anwendung oder im Vertrauen auf diese oder jede andere Publikation der IEC ergeben, haftbar gemacht werden.
- 8) Zu beachten sind die in dieser Publikation zitierten normativen Verweisungen. Für die korrekte Anwendung dieser Publikation ist die Verwendung der zitierten Publikationen unerlässlich.
- 9) Es wird auf die Möglichkeit hingewiesen, dass einige Texte dieses Dokuments Patentrechte berühren können. IEC ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Die Internationale Norm IEC 61226 wurde vom Technischen Unterkomitee 45A „Instrumentation and control of nuclear facilities“ des Technischen Komitees 45 „Nuclear instrumentation“ der IEC ausgearbeitet.

Diese zweite Ausgabe ersetzt die 1993 erschienene erste Ausgabe und stellt eine technische Überarbeitung dar. Die wesentlichen Änderungen gegenüber der früheren Ausgabe sind:

- Die fehlerhafte Verwendung von „ensurance“ wurde durch den Ersatz durch „assurance“ im gesamten Dokument korrigiert.
- Es wurde klargestellt, dass Funktionen kategorisiert werden, technische Anforderungen jedoch vor allem die zugehörigen Systeme und Geräte betreffen, mit denen diese Funktionen realisiert werden. Im Gegensatz zu FSE (Funktionen und zugehörige Systeme und Geräte) in der 1. Ausgabe der Norm beruht nunmehr die Kategorisierung allein auf der sicherheitstechnischen Bedeutung der Funktionen.
- Die Norm wurde redaktionell den neueren ISO/IEC-Direktiven angepasst.
- Die Norm wurde mit den überarbeiteten IAEA-Dokumenten NS-R-1 und NS-G-1.3 in Übereinstimmung gebracht. Dies schließt so weit wie möglich die Anpassung der Definitionen ein.
- Die Zuordnungskriterien für die Kategorien wurden klargestellt.

DIN IEC 61226 (VDE 0491-1):2005-09

- Die bestehenden Anforderungen wurden überprüft und Terminologie und Definitionen aktualisiert.
- So weit wie möglich wurden die zu den Kategorien gehörigen Anforderungen durch Verweisungen auf andere Normen ersetzt und neue, seit der 1. Ausgabe veröffentlichte Normen eingeführt, insbesondere IEC 61513.
- Anforderungen zur Mensch-Maschine-Schnittstelle und zur Elektromagnetischen Verträglichkeit wurden aufgenommen.
- Die Erlaubnis zur Verwendung der Ergebnisse probabilistischer Beurteilungen entsprechend IEC/TR 61838 bei der Kategorisierung wurde aufgenommen.

Dieser Text basiert auf den folgenden Dokumenten:

Internationaler Norm-Entwurf	Abstimmungsbericht
45A/547/FDIS	45A/555/RVD

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

Diese Norm wurde entsprechend den ISO/IEC-Direktiven, Teil 2 ausgearbeitet.

Das IEC-Komitee hat entschieden, dass der Inhalt dieser Publikation bis zu dem in der IEC-Website unter „<http://webstore.iec.ch>“ mit den Daten zu dieser Publikation angegebenen Pflegeergebnisdatum (maintenance result date) unverändert bleiben soll. Zu diesem Zeitpunkt wird entsprechend der Entscheidung des Komitees die Publikation

- bestätigt,
- zurückgezogen,
- durch eine Folgeausgabe ersetzt oder
- geändert.

Einleitung

Hintergrund, hauptsächliche Inhalte und Organisation der Norm

Mit dieser Internationalen Norm wird eine Forderung der IAEA umgesetzt¹⁾, 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 beabsichtigt,

- 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.

¹⁾ 5.1 von IAEA NS-R-1.

Gemäß Empfehlung der IAEA²⁾ beruhen die Methoden der Kategorisierung grundsätzlich auf der deterministischen Sicherheitsanalyse und sollten, wo angemessen, durch probabilistische Methoden ergänzt werden. Mehrere mögliche Vorgehensweisen für die Anwendung probabilistischer Sicherheitsanalysen zur Kategorisierung sind in IEC 61838:2001 beschrieben.

Die vorliegende Neuausgabe 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 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.

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 einzel-

²⁾ 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.

nen 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 (ist zu)“ Anforderung, 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 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 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.