

	DIN EN 60987 (VDE 0491-3-1)	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 „etx Elektrotechnik + Automation“ bekannt gegeben worden.	VDE
ICS 27.120.10; 35.240.50 Ersatz für DIN EN 60987 (VDE 0491-3-1):2010-03 Siehe Anwendungsbeginn Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Anforderungen an die Hardware-Auslegung rechnerbasierter Systeme (IEC 60987:2007 + A1:2013); Deutsche Fassung EN 60987:2015 Nuclear power plants – Instrumentation and control important to safety – Hardware design requirements for computer-based systems (IEC 60987:2007 + A1:2013); German version EN 60987:2015 Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Exigences applicables à la conception du matériel des systèmes informatisés (CEI 60987:2007 + A1:2013); Version allemande EN 60987:2015 Gesamtumfang 43 Seiten DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE		

Anwendungsbeginn

Anwendungsbeginn für die von CENELEC am 2015-02-16 angenommene Europäische Norm als DIN-Norm ist 2015-06-01.

Für **DIN EN 60987 (VDE 0491-3-1):2010-03** besteht eine Übergangsfrist bis 2018-02-16.

Nationales Vorwort

Vorausgegangener Norm-Entwurf: E DIN EN 60987/A1 (VDE 0491-3-1/A1):2011-05.

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.

Die enthaltene IEC-Publikation wurde vom SC 45A „Instrumentation, control and electrical systems of nuclear facilities“ erarbeitet.

Das IEC-Komitee hat entschieden, dass der Inhalt dieser Publikation bis zu dem Datum (stability date) unverändert bleiben soll, das auf der IEC-Website unter „<http://webstore.iec.ch>“ zu dieser Publikation angegeben ist. Zu diesem Zeitpunkt wird entsprechend der Entscheidung des Komitees die Publikation

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

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):2014-12**, 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
- **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 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 62671 (VDE 0491-3-6):2012-01, *Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Auswahl und Verwendung von industriellen digitalen Geräten mit begrenzter Funktionalität* (IEC 45A/845/CDV:2011)
- 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 – Änderungsmanagement* (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 62765-1 (VDE 0491-22-1):2015-06, *Kernkraftwerke – Leittechnik mit sicherheitstechnischer Bedeutung – Änderungsmanagement von Sensoren und Transmittern – Teil 1: Drucktransmitter* (IEC 45A/1001/FDIS:2015)
- E DIN IEC 60780-323 (VDE 0491-80):2014-03, *Kernkraftwerke – Elektrische Anlagen – Elektrisches Gerät mit sicherheitstechnischer Bedeutung – Qualifizierung* (IEC 45A/940/CD:2013)

Änderungen

Gegenüber **DIN EN 60987 (VDE 0491-3-1):2010-03** wurden folgende Änderungen vorgenommen:

- a) Abschnitt 9 „Herstellung“ wurde präzisiert;
- b) die Verweisungen im nationalen Vorwort wurden aktualisiert.

Frühere Ausgaben

DIN IEC 60987 (VDE 0491-3-1): 2008-04

DIN EN 60987 (VDE 0491-3-1): 2010-03

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 (1 von 2)

Europäische Norm	Internationale Norm	Deutsche Norm	Klassifikation im VDE-Vorschriftenwerk
–	IEC 60780:1998 z.Z. in Überarbeitung, siehe 45A/991/CDV ^a	DIN IEC 60780:2000-12	–
EN 60812:2006	IEC 60812:2006	DIN EN 60812:2006-11	–
EN 60880:2009	IEC 60880:2006	DIN EN 60880 (VDE 0491-3-2):2010-03	VDE 0491-3-2
Normen der Reihe EN 61000	Normen der Reihe IEC 61000	Normen der Reihe DIN EN 61000 (VDE 0838, VDE 0839, VDE 0847)	Normen der Reihen VDE 0838 VDE 0839 VDE 0847
EN 61025:2007	IEC 61025:2006	DIN EN 61025:2007-08	–
EN 61226:2010	IEC 61226:2009	DIN EN 61226 (VDE 0491-1):2010-08	VDE 0491-1
EN 61508-1:2010	IEC 61508-1:2010	DIN EN 61508-1 (VDE 0803-1):2011-02	VDE 0803-1
EN 61508-2:2010	IEC 61508-2:2010	DIN EN 61508-2 (VDE 0803-2):2011-02	VDE 0803-2

Tabelle NA.1 (2 von 2)

Europäische Norm	Internationale Norm	Deutsche Norm	Klassifikation im VDE-Vorschriftenwerk
EN 61508-3:2010	IEC 61508-3:2010	DIN EN 61508-3 (VDE 0803-3):2011-02	VDE 0803-3
EN 61508-4:2010	IEC 61508-4:2010	DIN EN 61508-4 (VDE 0803-4):2011-02	VDE 0803-4
EN 61513:2013	IEC 61513:2011	DIN EN 61513 (VDE 0491-2):2013-09	VDE 0491-2
EN 62138:2009	IEC 62138:2004	DIN EN 62138 (VDE 0491-3-3):2010-03	VDE 0491-3-3
–	ISO 2768-1:1989	DIN ISO 2768-1:1991-06	–
–	ISO 2768-2:1989	DIN ISO 2768-2:1991-04	–
–	ISO 3951-1:2005	DIN ISO 3951-1:2008-03	–
–	ISO 3951-2:2013	–	–
–	ISO 3951-3:2007	–	–
–	ISO 3951-4:2011	–	–
–	ISO 3951-5:2006	–	–
EN ISO 9001:2008	ISO 9001:2008	DIN EN ISO 9001:2008-12	–
–	ISO/IEC 12207:2008	–	–
–	IAEA NS-G 1.3	–	–
–	IAEA NS-R-1	–	–
–	IAEA 50-C/SG-Q	–	–
–	IAEA Safety Glossary	–	–
^a Zu beziehen über DKE-Schriftstückservice, Stresemannallee 15, 60596 Frankfurt am Main.			

DIN EN 62566
(VDE 0491-3-5):2015-02

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

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

Normen der Reihe DIN EN 61000 (VDE 0838, VDE 0839, VDE 0847), *Elektromagnetische Verträglichkeit (EMV)*

DIN EN 61025:2007-08, *Fehlzustandsbaumanalyse* (IEC 61025:2006); Deutsche Fassung EN 61025:2007

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 61508-1 (VDE 0803-1):2011-02, Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 1: Allgemeine Anforderungen (IEC 61508-1:2010); Deutsche Fassung EN 61508-1:2010

DIN EN 61508-2 (VDE 0803-2):2011-02, Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 2: Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme (IEC 61508-2:2010); Deutsche Fassung EN 61508-2:2010

DIN EN 61508-3 (VDE 0803-3):2011-02, Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 3: Anforderungen an Software (IEC 61508-3:2010); Deutsche Fassung EN 61508-3:2010

DIN EN 61508-4 (VDE 0803-4):2011-02, Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 4: Begriffe und Abkürzungen (IEC 61508-4:2010); Deutsche Fassung EN 61508-4:2010

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 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 ISO 9001:2008-12, Qualitätsmanagementsysteme – Anforderungen (ISO 9001:2008); Dreisprachige Fassung EN ISO 9001:2008

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

DIN ISO 2768-1:1991-06, Allgemeintoleranzen – Toleranzen für Längen- und Winkelmaße ohne einzelne Toleranzeintragung; (ISO 2768-1:1989)

DIN ISO 2768-2:1991-04, Allgemeintoleranzen – Toleranzen für Form und Lage ohne einzelne Toleranzeintragung; (ISO 2768-2:1989)

DIN ISO 3951-1:2008-03, Verfahren für die Stichprobenprüfung anhand quantitativer Merkmale (Variablenprüfung) – Teil 1: Spezifikation für Einfach-Stichprobenanweisungen für losweise Prüfung, geordnet nach der annehmbaren Qualitätsgrenzlage (AQL) für ein einfaches Qualitätsmerkmal und einfache AQL (ISO 3951-1:2005)

**Kernkraftwerke –
Leittechnische Systeme mit sicherheitstechnischer Bedeutung –
Anforderungen an die Hardware-Auslegung rechnerbasierter Systeme
(IEC 60987:2007 + A1:2013)**

Nuclear power plants –
Instrumentation and control important to safety –
Hardware design requirements for computer-
based systems
(IEC 60987:2007 + A1:2013)

Centrales nucléaires de puissance –
Instrumentation et contrôle-commande
importants pour la sûreté –
Exigences applicables à la conception du
matériel des systèmes informatisés
(CEI 60987:2007 + A1:2013)

Diese Europäische Norm wurde von CENELEC am 2015-02-16 angenommen. CENELEC-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist.

Auf dem letzten Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim CEN-CENELEC Management Centre oder bei jedem CENELEC-Mitglied auf Anfrage erhältlich.

Diese Europäische Norm besteht in drei offiziellen Fassungen (Deutsch, Englisch, Französisch). Eine Fassung in einer anderen Sprache, die von einem CENELEC-Mitglied in eigener Verantwortung durch Übersetzung in seine Landessprache gemacht und dem CEN-CENELEC Management Centre mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

CENELEC-Mitglieder sind die nationalen elektrotechnischen Komitees von Belgien, Bulgarien, Dänemark, Deutschland, der ehemaligen jugoslawischen Republik Mazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, der Schweiz, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, der Türkei, Ungarn, dem Vereinigten Königreich und Zypern.

CENELEC

Europäisches Komitee für Elektrotechnische Normung
European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brüssel

© 2015 CENELEC – Alle Rechte der Verwertung, gleich in welcher Form und in welchem Verfahren, sind weltweit den Mitgliedern von CENELEC vorbehalten.

Ref. Nr. EN 60987:2015 D

Vorwort

Dieses Dokument (EN 60987:2015) enthält den Text der IEC 60987:2007 + A1:2013, die vom SC 45A „Instrumentation, control and electrical systems of nuclear facilities“ des IEC/TC 45 „Nuclear instrumentation“ erarbeitet wurde.

Nachstehende Daten wurden festgelegt:

- spätestes Datum, zu dem dieses Dokument auf nationaler Ebene durch Veröffentlichung einer identischen nationalen Norm oder durch Anerkennung übernommen werden muss (dop): 2016-02-16
- spätestes Datum, zu dem nationale Normen, die diesem Dokument entgegenstehen, zurückgezogen werden müssen (dow): 2018-02-16

Dieses Dokument ersetzt EN 60987:2009.

Wie in der Richtlinie zur nuklearen Sicherheit 2009/71/EURATOM, Kapitel 1, Artikel 2, Punkt 2 angegeben, werden die Mitgliedsstaaten nicht davon abgehalten, strengere Sicherheitsmaßnahmen in dem von der Richtlinie behandelten Gebiet zu fordern, entsprechend dem Gemeinschaftsrecht. Auf vergleichbare Weise hindert diese Europäische Norm die Mitgliedsstaaten nicht daran, im Geltungsbereich dieser Europäischen Norm strengere Maßnahmen bezüglich der nuklearen Sicherheit zu fordern.

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

Anerkennungsnotiz

Der Text der Internationalen Norm IEC 60987:2007 + A1:2013 wurde von CENELEC ohne irgendeine Abänderung als Europäische Norm angenommen.

In der offiziellen Fassung ist unter „Literaturhinweise“ zu der aufgelisteten Norm die nachstehende Anmerkung einzutragen:

IEC 61226 ANMERKUNG Harmonisiert als EN 61226.

Inhalt

Seite

Vorwort	2
Einleitung	5
1 Anwendungsbereich	7
1.1 Allgemeines	7
1.2 Anwendung der Norm für die Beurteilung vorgefertigter Hardware	7
1.3 Anwendbarkeit dieser Norm für die Entwicklung programmierbarer logischer Einheiten	7
2 Normative Verweisungen	8
3 Begriffe	8
4 Projektstruktur	11
4.1 Allgemeines	11
4.2 Projektunterteilung	11
4.3 Qualitätssicherung	12
5 Hardwareanforderungen	12
5.1 Allgemeines	12
5.2 Funktionale und Leistungsfähigkeitsanforderungen	13
5.3 Zuverlässigkeits-/Verfügbarkeitsanforderungen	14
5.4 Umgebungsanforderungen	15
5.5 Dokumentationsanforderungen	15
6 Auslegung und Entwicklung	16
6.1 Allgemeines	16
6.2 Auslegungstätigkeiten	16
6.3 Zuverlässigkeit	17
6.4 Wartung	17
6.5 Schnittstellen	18
6.6 Änderungen	18
6.7 Ausfall der Energieversorgung	18
6.8 Komponentenauswahl	18
6.9 Auslegungsdokumentation	18
7 Verifizierung und Validierung	19
7.1 Allgemeines	19
7.2 Verifizierungsplan	19
7.3 Unabhängigkeit der Verifizierung	20
7.4 Methoden	20
7.5 Dokumentation	21
7.6 Unstimmigkeiten	21
7.7 Änderungen	21
7.8 Errichtungsverifizierung	21

	Seite
7.9 Validierung.....	21
7.10 Verifizierung von vorgefertigten Geräteplattformen	21
8 Qualifizierung.....	22
9 Herstellung	22
9.1 Qualitätssicherung.....	22
9.2 Ausbildung des Personals.....	23
9.3 Planung und Organisation der Herstellungsaktivitäten	23
9.4 Eingaben	23
9.5 Einkauf und Beschaffung	24
9.6 Produktion	25
10 Errichtung und Inbetriebnahme	28
11 Wartung	29
11.1 Wartungsanforderungen.....	29
11.2 Ausfalldaten.....	30
11.3 Wartungsdokumentation.....	30
12 Änderungen	31
13 Betrieb	31
Anhang A (informativ) Überblick über den Systemlebenszyklus.....	32
Anhang B (informativ) Übersicht über den Qualifizierungsvorgang	33
Anhang C (informativ) Beispiel einer Wartungsprozedur	34
Literaturhinweise.....	35
Anhang ZA (normativ) Normative Verweisungen auf internationale Publikationen mit ihren entsprechenden europäischen Publikationen	36

Einleitung

a) Technischer Hintergrund, hauptsächliche Inhalte und Organisation der Norm

Die Grundprinzipien für die Auslegung nuklearer Instrumentierung, speziell für Sicherheitssysteme von Kernkraftwerken, wurden zunächst in nuklearen Normen mit Bezug auf festverdrahtete Systeme dargestellt, wie z. B. im „Safety Guide 50-SG-D3“ der IAEA, der inzwischen durch NS-G 1.3 ersetzt wurde.

IEC 60987 wurde erstmals 1989 veröffentlicht, um die Hardwareaspekte der Auslegung digitaler Systeme für sicherheitstechnisch wichtige Einrichtungen, d. h. Sicherheitssysteme und sicherheitsrelevante Systeme, abzudecken.

Obwohl viele Anforderungen der ersten Ausgabe nach wie vor Gültigkeit haben, gibt es wichtige Faktoren, die eine überarbeitete Fassung der IEC 60987 rechtfertigen, insbesondere:

- eine inzwischen erarbeitete Norm, die im Detail die allgemeinen Anforderungen an sicherheitstechnisch wichtige Systeme anspricht (IEC 61513);
- vorgefertigte Systemplattformen, die im Vergleich zu speziellen Einzelentwicklungen zunehmend verwendet werden.

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

Für sicherheitstechnisch wichtige rechnerbasierte Systeme in Kernkraftwerken ist IEC 61513 die IEC/SC-45A-Norm der ersten Ebene. IEC 60987 ist eine IEC/SC-45A-Norm der zweiten Ebene, sie befasst sich mit den generischen Themen der Hardwareauslegung solcher Systeme.

IEC 60880 und IEC 62138 sind Normen der zweiten Ebene und decken zusammen die Software-Aspekte rechnerbasierter Systeme ab, die zur Ausführung sicherheitstechnisch wichtiger Funktionen in Kernkraftwerken verwendet werden. In IEC 60880 und IEC 62138 wird für die Hardwareauslegung direkt auf die hier vorliegende Norm verwiesen.

Bezüglich der Anforderungen zur Qualifizierung wird in der vorliegenden Norm auf IEC 60780 verwiesen. Für Module, die in der Auslegung eines spezifischen sicherheitstechnisch wichtigen Systems Verwendung finden, können einschlägige und auditierbare Betriebserfahrungen von nuklearen oder anderen Anwendungen in Verbindung mit strengen Qualitätssicherungsprogrammen eine akzeptable Qualifizierungsmethode darstellen, wie in IEC 60780 beschrieben.

Mehr Details über die Struktur der Normen des IEC/SC 45A sind in d) dieser Einleitung zu finden.

c) Empfehlungen und Einschränkungen der Anwendung der Norm

Es ist wichtig, darauf hinzuweisen, dass in dieser Norm keine zusätzlichen funktionalen Anforderungen für Systeme der Klassen 1 und 2 definiert werden (bezüglich der Systemklassifizierung siehe IEC 61513).

Aspekte, für die spezielle Empfehlungen gegeben werden (namentlich zur Sicherstellung der Herstellung hochzuverlässiger Systeme), sind:

- eine allgemeine Vorgehensweise zur Entwicklung von Rechnerhardware;
- eine allgemeine Vorgehensweise zur Hardware-Verifizierung und zu den Hardwareaspekten der Rechner-System-Validierung.

Es ist klar, dass sich die Rechnertechnologie ständig weiterentwickelt und dass es für eine Norm wie die vorliegende unmöglich ist, Hinweise auf alle modernen Entwicklungstechnologien zu berücksichtigen. Um sicherzustellen, dass die Norm auch in zukünftigen Jahren ihre Relevanz behält, wurde der Schwerpunkt eher auf prinzipielle Fragestellungen gelegt als auf spezifische Auslegungstechnologien. Wenn neue Auslegungstechniken entwickelt werden, sollte es möglich sein, ihre Eignung durch Adaption der in dieser Norm enthaltenen Auslegungsprinzipien zu beurteilen.

Der Anwendungsbereich dieser Norm deckt die Hardware digitaler Systeme in Systemen der Klassen 1 und 2 ab. Dies umfasst auch verteilte Multiprozessorsysteme und Einzelprozessorsysteme, wobei die Beurteilung und Verwendung vorgefertigter Einheiten (z. B. am Markt erhältliche Produkte (COTS)) und die Entwicklung neuer Hardware mit eingeschlossen sind.

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 **IEC 61513** wird die SC-45A-Normenreihe strukturiert.

In **IEC 61513** wird direkt auf andere IEC/SC-45A-Normen 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, Hardwareaspekte rechnerbasierter Systeme sowie Auslegung von Warten behandeln. Die Normen, die auf dieser zweiten Ebene direkt angezogen werden, sollten zusammen mit **IEC 61513** als ein in sich konsistenter Satz von Dokumenten betrachtet werden.

Die dritte Ebene bilden IEC/SC-45A-Normen, 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 IEC/SC-45A-Normenreihe um Technische Berichte, die nicht normativ sind.

Für **IEC 61513** wird ein Darstellungsformat verwendet, das dem der grundlegenden Sicherheitsnorm IEC 61508 ähnlich ist, mit einem Sicherheits-Lebenszyklus als Gesamtrahmen und zusätzlich einem System-Lebenszyklus. Mit **IEC 61513** werden die allgemeinen Anforderungen (für Sicherheitssysteme unterschiedlicher industrieller Anwendungen) von **IEC 61508-1**, **IEC 61508-2** und **IEC 61508-4** für die Anwendung auf dem nuklearen 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 9001 als auch auf IAEA 50-C/SG-Q.

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 und detailliert. Terminologie und Definitionen in den Normen des IEC/SC 45A sind mit den von der IAEA verwendeten konsistent.

1 Anwendungsbereich

1.1 Allgemeines

Diese Internationale Norm gilt für die Rechnerhardware von Systemen der Klassen 1 und 2 (wie in IEC 61513 definiert) in Kernkraftwerken.

Die Struktur dieser Norm hat sich im Vergleich zur Ausgabe von 1989 nicht wesentlich verändert, jedoch werden einige Gesichtspunkte durch Normen behandelt, die inzwischen herausgegeben wurden (z. B. IEC 61513 für die Auslegung von Systemarchitekturen); Verweisungen auf neue Normen wurden, wo zutreffend, eingeführt. Der Text der Norm wurde auch überarbeitet, um neuen Entwicklungen in der Rechnerhardwareauslegung, der Anwendung vorgefertigter Hardware (z. B. am Markt erhältlicher Produkte (COTS)) und Veränderungen in der Terminologie Rechnung zu tragen.

Rechnerhardware, die zum Laden und Überprüfen von Software verwendet wird, wird nicht als eigentlicher Teil eines sicherheitstechnisch wichtigen Systems erachtet und fällt daher nicht in den Anwendungsbereich dieser Norm.

ANMERKUNG 1 Hardware von Rechnersystemen der Klasse 3 wird in dieser Norm nicht angesprochen. Es wird empfohlen, solche Systeme nach kommerziellen Normen zu entwickeln.

ANMERKUNG 2 2006 wurde in IEC/SC 45A die Erarbeitung einer neuen Norm mit Anforderungen für „hoch komplexe“ Hardware diskutiert. Wenn eine solche Norm erarbeitet ist, sollte diese anstelle der IEC 60987 für „hoch komplexe“ Hardware angewandt werden.

1.2 Anwendung der Norm für die Beurteilung vorgefertigter Hardware

Obwohl es primäres Ziel dieser Norm ist, Aspekte der Hardwareentwicklung anzusprechen, können die hier definierten Prozesse auch als Anleitung für die Beurteilung und Anwendung vorgefertigter Hardware (z. B. am Markt erhältlicher Produkte (COTS)) benutzt werden. Im Text sind Hinweise zur Interpretation der Anforderungen dieser Norm für die Beurteilung solcher Komponenten vorgesehen. Insbesondere sind bezüglich der Konfigurationskontrolle die Anforderungen zur Qualitätssicherung nach 4.3 anzuwenden.

Vorgefertigte Komponenten können Firmware (wie in 3.4 definiert) enthalten. Wenn Software als Firmware eingebettet ist und für den Anwender effektiv „transparent“ ist, sollte IEC 60987 als Anleitung für die Beurteilung solcher Komponenten verwendet werden. Ein Beispiel, wo diese Vorgehensweise als geeignet erachtet wird, ist die Beurteilung moderner Prozessoren mit Mikrocode. Ein derartiger Code ist im Allgemeinen ein integraler Teil der „Hardware“, und daher ist es in diesem Fall zweckmäßig, den Prozessor (einschließlich Mikrocode) unter Anwendung der vorliegenden Norm zu beurteilen.

Software, die nicht wie oben beschrieben als Firmware zu betrachten ist, sollte nach den Anforderungen der relevanten Softwarenormen (z. B. IEC 60880 für Systeme der Klasse 1 und IEC 62138 für Systeme der Klasse 2) entwickelt oder beurteilt werden.

1.3 Anwendbarkeit dieser Norm für die Entwicklung programmierbarer logischer Einheiten

Leittechnische Komponenten können programmierbare logische Einheiten enthalten, deren spezifische anwendungsbezogene Auslegung der Logik vom Konstrukteur der leittechnischen Komponente stammt, nicht vom Chip-Hersteller. Beispiele solcher Einheiten sind auch komplexe programmierbare logische Einrichtungen (CPLD) und vor Ort programmierbare Gatter-Anordnungen (FPGA).

Die Programmierbarkeit der logischen Einheiten gibt den für sie benutzten Entwicklungsprozessen in gewisser Weise die Charakteristik einer Softwareentwicklung. Die Auslegungsprozesse für solche logische Einheiten sind sehr ähnlich denen für logische Schaltungen, die mit diskreten Gattern und integrierten Schaltungspaketen realisiert werden. Daher sollten Auslegungsprozesse und Verifizierung programmierbarer logischer Einheiten den relevanten Anforderungen der vorliegenden Norm entsprechen (d. h. die speziellen Merkmale der Auslegungsprozesse solcher Einheiten berücksichtigen). Werden Software-basierte Werkzeuge verwendet, um die Auslegungsprozesse für programmierbare logische Einheiten zu unterstützen, sollten diese im Allgemeinen den Anleitungen für derartige Werkzeuge in den einschlägigen Softwarenormen folgen, d. h. IEC 60880 für Systeme der Klasse 1 und IEC 62138 für Systeme der Klasse 2.