

	DIN IEC 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 „etz Elektrotechnik + Automation“ bekannt gegeben worden.	VDE
ICS 27.120.20 Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Anforderungen an die Hardwareauslegung rechnerbasierter Systeme (IEC 60987:2007) Nuclear power plants – Instrumentation and control important to safety – Hardware design requirements for computer-based systems (IEC 60987:2007) 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) Gesamtumfang 31 Seiten DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE		

Inhalt

Seite

Nationales Vorwort.....	4
Nationaler Anhang NA (informativ) Zusammenhang mit Europäischen und Internationalen Normen	5
Nationaler Anhang NB (informativ) Literaturhinweise	7
Einleitung.....	8
1 Anwendungsbereich	10
1.1 Allgemeines	10
1.2 Verwendung der Norm für die Beurteilung vorgefertigter Hardware	10
1.3 Anwendbarkeit dieser Norm für die Entwicklung programmierbarer logischer Einheiten	10
2 Normative Verweisungen.....	11
3 Begriffe.....	11
4 Projektstruktur.....	14
4.1 Allgemeines	14
4.2 Projektunterteilung	14
4.3 Qualitätssicherung	14
5 Hardwareanforderungen.....	15
5.1 Allgemeines	15
5.2 Funktionale und Leistungsfähigkeitsanforderungen	16
5.3 Zuverlässigkeits-/Verfügbarkeitsanforderungen	17
5.4 Umgebungsanforderungen	18
5.5 Dokumentationsanforderungen	18
6 Auslegung und Entwicklung.....	18
6.1 Allgemeines	18
6.2 Auslegungstätigkeiten.....	19
6.3 Zuverlässigkeit	19
6.4 Wartung	20
6.5 Schnittstellen.....	20
6.6 Änderungen	20
6.7 Ausfall der Energieversorgung	21
6.8 Komponentenauswahl	21
6.9 Auslegungsdokumentation	21
7 Verifizierung und Validierung.....	22
7.1 Allgemeines	22
7.2 Verifizierungsplan	22
7.3 Unabhängigkeit der Verifizierung.....	22
7.4 Methoden	23
7.5 Dokumentation.....	23
7.6 Unstimmigkeiten	23
7.7 Änderungen	24

	Seite
7.8 Errichtungsverifizierung	24
7.9 Validierung	24
7.10 Verifizierung von vorgefertigten Geräteplattformen	24
8 Qualifizierung	24
9 Herstellung	24
10 Errichtung und Inbetriebnahme	25
11 Wartung	25
11.1 Wartungsanforderungen	25
11.2 Ausfalldaten	26
11.3 Wartungsdokumentation	27
12 Änderungen	27
13 Betrieb	27
Anhang A (informativ) Überblick über den Systemlebenszyklus	28
Anhang B (informativ) Übersicht über den Qualifizierungsvorgang	29
Anhang C (informativ) Beispiel einer Wartungsprozedur	30
Literaturhinweise	31

Beginn der Gültigkeit

Diese Norm gilt ab 2008-04-01.

Nationales Vorwort

Vorausgegangener Norm-Entwurf: E DIN IEC 60987 (VDE 0491-3-1):2006-09.

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

Die enthaltene IEC-Publikation wurde vom SC 45A „Instrumentation and control of nuclear facilities“ erarbeitet. Diese Norm, deren Anwendung international empfohlen wird, gibt das höchstmögliche Maß internationaler Übereinstimmung für das behandelte Sachgebiet wieder. Bei Fragen der Interpretation von Aussagen wird empfohlen, ergänzend auf die zugrunde liegende, in englischer und französischer Sprache erschienene IEC-Publikation zurückzugreifen. Die Auslegung kerntechnischer Anlagen in Deutschland wird wesentlich durch die Strahlenschutzverordnung, die BMI-Kriterien, die KTA-Regeln und die RSK-Leitlinien bestimmt.

Das IEC-Komitee hat entschieden, dass der Inhalt dieser Publikation bis zu dem Datum (maintenance result 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 IEC 61226 (VDE 0491-1):2005-09**, *Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Kategorisierung leittechnischer Funktionen (IEC 61226:2005)*
- **DIN IEC 61513 (VDE 0491-2):2002-10**, *Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Allgemeine Systemanforderungen (IEC 61513:2001)*
- **DIN IEC 61513/A100 (VDE 0491-2/A100):2005-02**, *Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Allgemeine Systemanforderungen – Nationaler Anhang ND (informativ): Mitgeltende Festlegungen aus anderen IEC-Normen*
- **DIN IEC 60987 (VDE 0491-3-1):2008-04**, *Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Anforderungen an die Hardwareauslegung rechnerbasierter Systeme (IEC 60987:2007)*
- **DIN IEC 60880 (VDE 0491-3-2):2007-08**, *Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Softwareaspekte für rechnerbasierte Systeme zur Realisierung von Funktionen der Kategorie A (IEC 60880:2006)*
- **DIN IEC 62138 (VDE 0491-3-3):2004-09**, *Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Softwareaspekte für rechnerbasierte Systeme zur Realisierung von Funktionen der Kategorien B oder C (IEC 62138:2004)*
- **DIN IEC 62117 (VDE 0491-4):2001-10**, *Kernkraftwerke – Druckwasserreaktoren – Überwachung ausreichender Kühlung des Kerns im abgeschalteten Zustand des Reaktors (IEC 62117:1999)*
- **DIN IEC 61839 (VDE 0491-5):2002-09**, *Kernkraftwerke – Auslegung von Warten – Analyse und Zuordnung der Funktionen (IEC 61839:2000)*
- **DIN IEC 62241 (VDE 0491-5-2):2006-05**, *Kernkraftwerke – Hauptwarte – Funktionen zur Meldung und Anzeige von Störungen (IEC 62241:2004)*
- **DIN IEC 60568 (VDE 0491-6):2006-11**, *Kernkraftwerke – Instrumentierung mit sicherheitstechnischer Bedeutung – Kerninstrumentierung zur Messung der Neutronenflussdichte in Leistungsreaktoren (IEC 60568:2006)*

- **DIN IEC 60709 (VDE 0491-7):2006-05**, *Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Physikalische und elektrische Trennung (IEC 60709:2004)*
- **DIN IEC 60671 (VDE 0491-100):2007-12**, *Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Prüfungen zur Sicherstellung der Funktionsfähigkeit (IEC 60671:2007)*

Als Norm-Entwürfe liegen vor:

- E DIN IEC 60964 (VDE 0491-5-1):2007-11, *Kernkraftwerke – Warten – Auslegung (IEC 45A/652/CDV:2007)*
- E **DIN IEC 61227 (VDE 0491-5-3):2007-08**, *Kernkraftwerke – Warten – Handbedienungen (IEC 45A/649/CDV:2007)*
- E DIN IEC 62340 (VDE 0491-10):2006-04, *Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Versagen gemeinsamer Ursache (CCF) (IEC 45A/601/CDV:2005)*

Nationaler Anhang NA (informativ)

Zusammenhang mit Europäischen und Internationalen Normen

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

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

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

Tabelle NA.1

Europäische Norm	Internationale Norm	Deutsche Norm	Klassifikation im VDE-Vorschriftenwerk
–	IEC 60780:1998	DIN IEC 60780:2000-12	–
EN 60812:2006	IEC 60812:2006	DIN EN 60812:2006-11	–
–	IEC 60880:2006	DIN IEC 60880 (VDE 0491-3-2):2007-08	VDE 0491-3-2
Normen der Reihe EN 61000	Normen der Reihe IEC 61000	Normen der Reihe DIN EN 61000 (VDE 0838, VDE 0839, VDE 0847)	Normen der Reihe VDE 0838 VDE 0839 VDE 0847
EN 61025:2007	IEC 61025:2006	DIN EN 61025:2007-08	–
–	IEC 61226:2005	DIN IEC 61226 (VDE 0491-1):2005-09	VDE 0491-1
EN 61508-1:2001	IEC 61508-1:1998 + Corr.:1999	DIN EN 61508-1 (VDE 0803-1):2002-11	VDE 0803-1
EN 61508-2:2001	IEC 61508-2:2000	DIN EN 61508-2 (VDE 0803-2):2002-12	VDE 0803-2
EN 61508-3:2001	IEC 61508-3:1998 + Corr.:1999	DIN EN 61508-3 (VDE 0803-3):2002-12	VDE 0803-3
EN 61508-4:2001	IEC 61508-4:1998 + Corr.:1999	DIN EN 61508-4 (VDE 0803-4):2002-11	VDE 0803-4

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

Europäische Norm	Internationale Norm	Deutsche Norm	Klassifikation im VDE-Vorschriftenwerk
–	IEC 61513:2001	DIN IEC 61513 (VDE 0491-2):2002-10	VDE 0491-2
–	–	und DIN IEC 61513/A100 (VDE 0491-2/A100):2005-02	VDE 0491-2/A100
–	IEC 62138:2004	DIN IEC 62138 (VDE 0491-3-3):2006-09	VDE 0491-3-3
EN ISO 9001:2000	ISO 9001:2000	DIN EN ISO 9001:2000-12	–
–	ISO/IEC 12207:1995 + A1:2002 + A2:2004 Wird ersetzt durch Ausgabe 2008	–	–
–	IAEA NS-G 1.3	–	–
–	IAEA NS-R-1	–	–
–	IAEA 50-C/SG-Q	–	–
–	IAEA Safety Glossary	–	–

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 61000 (VDE 0838, VDE 0839, VDE 0847) Reihe, *Elektromagnetische Verträglichkeit (EMV)*

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

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

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

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

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

DIN EN ISO 9001:2000-12, *Qualitätsmanagementsysteme – Anforderungen (ISO 9001:2000-09); Dreisprachige Fassung EN ISO 9001:2000*

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

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

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

Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Anforderungen an die Hardwareauslegung rechnerbasierter Systeme

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 Hardware-Aspekte 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 Hardware-Aspekten 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 Auslegungs-

techniken 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) 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 die 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, Hardware-Aspekte 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, -2 und -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 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 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 Norm gilt für die Rechnerhardware von Systemen der Klassen 1 und 2 (siehe IEC 61513) 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); Verweise auf neue Normen wurden, wo zutreffend, eingeführt. Der Text der Norm wurde auch überarbeitet, um neuen Entwicklungen in der Rechnerhardwareauslegung, der Verwendung vorgefertigter Hardware (z. B. am Markt erhältlicher Produkte) 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 In IEC/SC 45A wurde 2006 über die Entwicklung einer neuen Norm für Anforderungen an „sehr komplexe“ Hardware diskutiert. Wenn eine solche Norm zur Verfügung steht, wäre sie dafür an Stelle von IEC 60987 anzuwenden.

1.2 Verwendung 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 Verwendung vorgefertigter Hardware (z. B. am Markt erhältlicher Produkte) 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 logischen 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 oder IEC 62138 für Systeme der Klasse 2.