

**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 „etz Elektrotechnik + Automation“ bekannt gegeben worden.

VDE

ICS 27.120.20; 35.240.50

Einsprüche bis 2019-05-22

Vorgesehen als Ersatz für
DIN EN 60987
(VDE 0491-3-1):2015-06

Entwurf

**Kernkraftwerke –
Leittechnische Systeme mit sicherheitstechnischer Bedeutung –
Anforderungen an die Hardware-Auslegung
(IEC 45A/1243/CD:2018);
Text Deutsch und Englisch**

Nuclear power plants –
Instrumentation and control systems important to safety –
Hardware design requirements
(IEC 45A/1243/CD:2018);
Text in German and English

Centrales nucléaires de puissance –
Systèmes d'instrumentation et de contrôle-commande importants pour la sûreté –
Exigences applicables à la conception du matériel
(IEC 45A/1243/CD:2018);
Texte en allemand et anglais

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2019-03-22 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 von DIN unter www.din.de/go/entwuerfe 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/go/stellungnahmen-norm-entwuerfe 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 101 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE

Anwendungsbeginn

Anwendungsbeginn dieser Norm ist

Nationales Vorwort

Das internationale Dokument IEC 45A/1243/CD:2018 „Nuclear power plants – Instrumentation and control systems important to safety – Hardware design requirements“ (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 power 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 FprEN nur 6 Wochen 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.

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.

Der Zusammenhang der zitierten Dokumente mit den entsprechenden deutschen Dokumenten ergibt sich, soweit ein Zusammenhang besteht, grundsätzlich über die Nummer der entsprechenden IEC-Publikation. Beispiel: IEC 60068 ist als EN 60068 als Europäische Norm durch CENELEC übernommen und als DIN EN 60068 ins Deutsche Normenwerk aufgenommen.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. IEC ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Änderungen

Gegenüber **DIN EN 60987 (VDE 0491-3-1):2015-06** wurden folgende Änderungen vorgenommen:

- a) Es wird berücksichtigt, dass Hardwareanforderungen für jede Art leittechnischer Technologie anzuwenden sind, einschließlich konventionell fest-verdrahteter Einrichtungen, programmierbarer digitaler Geräte oder Kombinationen von beiden;
- b) -der Anwendungsbereich wurde auf Hardware jeder Art leittechnischer Technologie ausgedehnt, gleich ob rechnergestützt oder nicht, und nach den Sicherheitsklassen 1, 2 und 3 unterschieden;
- c) Form und Gliederung wurde entsprechend den ISO/IEC-Direktiven überarbeitet;
- d) die Anforderungen und Definitionen wurden an die neueren IAEA-Dokumente angeglichen, insbesondere an IAEA SSR-2/1;
- e) die Verweisungen auf Anforderungen anderer Normen wurden ergänzt und aktualisiert, insbesondere auf **IEC 61513**, **IEC 60880**, **IEC 62138**, IEC 62566-1 und IEC 62566-2;

- f) für HDL-Entwicklungen wird auf IEC 62566-1 and IEC 62566-2 verwiesen;
- g) die Anforderungen für die Auswahl und Akzeptanz vorgefertigter (am Markt erhältlicher) Komponenten wurden ergänzt;
- h) die Anforderungen für Auslegung, Herstellung und Kontrolle elektronische Module wurden klarer gefasst;
- i) die Verfahren zur Beurteilung der Zuverlässigkeit und Wartbarkeit wurden ergänzt;
- j) Anforderungen bezüglich der Verwendung automatischer Test- oder Überwachungsgeräte wurden aufgenommen;
- k) das Thema Beschaffung und damit verbundene Akzeptanzkriterien wurde ergänzt;
- l) die Tätigkeiten zur Produktionskontrolle wurden ergänzt;
- m) -die Anforderungen wurden entsprechend den drei Geräteklassen (Sicherheitsklassen 1, 2 und 3) abgestuft.

Inhalt

Seite

Einleitung	7
1 Anwendungsbereich	10
1.1 Allgemeines	10
1.2 Anwendung der Norm für die Beurteilung vorgefertigter Hardware	10
1.3 Anwendbarkeit dieser Norm für die Entwicklung programmierbarer logischer Einheiten (HPDs)	10
2 Normative Verweisungen	11
3 Begriffe	12
4 Symbole und Abkürzungen	18
5 Projektstruktur	18
5.1 Allgemeines	18
5.2 Projektunterteilung	19
5.3 Qualitätsmanagement	19
6 Hardwareanforderungen	20
6.1 Allgemeines	20
6.1.1 Allgemeines für Gerät der Klassen 1 und 2	20
6.1.2 Allgemeines für Gerät der Klasse 3	21
6.2 Funktionale und Leistungsfähigkeitsanforderungen für Gerät der Klassen 1 und 2	21
6.3 Zuverlässigkeits-/Verfügbarkeitsanforderungen für Gerät der Klassen 1 und 2	22
6.4 Umgebungsanforderungen	24
6.4.1 Umgebungsanforderungen für Gerät der Klassen 1 und 2	24
6.4.2 Umgebungsanforderungen für Gerät der Klasse 3	24
6.5 Dokumentationsanforderungen	24
7 Auslegung und Entwicklung	25
7.1 Allgemeines	25
7.1.1 Allgemeine Anforderungen für Gerät der Klassen 1 und 2	25
7.1.2 Allgemeine Anforderungen für Gerät der Klasse 3	25
7.2 Auslegungstätigkeiten	25
7.3 Zuverlässigkeit	26
7.3.1 Zuverlässigkeit von Gerät der Klassen 1 und 2	26
7.3.2 Zuverlässigkeit von Gerät der Klasse 3	27
7.4 Wartung	27
7.5 Schnittstellen	28
7.6 Änderungen	28
7.7 Ausfall der Energieversorgung	28
7.8 Auswahl vorgefertigter Komponenten	28
7.9 Auslegungsdokumentation	29
8 Verifizierung und Validierung	30

8.1	Verifizierung und Validierung von Gerät der Klassen 1 und 2	30
8.1.1	Allgemeines.....	30
8.1.2	Verifizierungsplan.....	30
8.1.3	Unabhängigkeit der Verifizierung	31
8.1.4	Methoden	31
8.1.5	Dokumentation	32
8.1.6	Unstimmigkeiten.....	32
8.1.7	Änderungen.....	32
8.1.8	Errichtungsverifizierung.....	33
8.1.9	Validierung	33
8.1.10	Verifizierung von vorgefertigten Geräteplattformen	33
8.2	Verifizierung und Validierung von Gerät der Klasse 3	33
9	Qualifizierung	34
10	Produktion	34
10.1	Qualitätsmanagement	34
10.2	Ausbildung des Personals.....	35
10.3	Planung und Organisation der Herstellungsaktivitäten	35
10.4	Eingaben	35
10.5	Einkauf und Beschaffung	36
10.5.1	Einkaufs- und Beschaffungsvorgang	36
10.5.2	Beschaffungsvorgang bezüglich kommerziell verfügbarer Komponenten.....	36
10.5.3	Beschaffungsvorgang bezüglich im leittechnischen System verwendeter Teile	37
10.5.4	Verifizierung des zugekauften Produkts	37
10.6	Produktion	39
10.6.1	Produktionsüberwachung.....	39
10.6.2	Spezifikation und Überwachung der Umgebungsbedingungen während der Produktion	39
10.6.3	Validierung der Produktionsprozesse	40
10.6.4	Feststellung der Akzeptanz und Reproduzierbarkeit des hergestellten leittechnischen Geräts.....	40
10.6.5	Kontrolle der Produktionswerkzeuge, Überwachungs- und Messgeräte	41
10.6.6	Identifizierung und Rückverfolgbarkeit.....	41
10.6.7	Konservierung des Produkts	42
10.6.8	Erhalt der Werkzeuge und Fähigkeiten.....	42
10.6.9	Auflösung und Überwachung von Nonkonformitäten	42
11	Errichtung und Inbetriebnahme	43
12	Wartung	43
12.1	Wartungsanforderungen	43
12.2	Ausfalldaten.....	44
12.3	Wartungsdokumentation	45

13	Änderungen	45
14	Betrieb	46
Anhang A (informativ) Überblick über den Systemlebenszyklus		47
Anhang B (informativ) Übersicht über den Qualifizierungsvorgang		48
Anhang C (informativ) Beispiel einer Wartungsprozedur		49
Literaturhinweise		50

Einleitung

a) Technischer Hintergrund, hauptsächliche Inhalte und Organisation der Norm

Diese Internationale Norm stellt Anforderungen zu Hardwareaspekten für leittechnische Systeme, die Sicherheitsfunktionen nach IEC 61226 ausführen.

Sie ist konsistent mit IEC 61513:2011 und ergänzt diese. Aktivitäten, die hauptsächlich auf Systemebene erfolgen (z. B. Integration, Validierung und Installation) werden in diesem Dokument nicht erschöpfend behandelt: Zu Anforderungen, die nicht hardwarespezifisch sind, wird auf IEC 61513:2011 verwiesen.

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 IAEA Guide SSG-39 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:

- der Einsatz verschiedener Systemplattformen, die konventionell fest-verdrahtete Geräte, programmierbare digitale Geräte oder eine Kombination beider Arten umfassen;
- IEC 61226 und IEC 61513 decken die leittechnische Systeme für Funktionen drei verschiedener Kategorien (A, B und C) und drei Klassen von Systemen (Klassen 1, 2 und 3) ab;
- der Einsatz vorgefertigter 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 leittechnische 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 leittechnischen 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 IEC 60987 verwiesen.

IEC 62566-1 und IEC 62566-2 sind Normen der zweiten Ebene und decken zusammen die HDL-Aspekte rechnerbasierter Systeme ab, die zur Ausführung sicherheitstechnisch wichtiger Funktionen in Kernkraftwerken verwendet werden. In IEC 62566-1 und IEC 62566-2 wird für die Hardwareauslegung direkt auf IEC 60987 verwiesen.

Bezüglich der Anforderungen zur Qualifizierung wird in der vorliegenden Norm auf IEC/IEEE 60780-323 verwiesen.

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 klassifizierte Systeme definiert werden (zu Anforderungen bezüglich der Systemklassifizierung siehe IEC 61226).

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

- eine allgemeine Vorgehensweise zur Hardware-Entwicklung;
- eine allgemeine Vorgehensweise zur Hardware-Verifizierung und zu den Hardwareaspekten der Systemvalidierung.

Es ist klar, dass sich die Leittechniktechnologie 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, ist es möglich, ihre Eignung durch Adaption der in dieser Norm enthaltenen Auslegungsprinzipien zu beurteilen.

Der Anwendungsbereich dieser Norm deckt die Hardware leittechnischer Systeme in Systemen aller Sicherheitsklassen ab. Dies umfasst konventionell fest-verdrahtete Geräte, programmierbare digitale Geräte oder eine Kombination beider Arten, 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)

Die Eingangsdokumente der Dokumente des IEC/SC 45A sind IEC 61513 und IEC 63046. IEC 61513 enthält allgemeine Anforderungen an die leittechnischen Systeme und Geräte, die zur Ausführung sicherheitstechnisch wichtiger Funktionen in Kernkraftwerken genutzt werden. IEC 63046 enthält allgemeine Anforderungen für die Stromversorgungssysteme von Kernkraftwerken, sowohl Stromversorgungssysteme wie auch die Versorgungssysteme der leittechnischen Systeme. Durch IEC 61513 und IEC 63046 werden die Normen des IEC/SC 45A strukturiert, und sie bilden einen vollständigen Rahmen allgemeiner Anforderungen elektro- und leittechnischer Systeme für Kernkraftwerke.

In IEC 61513 und IEC 63046 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, Maßnahmen gegen Versagen aufgrund gemeinsamer Ursache, Auslegung von Warten, Elektromagnetische Verträglichkeit, Cybersecurity, Software- und Hardwareaspekte programmierbarer digitaler Systeme, die Koordination von Sicherheit und IT-Sicherheit sowie das Alterungsmanagement behandeln. Die Normen, die auf dieser zweiten Ebene direkt angezogen werden, sollten zusammen mit IEC 61513 und IEC 63046 als ein in sich konsistenter Satz von Dokumenten betrachtet werden.

Die dritte Ebene bilden Normen des IEC/SC 45A, auf die in IEC 61513 bzw. IEC 63046 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 um Technische Berichte, die nicht normativ sind.

In den Normen des IEC/SC 45A werden die Prinzipien und grundsätzlichen Aspekte der Sicherheit und IT-Sicherheit der IAEA-Sicherheitsstandards und der relevanten Dokumente der IAEA-Standards zur nuklearen IT-Sicherheit (NSS) umgesetzt. Dies betrifft insbesondere Anforderungen des IAEA Safety Standards SSR-2/1, in dem die Sicherheitsanforderungen für die Auslegung von Kernkraftwerken festgeschrieben werden, und der IAEA Safety Guides SSG-30 für die Sicherheitsklassifikation der Strukturen, Systeme und Komponenten in Kernkraftwerken, SSG-39 für die Auslegung der Leittechnik in Kernkraftwerken und SSG-34 für die Auslegung der Stromversorgung in Kernkraftwerken und des IAEA Implementing Guides NSS 17 für die IT-Sicherheit von Rechnern in kerntechnischen Anlagen. Terminologie und Definitionen in den Normen des IEC/SC 45A sind konsistent mit denen, die von der IAEA verwendet werden.

Für IEC 61513 und IEC 63046 wird ein Darstellungsformat verwendet, das dem der grundlegenden Sicherheitsnorm IEC 61508 ähnlich ist, mit einem Lebenszyklus als Gesamtrahmen und einem Systemlebenszyklus. Mit IEC 61513 und IEC 63046 werden die allgemeinen Anforderungen von IEC 61508-1, IEC 61508-2 und IEC 61508-4 für die Anwendung auf dem nuklearen Sektor umgesetzt. In diesem Rahmen entsprechen IEC 60880, IEC 62138 und IEC 62566 bezogen auf den nuklearen Sektor der IEC 61508-3. IEC 61513 und IEC 63046 beziehen sich bei den Themen der Qualitätssicherung (QS) sowohl auf ISO als auch auf IAEA GS-R-3, IAEA GS-G-3.1 und IAEA GS-G-3.5. Auf Ebene 2 ist IEC 62645 das Eingangsdokument für die Normen des IEC/SC 45A zur IT-Sicherheit. Es baut auf die übergeordneten Prinzipien und Hauptkonzepte

der generischen IT-Sicherheitsstandards auf, insbesondere auf ISO/IEC 27001 und ISO/IEC 27002; wobei es jene für die Anwendung im nuklearen Kontext adaptiert und vervollständigt sowie mit IEC 62443 koordiniert. Auf Ebene 2 ist IEC 60964 das Eingangsdokument für die Normen des IEC/SC 45A zu Warten, und IEC 62342 das Eingangsdokument für die Normen des IEC/SC 45A zum Alterungsmanagement.

ANMERKUNG 1 Es wird angenommen, dass für die Auslegung von leittechnischen Systemen in Kernkraftwerken, die konventionelle Sicherheitsfunktionen enthalten (z. B. in Bezug auf Arbeitssicherheit, Schutz von Vermögenswerten, chemische und prozesstechnische Gefährdungen), internationale und nationale Normen angewendet werden.

ANMERKUNG 2 Arbeitsbereich des IEC/SC 45A wurde 2013 erweitert, um auch elektrische Systeme abzudecken. In den Jahren 2014 und 2015 wurde in IEC/SC 45A diskutiert, wie und wo allgemeine Anforderungen für die Auslegung elektrischer Systeme behandelt werden sollten. Die Experten des IEC/SC 45A empfahlen, eine selbständige Norm auf derselben Ebene wie IEC 61513 zu entwickeln und allgemeine Anforderungen für elektrische Systeme aufzustellen. Dazu wurde jetzt das Projekt IEC 63046 gestartet. Sobald IEC 63046 veröffentlicht wird, verliert diese Anmerkung 2 der Einleitung der Normen des IEC/SC 45A ihre Gültigkeit.

**Kernkraftwerke –
Leittechnische Systeme mit sicherheitstechnischer Bedeutung –
Anforderungen an die Hardware-Auslegung**

1 Anwendungsbereich

1.1 Allgemeines

Sicherheitswichtige leittechnische Systeme können mit konventionell fest-verdrahteten Geräten, programmierbaren digitalen Geräten oder einer Kombination beider Arten ausgeführt werden.

Diese Internationale Norm enthält Anforderungen und Empfehlungen für die Auslegung und Produktion von Hardware jeder Art von Systemen aller Sicherheitsklassen (wie in IEC 61513 definiert).

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); Verweisungen auf neue Normen wurden, wo zutreffend, eingeführt. Der Text der Norm wurde auch überarbeitet, um neuen Entwicklungen der Auslegung von fest-verdrahteten Geräten und programmierbaren digitalen Geräten, der Anwendung vorgefertigter Hardware (z. B. am Markt erhältlicher Produkte (COTS)) und Veränderungen in der Terminologie Rechnung zu tragen.

Werkzeuge, die zum Laden und Überprüfen von Software oder HDL verwendet werden, werden nicht als eigentlicher Teil eines sicherheitstechnisch wichtigen Systems erachtet und fallen daher nicht in den Anwendungsbereich dieser Norm.

Die Anforderungen für Softwarewerkzeuge, die für Hardwarekomponenten während der Entwicklung, Verifizierung und Validierung verwendet werden, sind in IEC 61513 und IEC 62566 angegeben und sind zu beachten.

Werkzeuge, die zum Laden und Überprüfen von Software oder HDL verwendet werden, fallen daher nicht in den Anwendungsbereich dieser Norm. IEC 60880 und IEC 62566 geben Anforderungen und Anleitungen für die Beurteilung von Werkzeugen.

1.2 Anwendung der Norm für die Beurteilung vorgefertigter Hardware

Der in dieser Norm definierte Prozess ist eine Anleitung für die Beurteilung und Anwendung vorgefertigter Hardware (z. B. am Markt erhältlicher Produkte (COTS)). Im Text sind Hinweise zur Interpretation der Anforderungen dieser Norm für die Beurteilung solcher Komponenten vorgesehen.

Vorgefertigte Komponenten können Mikrocontroller oder HPD-Hardware enthalten und, wenn Firmware oder Programme eingebettet 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 eingebettet ist, muss nach den Anforderungen der relevanten Softwarenormen (z. B. IEC 60880 für Systeme der Klasse 1 und IEC 62138 für Systeme der Klassen 2 und 3) entwickelt oder beurteilt werden.

Auf die gleiche Weise werden elektronische Komponenten, die nicht konventionell sind (nicht änderbar, nicht konfigurierbar und transparent für die Anwender) oder Funktionen eines HPD, die keine nativen Blocks sind, entsprechend den Anforderungen der relevanten HPD-Norm entwickelt und bewertet (z. B. nach IEC 62566-1 für Systeme der Klasse 1, IEC 62566-2 für Systeme der Klassen 2 und 3).

1.3 Anwendbarkeit dieser Norm für die Entwicklung programmierbarer logischer Einheiten (HPDs)

Leittechnische Komponenten können programmierbare logische Einheiten (HPDs) enthalten, deren spezifische anwendungsbezogene Auslegung der Logik vom Konstrukteur der leittechnischen Komponente stammt, nicht vom Chip-Hersteller. Beispiele solcher Einheiten sind programmierbare logische Einrichtungen (PLDs),

komplexe programmierbare logische Einrichtungen (CPLDs) und vor Ort programmierbare Gatter-Anordnungen (FPGAs).

IEC 60987 ist nicht auf die Entwicklung für HPDs anzuwenden.

Die Entwicklung von eingebetteten HPDs der Klasse 1 muss nach IEC 62566-1 erfolgen.

Die Entwicklung von eingebetteten HPDs der Klassen 2 und 3 muss nach IEC 62566-2 erfolgen.

2 Normative Verweisungen

Die folgenden Dokumente werden im Text in solcher Weise in Bezug genommen, dass einige Teile davon oder ihr gesamter Inhalt Anforderungen des vorliegenden Dokuments darstellen. 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/IEEE 60780-323, *Nuclear power plants – Electrical equipment of the safety system – Qualification*

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

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

IEC 60880, *Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category A functions*

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

IEC 61000 (all parts), *Electromagnetic compatibility (EMC)*

IEC 61025, *Fault tree analysis (FTA)*

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

IEC 62003, *Nuclear power plants – Instrumentation and control important to safety – Requirements for electromagnetic compatibility testing*

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

IEC/TR 62380, *Reliability Data Handbook – Universal Model for Reliability Prediction of Electronics Components, PCBs and Equipment*

IEC 62566-1^{N1)}, *Nuclear power plants – Instrumentation and control important for safety – Development of HDL-programmed integrated circuits for systems performing category A functions*

IEC 62566-2, *Nuclear power plants – Instrumentation and control important for safety – Development of HDL-programmed integrated circuits – Part2: HDL-programmaed integrated circuits for systems performing category B or C functions*

IEC 62671, *Nuclear power plants – Instrumentation and control important to safety – Selection and use of industrial digital devices of limited functionality*

ISO 2859-10, *Sampling procedures for inspection by attributes – Part 10: Introduction to the ISO 2859 series of standards for sampling for inspection by attributes*

ISO 9001, *Quality management systems – Requirements*

^{N1)} Nationale Fußnote: Zurzeit veröffentlicht als IEC 62566:2012.

IAEA SSG-39, *Design of Instrumentation and Control Systems for Nuclear Power Plants*

IAEA SSR-2/1, *Safety of Nuclear Power Plants: Design*

IPC-A-610, *Acceptability of Electronic Assemblies*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach IEC 61513 und die folgenden Begriffe.

3.1

Klasse eines leittechnischen Systems

(en: class of an I&C system)

eine von drei möglichen Zuordnungen (1., 2 3) eines sicherheitswichtigen leittechnischen Systems entsprechend der durch dieses zu implementierenden leittechnischen Funktionen verschiedener sicherheitstechnischer Bedeutung

Anmerkung 1 zum Begriff: Wenn das Leittechnik keine sicherheitsrelevante Funktion implementiert, wird keine Klasse zugeordnet.

Anmerkung 2 zum Begriff: Siehe auch „Kategorie einer leittechnischen Funktion“, „sicherheitstechnisch wichtige Einrichtung“, „Sicherheitssystem“.

3.2

Ausfall aufgrund gemeinsamer Ursache

(en: common cause failure)

CCF

Ausfall einer oder mehrerer Strukturen, Systeme oder Komponenten aufgrund eines einzigen spezifischen Ereignisses oder Grunds

[QUELLE: IAEA Safety Glossary: 2007]

Anmerkung 1 zum Begriff: Die gemeinsame Ursache kann sowohl innerhalb als auch außerhalb des leittechnischen Systems liegen.

Anmerkung 2 zum Begriff: Die IEC-Definition weicht in zwei Punkten von der der IAEA ab:

- „specific“ wurde gestrichen, da ansonsten die Definition des CCF nicht konsistent mit der des CMF (common mode failure) ist. Zudem ist dieses zusätzliche Wort für das Verständnis der Definition nicht erforderlich.
- „and“ wurde durch „or“ ersetzt, da die Experten des IEC/SC 45A der Auffassung sind, dass hier ein Druckfehler vorliegt. Im IAEA Online Dictionary (NUSAFE) ist diese Korrektur bereits erfolgt.

3.3

Komponente

(en: component)

einer der Teile, aus dem ein System besteht

[QUELLE: IEC 61513]

Anmerkung 1 zum Begriff: Eine Komponente kann aus Hardware, Software oder HPD bestehen und in weitere Komponenten unterteilt werden.

Anmerkung 2 zum Begriff: Siehe auch „leittechnisches System“, „Gerät“.

Anmerkung 3 zum Begriff: Die Begriffe „Gerät“, „Komponente“, „Modul“ und „Produkt“ sind oft austauschbar. Unterschiede und Zusammenhang dieser Begriffe sind bislang in keiner Norm verbindlich festgelegt.

Anmerkung 4 zum Begriff: Diese IEC/SC-45A-Definition ist prinzipiell mit der im Rahmen der Erläuterung zu „Structures, Systems and Components (SCC)“ gegebenen Definition im IAEA Safety Glossary 2007 kompatibel. Da allerdings dort nur Beispiele von Hardwarekomponenten genannt werden, kann beim Leser ein Missverständnis entstehen; aus diesem Grund zieht SC 45A eine Definition vor, die ausdrücklich Softwarekomponenten mit abdeckt.

3.4

rechnerbasiertes Gerät

(en: computer-based item)

Gerät, das auf Softwareanweisungen basiert, die auf Mikroprozessoren oder Mikrocontrollern laufen

Anmerkung 1 zum Begriff: In Benennung und Definition dieses Begriffs kann „Gerät“ durch „System“, „Einrichtung“ oder „Anordnung“ ersetzt werden.

Anmerkung 2 zum Begriff: Ein rechnerbasiertes Gerät ist eine Art von programmierbarem digitalem Gerät.

Anmerkung 3 zum Begriff: Der Begriff ist gleichwertig mit software-basiertem Gerät.

Anmerkung 4 zum Begriff: Die Definitionen folgender Begriffe müssen gemeinsam gesehen werden und sind vollständig konsistent und kohärent: E/E/PE-Gerät, elektrisches Gerät, leittechnisches System, programmierbares digitales Gerät, rechnerbasiertes Gerät, fest-verdrahtetes Gerät, programmierbare Logikanordnung, HDL-programmiertes Gerät (HPD). Sie sind auch vollständig konsistent und kohärent mit den allgemeinen Anforderungen nach IEC 61513 und IEC 63046 für elektrische und leittechnische Systeme von Kernkraftwerken.

3.5

elektrisches/elektronisches/programmierbares elektronisches Gerät

E/E/PE-Gerät

(en: electrical/electronic/programmable electronic item)

E/E/PE item

Gerät, das auf elektrischer (E), elektronischer (E) und/oder programmierbarer elektronischer (PE) Technologie beruht

[QUELLE: IEC 61508:2008]

Anmerkung 1 zum Begriff: In Benennung und Definition dieses Begriffs kann „Gerät“ durch „System“, „Einrichtung“ oder „Anordnung“ ersetzt werden.

Anmerkung 2 zum Begriff: Die Definitionen folgender Begriffe müssen gemeinsam gesehen werden und sind vollständig konsistent und kohärent: E/E/PE-Gerät, elektrisches Gerät, leittechnisches System, programmierbares digitales Gerät, rechnerbasiertes Gerät, fest-verdrahtetes Gerät, programmierbare Logikanordnung, HDL-programmiertes Gerät (HPD). Sie sind auch vollständig konsistent und kohärent mit den allgemeinen Anforderungen nach IEC 61513 und IEC 63046 für elektrische und leittechnische Systeme von Kernkraftwerken.

3.6

elektrisches Energiesystem

(en: electrical power system)

System für die Erzeugung, Übertragung und Verteilung elektrischer Energie, mit der die leittechnischen Systeme der Anlage versorgt und andere Geräte der Anlage betrieben werden (Pumpen, Ventile, Heizer usw.)

Anmerkung 1 zum Begriff: Ein elektrisches System kann E/E/PE-Geräte beinhalten, mit denen seine interne elektrische Steuerung und sein Schutz realisiert werden.

3.7

Gerät

(en: equipment)

einer oder mehrere Teile eines Systems.

[QUELLE: IEC 61513]

Anmerkung 1 zum Begriff: Ein Gerät ist ein einzeln definierbares (üblicherweise austauschbares) Element oder Teil eines Systems.

Anmerkung 2 zum Begriff: Siehe auch „Komponente“, „leittechnisches System“.

Anmerkung 3 zum Begriff: Gerät kann Software beinhalten.

Anmerkung 4 zum Begriff: Die Benennungen „Gerät“, „Komponente“ und „Modul“ werden oft synonym verwendet. Das Verhältnis dieser Benennungen ist bisher nicht normiert.

Anmerkung 5 zum Begriff: Die Definition weicht von der der IEC/IEEE 60780-323 ab. Die Abweichung ist in dem Umstand begründet, dass IEC 61513 „Gerät“ als Teil eines Systems ansieht, während IEC/IEEE 60780-323 „Gerät“ als zu qualifizierendes Objekt ansieht.

3.8

Firmware

(en: firmware)

auf Hardware installierte Software, die eng an Eigenschaften der Hardware gekoppelt ist

Anmerkung 1 zum Begriff: Das Bestehen von Firmware ist für den Nutzer der Hardwarekomponente im Allgemeinen „transparent“ und kann daher effektiv als ein integraler Teil der Hardwareauslegung betrachtet werden (ein gutes Beispiel einer solchen Software ist Prozessor-Mikrocode).

Anmerkung 2 zum Begriff: Im Allgemeinen kann Firmware durch einen Benutzer nur modifiziert werden, indem die entsprechenden Hardwarekomponenten (z. B. Prozessorchip, Karte, EPROM), die diese Software enthalten, gegen Komponenten mit modifizierter Software (Firmware) ausgetauscht werden. Wo dies der Fall ist, wird über die Konfigurationskontrolle der Hardwarekomponenten durch den Benutzer auch eine effektive Konfigurationskontrolle der Firmware erreicht. Firmware, wie sie in dieser Norm verstanden wird, ist im Endeffekt in die Hardware fest eingebaute Software.

3.9

Funktion

(en: function)

spezifischer Zweck oder spezifisches Ziel, das zu erreichen ist, sie kann spezifiziert oder ohne Bezug auf die physikalischen Mittel, mit denen sie erreicht wird, beschrieben werden

3.10

fest-verdrahtetes Gerät

fest-verdrahtetes Element

(en: hardwired item)

Element, das auf Relais, analoger Elektronik oder diskreter digitaler Logik beruht

Anmerkung 1 zum Begriff: In dieser Definition kann „Element“ durch „System“, „Gerät“ und „Einrichtung“ ersetzt werden.

Anmerkung 2 zum Begriff: Dieser in IEC/SC 45A verwendete Begriff entspricht in etwa dem elektronischen Element, wie es in IEC 61508 verwendet wird. Relais sind elektromechanische Elemente, keine elektronischen, sind aber in die Definition des fest-verdrahteten Elements eingeschlossen.

Anmerkung 3 zum Begriff: Fest-verdrahtetes Element wird auch als konventionelles Element bezeichnet.

Anmerkung 4 zum Begriff: Die Definitionen folgender Begriffe müssen gemeinsam gesehen werden und sind vollständig konsistent und kohärent: E/E/PE-Gerät, elektrisches Gerät, leittechnisches System, programmierbares digitales Gerät, rechnerbasiertes Gerät, fest-verdrahtetes Gerät, programmierbare Logikanordnung, HDL-programmiertes Gerät (HPD). Sie sind auch vollständig konsistent und kohärent mit den allgemeinen Anforderungen nach IEC 61513 und IEC 63046 für elektrische und leittechnische Systeme von Kernkraftwerken.

3.11

Hardware-Beschreibungssprache

HDL

(en: Hardware Description Language)

Sprache, die dazu verwendet wird, die Funktionen und/oder die Struktur einer elektronischen Komponente für Dokumentation, Simulation oder Synthese formal zu beschreiben

Anmerkung 1 zum Begriff: Die verbreitetsten Hardware-Beschreibungssprachen sind VHDL (IEEE 1076) und Verilog (IEEE 1364)..

[QUELLE: IEC 62566^{N2)}]

3.12

HDL-programmierte Baugruppe

HPD

(en: HDL-programmed device)

integrierter Schaltkreis, der unter Verwendung von Hardware-Beschreibungssprachen und zugehörigen Softwarewerkzeugen konfiguriert wird

[QUELLE: IEC 62566]

^{N2)} Nationale Fußnote: Im IEC-Entwurf ist hier fälschlich IEC 61513 angegeben.

Anmerkung 1 zum Begriff: HDLs und zugehörige Werkzeuge (z. B. Simulatoren, Synthesizer) werden verwendet, um die Anforderungen in eine geeignete Anordnung von vor-entwickelten mikro-elektronischen Ressourcen zu implementieren.

Anmerkung 2 zum Begriff: Bei der Entwicklung von HPDs können vor-entwickelte Blöcke verwendet werden.

Anmerkung 3 zum Begriff: HPDs basieren typischerweise auf blanken FPGAs, PLDs oder ähnlichen mikro-elektronischen Technologien.

Anmerkung 4 zum Begriff: HPD ist eine Art von programmierbarem digitalem Gerät.

Anmerkung 5 zum Begriff: Die Definitionen folgender Begriffe müssen gemeinsam gesehen werden und sind vollständig konsistent und kohärent: E/E/PE-Gerät, elektrisches Gerät, leittechnisches System, programmierbares digitales Gerät, rechnerbasiertes Gerät, fest-verdrahtetes Gerät, programmierbare Logikanordnung, HDL-programmiertes Gerät (HPD). Sie sind auch vollständig konsistent und kohärent mit den allgemeinen Anforderungen nach IEC 61513 und IEC 63046 für elektrische und leittechnische Systeme von Kernkraftwerken.

3.13

leittechnisches System

(en: I&C system)

auf elektrischer und/oder elektronischer und/oder programmierbarer elektronischer Technologie beruhendes System, das sowohl leittechnische Funktionen als auch auf sich selbst bezogene Dienstleistungs- und Überwachungsfunktionen ausführt

Anmerkung 1 zum Begriff: Der Begriff wird allgemein verwendet und umfasst alle Elemente des Systems wie interne Energieversorgung, Messfühler und andere Eingangsgeräte, Datenbusse und andere Kommunikationspfade, Schnittstellen zu den Betätigungsgliedern und anderen Ausgangsgeräten. Die verschiedenen Funktionen in einem System können strikt zugeordnete oder gemeinsame Ressourcen verwenden.

Anmerkung 2 zum Begriff: Siehe auch „System“, „leittechnische Funktion“.

Anmerkung 3 zum Begriff: Die zu einem spezifischen leittechnischen System gehörenden Elemente sind durch die Spezifikation der Systemgrenzen definiert.

Anmerkung 4 zum Begriff: Entsprechend ihrer typischen Funktionalität unterscheidet IAEA zwischen Automatisierungs- und Steuerungs-/Regelsystemen, MMK-Systemen, Verriegelungssystemen und Schutzsystemen (siehe B.4).

[QUELLE: IEC 61513]

3.14

Integration

(en: integration)

fortschreitender Einbau und Verifizierung von Komponenten in ein vollständiges System

3.15

interner Block

(en: HPD native block)

Block, der in einem integrierten Schaltkreis eine vor-entwickelte Ressource darstellt, z. B. ein ODER-Gatter oder ein komplexerer Block wie ein Multiplier oder ein serieller Übertragungs-Controller.

Anmerkung 1 zum Begriff: Durch Programmieren der HPD werden die internen Blöcke konfiguriert und verbunden, um die gewünschte Funktion zu erzielen.

[QUELLE: IEC 62566]

3.16

vorgefertigt

(en: pre-developed)

bereits bestehendes, kommerziell oder in rechtlich geschützter Form verfügbares Produkt, das für die Verwendung in einem leittechnischen System in Betracht gezogen wird

Anmerkung 1 zum Begriff: Diese Definition ist mit der Definition von vorgefertigter Software in IEC 61513:2011 konsistent.

3.17

vorgefertigtes Element

(en: pre-existing items)

Hardware, fest-verdrahtetes oder programmierbares digitales Element, das als kommerziell oder in rechtlich geschützter Form verfügbares Produkt besteht und für die Verwendung in Betracht gezogen wird

Anmerkung 1 zum Begriff: Diese Definition schließt vorgefertigte Software oder HDL ein, siehe IEC 60880, IEC 62138, IEC 62566-1 und IEC 62566-2.

3.18

programmierbares digitales Element

(en: programmable digital item)

Element, das auf Programmanweisungen oder programmierbarer Logik beruht, um eine Funktion auszuführen

Anmerkung 1 zum Begriff: In dieser Definition kann „Element“ durch „System“, „Gerät“ und „Einrichtung“ ersetzt werden.

Anmerkung 2 zum Begriff: Die Hauptarten programmierbarer digitaler Elemente sind rechnerbasierte Elemente und programmierbare Logikeinheiten.

Anmerkung 3 zum Begriff: Dieser Begriff, der durch IEC/SC 45A benutzt wird, ist gleichbedeutend mit der programmierbaren digitalen Betrachtungseinheit (PE) wie sie in IEC 61508 definiert ist.

Anmerkung 4 zum Begriff: Die Definitionen folgender Begriffe müssen gemeinsam gesehen werden und sind vollständig konsistent und kohärent: E/E/PE-Gerät, elektrisches Gerät, leittechnisches System, programmierbares digitales Gerät, rechnerbasiertes Gerät, fest-verdrahtetes Gerät, programmierbare Logikanordnung, HDL-programmiertes Gerät (HPD). Sie sind auch vollständig konsistent und kohärent mit den allgemeinen Anforderungen nach IEC 61513 und IEC 63046 für elektrische und leittechnische Systeme von Kernkraftwerken.

[QUELLE: IEC 62138]

3.19

programmierbares logisches Element

(en: programmable logic device (PLD))

Element, das auf Logikkomponenten mit einem integrierten Schaltkreis, der aus Logikelementen mit einer Verbindungsstruktur besteht, beruht, wobei Teile davon durch die Nutzer programmierbar sind

Anmerkung 1 zum Begriff: Die Definitionen folgender Begriffe müssen gemeinsam gesehen werden und sind vollständig konsistent und kohärent: E/E/PE-Gerät, elektrisches Gerät, leittechnisches System, programmierbares digitales Gerät, rechnerbasiertes Gerät, fest-verdrahtetes Gerät, programmierbare Logikanordnung, HDL-programmiertes Gerät (HPD). Sie sind auch vollständig konsistent und kohärent mit den allgemeinen Anforderungen nach IEC 61513 und IEC 63046 für elektrische und leittechnische Systeme von Kernkraftwerken.

3.20

Qualifizierung

(en: qualification)

Vorgang, im Rahmen dessen die Eignung eines Systems oder einer Komponente für den betrieblichen Gebrauch bestimmt wird. Die Qualifizierung wird im Zusammenhang mit der spezifischen Klasse des leittechnischen Systems und einem entsprechenden Satz von Qualifizierungsanforderungen durchgeführt.

Anmerkung 1 zum Begriff: Die Qualifizierungsanforderungen leiten sich aus der spezifischen Klasse des leittechnischen Systems und seiner Verwendung ab.

Anmerkung 2 zum Begriff: Leittechnische Systeme werden üblicherweise auf der Grundlage miteinander agierender Gerätesätze realisiert. Derartiges Gerät kann im Rahmen des Projekts entwickelt werden oder es kann bereits verfügbares Gerät sein (d. h. entwickelt in einem früheren Projekt oder ein COTS-Produkt). Üblicherweise wird die Qualifizierung eines leittechnischen Systems in Stufen durchgeführt: zuerst durch Qualifizierung von individuellem bereits verfügbarem Gerät (gewöhnlich früh im Prozess der Systemrealisierung); in einem zweiten Schritt durch Qualifizierung des integrierten leittechnischen Systems (d. h. des endgültigen, realisierten Systems).

Anmerkung 3 zum Begriff: Die Qualifizierung von leittechnischen Systemen ist immer eine anlagen- und anwendungsspezifische Tätigkeit. Die Qualifizierung von leittechnischen Systemen ist immer eine anlagen- und anwendungsspezifische Tätigkeit. Sie kann jedoch in hohem Maß auf Qualifizierungsarbeiten beruhen, die nicht im Rahmen eines spezifischen Anlagenprojekts durchgeführt werden („generische Qualifizierung“ oder „Vorqualifizierung“ genannt). Vorqualifizierung kann

den Aufwand für anlagenspezifische Qualifizierung erheblich reduzieren, es muss jedoch gezeigt werden, dass die anwendungsbezogenen Qualifizierungsanforderungen nach wie vor eingehalten werden.

3.21

qualifizierte Lebensdauer

(en: qualified life)

Zeitspanne, für die durch Prüfungen, Analysen und Erfahrung nachgewiesen wurde, dass eine Struktur, ein System oder eine Komponente innerhalb bestimmter Akzeptanzkriterien bei speziellen Betriebsbedingungen funktionsfähig ist und die Fähigkeit behält, ihre/seine Sicherheitsfunktionen bei einem Auslegungsstörfall oder bei Erdbeben auszuführen

[QUELLE: IAEA Safety Glossary:2007]

3.22

Zufallsfehler

(en: random fault)

nicht-systematischer Fehler von Hardwarekomponenten

Anmerkung 1 zum Begriff: Fehler von Hardwarekomponenten aufgrund physikalischer oder chemischer Effekte, die zu irgendeinem Zeitpunkt auftreten können. Eine gute Beschreibungsmöglichkeit für das Eintreten zufälliger Fehler ist mit Hilfe statistischer Verfahren möglich (Fehlerrate). Erhöhte Fehlerraten können die Folge systematischer Fehler bei der Hardwareauslegung oder -herstellung sein, wenn diese ohne zeitliche Korrelation auftreten, wie z. B. als eine Folge von vorzeitiger Alterung.

[QUELLE: IEC 62340]

3.23

Sicherheitsfunktion

(en: safety function)

für das Erreichen der wesentlichen Sicherheitsziele in den verschiedenen Anlagenzuständen, einschließlich aller Betriebsarten des Normalbetriebs, erforderliche Funktion

3.24

sicherheitsrelevantes System

(en: safety-related system)

sicherheitstechnisch wichtiges System, das nicht Teil des Sicherheitssystems ist

[QUELLE: IAEA Safety Glossary:2007]

3.25

Sicherheitssystem

(en: safety system)

sicherheitstechnisch wichtiges System, das für die Sicherstellung der Reaktorabschaltung oder der Abfuhr der Restwärme aus dem Kern oder der Begrenzung von Folgen anzunehmender betrieblicher Ereignisse und Auslegungsstörfällen vorgesehen ist

[QUELLE: IAEA Safety Glossary:2007]

3.26

System

(en: system)

Satz entsprechend einer Auslegung interagierender Komponente, wobei ein System Teil eines anderen Systems sein kann, genannt Teilsystem

[QUELLE: IEC 61508-4:2010, 3.3.1, modifiziert]

Anmerkung 1 zum Begriff: Siehe auch „leittechnisches System“.

Anmerkung 2 zum Begriff: Leittechnische Systeme sind von mechanischen Systemen und elektrischen Energiesystemen des Kernkraftwerks zu unterscheiden.

Anmerkung 3 zum Begriff: Diese Definition des IEC/SC 45A ist mit der Teildefinition des „Systems“ in der Definition von „structures, systems and components (SCC)“ des IAEA Safety Glossary:2007 kompatibel.

3.27

Systemvalidierung

(en: system validation)

Bestätigung durch Prüfung und Nachweis, dass ein System in seiner Gesamtheit die Anforderungsspezifikation wie vorgesehen erfüllt

[QUELLE: IEC 60880]

3.28

unentdeckter Hardwareausfall

(en: unrevealed hardware failure)

Hardwareausfall, der durch das System nicht automatisch entdeckt wird und der nur offensichtlich wird, wenn versucht wird, eine Funktion zu nutzen, die von der ausgefallenen Hardware abhängt

Anmerkung 1 zum Begriff: Solche Ausfälle können durch Funktionsprüfungen entdeckt werden oder wenn eine entsprechende betriebliche Anforderung erfolgt.

3.29

Verifizierung

(en: verification)

Bestätigung durch Prüfung und durch Beibringung objektiver Nachweise, dass die Resultate einer Tätigkeit die Ziele und Anforderungen erfüllen, die für diese Tätigkeit definiert wurden

[QUELLE: IEC 61513]

Anmerkung 1 zum Begriff: Im IAEA Safety Glossary:2007 sind folgende Definitionen zu finden:

Validierung: Der Nachweisprozess, ob ein Produkt oder eine Dienstleistung geeignet ist, um seine (ihre) beabsichtigte Funktion zufriedenstellend auszuführen. Validierung ist breiter angelegt und kann einen größeren Anteil Beurteilung beinhalten als die Verifizierung.

Rechnersystem-Validierung: Der Prozess von Prüfung und Beurteilung des integrierten Rechnersystems (Hardware und Software), um Übereinstimmung mit den Funktions-, Leistungsfähigkeits- und Schnittstellenanforderungen sicherzustellen.

Die Definition „Systemvalidierung“ stellt einen Spezialfall dar. Sie bezieht sich auf ein spezifisches Produkt, nämlich die Validierung eines leittechnischen Systems, stimmt also mit der IAEA-Definition überein. Außerdem wird in der IEC-Definition die Referenz der Validierung spezifiziert, nämlich die Anforderungsspezifikation, wohingegen sich die IAEA-Definition lediglich auf „beabsichtigte Funktion“ bezieht.

4 Symbole und Abkürzungen

	Englisch	Deutsch
ATE	automated test equipment	automatisches Prüfgerät
COTS	commercial off the shelf	kommerziell verfügbar
FMEA	failure modes and effects analysis	Ausfallart- und -effektanalyse
FTA	fault tree analysis	Fehlerbaumanalyse
HDL	Hardware Description Language	Hardware-Beschreibungssprache
HPD	HDL-programmed device	HDL-programmierte Baugruppe
NPP	nuclear power plant	Kernkraftwerke

5 Projektstruktur

5.1 Allgemeines

5.1.1 Für Gerät aller Klassen sollte ein Projekt, das zur Erstellung eines sicherheitstechnisch wichtigen leittechnischen Systems eingerichtet wird, in mehrere Phasen unterteilt werden.

5.1.2 Jede Phase sollte in gewissem Ausmaß in sich abgeschlossen sein, wird jedoch hinsichtlich ihrer Eingangsdaten von anderen Phasen abhängig sein und umgekehrt ihre Ausgangsdaten für weitere Phasen zur Verfügung stellen.

ANMERKUNG 1 Die verschiedenen Projektphasen zusammen bilden den gesamten Lebenszyklus (siehe IEC 61513, Abschnitt 5, in dem Anforderungen für Systemlebenszyklen enthalten sind). Nach IEC 61513 ist es erlaubt, Projektphasen parallel durchzuführen, vorausgesetzt, die Integrität des Entwicklungsprozesses wird dadurch nicht beeinträchtigt.

5.2 Projektunterteilung

Für Gerät der Klassen 1 und 2 werden die allgemeinen Anforderungen für den Lebenszyklus der Hardwareentwicklung eines leittechnischen Systems im Rahmen des Anwendungsbereichs dieser Norm definiert.

5.2.1 Der Lebenszyklus der Hardwareentwicklung muss mit dem gesamten Systemlebenszyklus kompatibel sein (Anhang A).

5.2.2 Jede Teilphase des Lebenszyklus der Hardwareentwicklung muss aus wohldefinierten und dokumentierten Tätigkeiten bestehen.

5.2.3 Vorgefertigte Hardware (z. B. am Markt erhältliche Produkte), die in der Auslegung Verwendung finden, müssen vor ihrem Einsatz geeignet überprüft, verifiziert und getestet werden.

5.2.4 Es müssen geeignete Mittel (d. h. Ersatzteile, Einrichtungen zur Prüfung und Wartung usw.) und Räumlichkeiten (d. h. Laboratorien, Werkstätten, ausreichendes Platzangebot usw.) für die Ausführung der Aufgaben in jeder Phase vorgesehen sein.

5.2.5 Jede Phase muss entsprechend dokumentiert werden.

5.2.6 Jede Phase muss mit der Durchführung einer Verifizierung abgeschlossen werden (siehe Abschnitt 8).

5.2.7 Jeder Verifizierungsschritt muss mit auditierbaren Aufzeichnungen enden, in denen die erzielten Schlussfolgerungen und alle Änderungen, die aus der Verifizierung resultieren, dokumentiert werden.

5.2.8 Alle Arbeitsschritte müssen eingeplant werden, um sicherzustellen, dass für folgende Tätigkeiten genügend Zeit zur Verfügung steht:

- die Auflösung jedweder Wechselwirkung zwischen den Hardware- und HPD- oder Softwareentwicklungsphasen, die für die Sicherstellung der Kompatibilität zwischen Systemhardware und -software bzw. -HPD erforderlich ist;
- die Erstellung der Dokumentation und die Durchführung der Prüfungs-, Verifizierungs- und Qualitätssicherungstätigkeiten.

5.3 Qualitätsmanagement

5.3.1 Für Gerät aller Klassen muss der Auslegungs- und Entwicklungsprozess den relevanten Anforderungen von IEC 61513 genügen.

5.3.2 Ein Hardware-Qualitätssicherungsplan muss entweder als separates Dokument (oder eine Reihe mehrerer Dokumente) oder als Teil eines gesamten Qualitätssicherungsplans verfügbar sein.

5.3.3 Der Qualitätssicherungsplan muss je nach Notwendigkeit die Nutzung vorgefertigter Hardware und die Entwicklung von Hardware ansprechen.

ANMERKUNG 1 Die Anforderungen des Qualitätssicherungsplans für Software- oder HDP-Entwicklungen sind in IEC 60880, 5.5, IEC 62138, 6.2.1, IEC 62566-1, 5.4 und IEC 62566-2, 5.4 angegeben.

5.3.4 Dabei sollten alle Tätigkeiten die Hardwarequalität betreffend, die von Anlagenbetreiber, Eigentümer, Lieferanten und Unterlieferanten als Teil des Hardwareentwicklungsprozesses auszuführen sind, in den Qualitätssicherungsplan mit eingeschlossen werden.

5.3.5 Der Qualitätssicherungsplan sollte folgende Phasen ansprechen, so wie sie für jedes spezielle System oder jede Entwicklung anwendbar sind:

- a) Auslegung und Entwicklung;
- b) Beschaffung;
- c) Produktion;
- d) Errichtung und Inbetriebnahme;
- e) Betrieb und Wartung.

5.3.6 Es müssen nicht alle oben aufgezählten Phasen vor Beginn des Auslegungsprozesses angesprochen werden, aber für Gerät der Klassen 1 und 2 muss, bevor jede Phase begonnen wird, ein Plan verfügbar sein, in dem die Anforderungen für diese Phase enthalten sind.

5.3.7 Für Gerät der Klassen 1 und 2 sollte(n) der (die) Qualitätssicherungsplan (-pläne) Organisation, Management und Ausführung von qualitätsbezogenen Tätigkeiten beschreiben, wenn relevant, einschließlich:

- a) Dokumentation der Konfigurationskontrolle;
- b) Auslegungsprozess;
- c) Beschaffungsprozess für Waren und Dienste;
- d) Konfigurationskontrolle der Bauvorschriften, Bauverfahren und Zeichnungen;
- e) Konfigurationskontrolle der Materialien und Teile, die für den Aufbau der Systemhardware verwendet werden;
- f) Qualitätskontrollen, z. B. formale Inspektionen;
- g) Kontrolle der Prüfeinrichtungen;
- h) Kontrolle von Handhabung/Lagerung/Transport der Hardware;
- i) Prüfprozesse;
- j) Überwachung der festgestellten Nicht-Konformitäten und Umsetzung der Korrekturmaßnahmen;
- k) Verfahren für die Aufbewahrung der Qualitätssicherungsaufzeichnungen;
- l) Prozedur für interne Auditierung.

6 Hardwareanforderungen

6.1 Allgemeines

6.1.1 Allgemeines für Gerät der Klassen 1 und 2

6.1.1.1 Die Hardwareanforderungen müssen mit den Anforderungen des Systems welcher Technologie auch immer übereinstimmen (siehe [IEC 61513:2011, Abschnitt 6](#)). Die Systemspezifikation ist eine Beschreibung des kombinierten Hardware- und anwendungsspezifischen Aspekte und Auslegungsziele für das System und die vom System durchzuführenden Funktionen (Systeme können für eine spezielle Anwendung oder auf Basis einer generischen Plattform entwickelt werden, die sich auf abgeleitete generische Systemanforderungen abstützt).

6.1.1.2 Die Hardwareanforderungen müssen in der Spezifikation der Anforderungen für die Hardware oder in einem anderen geeigneten Dokument spezifiziert werden.

6.1.1.3 Die Hardwareanforderungen müssen methodisch so dargestellt werden, dass die Lesbarkeit nicht beeinträchtigt wird, d. h., es sollte keine Schwierigkeiten machen, den Text zu verstehen.

6.1.1.4 Hardwareanforderungen müssen eindeutig, prüfbar und/oder verifizierbar und erfüllbar sein.

6.1.1.5 Die Hardware-Anforderungsspezifikation sollte einen Überblick der Hardwareanforderungen geben, die sicherheitstechnisch wichtigen Hardwarefunktionen festlegen (wenn diese jedoch in Kombination mit der Systemsoftware oder HDL vorgesehen werden, sollten sie in der System-Anforderungsspezifikation definiert

werden), die Anforderungen an die Hardwareauslegung festlegen, die Zuverlässigkeitsanforderungen an die Hardware und die Umgebungsanforderungen angeben.

6.1.1.6 Die funktionalen Hardwareanforderungen sollten allgemein beschreiben, was zu machen ist, und nicht, wie es zu machen ist.

6.1.1.7 Bevor vorgefertigte Komponenten zur Verwendung ausgewählt werden, muss eine Bewertung vorgenommen werden, um die Übereinstimmung der Leistungscharakteristiken und Fehlermodi der Hardware mit den Systemanforderungen zu bestätigen. Der Auswahlprozess für vorgefertigte Komponenten ist in [7.8](#) beschrieben.

6.1.1.8 Werden während dieser Bewertung irgendwelche Anomalien festgestellt, müssen diese behoben werden, und zwar entweder durch Änderung der Hardware- oder der Systemauslegung (wobei sichergestellt werden muss, dass Sicherheitsanforderungen für das System nicht beeinträchtigt werden).

6.1.1.9 Die Hardwareanforderungen müssen alle nicht erlaubten Konstruktionsmaterialien sowie Anforderungen für jedes zu verwendende Material oder bestimmte Herstellungsarten angeben.

6.1.1.10 Während der Spezifikation der elektronischen Module muss der Lieferant der Leittechnik die Modulspezifikation aus der Gerätespezifikation ableiten, und zwar in Bezug auf:

- Austauschbarkeit,
- Akzeptanzkriterien, mindestens IPC-A-610 (siehe [10.5.4](#)).

6.1.2 Allgemeines für Gerät der Klasse 3

Während der Spezifikation der Hardwareanforderungen für die elektronischen Module muss der Hersteller die Modulspezifikation aus der Gerätespezifikation ableiten, und zwar in Bezug auf:

- Funktionalität,
- Umgebungsbedingungen (elektrisch, klimatisch, mechanisch, aggressive Umgebung, EMV usw.),
- Produktion (Verpackung, Akzeptanzkriterien, mindestens IPC-A-610, usw.),
- Zuverlässigkeit,
- Lebensdauer (elektrochemische Widerstände, Erhaltungszeit gespeicherter Daten usw.),
- Wartbarkeit,
- Austauschbarkeit,
- nicht erlaubte Konstruktionsmaterialien.

6.2 Funktionale und Leistungsfähigkeitsanforderungen für Gerät der Klassen 1 und 2

6.2.1 Die funktionalen und Leistungsfähigkeitsanforderungen für die Hardware müssen mit den funktionalen und Leistungsfähigkeitsanforderungen für das sicherheitstechnisch wichtige System übereinstimmen.

6.2.2 Für die funktionalen und Leistungsfähigkeitsanforderungen der Hardware, kombiniert mit den Anforderungen an fest-verdrahtete oder programmierbare digitale Geräte (in dem für die Hardwareanforderungen erforderlichen Umfang), muss die Verträglichkeit mit den Systemanforderungen nachgewiesen werden.

6.2.3 Alle Teile des Systems bis hinunter auf die Ebene der Software oder HDPs enthaltenden Komponenten müssen, wie in [1.2](#) dieser Norm beschrieben und mit Bezug auf die für Software- bzw. HPD-Aspekte anwendbare Norm, beurteilt werden.

6.2.4 Die funktionalen Anforderungen an die Hardware müssen folgende Beschreibungen einschließen, sind aber nicht darauf beschränkt

- Zweck der gesamten Rechnersystem-Hardware und jedes Hardware-Teilsystems;
- Anzahl und Arten der Messfühler und Betätigungsbausteine, die mit dem Rechnersystem zu verbinden sind;
- Anzahl und Arten der Einrichtungen für die Mensch/Maschine-Schnittstelle, wie z. B. Bildschirme, Drucker und Tastaturen.

6.2.5 Jeder Komponente oder jedem Teilsystem, die/das zugeliefert wird und in das System zu integrieren ist, sollte eine Spezifikation beigelegt sein, in der alle sicherheitsbezogenen Aspekte der Leistungsfähigkeit von Komponente bzw. System angesprochen werden. Steht eine solche Spezifikation nicht zur Verfügung, so muss eine Analyse der Hardwareauslegungseigenschaften im erforderlichen Umfang durchgeführt werden, um die Eignung bestätigen zu können.

6.2.6 Die Anforderungen an die Leistungsfähigkeit der Hardware müssen umfassen (je nach Anwendbarkeit für die jeweilige Nutzung):

- geforderte Datenerfassungsrate;
- geforderte Fähigkeiten für die Datenverarbeitung;
- geforderte Rechenkapazität;
- geforderte Zuverlässigkeit/Verfügbarkeit;
- geforderte Kommunikationsschnittstellen (Protokolle, Übertragungsgeschwindigkeiten);
- geforderte Rechen- und Konversionsgenauigkeit;
- geforderte Fähigkeit zur Rauschunterdrückung;
- geforderte Ansprechzeiten;
- physikalische Größenbeschränkungen;
- Anforderungen aufgrund der räumlichen Gegebenheiten (z. B. Länge der Datenleitungen);
- geforderter Umfang von Ersatzkapazität (wenn verlangt);
- Umgebungsanforderungen;
- Anforderungen für die elektrische Energieversorgung.

6.2.7 Alle Einschränkungen, denen die Hardwareauslegung durch die System- oder Softwareauslegung unterliegt, müssen angegeben werden.

6.3 Zuverlässigkeits-/Verfügbarkeitsanforderungen für Gerät der Klassen 1 und 2

6.3.1 Die Zuverlässigkeits-/Verfügbarkeitsanforderungen für Hardware müssen mit den Zuverlässigkeitsanforderungen für das Gesamtsystem übereinstimmen.

6.3.2 Die Zuverlässigkeits-/Verfügbarkeitsanforderungen für Hardware müssen eine Beschreibung aller Versagensarten einschließen, die ohne Verlust der Funktion oder mit einem begrenzten Verlust der Funktion zu tolerieren sind.

6.3.3 Zuverlässigkeitsziele für Hardware sollten vorgesehen sein.

ANMERKUNG 1 In diesem Zusammenhang bezieht sich Hardwarezuverlässigkeit auf zufällige Hardwareausfälle; jedes Versagen infolge logischer Auslegungsfehler wird ausgeschlossen.

6.3.4 Die Hardwareanforderungen sollten Zielwerte für die Parameter der Hardwarezuverlässigkeit enthalten (wie z. B. mittlere Zeitspanne zwischen Ausfällen (entdeckt), mittlere Zeitspanne zwischen Ausfällen (unentdeckt), mittlere Reparaturdauer für entdeckte Ausfälle).

6.3.5 Jede Anforderung für in Anspruch genommene Zuverlässigkeitsangaben, die durch detaillierte Analysen der Hardwareauslegung zu stützen sind, sollte dargelegt werden, d. h. Analysen auf Ebene der Teileinheit, Karten oder Komponenten.

ANMERKUNG 1 Die Methoden, die zur Analyse der Zuverlässigkeit und der Auswirkungen von Ausfällen der Systemhardware verwendet werden können, sind:

- Die Fehlerbaumanalyse (FTA), die sich mit der Feststellung und Analyse von Bedingungen und Faktoren befasst, die das Auftreten eines definierten unerwünschten Ereignisses – oder einen Beitrag zu diesem Ereignis – verursachen (zu Hinweisen für diese Technik siehe IEC 61025).

- Die Ausfallart- und -effektanalyse (FMEA), mit der Ausfälle festgestellt werden, die signifikante Auswirkungen auf die Leistungsfähigkeit des Systems haben, z. B. auf Zuverlässigkeit, Sicherheit, Verfügbarkeit (zu Hinweisen für diese Technik siehe IEC 60812).
- Wo relevant, kann eine geeignete Technik zur Analyse von Hardwaresystemen der Klassen 1 und 2 angewendet werden, um sicherzustellen, dass ein potenzieller Hardwareausfall keine inakzeptablen Auswirkungen auf die Sicherheit hat.

Wenn Ausfallraten verfügbar sind, die sich auf unterschiedliche Umgebungsbedingungen beziehen, müssen die in die Hardwareanforderungen aufgenommenen Fehlerraten re-evaluiert werden. Eine Anleitung dazu ist in IEC 62380 zu finden.

6.3.6 Eine Methode wie z. B. Fehlerbaumanalyse (FTA), kombiniert mit bekannten Komponentenausfalldaten, kann verwendet werden, um Werte für die Zuverlässigkeitseigenschaften der Systemhardware zu errechnen. Ein derartiges Vorgehen muss angewendet werden, um die Hardware von Systemen der Klasse 1 zu analysieren (siehe IEC 61513), es sei denn, es ist genügend Betriebserfahrung verfügbar, die mit großem Vertrauen erwarten lässt, dass die Zuverlässigkeitsziele der Hardware erreicht werden.

6.3.7 Solch eine Methode wie z. B. Fehlerbaumanalyse (FTA), sollte auch für Systeme der Klasse 2 verwendet werden, oder es ist alternativ eine Rechtfertigung hinreichender Zuverlässigkeit auf der Basis qualitativer Überlegungen möglich (z. B. Qualität der Komponenten, Hardware-Redundanz, Betriebserfahrung, Anteil der entdeckten gegenüber unentdeckten Hardwareausfällen usw.), zumal wenn Zuverlässigkeitsanforderungen an die Hardware keine allzu große Herausforderung darstellen.

6.3.8 Strategien und Vorkehrungen zur Sicherstellung der Zuverlässigkeit und Verfügbarkeit über die Lebensdauer des leittechnischen Systems müssen festgelegt werden. Diese Maßnahmen müssen als Wartungsanforderungen dokumentiert werden. Sie müssen Anforderungen zur Verhinderung des Einschleppens von Fehlern durch Wartung einschließen, die zu Ausfällen gemeinsamer Ursache führen könnten. Wartungsarbeiten an mehrsträngigen Systemen werden im Allgemeinen als die wahrscheinlichste Ursache für derartige Fehler erachtet, und deshalb müssen die Systeme so ausgelegt werden, dass die Notwendigkeit solcher Tätigkeiten so weit wie möglich reduziert wird. Wo Wartungsarbeiten erforderlich sind, die das Potenzial haben, zu Ausfällen gemeinsamer Ursache zu führen, muss in den Auslegungsanforderungen spezifiziert werden, wie das Risiko solcher Ausfälle zu minimieren ist.

6.3.9 Wartungsanforderungen sollten (je nach Anwendbarkeit auf ein spezielles System) enthalten:

- a) Anforderungen für den Systembetrieb während Tätigkeiten zur Hardwarewartung;
- b) Ersatz von Verbrauchsteilen, z. B. Luftfilter;
- c) Anforderungen für den regulären Ersatz von Teilsystemen, Modulen und/oder Komponenten;
- d) erforderlicher Umfang der Revalidierung (z. B. Prüfungen) nach Wartungsarbeiten an der Hardware.

6.3.10 Unter Berücksichtigung der Vorgabe, dass die Anforderungsspezifikation das „Was“ und nicht das „Wie“ definieren sollte, kann es jedoch unpraktisch sein, in der Phase der Anforderungsspezifikation des Projekts die Wartungsanforderungen im Detail zu definieren; in diesem Fall sollten derartige Anforderungen in einer späteren Phase des Entwicklungsprozesses vollständig definiert werden.

6.3.11 Die für die Durchführung der Zuverlässigkeits- und Ausfallanalyse, die für Systeme der Klasse 1 gefordert und für Systeme der Klasse 2 empfohlen sind, verwendete Methode muss bezüglich der zu verfolgenden Ziele geeignet sein.

ANMERKUNG 1 Zum Beispiel beschreibt IEC 60812 eine Anzahl von Techniken für die Durchführung von Ausfallart- und -effektanalysen (FMEA) und Ausfallart- und -kritikalitätsanalysen (FMECA) und gibt Anweisungen für die Anwendung dieser Methoden entsprechend den zu verfolgenden Zielen. Für die Durchführung von FMEA- und FMECA-Analyse wäre die Anwendung der in IEC 60812 beschriebenen Methoden eine akzeptable Praxis.

6.3.12 Wartungsanforderungen können während der Spezifikation der Hardwareanforderungen nicht endgültig definiert werden. Die Wartungsanforderungen sollten in einem späteren Stadium vor der Inbetriebnahme finalisiert werden.

6.4 Umgebungsanforderungen

6.4.1 Umgebungsanforderungen für Gerät der Klassen 1 und 2

6.4.1.1 In den Umgebungsanforderungen für Hardware müssen physikalische Einschränkungen, klimatische, seismische, chemische, elektrische und Strahlungsbedingungen je nach Anwendungsfall angesprochen werden.

6.4.1.2 Jede spezielle Anforderung während der Errichtung und Inbetriebnahme sollte ebenso mit eingeschlossen werden.

6.4.1.3 Die Bereiche normaler und extremer Umgebungsbedingungen, denen das System widerstehen muss, müssen in Übereinstimmung mit den Randbedingungen aus der Anlagenauslegung spezifiziert werden (siehe IEC 61513, 5.2.4).

6.4.1.4 Die Systeme müssen für ihre Umgebungsbedingungen qualifiziert werden, entsprechend den Anforderungen in IEC/IEEE 60780-323 und IEC 60980.

6.4.1.5 Der Grad der Störfestigkeit gegenüber elektromagnetischen Beeinflussungen muss entsprechend den Anforderungen der betrieblichen Umgebung spezifiziert und nach den einschlägigen Normen geprüft werden, z. B. nach IEC 62003. Das elektromagnetische betriebliche Umfeld kann möglicherweise durch eine Vielfalt von Quellen mit elektrischer Wechselwirkung geprägt sein, z. B. Schaltgetrieben, mobilen Telefonen, Relais, Walkie-Talkies, elektrostatischen Entladungen, Blitz, Erdungsfehler.

6.4.1.6 Die spezifizierten elektromagnetischen Qualifizierungsniveaus sollten auf realistischen Abschätzungen der Betriebsbedingungen unter allen glaubhaften Worst-Case-Umständen beruhen.

6.4.1.7 In den Hardwareanforderungen müssen alle nicht zugelassenen Konstruktionsmaterialien festgelegt werden sowie alle Anforderungen für einzusetzende Materialien oder für spezielle Arten von Produktionsprozessen.

6.4.2 Umgebungsanforderungen für Gerät der Klasse 3

Systeme der Klasse 3, für die eine Umweltqualifizierung gefordert ist (z. B. seismische Qualifizierung oder bezüglich bestimmter Betriebsbedingungen) dürfen nach industriellen Normen qualifiziert werden. Die Behauptung der Eignung für Betrieb in anomalen Umgebungsbedingungen, seismischer Qualifizierung nach industriellen Normen oder angegebener Funktionalitäten muss durch dokumentierte Nachweise begründet werden. Wenn signifikante Alterungseffekte bestehen oder die qualifizierte Lebensdauer nicht nach der in IEC/IEEE 60780-323 gegebenen Definition nicht nachgewiesen werden kann, muss ein Programm zur betriebsbegleitenden Qualifizierung nach IEC/IEEE 60780-323 vorgeschlagen und begründet werden.

6.5 Dokumentationsanforderungen

6.5.1 Die Dokumentationsanforderungen für Hardware müssen als Teil der Dokumentationsanforderungen des leittechnischen Systems spezifiziert werden (siehe IEC 61513).

6.5.2 Die zu erstellende Dokumentation sollte, je nach Relevanz, einschließen:

- Auslegungsdokumente (Systemhardwarekomponenten, Hardwareauslegung der Schnittstellen usw.);
- Betriebshandbücher;
- Wartungshandbücher.

7 Auslegung und Entwicklung

7.1 Allgemeines

Dieser Abschnitt ist anwendbar für Hardwareauslegung und -entwicklung auf System-, Teilsystem- und Modulebene.

7.1.1 Allgemeine Anforderungen für Gerät der Klassen 1 und 2

7.1.1.1 Für den Auslegungs- und Entwicklungsprozess neuer Hardware muss als Eingangsinformation die Hardware-Anforderungsspezifikation verwendet werden.

7.1.1.2 Der Auslegungsprozess sollte über verschiedene Auslegungsstufen fortschreiten, die schließlich mit der Herstellung von Hardware entsprechend der Hardware-Anforderungsspezifikation abgeschlossen werden. Die allgemeinere Ebene der Auslegungstätigkeit kann man als „vorläufige Auslegung“ bezeichnen. Sie besteht aus der Analyse verschiedener Auslegungsalternativen zur Definition der Hardwarearchitektur in Form von Teilsystemen und Modulen.

7.1.1.3 Der vorläufigen Auslegung folgen im Allgemeinen eine oder mehrere detaillierte Auslegungsebenen. Die detaillierten Auslegungstätigkeiten müssen die vorläufige Auslegung ausweiten und die detaillierte Auslegung der Teilsysteme, Module und Komponenten in dem Ausmaß behandeln, dass die gesamte Hardwareauslegungsbeschreibung für die Realisierung hinreichend vollständig ist.

7.1.1.4 Prototyp-Hardware kann gebaut werden, und zwar nicht nur zur Demonstration erfolgreichen Zusammenwirkens der Hardwaremodule, sondern auch zur Überprüfung der Hardware- und Software- und HPD-Kompatibilität.

7.1.1.5 Vorgefertigte (z. B. am Markt erhältliche) Komponenten können für die ganze Systemhardware oder als Teilmenge der Hardwarekomponenten verwendet werden.

7.1.1.6 Wenn die Auslegung in einer einzelnen Phase erfolgt, muss diese Phase die detaillierte Hardwareauslegung einschließen.

7.1.1.7 Die Unterabschnitte 7.2 bis 7.7 sind nicht auf vorgefertigte Komponenten anzuwenden. [Unterabschnitt 7.8](#) stellt spezifische Anforderungen für vorgefertigte Komponenten.

7.1.2 Allgemeine Anforderungen für Gerät der Klasse 3

7.1.2.1 Die Hardwareauslegung von Modulen muss alle in [5.1.2](#) angegebenen Anforderungen berücksichtigen.

7.1.2.2 Die Dokumentation der Hardwareauslegung und -entwicklung muss die Hardwareauslegung und die Mittel, mit denen die Hardwareanforderungen erfüllt werden, beschreiben.

7.1.2.3 Während der Auslegung müssen die folgenden Dokumente erstellt werden: Produktion und Montage, Werksabnahmeprüfung, Errichtung, Inbetriebnahme, Wartung und Betrieb.

7.1.2.4 Am Ende der Auslegungs- und Entwicklungsphase muss die geforderte Dokumentation erstellt sein und eine vollständige Beschreibung aller Auslegungsdetails enthalten, die zusätzlich die Funktionalitäten, Einschränkungen und sonstigen Hardwareeigenschaften abdeckt, um zu zeigen, dass die in [5.1.2](#) angegebenen Anforderungen erfüllt sind.

7.2 Auslegungstätigkeiten

7.2.1 Die von der Hardware abhängigen Anforderungen an das System müssen in der Hardwareauslegung angesprochen werden; entweder durch Analyse oder Prüfungen muss der Nachweis erbracht werden, dass die Hardwareauslegung diese Anforderungen erfüllt. Solche Anforderungen umfassen im Allgemeinen Rechengenauigkeit, Ansprechzeit, die Auslegung hinsichtlich Umgebungsbedingungen und Anforderungen

an die elektrische Energieversorgung (für vorgefertigte Komponenten muss die Hardwarespezifikation der Komponenten gegen die Anforderungen für die Systemhardware verifiziert werden, um sicherzustellen, dass die vorgefertigten Komponenten die spezifizierten Anforderungen erfüllen, oder die Leistungsfähigkeit muss durch Prüfungen nachgewiesen werden).

7.2.2 Alle Unstimmigkeiten gegenüber den Hardwareanforderungen müssen behoben werden, sei es durch Änderungen der Auslegung oder durch Änderungen der Anforderungen (wobei die Auswirkung der Änderungen vollständig zu analysieren und zu dokumentieren sind).

7.2.3 Die Hardwarekonstrukteure müssen die erforderlichen Prüfungen festlegen, mit denen gezeigt wird, dass die geforderte Leistungsfähigkeit erreicht wird. Derartige Prüfungen können allein mit der Hardware oder zusammen mit der integrierten Software und/oder HPDs durchgeführt werden, d. h. als Teil der Prüfphase der Systemintegration.

7.2.4 Die Hardwarekonstrukteure müssen alle Wartungstätigkeiten spezifizieren, die für den Nachweis erforderlich sind, dass die Leistungsfähigkeits- und Zuverlässigkeitsanforderungen über die volle Betriebsdauer der Geräte eingehalten werden. Das kann betriebliche Prüfungen, Kalibrierung, Reparaturen, periodischen Ersatz und Wartungsprozeduren umfassen. Alle diese Aktivitäten müssen in der Wartungsanleitung dokumentiert werden.

7.2.5 Solche Tätigkeiten sollten in einem Ausmaß durchgeführt werden, das genügend Vertrauen in das richtige Arbeiten der Geräte erzeugt und trotzdem die Wechselwirkung mit dem Menschen und die Durchführung von intensiven Arbeiten an den Systemen auf ein Minimum beschränkt, um die Wahrscheinlichkeit des Einschleppens von Fehlern (auch solchen, die zu Ausfällen gemeinsamer Ursache führen könnten) durch die Wartungsarbeiten zu reduzieren.

7.2.5 Wenn eine qualifizierte Lebensdauer spezifiziert wird, muss gerechtfertigt werden, dass diese realistisch und erreichbar ist.

7.3 Zuverlässigkeit

7.3.1 Zuverlässigkeit von Gerät der Klassen 1 und 2

7.3.1.1 Zuverlässigkeitsanforderungen sollten in der Dokumentation der Hardwareanforderungen spezifiziert werden (siehe 6.3).

7.3.1.2 Um wie verlangt die Sicherheitsanalyse auf Systemebene zu unterstützen, muss während der Auslegung eine Analyse des Potenzials von Hardwareausfällen gemacht werden.

7.3.1.3 Wenn Mehrfachstränge eines Systems oder Mehrfachsysteme (von denen jedes einen Einzelstrang oder Mehrfachstränge von Geräten aufweisen kann) verwendet werden, um eine Sicherheitsfunktion zu realisieren, muss in diese Analyse eine geeignete Betrachtung des Potenzials für Hardwareausfälle gemeinsamer Ursache eingeschlossen werden. Mögliche Quellen von Hardware-basierten Ausfällen gemeinsamer Ursache sind:

- Wartungsarbeiten, die gleichzeitig oder hintereinander an Mehrfachsträngen von Geräten eines redundanten Systems durchgeführt werden (speziell, wenn durch solche Tätigkeiten unentdeckte Fehler eingeschleppt werden können);
- periodisches Prüfen;
- koinzidente unentdeckte zufällige Hardwareausfälle an Mehrfachsträngen von Geräten, die sich auf dieselbe(n) Sicherheitsfunktion(en) auswirken;
- latente Auslegungsfehler, die sich auf Mehrfachstränge von Geräten auswirken und die im Zuge des Auslegungsprozesses nicht entdeckt wurden.

ANMERKUNG 1 Methoden, die für die Analyse der Hardwarezuverlässigkeit und der Auswirkungen von Hardwarefehlern auf das System verwendet werden, schließen FTA und FMEA ein (siehe 6.3.7).

7.3.1.4 Durch die Hardwareauslegung sollte die mögliche Auswirkung folgender Faktoren auf die Sicherheit minimiert werden:

- Wartungstätigkeiten;
- Komponentenausfall aufgrund eines zufälligen Hardwareausfalls;
- Hardwareausfall infolge der Umgebungsbedingungen.

7.3.1.5 Wenn die abgeschätzte Hardwarezuverlässigkeit für eine bestimmte Anwendung als nicht ausreichend erachtet wird, müssen Ausgleichsmaßnahmen ergriffen werden. Dies können Verbesserungen der Auslegung oder betriebliche Änderungen sein, wie etwa die Erhöhung der Häufigkeit betrieblicher Prüfungen. Wenn man sich jedoch für die Option häufigerer betrieblicher Prüfungen entscheidet, ist Sorgfalt angebracht, weil jede intensivere Tätigkeit an der in Betrieb befindlichen Anlage ein echtes Risiko der Fehlereinschleppung mit sich bringt (d. h. die Gesamtwirkung der Maßnahme auf die Sicherheit negativ sein kann). Im Idealfall sollten Prüfungen nur durchgeführt werden, wenn mögliche Fehler beim Prüfvorgang keine Auswirkung auf die Sicherheit haben würden, z. B. während einer Abschaltung der Anlage oder wenn das zu prüfende Gerät von der in Betrieb befindlichen Anlage getrennt wird.

ANMERKUNG 1 Wenn eine probabilistische Sicherheitsbewertung durchgeführt wird, um die Sicherheitsbeurteilung eines Kernkraftwerks zu unterstützen, können die ermittelten probabilistischen Zuverlässigkeitsdaten der Hardware (z. B. mittels Fehlerbaumanalyse (FTA)) in die Kraftwerksanalyse eingebracht werden und so zur Genauigkeit der Zuverlässigkeitsrechnungen für das gesamte Kernkraftwerk beitragen.

7.3.2 Zuverlässigkeit von Gerät der Klasse 3

7.3.2.1 Zuverlässigkeitsanforderungen sollten in der Hardware-Anforderungsspezifikation spezifiziert werden (siehe 6.3).

7.3.2.2 Wenn für die Unterstützung der Sicherheitsanalyse auf Systemebene gefordert, sollte das Potenzial von Hardwarefehlern während der Auslegung untersucht werden.

7.3.2.3 Wenn Mehrfachstränge eines Systems oder Mehrfachsysteme (von denen jedes einen Einzelstrang oder Mehrfachstränge von Geräten aufweisen kann) verwendet werden, um eine Sicherheitsfunktion zu realisieren, muss in diese Analyse eine geeignete Betrachtung des Potenzials für Hardwareausfälle gemeinsamer Ursache eingeschlossen werden. Mögliche Quellen von Hardware-basierten Ausfällen gemeinsamer Ursache sind in 7.3.1.3 genannt.

7.4 Wartung

7.4.1 Der Hersteller muss für alle elektronischen Module, aus denen sein Gerät besteht, angeben, welche repariert werden können, und welche nicht.

7.4.2 Bei der Hardwareauslegung müssen alle in der Anforderungsspezifikation der Hardware enthaltenen spezifischen Wartungsanforderungen angesprochen werden. Zusätzlich sollte die Auslegung, wo praktikabel, so gestaltet werden, dass das Risiko, durch die Wartungsarbeiten Fehler einzuschleppen, reduziert wird, z. B.:

- sollten Komponenten, deren Austausch bei Versagen erforderlich ist, leicht zugänglich sein;
- sollten ersetzbare Komponenten klar festgelegt werden, so dass das Wartungspersonal leicht überprüfen kann, ob die richtigen Komponenten verwendet werden;
- sollten ausreichende Abstände für Endverbindungen vorhanden sein;
- sollten in ausreichendem Umfang geeignete Anschlüsse zur Verwendung bei Kalibrierungs- und Prüftätigkeiten vorgesehen werden (so dass bestehende Verdrahtung zur Erleichterung solcher Tätigkeiten nicht gelöst werden muss);
- sollte die Hardware eine strukturierte Auslegung mit eindeutigen Bezeichnungen aufweisen, um das Potenzial von Wartungsfehlern zu reduzieren.

7.4.3 Die Wartungsanleitung muss die Verfahren zur Wartung, Diagnose und Reparatur beschreiben. Sie muss die Art und den Umfang der zur Unterstützung dieser Aktivität zu erstellenden Berichte angeben, zusätzlich zu der Qualifikation des damit befassten Personals.

7.4.4 Die Wartungsarbeiten sollten so durchgeführt werden, dass ein hinreichender Grad von Vertrauen in den korrekten Betrieb der Hardware hergestellt wird.

7.5 Schnittstellen

In IEC 61513, 6.2.2.3.2, 6.2.2.4, 6.2.2.5, 6.2.3.3.3 und 6.2.3.3.4, sind Anforderungen für Systemschnittstellen enthalten, die darauf abzielen, das Fortschreiten von Ausfällen über Systemschnittstellen hinweg zu verhindern.

7.6 Änderungen

In dem von der Hardware-Anforderungsspezifikation verlangten Ausmaß muss die Hardware auch auf Änderungs- und Reparaturfähigkeit ausgelegt sein (siehe Abschnitt 13).

7.7 Ausfall der Energieversorgung

In dem von der Hardware-Anforderungsspezifikation verlangten Ausmaß muss das leittechnische System gegen Folgen kurzzeitiger Ausfälle und möglicher Schwankungen (Spannung/Frequenz) in der Energieversorgung unempfindlich ausgelegt sein. Mittel müssen vorgesehen sein, um Betriebs- und Wartungspersonal auf solche Unregelmäßigkeiten aufmerksam zu machen (diese Aufgabe lässt sich nicht unbedingt der Hardware zuordnen und mag daher außerhalb des Anwendungsbereichs dieser Norm liegen).

7.8 Auswahl vorgefertigter Komponenten

Wenn vorgefertigte Komponenten verwendet werden, muss die Kompatibilität ihrer Auslegung mit ihrer Aufgabe innerhalb der Systemhardware sowie die Qualität der Auslegung wie folgt verifiziert werden.

7.8.1 Die angegebenen Eigenschaften vorgefertigter Komponenten müssen die Hardwareanforderungen des Systems erfüllen, ansonsten muss die Einhaltung der Systemanforderungen durch Prüfung verifiziert werden.

7.8.2 Alle für die Sicherstellung der Zuverlässigkeit und funktionalen Anforderungen erforderlichen Wartungsarbeiten müssen spezifiziert werden und sind während der gesamten Betriebszeit der Hardware zu erfüllen. Dies kann Verfahren zur betriebsbegleitenden Prüfung, Kalibrierung, Reparaturen, periodischer Austausch und Wartung umfassen.

7.8.3 Vorgefertigte Hardware muss so ausgewählt werden, dass menschliche Eingriffe oder andere Eingriffe in das System auf ein Minimum reduziert werden, wozu die Reduzierung der Wahrscheinlichkeit der Einbringung von Fehlern (wie z. B. das CCF-Potenzial) durch Wartungsarbeiten gehört.

7.8.4 Wenn die Ziele bezüglich der qualifizierten Lebensdauer gesetzt werden, müssen Begründungen gegeben werden, mit denen zu zeigen ist, dass diese Ziele realistisch sind und erreicht werden können.

7.8.5 Wenn es erforderlich ist, eine Sicherheitsanalyse auf Systemebene zu unterstützen, muss eine Analyse des Potenzials von Hardwarefehlern während der Auslegungsphase erfolgen. Wenn Gerät eines redundanten Systems oder in mehreren Systemen für Sicherheitsfunktionen eingesetzt wird, muss diese Analyse auch das CCF-Potenzial einschließen. Mögliche Ursachen für die Einbringung von CCF-empfindlichem Gerät sind die Folgenden:

- Wartungsarbeiten, die gleichzeitig oder sequentiell an mehreren Elementen der Geräte durchgeführt werden (insbesondere wenn diese Aktivitäten Hardwarefehler einbringen können);
- periodische Überprüfung;
- verborgene Auslegungsfehler, die während der Entwicklung nicht erkannt wurden.

7.8.6 Wenn die Zuverlässigkeit der Hardware für die spezifische Aufgabe nicht ausreicht, müssen kompensierende Maßnahmen ergriffen werden. Solche Maßnahmen können Verbesserungen der Auslegung oder Änderungen in Bezug auf den Betrieb sein (wie z. B. häufigeres betriebsbegleitendes Prüfen).

7.8.7 Wenn entschieden wurde, das betriebsbegleitende Prüfen zu intensivieren, sollte bedacht werden, dass alle Eingriffe in das installierte Gerät ein intrinsisches Risiko einer direkten oder indirekten Einbringung von Fehlern haben (z. B. kann die Gesamtauswirkung eines betriebsbegleitenden Prüfens einen negativen Einfluss auf die Sicherheit haben). Idealerweise sollten Prüfungen durchgeführt werden, wenn mögliche Fehler des Prüfverfahrens keinen Einfluss auf die Sicherheit haben können, z. B. während einer Abschaltung oder wenn das zu prüfende Gerät von der übrigen Installation getrennt ist.

7.8.8 Die Hardwareauslegung muss alle spezifischen Wartungsanforderungen adressieren, sie sich aus der Hardware-Anforderungsspezifikation ergeben.

7.8.9 Wo immer möglich, sollte die Auslegung Vorkehrungen zur Reduzierung des Risikos menschlicher Fehler während Wartungsarbeiten reduzieren.

Beispiele solcher Vorkehrungen sind:

- leichte Zugänglichkeit zu Komponenten, die wahrscheinlich nach Ausfällen ausgetauscht werden müssen;
- klare Kennzeichnung austauschbarer Komponenten, um sicherzustellen, dass das Wartungspersonal leicht verifizieren kann, dass die richtigen Ersatzkomponenten verwendet werden;
- Einsatz von Komponenten, die ohne Eingriff in die Anlagenverkabelung ausgetauscht werden können;
- ausreichender Abstand zwischen Verteilern;
- gut strukturiertes Modell der Hardwareauslegung mit klarer Identifizierung festgelegter Teile, um das Risiko von Wartungsfehlern zu reduzieren.

7.8.10 Wenn eines oder mehrere der Anforderungen 6.8.1 bis 6.8.8 nicht erfüllt werden können, sollten kompensierende Maßnahmen ergriffen werden.

7.8.11 Der Hersteller muss nachweisen, dass die in seinem Gerät verwendeten Komponenten und vorgefertigten Module die spezifizierten Anforderungen erfüllen.

7.9 Auslegungsdokumentation

7.9.1 Die Auslegungsdokumentation der Hardware muss die Hardwareauslegung beschreiben und die Mittel angeben, mit denen die Hardwareanforderungen realisiert werden. Standardisierte Formen der Auslegungsdokumentation und die Anwendung automatischer Auslegungswerkzeuge werden empfohlen.

7.9.2 Die Auslegungsdokumente für die Hardware des leittechnischen Systems sollten in Form einer Hierarchie erstellt werden, die aus einer Anzahl von Dokumentationsebenen besteht.

7.9.3 In der Auslegungsdokumentation jeder Ebene sollten die für diese Ebene relevanten Auslegungsaspekte spezifiziert und die Hardwareanforderungen für die niedrigeren Ebenen definiert werden.

7.9.4 Dokumente für Produktion/Zusammenbau, Werksprüfungen, Errichtung, Inbetriebnahme, Wartung und Betrieb müssen (je nach Situation) während des Auslegungsprozesses erstellt werden.

7.9.5 Es muss eine vorläufige Hardwareauslegungsbeschreibung erstellt werden, in der die Hardwarearchitektur definiert wird, d. h. Struktur und Beziehung der Systemteile.

7.9.6 Die vorläufige Hardwareauslegungsbeschreibung sollte die allgemeine Auslegung der Hardware mit Blockdiagrammen der Teilsysteme und Modulen der niedrigeren Ebenen umfassen.

7.9.7 Die vorläufige Hardwareauslegungsbeschreibung sollte auch Hardwareanforderungen für die detaillierte Auslegung mit einschließen, wie:

- Anzahl und Typen der zentralen Prozessoren und anderer Prozessoren;
- Hardwareanforderungen für den Rechnerpeicher;
- Anzahl und Typen der Schnittstellen;
- Anzahl und Typen der Datenverbindungen und Datenbusse.

7.9.8 Bei Abschluss der Auslegung und Entwicklung der Hardware muss die Auslegungsdokumentation mit einer vollständigen und endgültigen Beschreibung erstellt werden, die sowohl die Auslegungsdetails bis hinunter zu den niedrigeren Ebenen als auch die Fähigkeiten, Begrenzungen und andere Eigenschaften der Hardware wiedergibt.

7.9.9 Die endgültige Beschreibung muss folgende Information enthalten:

- a) eine Auslegungsübersicht;
- b) Querverweise zur Unterstützung der Auslegungsdokumentation;
- c) eine Beschreibung der Unterteilung der Hardware in Form von Hardware-Teilsystemen;
- d) eine Beschreibung jedes Teilsystems in Form seiner größeren Module und Komponenten (z. B. durch Verwendung von Blockdiagrammen und Schaltkreisdigrammen);
- e) eine Beschreibung von Teilsystem-Hardwareschnittstellen; Schnittstellen müssen je nach Notwendigkeit bezüglich logischer, physikalischer und elektrischer oder sonstiger Eigenschaften beschrieben werden;
- f) eine Beschreibung der Hardwareschnittstellen des leittechnischen Systems; Schnittstellen mit anderen Systemen entweder innerhalb oder außerhalb des Kernkraftwerks müssen festgelegt werden, indem die spezifischen Schnittstellen und die dazugehörigen Hardwareanforderungen aufgezeigt werden;
- g) die physikalische Auslegung – eine Beschreibung mit schematischen Darstellungen der physikalischen Auslegung der Geräte sollte vorgesehen werden;
- h) Qualifizierungsdaten (siehe Abschnitt 8), einschließlich Angabe aller notwendigen Tätigkeiten (wie z. B. Austausch von Komponenten), um die spezifizierte qualifizierte Lebensdauer aufrechtzuerhalten; für die Lagerdauer von Ersatzteilen wichtige Qualifizierungsdaten sollten auch, wo relevant, zur Verfügung stehen;
- i) Wartungsanforderungen;
- j) eine Beschreibung, wie die Anforderungen für Hardwarezuverlässigkeit und „fail-safe“-Eigenschaften erfüllt werden.

8 Verifizierung und Validierung

8.1 Verifizierung und Validierung von Gerät der Klassen 1 und 2

8.1.1 Allgemeines

Der Auslegungs- und Entwicklungsprozess muss formale Überprüfungen einschließen, dass die Ergebnisse jeder Phase der Hardwareauslegung und Entwicklung die Anforderungen erfüllen, die von der vorhergegangenen Phase vorgegeben wurden.

ANMERKUNG Der Hardware-Verifizierungsprozess beginnt im Allgemeinen mit der Verifizierung der Hardwareauslegungsanforderungen gegen die System-Auslegungsanforderungen und wird als abgeschlossen betrachtet, wenn die HPDs und die Systemsoftware auf der Hardware integriert ist. Für Systeme der Klassen 1 oder 2 enthalten IEC 60880, IEC 62138, IEC 62566-1 und IEC 62566-2 relevante Anforderungen bezüglich der Hardware/Software/HDP-Integrationsphasen.

8.1.2 Verifizierungsplan

Ein formaler Verifizierungsplan muss vorbereitet werden, um die Vorgehensweise zur Verifizierung der Hardwareauslegung zu definieren und den Verifizierungsprozess zu kontrollieren. Der Plan muss vor Beginn der Verifizierungstätigkeiten erstellt werden. In dem Plan (den Plänen) sollte(n) das einzusetzende Personal und die Organisation dokumentiert werden, die Organisationsstruktur, die Verifizierungsmethoden, die Verifizierungsebene, Zeitpläne sowie andere wichtige Tätigkeiten, die in Zusammenhang mit der Verifizierung stehen:

- a) Die Verifizierung kann parallel zum Auslegungsprozess durchgeführt werden (vorausgesetzt, eine geeignete Konfigurationskontrolle ist vorhanden), so dass Fehler so bald wie möglich entdeckt und korrigiert werden können.

- b) Formale Verifizierungstätigkeiten dürfen nicht durchgeführt werden, bis die Komponenten vom Auslegungsteam zur Verifizierung freigegeben werden. Nach Freigabe zur Verifizierung müssen die Auslegung und die zugehörige Dokumentation unter formaler Konfigurationskontrolle gehalten werden.
- c) Nach der Freigabe zur Verifizierung muss durch den Auslegungsänderungsprozess sichergestellt werden, dass alle nun folgenden Änderungen an der Hardwareauslegung in geeigneter Weise verifiziert werden (d. h. wie in 8.1.7 gefordert).

8.1.3 Unabhängigkeit der Verifizierung

8.1.3.1 Bei der Erstellung von Systemen der Klasse 1 muss das Verifizierungspersonal organisatorisch unabhängig vom Auslegungsteam sein, z. B. von verschiedenen organisatorisch getrennten Abteilungen derselben Organisation oder von verschiedenen Organisationen.

8.1.3.2 Bei Systemen der Klasse 2 dürfen die für die Verifizierung zuständigen Personen nicht die zu verifizierenden Geräte ausgelegt haben, jedoch darf das Verifizierungspersonal derselben Organisation angehören wie das Auslegungsteam. Zusätzlich zu diesen Anforderungen ist zu beachten:

8.1.3.3 Das Verifizierungspersonal muss technisch kompetent sein.

8.1.3.4 Alle Befunde der Verifizierung und die vom Auslegungsteam dazu gelieferten Antworten müssen formal dokumentiert werden.

8.1.3.5 Die Verifizierung muss nach dokumentierten Prozeduren durchgeführt werden.

8.1.3.6 Wenn automatisches Prüfgerät zur Verifizierung der Richtigkeit von Hardware der Klasse 2 verwendet wird, beziehen sich die oben genannten detaillierten Unabhängigkeitsforderungen eher auf jenes Personal, das das automatische Prüfgerät auslegt, als auf das Personal, das die mit automatischem Prüfgerät durchgeführten Prüfungen überwacht. Jedoch bei Hardware der Klasse 1 dürfen Personen nicht für die Durchführung von Prüfungen (mit oder ohne automatischem Prüfgerät) an Hardwarekomponenten verantwortlich sein, die von ihnen entwickelt wurden.

8.1.3.7 Wenn für die Entwicklung von Hardware der Klasse 1 ein automatisches Prüfgerät verwendet wird und automatisch Testläufe durchführt, muss Unabhängigkeit sichergestellt werden zwischen:

- den Personen, die die Hardware auslegen und den Entwicklern des Prüfszenarios;
- den Personen, die die Hardware auslegen und dem für die Durchführung der Prüfungen verantwortlichen Gerät.

8.1.3.8 Für die Entwicklung von Hardware der Klasse 2 muss Unabhängigkeit sichergestellt werden:

- wenn kein automatisches Prüfgerät verwendet wird, zwischen den Personen, die die Verifizierung vornehmen, und denen, die die Hardware auslegen;
- wenn ein automatisches Prüfgerät verwendet wird, das automatisch Testläufe durchführt, zwischen den Personen, die das zu prüfende Produkt auslegen und den Entwicklern des Prüfszenarios.

8.1.4 Methoden

8.1.4.1 Kritische Überprüfungen, Audits, Analysen, manuelle oder automatische Prüfungen oder eine Kombination dieser Methoden können verwendet werden, um die Verifizierung der Hardwareauslegung durchzuführen.

8.1.4.2 Die Grundlage für die Auswahl der angewendeten Verifizierungsmethode(n) muss genügend detailliert dokumentiert werden, um eine Auditierung durch Personen zu erlauben, die nicht direkt mit Auslegungs- oder Verifizierungstätigkeiten befasst sind.

8.1.4.3 Für die Auswahl geeigneter Verifizierungsmethoden müssen folgende Punkte, wenn relevant, in Betracht gezogen werden:

- die Sicherheitsklassifizierung des Systems (d. h. Klasse 1 oder Klasse 2, wobei für Klasse 1 die strengsten Verifizierungstechniken verlangt werden);