

	Kernkraftwerke Software für Rechner mit sicherheitstechnischer Bedeutung Teil 2: Vorkehrungen gegen Versagen aufgrund von Softwarefehlern, Verwendung von Software-Werkzeugen und von vorgefertigter Software (IEC 60880-2:2000)	DIN IEC 60880-2
VDE	Diese Norm ist zugleich eine VDE-Bestimmung im Sinne von VDE 0022. Sie ist nach Durchführung des vom VDE-Vorstand beschlossenen Genehmigungsverfahrens unter nebenstehenden Nummern in das VDE-Vorschriftenwerk aufgenommen und in der etz Elektrotechnische Zeitschrift bekannt gegeben worden.	Klassifikation VDE 0491 Teil 3-2
ICS 27.120.20; 35.080 Nuclear power plants – Software for computers important to safety – Part 2: Software aspects of defence against common cause failures, use of software tools and of pre-developed software (IEC 60880-2:2000) Centrales nucléaires – Logiciel pour les calculateurs de sûreté – Partie 2: Défense contre les défaillances de cause commune provoquées par le logiciel, utilisation d'outils logiciels et de logiciels prédéveloppés (CEI 60880-2:2000) Die Internationale Norm IEC 60880-2:2000 „Software for computers important to safety for nuclear power plants – Part 2: Software aspects of defence against common cause failures, use of software tools and of pre-developed software“ ist unverändert in diese Deutsche Norm übernommen worden. Beginn der Gültigkeit Diese Norm gilt ab 1. 12. 2001 Nationales Vorwort Für die vorliegende Norm ist das nationale Arbeitsgremium GUK 967.1 „Reaktorinstrumentierung“ der DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE zuständig. Bei Fragen der Interpretation von Aussagen wird empfohlen, ergänzend auf die zu Grunde liegende, in englischer und französischer Sprache erschienene IEC-Publikation zurückzugreifen. Norm-Inhalt war veröffentlicht als E DIN IEC 60880-1:1999-11. Die Internationale Norm wurde vom SC 45A „Reactor instrumentation“ des TC 45 „Nuclear instrumentation“ der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet. Diese Norm, deren Anwendung international empfohlen wird, gibt das höchstmögliche Maß internationaler Übereinstimmung für das behandelte Sachgebiet wieder. Die Auslegung kerntechnischer Anlagen in Deutschland wird wesentlich durch die Strahlenschutzverordnung, die BMI-Kriterien, die KTA-Regeln und die RSK-Leitlinien bestimmt. Fortsetzung Seite 2 bis 39 DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE		

In der Reihe VDE 0491 sind erschienen:

- **DIN IEC 61226 (VDE 0491 Teil 1)**, *Kernkraftwerke – Sicherheitsleittechnik – Kategorisierung (IEC 61226:1993)*
- **DIN IEC 60880-2 (VDE 0491 Teil 3-2)**, *Kernkraftwerke – Software für Rechner mit sicherheitstechnischer Bedeutung – Teil 2: Vorkehrungen gegen Versagen aufgrund von Softwarefehlern, Verwendung von Software-Werkzeugen und von vorgefertigter Software (IEC 60880-2:2000)*
- **DIN IEC 62117 (VDE 0491 Teil 4)**, *Kernkraftwerke – Druckwasserreaktoren – Überwachung ausreichender Kühlung des Kerns im abgeschalteten Zustand des Reaktors (IEC 62117:1999)*

Als weitere Teile der Reihe VDE 0491 sind derzeit vorgesehen:

- **DIN IEC 61513 (VDE 0491 Teil 2)**, *Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Allgemeine Systemanforderungen (IEC 61513:2001)*
- **DIN IEC 61839 (VDE 0491 Teil 5)**, *Kernkraftwerke – Auslegung von Warten – Analyse und Zuordnung der Funktionen (IEC 61839:2000)*

Änderungen

Gegenüber DIN IEC 60880:1987-08 wurden folgende Änderungen vorgenommen:

- a) Diese Norm ersetzt bzw. ergänzt DIN IEC 60880:1987-08 in Bezug auf die im Titel genannten Aspekte der Vorkehrungen gegen Versagen aufgrund von Softwarefehlern, Verwendung von Software-Werkzeugen und von vorgefertigter Software.
- b) Beschränkung auf Software-Aspekte (Systemaspekte werden in **DIN IEC 61513 (VDE 0491 Teil 2)** behandelt – z. Z. in Vorbereitung.
- c) Vollständige Überarbeitung und Aktualisierung des gesamten Inhalts.

Frühere Ausgaben

DIN IEC 60880:1987-08

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.

Der Zusammenhang der zitierten Normen mit den entsprechenden Deutschen Normen ist nachstehend wiedergegeben. Zum Zeitpunkt der Veröffentlichung dieser Norm waren die angegebenen Ausgaben gültig.

IEC hat 1997 die Benummerung der IEC-Publikationen geändert. Zu den bisher verwendeten Normnummern wird jeweils 60000 addiert. So ist zum Beispiel aus IEC 68 nun IEC 60068 geworden.

Tabelle NA.1

Europäische Norm	Internationale Norm	Deutsche Norm	Klassifikation im VDE-Vorschriftenwerk
–	IEC 60880:1986 ^{a)}	DIN IEC 60880:1987-08	–
–	IEC 61226:1993 ^{a)}	DIN IEC 61226 (VDE 0491 Teil 1):1997-07	VDE 0491 Teil 1
EN 61508-4:2001	IEC 61508-4:1998	–	–
–	IEC 61513:2001 ^{a)}	– ^{b)}	– ^{b)}
–	ISO/IEC 9126:1991	DIN 66272:1994-10	–
–	IAEA 50-C-D:1988	–	–
–	IAEA 50-SG-D11:1986	–	–
–	IEEE 610:1990	–	–

^{a)} Im Originaltext der IEC 60880-2:2000 wird immer nur undatiert auf IEC 60880, IEC 61226 bzw. IEC 61513 verwiesen, gemeint sind aber jeweils die angegebenen Ausgaben.

^{b)} In Vorbereitung, siehe Nationales Vorwort; z. Z. Entwurf E DIN IEC 61513:2000-01

Nationaler Anhang NB (informativ) Literaturhinweise

DIN 40719-6, *Schaltungsunterlagen – Regeln für Funktionspläne*; IEC 60848 modifiziert

DIN 66272, *Informationstechnik – Bewerten von Softwareprodukten – Qualitätsmerkmale und Leitfaden zu ihrer Verwendung*; Identisch mit ISO/IEC 9126:1991

DIN EN 61069-2, *Leittechnik für industrielle Prozesse – Ermittlung der Systemeigenschaften zum Zweck der Eignungsbeurteilung eines Systems – Teil 2: Methodik der Eignungsbeurteilung (IEC 61069-2:1993)*; Deutsche Fassung EN 61069-2:1994

DIN EN ISO 9001, *Qualitätsmanagementsysteme – Modell zur Qualitätssicherung/QM-Darlegung in Design/Entwicklung, Produktion, Montage und Wartung (ISO 9001:1994)*; Dreisprachige Fassung EN ISO 9001:1994

Diese wurde 2000-12 ersetzt durch DIN EN ISO 9001, *Qualitätsmanagementsysteme – Anforderungen (ISO 9001:2000)*; Dreisprachige Fassung EN ISO 9001:2000

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

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

DIN IEC 61226 (VDE 0491 Teil 1), *Kernkraftwerke – Sicherheitsleittechnik – Kategorisierung (IEC 61226:1993)*

E DIN IEC 61513, *Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Allgemeine Systemanforderungen (IEC 45A/355/CDV:1999)*

Deutsche Übersetzung

Software für Rechner mit sicherheitstechnischer Bedeutung in Kernkraftwerken
Teil 2: Vorkehrungen gegen Versagen aufgrund von Softwarefehlern,
Verwendung von Software-Werkzeugen und von vorgefertigter Software

Inhalt

	Seite
Vorwort	5
Einführung	6
1 Anwendungsbereich.....	6
2 Normative Verweisungen	7
3 Begriffe und Abkürzungen.....	7
4 Anforderungen und Empfehlungen	11
4.1 Vorkehrungen gegen Software-CCF.....	11
4.1.1 Allgemeines.....	11
4.1.2 Software-Auslegung gegen CCF	12
4.1.3 Ursachen und Auswirkungen von Software-CCF	12
4.1.4 Implementierung von Diversität	13
4.1.5 Abwägung der Vor- und Nachteile bei Verwendung von Diversität.....	14
4.2 Software-Werkzeuge für die Erstellung von Software	14
4.2.1 Allgemeines.....	14
4.2.2 Auswahl der Werkzeuge	14
4.2.3 Anforderungen an Werkzeuge	15
4.3 Qualifizierung vorgefertigter Software.....	19
4.3.1 Allgemeines.....	19
4.3.2 Allgemeine Anforderungen.....	20
4.3.3 Bewertungs- und Beurteilungsprozess	20
4.3.4 Anforderungen an die Systemintegration und Wartung vorgefertigter Software	26
 Anhang A (informativ) Betrachtungen zum CCF und zur Diversität.....	 29
A.1 Software-CCF.....	29
A.2 Mögliche CCF-Ursachen und -Auswirkungen.....	29
A.3 Vorkehrungen gegen CCF	30
A.4 Nachweis der Fehlerfreiheit.....	30
A.5 Diversitätseigenschaften	31
A.6 Nachteile, Vorteile und Begründung von Diversität	32
 Anhang B (informativ) Anforderungen der IEC 60880:1986 zur Verwendung und Qualifizierung von Software-Werkzeugen.....	 33

Anhang C (informativ) Werkzeuge zur Erstellung und Prüfung von Spezifikation, Entwurf und Code.....	34
C.1 Konstruktionswerkzeuge.....	34
C.2 Analysewerkzeuge.....	35
 Anhang D (informativ) Anforderungen der IEC 60880:1986 in Hinblick auf vorgefertigte Software.....	36
D.1 Zusammenfassung der Anforderungen der IEC 60880:1986 zur Verwendung vorgefertigter Software).....	36
D.2 Dokumentation der Bewertung vorgefertigter Software.....	36
D.3 Anleitung zur Auswahl relevanter Anforderungen der IEC 60880:1986.....	37
D.4 Anleitung zur Einstufung von Mängeln und kompensierenden Faktoren.....	37
D.5 Sammlung und Bewertung von Daten zur Betriebshistorie.....	38
 Literaturhinweise.....	39
 Bild 1 – Übersicht über den Qualifizierungsprozess vorgefertigter Software.....	27
Bild 2 – Zusammenhänge zwischen der Bewertung und Beurteilung vorgefertigter Software und dem Qualifizierungsplan des Systems, in das die Software integriert ist.....	28

Vorwort

- 1) Die IEC (Internationale Elektrotechnische Kommission) ist eine weltweite Normungsorganisation, die alle Nationalen Elektrotechnischen Komitees (Nationale Komitees der IEC) umfasst. Die IEC hat das Ziel, die internationale Zusammenarbeit in allen Fragen der Normung auf dem Gebiet der Elektrotechnik und Elektronik zu fördern. Zu diesem Zweck und neben anderen Aktivitäten veröffentlicht die IEC Internationale Normen. Mit der Vorbereitung sind die Technischen Komitees beauftragt. Jedes Nationale Komitee der IEC, das an dem behandelten Thema interessiert ist, darf an dieser Vorbereitungsarbeit teilnehmen. Internationale Organisationen, Regierungs- und Nichtregierungsstellen, die mit der IEC in Verbindung stehen, nehmen ebenfalls an diesen Vorbereitungsarbeiten teil. Die IEC arbeitet eng mit der Internationalen Organisation für Normung (ISO) nach den in der Vereinbarung zwischen beiden Organisationen festgelegten Bedingungen zusammen.
- 2) Die offiziellen Beschlüsse oder Vereinbarungen der IEC über technische Fragen, die in Technischen Komitees von Vertretern aller an dem behandelten Thema besonders interessierten Nationalen Komitees erarbeitet werden, bringen das höchstmögliche Maß internationaler Übereinstimmung für das behandelte Sachgebiet zum Ausdruck.
- 3) Sie stellen Empfehlungen zur internationalen Anwendung dar, die als Normen, Fachberichte oder Leitlinien veröffentlicht werden und als solche von den Nationalen Komitees angenommen sind.
- 4) Um die internationale Vereinheitlichung zu fördern, verpflichten sich die Nationalen Komitees der IEC, Internationale Normen der IEC so durchschaubar wie möglich in ihren nationalen und regionalen Normen anzuwenden. Jede Abweichung zwischen der IEC-Norm und der entsprechenden nationalen oder regionalen Norm muss in dieser deutlich gekennzeichnet werden.
- 5) Die IEC hat kein Verfahren für die Kennzeichnung der Konformität festgelegt und übernimmt keine Verantwortung, wenn ein Gegenstand als konform mit einer ihrer Normen erklärt wird.
- 6) Es besteht die Möglichkeit, dass Bestandteile dieser Internationalen Norm Gegenstand von Patentrechten sind. Die IEC hat nicht die Verantwortung, das Vorhandensein solcher Patentrechte festzustellen und auf deren Existenz hinzuweisen.

Die Internationale Norm IEC 60880-2 wurde vom Unterkomitee 45A „Reactor instrumentation“ des Technischen Komitees 45 „Nuclear instrumentation“ der IEC ausgearbeitet.

Der Text dieser Norm basiert auf den folgenden Dokumenten:

FDIS	Abstimmungsbericht
45A/402/FDIS	45A/406/RVD

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

Die Anhänge A, B, C und D dienen nur zur Information.

Wenn IEC 60880:1986 überarbeitet ist, wird diese als IEC 60880-1 veröffentlicht werden.

Das Komitee hat entschieden, dass diese Publikation bis 2006 unverändert gültig sein soll. Dann wird die Publikation entsprechend der Entscheidung des Komitees

- bestätigt,
- zurückgezogen,
- durch eine überarbeitete Ausgabe ersetzt oder
- geändert.

Einführung

Der vorliegende Teil der Reihe IEC 60880 beschreibt Anforderungen an die Software für rechnerbasierte Sicherheitssysteme in Kernkraftwerken und sollte zusammen mit IEC 60880 gelesen werden. Dieser Teil enthält Anforderungen zu verschiedenen Themen, die sich aufgrund der Entwicklung der Technik und Erfahrungen mit Software-Systemen in sicherheitsrelevanten Anwendungen seit der Publikation der IEC 60880:1986 ergeben haben.

Vorkehrungen gegen Softwarefehler, die zum Versagen rechnerbasierter Systeme aufgrund gemeinsamer Ursache führen können, sind entsprechend IAEA 50-C-D zu treffen; technische Anforderungen für solche Vorkehrungen werden angegeben. Die Anwendung rechnergestützter Werkzeuge hat erheblich zugenommen; Empfehlungen zu deren Verwendung werden gegeben. Praktische Anwendungen von Software für rechnerbasierte Sicherheitssysteme hängen oft vom Einsatz vorgefertigter Software ab; auch dazu werden Anforderungen und Empfehlungen gegeben.

Der vorliegende Teil der Reihe IEC 60880 bezieht sich auf die grundlegende Sicherheitsnorm **IEC 61513**.

Er gilt für leittechnische Funktionen der Kategorie A nach **IEC 61226** und die diese realisierenden Systeme und Einrichtungen (FSE).

ANMERKUNG Entsprechend dem Klassifikationsschema der **IEC 61513** werden Funktionen der Kategorie A durch Systeme der Klasse 1 realisiert, die den Sicherheitssystemen nach IAEA entsprechen.

1 Anwendungsbereich

Dieser Teil der IEC 60880 gilt für Software rechnerbasierter Sicherheitssysteme in Kernkraftwerken. Er beinhaltet Anforderungen an Software für leittechnische Funktionen der Kategorie A und die diese realisierenden Systeme und Einrichtungen (FSE). Er behandelt

- Vorkehrungen gegen durch Software verursachtes Versagen aufgrund gemeinsamer Ursache (CCF);
- automatisierte Werkzeuge zur Erstellung von Software für sicherheitstechnisch wichtige Systeme;
- Verwendung vorgefertigter Software.

Die angemessene Aufbereitung und Überprüfung von Daten wird innerhalb dieser Themen behandelt.

2 Normative Verweisungen

Die folgenden normativen Dokumente enthalten Festlegungen, die durch Verweisung in diesem Text Bestandteil dieser Internationalen Norm sind. Bei datierten Verweisungen gelten spätere Änderungen oder Überarbeitungen dieser Publikationen nicht. Anwender dieser Internationalen Norm werden jedoch gebeten, die Möglichkeit zu prüfen, die jeweils neuesten Ausgaben der nachfolgend angegebenen normativen Dokumente anzuwenden. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen normativen Dokuments. Mitglieder von ISO und IEC führen Verzeichnisse der gültigen Internationalen Normen.

IEC 60880:1986, *Software for computers in the safety systems of nuclear power stations*^{N1)}

IEC 61226:1993, *Nuclear power plants - Instrumentation and control systems important for safety – Classification*^{N1)}

IEC 61508-4:1998, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations*

IEC 61513, *Nuclear power plants – Instrumentation and control for systems important to safety – General requirements for systems (wird demnächst veröffentlicht)*^{N1) N2)}

ISO/IEC 9126:1991, *Information technology – Software product evaluation - Quality characteristics and guidelines for their use*

IAEA 50-C-D (rev. 1):1988, *Code on the safety of nuclear power plants – Design*^{N3)}

IAEA 50-SG-D11:1986, *General design safety principles for nuclear power plants – A safety guide*^{N3)}

IEEE 610:1990, *Standard glossary of software engineering terminology*

3 Begriffe und Abkürzungen

Für die Anwendung dieser Norm gelten die in IEC 60880 und IAEA Safety Series 50-C-D angegebenen und die nachfolgenden Begriffe.^{N4)}

ANMERKUNG 1 „Muss“ (en: shall), „sollte“ (en: should) und „kann/darf“ (en: may) werden entsprechend den IEC-Direktiven verwendet.

ANMERKUNG 2 Zur Verdeutlichung der Begriffe Fehlverhalten/Irrtum (en: mistake/error), Fehler (en: fault), Versagen (en: failure) und Signaltrajektorie (en: signal trajectory) wird das folgende Beispiel gegeben:

Ein **Fehlverhalten/Irrtum** einer Person oder ein fehlerhafter Prozess bei der Produktion hat einen **Fehler** im Produkt zur Folge. Wird das Produkt verwendet, ohne dass der **Fehler** behoben wurde, kann es dennoch zufriedenstellend arbeiten oder aber versagen. Wird durch die Anwendung der fehlerhafte Produktteil angesprochen, so versagt das Produkt, wenn keine andere Vorkehrung das **Versagen** verhindert. Ein **Versagen** tritt also ein, wenn sowohl ein Fehler im Produkt vorhanden ist als auch der fehlerhafte Produktteil angesprochen wird, insoweit keine andere Vorkehrung gegen dieses Versagen getroffen ist. Bei Software erfolgt das Ansprechen eines **fehlerhaften Programmteils** durch eine **Signaltrajektorie**.

^{N1)} Nationale Fußnote: Im weiteren Text der IEC 60880-2:1990 wird immer nur undatiert auf IEC 60880, **IEC 61226** bzw. IEC 61513 verwiesen, gemeint sind aber jeweils die angegebenen Ausgaben. Die Verweisungen im Text sind in der deutschen Übersetzung entsprechend korrigiert.

^{N2)} Nationale Fußnote: IEC 61513 ist mit Ausgabe 2001-03 erschienen; siehe Nationales Vorwort.

^{N3)} Nationale Fußnote: Die Neuausgaben der IAEA-Dokumente werden voraussichtlich 2001 erscheinen.

^{N4)} Nationale Fußnote: Die angegebenen Begriffe wurden nach deutscher Benennung sortiert, um ein Auffinden durch den Anwender dieser Norm zu erleichtern. Daher entfällt hier die Nummerierung der deutschen Benennungen, die englischen Benennungen und ihre Nummerierung nach IEC 60880-2:2000 sind in Klammern angegeben.

Animation

(en: animation; 3.1)

Prozess, durch den das in einer Spezifikation festgelegte Verhalten mit aktuellen Werten angezeigt wird, abgeleitet aus den Gleichungen für dieses Verhalten und einigen Eingangswerten

Anwendungsfunktion

(en: application function; 3.2)

Funktion eines leittechnischen Systems, die eine Aufgabe in Verbindung mit dem gesteuerten Prozess und nicht mit dem Funktionieren des Systems selbst erfüllt

[abgeleitet von 2.1 von IEC 60880:1986]

anzunehmende versagensauslösende Ereignisse

AVE

(en: postulated initiating events (PIE); 3.16)

Ereignisse, die zu den zu betrachtenden betrieblichen Vorkommnissen oder Auslegungsstörfällen und deren Folgewirkungen führen

[IAEA 50-C-D]^{N5})

Betriebssoftware

(en: operational system software; 3.15)

Software, die auf dem Zielprozessor während dessen Betriebs läuft, wie z. B.: Eingangs-/Ausgangstreiber und Dienste, Interrupt-Management, Scheduler, Kommunikationstreiber, anwendungsorientierte Bibliotheken, on-line-Diagnostik, Redundanz und Management der abgestuften Reduktion von Funktionalität (en: graceful degradation)

Bibliothek

(en: library; 3.13)

Sammlung von Software-Elementen, die miteinander in Beziehung stehen, aber zur Integration in das letztliche Software-Produkt einzeln ausgewählt werden

Daten

(en: data; 3.5)

Darstellung von Information oder Anweisungen in einer für die Übertragung, Auswertung oder Verarbeitung mittels Rechnern geeigneten Weise

[übernommen aus IEEE 610]

ANMERKUNG Daten, die zur Definition von Parametern und zur Durchführung von Anwendungs- und Servicefunktionen im System dienen, werden „Applikationsdaten“ genannt.

Diversität^{N6})

(en: diversity; 3.6)

Vorhandensein von zwei oder mehreren unterschiedlichen Verfahren oder Mitteln, um ein bestimmtes Ziel zu erreichen. Diversität ist besonders geeignet als Schutzmaßnahme gegen „Common-Mode-Fehler“. Sie kann erreicht werden, indem physikalisch unterschiedliche Systeme eingesetzt werden oder durch funktionale Diversität, bei der gleichartige Systeme ein bestimmtes Ziel über unterschiedliche Verfahren erreichen (siehe [Abschnitt 3 von IEC 61226:1993](#))

dynamische Analyse

(en: dynamic analysis; 3.7)

Prozess der Bewertung eines Systems oder einer Komponente aufgrund des dynamischen Verhaltens im Betrieb. Gegenstück zur statischen Analyse (siehe IEEE 610)

^{N5}) Nationale Fußnote: In der IAEA-Definition sind auch auslegungsüberschreitende Störfälle eingeschlossen.

^{N6}) Nationale Fußnote: Auch „diversitäre Redundanz“ genannt.

Fehler

(en: fault; 3.9)

Mangel an einer Hardware-, Software- oder Systemkomponente. Fehler werden eingeteilt in zufällige Fehler (z. B. aufgrund von Verschleißerscheinungen von Hardware) und systematische Fehler (z. B. Auslegungsfehler); bei Software schließen diese Programmier- und Spezifikationsfehler ein

ANMERKUNG Ein Fehler (insbesondere ein Auslegungsfehler) kann in einem Teil des Systems unentdeckt bleiben, bis besondere Bedingungen oder Signaltrajektorien auf diesen Teil des Systems so einwirken, dass die resultierende Funktion nicht mit der vorgesehenen Funktion übereinstimmt. Dies führt zu einem Versagen des betreffenden Teils des Systems.

funktionale Diversität

(en: functional diversity; 3.10)

Anwendung der Diversität auf der Funktionsebene (z. B. Ableitung eines Abschaltkriteriums sowohl aus Druck- als auch Temperaturgrenzwerten)

Funktionen und die dazugehörigen Systeme und Einrichtungen

(en: functions, and associated systems and equipment (FSE); 3.11)

Funktionen werden zu einem bestimmten Zweck ausgeführt oder um ein Ziel zu erreichen. Die dazugehörigen Systeme und Einrichtungen sind die Komponentengruppen und die Komponenten selbst, die eingesetzt werden, um die Funktionen durchzuführen (siehe [Abschnitt 3 von IEC 61226:1993](#))

Hilfssoftware

(en: support software; 3.23)

Software, die Entwicklung, Prüfung oder Pflege anderer Software unterstützt, wie z.B. Compiler, Code-Generatoren, Simulatoren, off-line-Diagnostik, Initialisierer (siehe [4.2](#))

Kanal

(en: channel; 3.3)

eigenständiger Pfad, über den Informationen durch ein redundantes oder verteiltes System übertragen werden. Dieser Pfad kann ebenfalls Redundanz enthalten

menschliches Fehlverhalten (oder Irrtum)

(en: human error (or mistake); 3.12)

Handlung oder Vorgehensweise eines Menschen, die eine unbeabsichtigte Folge hat

Multiversions-Software

(en: n-version or multi-version software; 3.14)

Satz unterschiedlicher Programme, die entwickelt wurden, um einer gemeinsamen Anforderung und einer gemeinsamen Abnahmeprüfung zu genügen. Diese Versionen laufen gleichzeitig und voneinander unabhängig ab, üblicherweise in redundanter Hardware. Identische Eingangssignale von Prüfsystemen oder entsprechende Eingangssignale in redundanten Systemen werden verwendet. Zur Entscheidung bei unterschiedlichen/widersprüchlichen Ausgangssignalen der verschiedenen Versionen werden vorbestimmte Strategien eingesetzt, wie z. B. Mehrheitsentscheidungen.

Signaltrajektorie

(en: signal trajectory; 3.19)

Zeitabläufe aller Gerätezustände, interner Zustände, Eingangssignale und Bediener-Eingaben, die den Ausgangszustand eines Systems bestimmen

Software-Version

(en: software version; 3.20)

jeweilige Ausgabe eines Software-Produkts, die durch Änderung oder Korrektur eines vorhergehenden Software-Produkts erstellt wurde

Spezifikation

(en: specification; 3.21)

Dokument, in dem die Anforderungen, Funktionsweisen oder andere Eigenschaften eines Systems oder einer Komponente, oft auch die Verfahren zur Überprüfung der Einhaltung dieser Angaben, in kompletter, präziser und verifizierbarer Weise angegeben sind (siehe IEEE 610)

ANMERKUNG Es gibt verschiedene Arten von Spezifikationen, z. B. Anforderungs- oder Systemspezifikationen.

statische Analyse

(en: static analysis; 3.22)

Prozess der Bewertung eines Systems oder einer Komponente aufgrund von Form, Struktur, Inhalt oder Dokumentation. Gegenstück zur dynamischen Analyse

Systemsoftware

(en: system software; 3.24)

Software, die für ein bestimmtes Rechnersystem oder eine Rechnerfamilie erstellt wurde, um den Betrieb und die Instandhaltung/Pflege des Rechnersystems und zugehöriger Programme zu erleichtern, z. B. Betriebssysteme, Compiler, Dienstprogramme. Systemsoftware besteht üblicherweise aus Betriebssoftware und Hilfssoftware

Versagen Ausfall ^{N7)}

(en: failure; 3.8)

Versagen liegt vor, wenn die ausgeführte Funktion von der vorgesehenen Funktion abweicht

ANMERKUNG Ein Versagen ist das Ergebnis eines Hardwarefehlers, eines Softwarefehlers, eines Systemfehlers oder von Fehlverhalten bei Bedienung oder Wartung und einer damit verbundenen Signaltrajektorie, die zu dem Versagen führt ^{N8)}.

Versagen aufgrund gemeinsamer Ursache

CCF ^{N9)}

(en: common cause failure (CCF); 3.4)

Versagen infolge eines oder mehrerer Ereignisse, das/die ein koinzidentes Versagen in zwei oder mehreren eigenständigen Kanälen eines mehrkanaligen Systems oder in verschiedenen Systemen verursacht/verursachen, so dass es zu einem Versagen des Systems/der Systeme kommt

[3.6.10 von IEC 61508-4, modifiziert]

ANMERKUNG 1 Abhängig von den Umständen kann der CCF auf Systemebene oder auf der Ebene von Systemen betrachtet werden, die eine Sicherheitsgruppe darstellen.

ANMERKUNG 2 Siehe Definition von „Versagen“.

vorgefertigte Software

(en: pre-developed software (PDS); 3.17)

Software, die bereits vorgefertigt, als kommerzielles oder proprietäres Produkt verfügbar und für den Einsatz in einem rechnerbasierten System vorgesehen ist

wiederverwendbar

(en: reusable; 3.18)

bezieht sich auf ein Software-Modul, das in mehr als einem Rechnerprogramm oder Software-System verwendet werden kann (abgeleitet von IEEE 610).

^{N7)} Nationale Fußnote: Wenn Hardware oder Teilsysteme (z. B. ein Strang eines redundanten Systems) betroffen sind, wird „failure“ mit „Ausfall“ übersetzt.

^{N8)} Nationale Fußnote: Bei Hardware kann der Ausfall allein aufgrund des Alterungseffekts einer Komponente erfolgen.

^{N9)} Nationale Fußnote: Im Folgenden wird für „Versagen aufgrund gemeinsamer Ursache“ die Abkürzung „CCF“ verwendet. Durch Softwarefehler verursachtes CCF wird kurz „Software-CCF“ genannt.

4 Anforderungen und Empfehlungen

Im Folgenden wird der Begriff „Anforderungen“ als umfassender Begriff sowohl für Anforderungen als auch für Empfehlungen verwendet. Die Unterscheidung erfolgt in den jeweiligen Abschnitten durch die Verwendung von „muss“ für Anforderungen und „sollte“ für Empfehlungen.

4.1 Vorkehrungen gegen Software-CCF

Dieser Abschnitt enthält Anforderungen für Vorkehrungen gegen Fehler bei der Softwareentwicklung und -Programmierung, die zu CCF von Funktionen der **Kategorie A nach IEC 61226** führen können.

4.1.1 Allgemeines

CCF kann in leittechnischen Systemen und Einrichtungen auftreten, in denen verschiedene Maßnahmen gegen die Auswirkungen ein und desselben versagenauslösenden Ereignisses getroffen wurden (siehe 5.3.1 von IEC 61513:2001). Software selbst hat kein CCF-Verhalten. Vielmehr bezieht sich CCF auf das Versagen des Systems aufgrund von Fehlern in den funktionalen Anforderungen, der Systemauslegung oder der Software.

Gestufte Maßnahmen (en: defence in depth) werden durch die Internationale Atomenergiebehörde für alle Sicherheitsmaßnahmen gefordert (siehe 204 von IAEA 50-C-D), seien sie organisatorischer oder betrieblicher Art oder auf die Auslegung bezogen, um überlappende Maßnahmen sicherzustellen, so dass ein Versagen eines Teilsystems innerhalb des Gesamtsystems kompensiert oder korrigiert wird. ^{N10)}

Das Einzelausfallkriterium (siehe 329 bis 336 von IAEA 50-C-D) erfordert, dass die Gesamtheit der Sicherheitssysteme in der Lage ist, ihren vorgesehenen Zweck auch bei einem zufällig auftretenden Einzelausfall an einer beliebigen Stelle innerhalb der Sicherheitssysteme zu erfüllen.

Softwarefehler sind systematische Fehler, keine zufälligen Fehler, und daher kann das Einzelausfallkriterium auf die Softwareentwicklung nicht in gleicher Weise angewendet werden wie auf die Hardware. Für die Anwendung des DiD-Konzepts müssen während des gesamten Entwicklungs- und Prüfprozesses mögliche Auswirkungen von Software-CCF aufgrund von Softwarefehlern innerhalb jeder Maßnahmenstufe und zwischen redundanten Maßnahmenstufen betrachtet und geeignete Gegenmaßnahmen getroffen werden, z. B.:

- a) bei der Entwicklung, Verifizierung und Validierung jeder einzelnen Maßnahmenstufe;
- b) bei der Bewertung der Unabhängigkeit und Diversität redundanter Maßnahmenstufen.

Eine Möglichkeit zur Erhöhung der Zuverlässigkeit von Systemen und zur Verringerung des CCF-Potentials ist die Verwendung der Diversität (siehe 337 bis 339 von IAEA 50-C-D Rev. 1).

4.1.1.1 Anforderungen der IEC 60880:1986

4.2 von IEC 60880:1986 fordert, dass Anforderungen zur Zuverlässigkeit des Systems Grundlage der Beschreibung der Konfiguration des Rechnersystems sein müssen, und verweist auf A2.2 der IEC 60880:1986. Dieser gibt relevante Faktoren an (einschließlich DiD, abgestufte Reduktion von Funktionalität (en: graceful degradation), Beherrschung von Versagen, funktionale Diversität, Software-Diversität, räumliche Trennung und Modulbauweise, Entkopplung, logische Trennung), die zur Vermeidung von CCF verwendet werden können, beschreibt diese aber nicht näher. Daher werden in 4.1 dieser Norm Wege zur Beurteilung des Potentials für Software-CCF und Techniken zur Vermeidung von Software-CCF beschrieben.

^{N10)} Nationale Fußnote: Für dieses Auslegungsprinzip hat sich inzwischen der englische Begriff „defence in depth“ (DiD) etabliert. Im Folgenden wird die Abkürzung „DiD“ verwendet. Das DiD-Konzept ist durch die Anwendung gestufter Maßnahmen gegen die Auswirkungen versagenauslösender Ereignisse gekennzeichnet. In IAEA 50-C-D sind 4 Stufen definiert, die von Maßnahmen bei der Abweichung vom Normalbetrieb (Stufe 1) bis zur Verminderung der Konsequenzen schwerer Störfälle (Stufe 4) reichen. Je nach Anforderung können innerhalb einer Maßnahmenstufe redundante oder auch diversitäre Maßnahmen getroffen werden.

4.1.1.2 Grundlagen für Maßnahmen gegen Software-CCF

Der grundlegende Ansatz für das Treffen von Maßnahmen gegen Softwarefehler ergibt sich aus der Überlegung, dass jeder Softwarefehler so lange im betroffenen System oder Kanal verbleibt, bis er erkannt und berichtigt ist, und dass jeder Softwarefehler vor der Berichtigung ein Versagen aufgrund einer den fehlerhaften Programmteil ansprechenden Signaltrajektorie verursachen kann. Wenn der Fehler in zwei oder mehr Systemen oder Kanälen, die unterschiedliche Maßnahmenstufen gegen die Auswirkungen desselben anzunehmenden versagenauslösenden Ereignisses realisieren, enthalten ist (siehe 5.3.1.5 von IEC 61513:2001), und diese den spezifischen Signaltrajektorien innerhalb eines kritischen Zeitintervalls ausgesetzt werden, können beide (oder alle) Systeme oder Kanäle versagen, d. h. es tritt ein CCF ein. Eine ausführliche Beschreibung dieser Bedingungen ist in [A.1](#) angegeben.

Die Möglichkeit von Software-CCF sollte daher in der Entwurfsphase berücksichtigt werden. Wenn CCF-Bedingungen vorhersehbar sind, können Änderungen der Auslegung und Gegenmaßnahmen, einschließlich des Einsatzes diversitärer Software, zum Schutz gegen Software-CCF erforderlich sein.

Der Grad der Verbesserung durch Vorkehrungen gegen CCF und der durch Diversität erreichbaren Steigerung der Zuverlässigkeit kann nicht quantifiziert werden. Es ist eine Beurteilung erforderlich, die von der durch die Software erreichbaren qualitativen Zuverlässigkeit ausgeht.

Wenn Fehler aufgrund von menschlichem Fehlverhalten oder Fehlbeurteilungen vor Beginn der Softwareentwicklung gemacht wurden, können diese Fehler zu Fehlern in den Anforderungen und möglichen Systemausfällen führen, gegen die durch Softwareentwicklung alleine keine geeigneten Vorkehrungen getroffen werden können. Vorkehrungen gegen solche CCF auf Systemebene sind in 5.3.1.5 von IEC 61513:2001 behandelt.

Wenn menschliche Fehler während der Softwareentwicklung gemacht werden, können diese Fehler zu Fehlern in der Software und möglicherweise zu Systemversagen führen. Wo solche Fehler den Ausfall von mehr als einem Schutzstrang verursachen, werden sie als Software-CCF betrachtet.

4.1.2 Software-Auslegung gegen CCF

Die grundlegende und wichtigste Maßnahme gegen Software-CCF ist die Erstellung von Software höchster Qualität, d. h. so fehlerfrei wie möglich. Die umfassende Anwendung von Selbsttestfunktionen nach 4.8, 5.1 und A.2.8 von IEC 60880:1986, wie Daten-Plausibilitätsprüfung, Überwachung der Parameterbereiche, zeitliche Begrenzung von Schleifendurchläufen usw., ist ein weiterer wichtiger Faktor zur Begrenzung möglicher Software-CCF.

Anforderungen zur Erzielung einer hoch zuverlässigen Software mit Selbsttestfunktionen werden in IEC 60880:1986 und den nachfolgenden Abschnitten dieser Norm gegeben.

Die Anwendung bewährter Verfahren zur Softwareentwicklung mit Unterstützung durch Software-Werkzeuge zur Erstellung und Prüfung von Software kann die Anzahl der zu treffenden Entwurfsentscheidungen verringern helfen und so zu einer Verringerung der Anzahl der Fehler in der entwickelten Software beitragen.

4.1.3 Ursachen und Auswirkungen von Software-CCF

4.1.3.1 Eine Analyse des Potentials von Software-CCF muss auf Systemebene und/oder auf der Ebene der Gesamtarchitektur der sicherheitstechnisch wichtigen leittechnischen Systeme des Kernkraftwerks durchgeführt und dokumentiert werden.

ANMERKUNG 1 Anforderungen an die leittechnische Architektur sind in 5.3.1 von IEC 61513:2001 angegeben.

ANMERKUNG 2 Anforderungen an die Architektur der einzelnen leittechnischen Systeme sind in 6.1.2 von IEC 61513:2001 angegeben.