

	DIN IEC 62340 (VDE 0491-10)	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

Einsprüche bis 2006-05-31

Entwurf

**Kernkraftwerke –
Leittechnische Systeme mit sicherheitstechnischer Bedeutung –
Versagen gemeinsamer Ursache (CCF)
(IEC 45A/601/CDV:2005)**

Nuclear power plants –
Instrumentation and control systems important to safety –
Common Cause Failure (CCF)
(IEC 45A/601/CDV:2005)

Centrales nucléaires de puissance –
Instrumentation et contrôle commande importants pour la sûreté –
Défaillance de Cause Commune (DCC)
(CEI 45A/601/CDV:2005)

Anwendungswarnvermerk

Dieser Norm-Entwurf wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfes besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise als Datei per E-Mail an **dke@vde.com** in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter **www.dke.de/stellungnahme** abgerufen werden
- oder in Papierform an die DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE, Stresemannallee 15, 60596 Frankfurt am Main.

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevante Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 38 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE

– Entwurf –

E DIN IEC 62340 (VDE 0491-10):2006-04

Beginn der Gültigkeit

Diese Norm gilt ab ...

Nationales Vorwort

Das internationale Dokument IEC 45A/601/CDV:2005 „Nuclear power plants – Instrumentation and control systems important to safety – Common Cause Failure (CCF)“ (CDV, en: Committee Draft for Vote) 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 CDV entsprechend der diesbezüglich durch die IEC erteilten Erlaubnis beigelegt. Die Nutzungsbedingungen für den deutschen Teil des Norm-Entwurfes gelten gleichermaßen auch für den englischen IEC-Text.

Das internationale Dokument wurde vom SC 45A „Instrumentation and control of nuclear facilities“ der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet und den nationalen Komitees zur Stellungnahme und Abstimmung vorgelegt. Es wird jedoch nicht zeitgleich (parallel) bei IEC und CENELEC zur Umfrage gestellt. Derzeit ist also nicht vorgesehen, dieses Dokument als Europäische Norm zu übernehmen.

Da der Abstimmungszeitraum für einen FDIS (en: Final Draft International Standard) nur 2 Monate 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 CDV als DIN-Norm-Entwurf veröffentlicht, um die Stellungnahmen aus der Öffentlichkeit noch vor der Abstimmung berücksichtigen zu können.

Für diesen Norm-Entwurf ist das nationale Arbeitsgremium UK 967.1 „Leittechnik für kerntechnische Anlagen“ der DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE (<http://www.dke.de>) zuständig.

Nationaler Anhang NA (informativ)

Zusammenhang mit Europäischen und Internationalen Normen

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

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

Eine Information über den Zusammenhang der zitierten Normen mit den entsprechenden Deutschen Normen ist nachstehend wiedergegeben.

Tabelle NA.1

Europäische Norm	Internationale Norm	Deutsche Norm	Klassifikation im VDE-Vorschriftenwerk
–	IEC 60671 Neuauflage	DIN IEC 60671 (VDE 0491-100) Entwurf zurzeit in Vorbereitung	VDE 0491-100
–	IEC 60709:2004	DIN IEC 60709 (VDE 0491-7):2006-.... zurzeit in Druck	VDE 0491-7
–	IEC 60780:1998	DIN IEC 60780:2000-12	–
–	IEC 60880:2006 zurzeit in Vorbereitung	vorgesehen als DIN IEC 60880 (VDE 0491-3-2)	VDE 0491-3-2
–	Normen der Reihe IEC 61000-4	Normen der Reihe DIN EN 61000-4 (VDE 0847)	VDE 0847
–	IEC 61226:2005	DIN IEC 61226 (VDE 0491-1):2005-09	VDE 0491-1
–	IEC 61513:2001	DIN IEC 61513 (VDE 0491-2):2002-10 und DIN IEC 61513/A100 (VDE 0491-2/A100):2005-02	VDE 0491-2 VDE 0491-2/A100

Nationaler Anhang NB (informativ)

Literaturhinweise

Normen der Reihe

DIN EN 61000-4 (VDE 0847), *Elektromagnetische Verträglichkeit (EMV) – Prüf- und Messverfahren*.

DIN IEC 60709 (VDE 0491-7):2006-..., *Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Physikalische und elektrische Trennung (IEC 60709:2004)*.

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

DIN IEC 61226 (VDE 0491-1):2005-09, *Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Kategorisierung leittechnischer Funktionen (IEC 61226:2005)*.

DIN IEC 61513 (VDE 0491-2):2002-10, *Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Allgemeine Systemanforderungen (IEC 61513:2001)*.

DIN IEC 61513/A100 (VDE 0491-2/A100):2005-02, *Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Allgemeine Systemanforderungen – Nationaler Anhang ND (informativ): Mitgeltende Festlegungen aus anderen IEC-Normen*.

**Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung –
Versagen gemeinsamer Ursache (CCF)**

Inhalt

	Seite
Einleitung	5
1 Anwendungsbereich	6
2 Normative Verweisungen	7
3 Begriffe	8
4 Abkürzungen	12
5 Auslegungsstrategie zur Beherrschung von CCF	13
5.1 Einleitung	13
5.2 Das Prinzip der Unabhängigkeit	13
6 Anforderungen zur Beherrschung von Fehlern in der Anforderungsspezifikation	14
6.1 Ableitung der Anforderungsspezifikation für die Leittechnik aus der sicherheitstechnischen Auslegungsbasis der Anlage	14
6.2 Anwendung des DiD-Prinzips und der funktionalen Diversität	15
7 Anforderungen für die Spezifikation leittechnischer Systeme	15
7.1 Prinzipielle Fehlermechanismen	15
7.2 Anwendung des DiD-Prinzips in der Systemauslegung	16
8 Toleranz gegen angenommene latente Softwarefehler	16
9 Auslegungsmaßnahmen zur Vermeidung des koinzidenten Versagens von leittechnischen Systemen	17
9.1 Auslegung unabhängiger leittechnischer Systeme	17
9.2 Anwendung funktionaler Diversität	17
9.3 Vermeidung von Ausfallfortpflanzung über Kommunikationspfade	18
9.4 Auslegungsmaßnahmen gegen Systemausfall wegen Wartungsarbeiten	18
9.5 Integrität der leittechnischen Systemhardware	19
9.6 Vorkehrungen gegen Abhängigkeit von externen Daten oder Meldungen	19
9.7 Sicherstellung physikalischer Trennung und Robustheit bezüglich Umgebungsbedingungen	19
10 Anforderungen zur Vermeidung von Systemversagen infolge Wartung während des Betriebs	20

Einleitung

Hintergrund, hauptsächliche Inhalte und Organisation der Norm

Um ein hohes Sicherheitsniveau zu erreichen, wird Redundanz als eines der Schlüsselmerkmale für die Auslegung sicherheitstechnisch wichtiger leittechnischer Systeme angewendet. Weil ein Versagen gemeinsamer Ursache die Wirksamkeit der Redundanz aufheben würde, ist es wesentlich, geeignete Maßnahmen dagegen zu treffen. Die Nuklearindustrie hat Pionierarbeit in Systemauslegung und -konstruktion geleistet, um Versagen gemeinsamer Ursache zu beherrschen. In den vergangenen zwanzig bis dreißig Jahren wurde Übereinstimmung zur Umsetzung einer Reihe von Praktiken für die Bekämpfung des Versagens gemeinsamer Ursache erreicht.

Die vorliegende Norm spricht viele dieser Praktiken an, die für sicherheitstechnisch wichtige Systeme von Kernkraftwerken anwendbar sind. Dabei ist beabsichtigt, den ganzen Umfang der Aspekte zur Beherrschung des Versagens gemeinsamer Ursache anzusprechen und einen Überblick über relevante Anforderungen für leittechnische Systeme zu geben, die für die Ausführung sicherheitstechnisch wichtiger Funktionen (entsprechend IEC 61226) in Kernkraftwerken eingesetzt werden.

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

Die vorliegende Norm ist ein IEC/SC 45A-Dokument der zweiten Ebene, das Versagen gemeinsamer Ursache behandelt. Es ergänzt IEC 61513 und verwandte Normen mit Anforderungen zur Reduzierung und Beherrschung von Ausfällen gemeinsamer Ursache von sicherheitstechnisch wichtigen leittechnischen Funktionen. Die Anforderungen in dieser Norm sind in Sonderheit von den Funktionen der Kategorie A (IEC 61226) einzuhalten, wenn ihr Versagen in Hinblick auf die sicherheitstechnische Auslegung der Anlage nicht akzeptierbar sein würde.

Mehr Details über die Struktur der SC 45A-Normenreihe sind im vierten Abschnitt dieser Einleitung enthalten.

Empfehlungen und Einschränkungen der Anwendung der Norm

Diese Norm gilt für sicherheitstechnisch wichtige leittechnische Systeme neuer Kernkraftwerke sowie für den Ersatz derartiger Systeme in bestehenden Anlagen. Beim Austausch von Systemen kann es notwendig sein, die leittechnischen Funktionen beizubehalten oder zu ertüchtigen. Die Anforderungen in dieser Norm berücksichtigen auch den Ersatz von Leittechnik, der Änderungen in der leittechnischen Struktur nach sich zieht.

Es kann sein, dass für bestehende Anlagen nur eine Teilmenge der Anforderungen anwendbar ist; diese Teilmenge sollte zu Beginn jedes Projekts festgestellt werden. Werden Anforderungen und Empfehlungen in einem leittechnischen Ertüchtigungs- oder Austauschprojekt nicht realisiert, so sollte dies von Fall zu Fall durch eine umfassende Sicherheitsbeurteilung gerechtfertigt werden.

Um die Überlappung von Anforderungen zu vermeiden, wird in dieser Norm auf die relevanten Abschnitte in anderen bestehenden Normen Bezug genommen, insbesondere auf die Normen des nuklearen Sektors IEC 61513, IEC 60709, IEC 60780, IEC 60880. Neue Anforderungen werden formuliert, wenn sie durch diese Normen nicht abgedeckt sind.

Beschreibung der Struktur der IEC SC45A-Normenreihe und der Beziehungen zu weiteren Dokumenten der IEC sowie Dokumenten anderer Organisationen (IAEA, ISO)

Das Eingangsdokument zur IEC/SC 45A-Normenreihe stellt die Norm IEC 61513 dar. Sie enthält allgemeine Anforderungen an die leittechnischen Systeme und Geräte, die zur Ausführung sicherheitstechnisch wichtiger Funktionen in KKW genutzt werden. Durch die IEC 61513 wird die SC 45A-Normenreihe strukturiert.

In IEC 61513 wird direkt auf andere SC 45A-Normen verwiesen, die allgemeine Themen wie die Kategorisierung von Funktionen und die Klassifizierung von Systemen, Qualifizierung, Trennung von Systemen, Maßnahmen gegen Versagen aufgrund gemeinsamer Ursache, Software-Aspekte rechnerbasierter Systeme, Hardware-Aspekte rechnerbasierter Systeme sowie Auslegung von Warten behandeln. Die Normen, auf die

E DIN IEC 62340 (VDE 0491-10):2006-04

direkt verwiesen wird, bilden die zweite Ebene und sollten zusammen mit IEC 61513 als ein in sich konsistenter Satz von Dokumenten betrachtet werden.

Die dritte Ebene bilden SC 45A-Normen, auf die in IEC 61513 nicht direkt verwiesen wird. Diese Normen behandeln spezielles Gerät, technische Methoden oder spezifische Aktivitäten. Sie beziehen sich hinsichtlich der allgemeinen Themen auf die Dokumente der zweiten Ebene, können jedoch im Allgemeinen für sich allein benutzt werden.

Eine vierte Ebene erweitert die SC 45A-Normenreihe mit Technischen Berichten, die nicht normativ sind.

Für IEC 61513 wird ein Darstellungsformat verwendet, das dem der grundlegenden Sicherheitsnorm IEC 61508 ähnlich ist, mit einem Sicherheits-Lebenszyklus als Gesamtrahmen und zusätzlich einem System-Lebenszyklus. Mit IEC 61513 werden die allgemeinen Anforderungen (für Sicherheitssysteme unterschiedlicher industrieller Anwendungen) von IEC 61508-1, -2 und -4, für die Anwendung auf dem nuklearen Sektor umgesetzt. Die Einhaltung der IEC 61513 erleichtert somit die Übereinstimmung mit der Norm IEC 61508, weil deren allgemeine Anforderungen für die nukleare Industrie berücksichtigt wurden. In diesem Rahmen entsprechen IEC 60880 und IEC 62138 für den nuklearen Sektor der Norm IEC 61508-3.

IEC 61513 stützt sich für Themen der Qualitätssicherung sowohl auf ISO als auch auf IAEA 50-C-QA ab.

In der SC 45A-Normenreihe werden die Prinzipien und grundsätzlichen Sicherheitsaspekte im IAEA Code für die Sicherheit von KKW und in der IAEA Sicherheitsserie umgesetzt, insbesondere die Requirements NS-R-1 „Safety of Nuclear Power Plants: Design“ und der Safety Guide NS-G-1.3 „Instrumentation and control systems important to safety in Nuclear Power Plants“. Terminologie und Definitionen in den SC 45A-Normen stimmen mit den von der IAEA verwendeten überein.

1 Anwendungsbereich

Sicherheitstechnisch wichtige leittechnische Systeme können unter Verwendung konventioneller fest-verdrahteter Geräte, rechnerbasierter Geräte oder einer Kombination beider Gerätearten gebaut werden. In dieser Norm werden Anforderungen und Empfehlungen²⁾ für die gesamte Architektur der leittechnischen Systeme angegeben, die entweder eine oder beide der genannten Technologien enthalten können.

Die Zielsetzung dieser Internationalen Norm besteht darin,

- 1) Anforderungen in Bezug auf die Vermeidung von Ausfällen gemeinsamer Ursache (CCF) zu entwickeln, beginnend mit übergeordneten Sicherheitsprinzipien (insbesondere IEC 61226), und CCF durch die Realisierung von unabhängigen leittechnischen Systemen zu beherrschen;
- 2) einen Überblick des gesamten Bereichs der für CCF relevanten Anforderungen zu geben, aber die Überlappung mit Aufgabenfeldern, die schon in anderen Normen angesprochen werden, zu vermeiden (z. B. IEC 60709 für die physikalische und elektische Trennung oder IEC 60880 und IEC 61513).

In vorliegender Norm wird auf die Notwendigkeit einer vollständigen und präzisen Spezifikation der Sicherheitsfunktionen, basierend auf der Analyse der Auslegungsstörfälle und unter Berücksichtigung der hauptsächlichsten Sicherheitsziele der Anlage, abgehoben. Diese Spezifikation ist Voraussetzung für die Entwicklung eines umfassenden Satzes detaillierter Anforderungen für die Auslegung der leittechnischen Systeme in Hinblick auf CCF.

²⁾ Im Folgenden wird der Ausdruck „Anforderungen“ als umfassend für Anforderungen und Empfehlungen verwendet. Die Unterscheidung wird später bei der Diskussion spezieller Vorkehrungen gemacht, wobei Anforderungen durch „muss“ und Empfehlungen durch „sollte“ ausgedrückt werden. Um alle Anforderungen und Empfehlungen klar hervorzuheben, werden die entsprechenden Absätze jeweils mit der Bezeichnung N.N.A, N.N.B usw. begonnen.

Diese Norm stellt Prinzipien und Anforderungen zur Beherrschung von CCF durch Mittel zur Verfügung, die Unabhängigkeit sicherstellen:

- 1) zwischen leittechnischen Systemen, die diversitäre Sicherheitsfunktionen der Kategorie A ausführen, die zum Erreichen desselben Sicherheitszieles beitragen;
- 2) zwischen leittechnischen Systemen mit verschiedenen Funktionen unterschiedlicher Kategorien, wenn z. B. eine Funktion der Kategorie B als Back-up einer Funktion der Kategorie A deklariert wird; und
- 3) zwischen redundanten Strängen ein und desselben leittechnischen Systems.

Die Umsetzung dieser Anforderungen führt zu verschiedenen Arten von Maßnahmen gegen CCF auslösende Ereignisse.

Maßnahmen zum Erreichen eines Schutzes gegen CCF werden in dieser Norm diskutiert in Hinblick auf

- 1) Empfindlichkeit für interne Anlagenstörfälle und externe Störfälle;
- 2) Fortpflanzung physikalischer Effekte in der Hardware (z. B. hohe Spannungen); und
- 3) Vermeidung spezifischer Fehler innerhalb der leittechnischen Systeme, insbesondere
 - Fortpflanzung funktionaler Fehler innerhalb leittechnischer Systeme oder zwischen verschiedenen leittechnischen Systemen (z. B. durch Kommunikation),
 - Bestehen gemeinsamer Fehler, die bei der Auslegung oder während des Betriebs (z. B. Wartungsfehler) eingeschleppt wurden,
 - ungenügende Systemvalidierung, so dass das Systemverhalten als Antwort auf Eingangssignaltransienten nicht den beabsichtigten Sicherheitsfunktionen entspricht,
 - ungenügende Qualifizierung der geforderten Hardware-Eigenschaften, ungenügende Verifizierung der Software-Komponenten, oder ungenügende Verifizierung der Kompatibilität zwischen ausgetauschten und bestehenden Systemkomponenten.

2 Normative Verweisungen

Die folgenden zitierten Dokumente sind für die Anwendung dieses Dokuments erforderlich. 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 60671, *Nuclear power plants – Instrumentation and control systems important to safety – Surveillance testing*

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

IEC 60780, *Nuclear power plants – Electrical equipment of the safety system – Qualification*

IEC 60880, *Nuclear power plants – I&C systems important to safety – Software aspects for computer-based systems performing category A functions*

IEC 61000-4, *Electromagnetic compatibility (EMC) - Part 4: Testing and measurement techniques*

IEC 61226, *Nuclear power plants – Instrumentation and control systems important to safety – Classification of I&C functions*

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

3 Begriffe

Für die Anwendung dieses Dokuments gelten im Allgemeinen die in IEC 61513 und IEC 61226 angegebenen Definitionen. Im Folgenden sind Definitionen genannt, die in Hinblick auf die vorliegende Norm einer besonderen Interpretation bedürfen.

3.1

Versagen gemeinsamer Ursache (CCF)

(en: common cause failure – CCF)

Versagen von zwei oder mehreren Strukturen, Systemen oder Komponenten infolge eines einzelnen spezifischen Ereignisses (IAEA NS-G-1.3)

ANMERKUNG 1 Unter dem koinzidente Versagen von zwei oder mehreren Strukturen, Systemen oder Komponenten wird jenes Versagen verstanden, das durch einen latenten Mangel bei Auslegung oder Herstellung, von Fehlern bei Betrieb oder Wartung verursacht wird, und das durch ein Ereignis, angestoßen von natürlichen Phänomenen oder dem Anlagenbetrieb oder einer menschlichen Handlung oder einem internen Ereignis im leittechnischen System ausgelöst wird.

ANMERKUNG 2 Das koinzidente Versagen wird so interpretiert, dass es auch eine Abfolge von System- oder Komponenten-Ausfällen mit einschließt, wenn die Zeitabstände zwischen den Ausfällen für Reparaturmaßnahmen zu kurz sind.

3.2

Konzept der gestaffelten Verteidigung

(en: defence in depth – DiD)

Vorsehen von mehr als einer Schutzmaßnahme für ein gegebenes Sicherheitsziel, sodass dieses auch erreicht wird, wenn eine der Schutzmaßnahmen versagt

[Siehe auch IAEA Safety Glossary V1 vom April 2000 und IEC 61513 – A3]

ANMERKUNG Die Schutzmaßnahmen für DiD können eines oder mehrere folgender Elemente umfassen:

- Das Bestehen mehrerer Gruppen von Sicherheitsfunktionen, wobei für jede Gruppe volle Übereinstimmung mit den Auslegungsspezifikationen sichergestellt ist.
- Das parallele Bestehen von passiven und aktiven Systemen.
- Das Bestehen gegenseitig unabhängiger Sicherheits- und Betriebssysteme, deren Aktionen im Anforderungsfall kumulativ sind.
- Die parallele Anwendung unterschiedlicher Auslegungsmethoden, um die Robustheit und Fehlertoleranz der Systeme zu steigern.

3.3

Diversität^{N1)}

(en: diversity)

Vorhandensein von zwei oder mehreren unterschiedlichen Verfahren oder Mitteln, um ein bestimmtes Ziel zu erreichen. Diversität ist besonders geeignet als Schutzmaßnahme gegen CCF. 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

[IEC 60880]

ANMERKUNG Siehe auch „funktionale Diversität“

3.4

Fail-safe-Auslegung

(en: fail-safe design)

Auslegung von Systemfunktionen derart, dass sie auf spezifizierte Fehler in einer vordefinierten, sicheren Weise reagieren

^{N1)} Nationale Fußnote: Auch „diversitäre Redundanz“ genannt.

3.5

Versagen^{N2)}

Ausfall

(en: failure)

Abweichen des vorliegenden Verhaltens von dem beabsichtigten Verhalten

[IEC 61513]

ANMERKUNG 1 Ein Versagen ist das Ergebnis eines Hardwarefehlers, Systemfehlers, menschlichen Fehlers, und der entsprechenden Signaltrajektorie, die das Versagen triggert.

ANMERKUNG 2 Siehe auch „Fehler“ und „Software-Versagen“

3.6

Fehler

(en: fault)

Mangel an einer Hardware-, Software- oder Systemkomponente

[IEC 61513]

ANMERKUNG 1 Fehler können in Zufallsfehler (z. B. Hardwarefehler) und systematische Fehler (z. B. Auslegungsfehler) unterteilt werden.

ANMERKUNG 2 Ein Fehler (insbesondere ein Auslegungsfehler) kann unentdeckt im System verbleiben, bis spezifische Bedingungen auftreten, als deren Ergebnis die Funktion nicht der gewünschten entspricht, d. h. ein Versagen auftritt.

ANMERKUNG 3 Siehe auch „Zufallsfehler“, „Softwarefehler“

3.7

Fehlervermeidung

(en: fault avoidance)

Verwendung von Techniken und Vorgehensweisen, die darauf abzielen, die Einschleppung von Fehlern während irgendeiner Phase des Sicherheits-Lebenszyklus zu vermeiden und damit Fehler in sicherheitsrelevanten Systemen zu vermeiden

3.8

Fehlertoleranz

(en: fault tolerance)

Fähigkeit eines Systems, die gewünschte Funktion trotz bestehender Fehler von oder in Teilsystemen auszuführen

3.9

funktionale Diversität

(en: functional diversity)

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

[IEC 60880]

ANMERKUNG Siehe auch „Diversität“

3.10

menschliches Fehlverhalten

(en: human error)

Handlung oder Vorgehensweise eines Menschen, die eine unbeabsichtigte Folge hat

^{N2)} Nationale Fußnote: Wenn Hardware oder Teilsysteme (z. B. ein Strang eines redundanten Systems) betroffen sind, wird „failure“ mit „Ausfall“ übersetzt.

3.11

unabhängige leittechnische Systeme

(en: independent I&C systems)

beide folgende Eigenschaften aufweisende Systeme:

- a) die Fähigkeit eines der beiden Systeme, die gewünschte Funktion auszuführen, wird durch Betrieb oder Versagen des anderen Systems nicht beeinflusst;
- b) die Fähigkeit, seine Funktion auszuführen, wird von Effekten nicht beeinflusst, die von dem angenommenen auslösenden Ereignis herrühren, für das diese Funktion gefordert wird.

[Definition über „unabhängige Geräte“ in IEC 61513]

ANMERKUNG Auslegungsmittel zur Erzielung von Unabhängigkeit in Übereinstimmung mit geeigneten Auslegungsprinzipien sind elektrische und physikalische Trennung, unabhängige Kommunikation und Rückwirkungsfreiheit von den zu steuernden Prozessen.

3.12

Eingangssignal-Transiente

(en: input signal transient)

Zeitverhalten aller Prozeßsignale, die zur Weiterverarbeitung in das leittechnische System eingespeist werden

ANMERKUNG Das Verhalten des leittechnischen Systems ist letztlich durch die Signaltrajektorie bestimmt, die auch die internen Zustände der leittechnischen Geräte umfasst. Die Anforderungsspezifikation definiert jedoch die sicherheitsbezogenen Reaktionen des leittechnischen Systems in bezug auf die „Eingangssignal-Transienten“.

3.13

latenter Fehler

(en: latent fault)

in einem leittechnischen System enthaltener, unentdeckter Fehler

ANMERKUNG Latente Fehler können aus Fehlern bei der Erstellung der Spezifikation, des Entwurfs, der Herstellung oder aus anderen vernünftigerweise anzunehmenden physikalischen oder technischen Gründen resultieren. Im Falle von Fehlern der Spezifikation oder des Entwurfs sollte davon ausgegangen werden, dass der gleiche latente Fehler in allen redundanten Teilsystemen vorliegt, sodass eine spezielle Signaltrajektorie einen CCF des betreffenden Systems auslösen kann.

3.14

Sicherheitsanalyse der Anlage

(en: plant safety analysis)

eine Sicherheitsanalyse der Auslegung eines Kernkraftwerks wird zur Bestimmung und Bestätigung der Auslegungsgrundlagen der Sicherheitsfunktionen durchgeführt, sowie zur Sicherstellung, dass die Auslegung der Gesamtanlage die vom Gesetzgeber vorgeschriebenen Grenz- und Referenzwerte für Strahlungsdosis und radioaktive Ableitungen unter jeder Anlagenbedingung einhält (siehe A2 und Abschnitt 6 der IEC 61513 und Abschnitt 6 von IAEA 50-SG-D11)

3.15

Zufallsfehler

(en: random fault)

nicht-systematischer Fehler von Hardwarekomponenten

ANMERKUNG 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 Hardware-Auslegung oder -Herstellung sein, wenn diese ohne zeitliche Korrelation auftreten, z.B. als eine Folge von vorzeitiger Alterung.

3.16

Software-Robustheit

(en: software robustness)

Ein die Software-Spezifikation leitendes Prinzip, aufgrund dessen die Software bei einem „nicht-tolerierbaren“ Versagen in einen vorherbestimmten Zustand übergeht

[Quelle: Fundamental Safety Rule (FSR), Frankreich]

3.17

Signaltrajektorie

(en: signal trajectory)

Zeitabläufe aller Gerätezustände, interner Zustände, Eingangssignale und Bedieneingaben, die den Ausgangszustand eines Systems bestimmen

[IEC 60880]

3.18

Einzelversagen^{N3)}

Einzelausfall

(en: single failure)

Zufälliges Versagen mit dem Ergebnis, dass eine Komponenten oder ein System die gewünschten Funktionen nicht ausführen kann. Folgeversagen, das aus einem angenommenen Einzelversagen resultiert, wird als Teil des Einzelausfalls betrachtet.

3.19

Einzelversagens-Kriterium

Einzelausfall-Kriterium

(en: single-failure criterion)

Eine Anordnung von Geräten erfüllt dieses Kriterium, wenn es trotz eines angenommenen zufälligen Einzelversagens an irgendeiner Stelle der Anordnung seine Aufgabe erfüllen kann. Folgeversagen, das aus dem angenommenen Einzelversagen resultiert, wird als integraler Teil des Einzelversagens betrachtet.

[IEC 61513]

ANMERKUNG Siehe auch „Einzelversagen“, „Softwareversagen“

3.20

Softwareversagen

(en: software failure)

Systemversagen infolge der Aktivierung eines Entwicklungsfehlers in einer Softwarekomponente

[IEC 61513]

ANMERKUNG 1 Jedes Softwareversagen ist die Folge eines Entwicklungsfehlers, weil Softwarefehler nur im Zuge der Entwicklung gemacht werden können, Software nicht altert oder physikalischen Effekten unterliegt. Da die Trigger, die Softwarefehler aktivieren, während des Systembetriebs zufällig auftreten, ist auch das Auftreten von Softwareversagen zufälliger Natur.

ANMERKUNG 2 Siehe auch „Versagen“, „Fehler“, „Softwarefehler“

3.21

Softwarefehler

(en: software fault)

Entwicklungsfehler in einer Softwarekomponente

[IEC 61513]

ANMERKUNG Siehe auch „Fehler“

3.22

Spezifikation

(en: specification)

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

[IEC 60880]

^{N3)} Nationale Fußnote: Wenn Hardware oder Teilsysteme (z. B. ein Strang eines redundanten Systems) betroffen sind, wird „failure“ mit „Ausfall“ übersetzt.

3.23

systematisches Versagen

systematischer Ausfall

(systematic failure)

Versagen, das deterministisch auf eine Ursache zurückgeführt werden kann und das nur durch eine Änderung der Auslegung oder des Produktionsprozesses, der Bedienungsanleitungen, Dokumentation oder anderer relevanter Faktoren zu beheben ist

[IEC 61513]

ANMERKUNG CCF ist ein spezieller Typ des systematischen Versagens, insofern als das Versagen getrennter Systeme, Redundanzen oder Komponenten koinzident getriggert werden kann.

3.24

funktionale Validierung

(en: funktional Validation)

Nachweis der Übereinstimmung von Spezifikationen der Anwendungsfunktionen mit den funktionalen und Leistungsfähigkeitsanforderungen der Anlage. Die funktionale Validierung stellt eine Ergänzung der Systemvalidierung dar, bei der die Übereinstimmung des Systems mit den Funktions-Spezifikationen nachgewiesen wird.

[IEC 61513]

3.25

Systemvalidierung

(en: system Validation)

Nachweis durch Prüfung und Nutzung von Evidenz, dass ein System in seiner Gesamtheit der Anforderungsspezifikation entspricht, so wie ursprünglich beabsichtigt (Funktionalität, Antwortzeit, Fehler-tolerant, Robustheit)

[IEC 60880]

3.26

Verifizierung

(en: verification)

Durch Prüfen und Vorlegen objektiver Beweise sicherstellen, dass die Ergebnisse einer Tätigkeit den Zielen und Anforderungen entsprechen, die für diese Tätigkeit definiert wurden

4 Abkürzungen

Englisch	Deutsch
CCF common cause failure	CCF Versagen (Ausfall) gemeinsamer Ursache
DBA design basis accident	DBA Auslegungsstörfall
DBE design basis event	DBE Auslegungsereignis
DiD defenth in depth	DiD Konzept der gestaffelten Verteidigung
FAT factory acceptance test	WAP Werksabnahmeprüfung
IAEA International Atomic Energy Agency	IAEO Internationale Atomenergie Organisation
NPP nuclear power plant	KKW Kernkraftwerk
PIE postulated initiating event	AVE anzunehmendes versagenauslösendes Ereignis
SAT site acceptance test	AAA Abnahmeprüfung auf der Anlage