

DIN IEC 63160
(VDE 0491-10-2)
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 2019-07-24

Entwurf

**Kerntechnische Anlagen –
 Elektro- und leittechnische Systeme mit sicherheitstechnischer
 Bedeutung –
 Versagen aufgrund gemeinsamer Ursache, Systemanalyse und
 Diversität
 (IEC 45A/1257/CD:2018);
 Text Deutsch und Englisch**

Nuclear facilities –
 Instrumentation, control and electrical power systems important to safety –
 Common cause failure, system analysis and diversity
 (IEC 45A/1257/CD:2018);
 Text in German and English

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2019-05-24 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 57 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE

Anwendungsbeginn

Anwendungsbeginn dieser Norm ist

Inhalt	Seite
Nationales Vorwort.....	3
Einleitung	4
1 Anwendungsbereich	8
2 Normative Verweisungen	8
3 Begriffe	9
4 Abkürzungen	14
5 Fehler aufgrund gemeinsamer Ursache.....	14
5.1 Allgemeines	14
5.2 Anlagenanalyse	15
5.3 Timing der Analyse.....	16
6 CCF infolge von Gefährdung.....	17
6.1 Allgemeines	17
6.2 Schutz gegen Gefährdungen	17
7 CCF infolge von Fehlerfortpflanzung.....	18
7.1 Allgemeines	18
7.2 Schutz gegen Fehlerfortpflanzung	19
8 Systematische Fehler	20
8.1 Allgemeines	20
8.2 Schutz gegen systematische Fehler	20
8.3 Diversität.....	21
Anhang A (informativ) Gefährdungen	24
Anhang B (informativ) Diversität elektrischer und leittechnischer Systeme	25
Literaturhinweise.....	27

Nationales Vorwort

Das internationale Dokument IEC 45A/1257/CD:2018 „Nuclear facilities – Instrumentation, control and electrical power systems important to safety – Common cause failure, system analysis and diversity“ (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 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.

Die Deutsche Fassung wurde im [Abschnitt 2](#) an den aktuellen Standardtext angepasst.

Einleitung

a) Technischer Hintergrund, hauptsächliche Inhalte und Organisation der Norm

Diese Internationale Norm bezieht sich auf eine Anforderung der IAEA zur Optimierung des Schutzes kerntechnischer Anlagen durch Anwendung gestufter Maßnahmen (en: defence in depth, DiD) gegen Fehler, die zu schwerwiegenden Folgen führen könnten. Diese Norm befasst sich damit, wie für aktive Vorkehrungen der leittechnischen und elektrischen Systeme in den verschiedenen Maßnahmenstufen sichergestellt werden kann, gegen Versagen/Fehler aufgrund gemeinsamer Ursache (en: common cause failure, CCF) wirksam und selbst möglichst frei von CCF zu sein. Das war für einfache Systeme immer wichtig und wird hinsichtlich rechnerbasierter verteilter und komplexer elektronischer Systeme, die für sicherheitstechnisch wichtige Funktionen in kerntechnischen Anlagen verwendet werden, für besonders bedeutend gehalten, weil diese gegenüber CCF als empfindlicher gelten.

Die Sicherheit kerntechnischer Installationen wird auf vielen Wegen erreicht; eine von Haus aus sichere Auslegung, passive und aktive Systeme zur Steuerung der Prozesse und Vorsehen von Schutz im Fall eines Fehlers. Die IAEA Safety Fundamentals SF-1 [1], Principle 5, fordern die Optimierung des Schutzes: „Protection must be optimized to provide the highest level of safety that can reasonable be achieved“. Teil einer solchen Optimierung ist die Einplanung von DiD entsprechend dem Risiko, das die Anlage darstellt.

Die Herangehensweise zum DiD-Konzept wird bei IAEA mit einem Satz aufeinander folgender Barrieren (Maßnahmenstufen) zur Schadensvermeidung beschrieben.

	Ziel	Essentielle Maßnahmen
Maßnahmenstufe 1	Verhinderung von anomalem Betrieb und Fehlern	Konservative Auslegung und hohe Qualität in Auslegung und Betrieb
Maßnahmenstufe 2	Kontrolle des anomalen Betriebs und Fehleraufdeckung	Steuerungs-, Begrenzungs- und Schutzsysteme und andere Überwachungseinrichtungen
Maßnahmenstufe 3	Kontrolle der Auslegungsstörfälle	Technische Sicherheitsmerkmale und Störfall-Prozeduren
Maßnahmenstufe 4	Kontrolle auslegungsüberschreitender Störfälle, einschließlich Verhinderung von Störfall-Ausbreitung und Abschwächung der Folgen schwerer Störfälle	Ergänzende Maßnahmen und Notfall-Management
Maßnahmenstufe 5	Abschwächung von radiologischen Folgen signifikanter Freisetzung radioaktiver Stoffe	Notfall-Maßnahmen außerhalb der Anlage

Für Kernkraftwerke ist dies in IAEA SSR-2/1 [2], Design Requirement 7, beschrieben: „Anwendung von DiD – Die Auslegung eines Kernkraftwerks muss DiD beinhalten. Die Maßnahmenstufen müssen, soweit praktikabel, voneinander unabhängig sein“.

In der Praxis wird das durch passive Vorkehrungen, unterstützt durch aktive Systeme, erreicht. Die aktiven Systeme können umfassen:

- das Steuerungs- und Regelungssystem der Anlage als Maßnahmenstufe 1;
- das Sicherheitssystem der Anlage als Maßnahmenstufe 2;
- zusätzliche (automatische/händische) sicherheitstechnische Systeme mit Sicherheitsfunktionen, die zusätzlichen Schutz gegen häufige Fehler bieten;
- zusätzlich Maßnahmen, um die Folgen schwerer Störfälle abzuschwächen; und
- Unterstützung für Störfall-Management außerhalb der Anlage.

Die Überlegungen zur Unabhängigkeit sind in IAEA SSR-2/1 [2] Requirement 21: Physikalische Trennung und Unabhängigkeit von Sicherheitssystemen – „Wechselwirkung zwischen Sicherheitssystemen oder zwischen redundanten Elementen eines Systems müssen durch Mittel wie physikalische Trennung, elektrische Trennung, funktionale Unabhängigkeit und Unabhängigkeit der Kommunikation (Datenübertragung), soweit zutreffend, vermieden werden.“ und Requirement 24: CCF – „Die Auslegung des Geräts muss dem CCF-Potential von sicherheitstechnisch wichtigen Einheiten ausreichend Rechnung tragen, um festzustellen, wie die Konzepte von Diversität, Redundanz, physikalischer Trennung und funktionaler Unabhängigkeit anzuwenden sind, um die notwendige Zuverlässigkeit zu erreichen“. Damit diese Ebenen/Maßnahmenstufen wirksam sind, müssen sie so beschaffen sein, dass sie nicht von CCF betroffen sind; z. B. durch einen replizierten Fehler oder eine Gefährdung, die den Ausfall mehrerer Maßnahmenstufen verursacht, oder durch Fehler-Fortpflanzung von einer Maßnahmenstufe zur nächsten.

Redundante, aber identischer Zweige in elektrischen und leittechnischen Systemen nuklearer Anlagen werden oft verwendet, um hohe Zuverlässigkeit und Verfügbarkeit zu erzielen, und bieten einen Schutz gegen randome Fehler, um das Einzelfehler-Kriterium zu erfüllen; IAEA SSR-2/1 [2] Requirement 25.

Die Verwendung redundanter, aber identischer Zweige als Auswahlhaltung hilft nicht gegen Fehler in den System-Srängen, die systematischer Natur sind. Die primäre Abhilfe dagegen ist die ‚Herstellungs-Güte‘. In einem gut konstruierten System jedoch kann Abhilfe gegen CCF von beiden Gefährdungen, externen (z. B. Erdbeben, Flugzeug-Absturz) und internen (z. B. Brand, Überflutung), geschaffen werden. Typischerweise wird das durch Maßnahmen erreicht, die physikalische Trennung der Replizierungen durch physikalische und andere technische Barrieren, die gegen Gefährdungen resistent sind, einschließen; IAEA NS-G-1.5 [3] und IAEA NS-G-1.6 [4] für externe Gefährdungen und IAEA NS-G-1.7 [5] und IAEA NS-G-1.11 [6] für interne Gefährdungen.

Mehrfache elektrische und leittechnischer Systeme zur Erzielung von DiD werden in nuklearen Anlagen auch oft verwendet; z. B. gibt es nukleare Brennstoff- und Wiederaufbereitungs-Anlagen mit normaler und Notstromversorgung und getrennten Systemen für Steuerung und Schutz.

Jedoch muss CCF der Systeme selbst daraufhin betrachtet werden, dass Ausfälle aufgrund von Faktoren wie der Verwendung gemeinsamer Komponenten mit systematischen Fehlern, die während der Lieferungsprozesse eingeschleppt werden, entstehen können.

Daher ist es Aufgabe dieser Norm, Anforderungen zu identifizieren bezüglich

- Aufgabenbereich der zu betrachtenden Systeme,
- Aufgabenbereich der durchzuführenden Analysen und zu berücksichtigenden Faktoren, und
- der notwendigen Information, um die Eignung der Vorkehrungen zur Vermeidung von CCF beurteilen zu können.

Die Anforderungen zur Beurteilung der Eignung der Vorkehrungen gegen CCF gehören nicht zum Anwendungsbereich dieser Norm. Dies liegt zum Teil an den Unterschieden in den nationalen Herangehensweisen zum CCF (in einigen Ländern ist es ein Auslegungsstörfall, in anderen eine auslegungsüberschreitende Bedingung), zum Teil auch an der Abhängigkeit vom Typ der Anlage und den anlagenspezifischen Details.

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

Dies ist eine neue Norm des IEC/SC 45A der dritten Ebene und wird in bestehenden IEC-Normen oder SC-45A-Dokumenten nicht zitiert. Sie sollte in Zusammenhang mit IEC 61513 [7], IEC 63046 [8] und IEC 61226 [9] betrachtet werden, die übergeordnete Anforderungen zur Unabhängigkeit von Systemen, die verschiedene Kategorien von Funktionen realisieren, festlegen, und mit IEC 62340 [10], in der Auslegungs- und Software-CCF behandelt werden.

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

c) Empfehlungen und Einschränkungen der Anwendung dieser Norm

Die Anforderungen können auf jeden Typ einer kerntechnischen Anlage angewendet werden.

Die Norm enthält keine Anforderungen zur Bestimmung der Eignung von vorgesehenen Maßnahmen gegen CCF.

In dieser Norm bezeichnet „muss“ Anforderungen, deren Erfüllung zur Einhaltung dieser Norm zwingend ist; „sollte“ bezeichnet Anforderungen, deren Einhaltung zur Erfüllung dieser Norm zwar nicht zwingend ist, die aber dringend empfohlen werden; „darf“ bezeichnet optionale Anforderungen.

d) Beschreibung der Struktur der Normen des IEC/SC 45A und der Beziehungen zu weiteren Dokumenten der IEC sowie Dokumenten anderer Organisationen (IAEA, ISO)

Die Eingangsdokumente der Normen 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 elektrische Systeme von Kernkraftwerken, die umfasst Stromversorgungssysteme einschließlich der Versorgungssysteme für die Leittechnik. IEC 61513 und IEC 63046 sind miteinander und gleichrangig zu berücksichtigen. Durch IEC 61513 und IEC 63064 werden die Normen des IEC/SC 45A strukturiert und ein komplettes Rahmenwerk allgemeiner Anforderungen für leittechnische und elektrische Systeme von Kernkraftwerken aufgebaut.

In IEC 61513 und IEC 63046 wird für allgemeine Themen direkt auf andere Normen des IEC/SC 45A verwiesen, dazu gehören die Kategorisierung von Funktionen und Klassifizierung von Systemen, Qualifizierung, Trennung, Maßnahmen gegen Versagen aufgrund gemeinsamer Ursache (CCF), Wartenauslegung, elektromagnetische Verträglichkeit, Cybersicherheit, Software- und Hardwareaspekte programmierbarer digitaler Systeme, Koordination von Maßnahmen zur Sicherheit und IT-Sicherheit sowie Alterungsmanagement. Die Normen, auf die direkt verwiesen wird, bilden die zweite Ebene und 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 oder IEC 63046 nicht direkt verwiesen wird, dazu gehören Normen für spezielles Gerät, technische Verfahren 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.

Kerntechnische Anlagen – Elektro- und leittechnische Systeme mit sicherheitstechnischer Bedeutung – Versagen aufgrund gemeinsamer Ursache, Systemanalyse und Diversität

1 Anwendungsbereich

Diese Internationale Norm enthält Anforderungen zur Vermeidung von CCF in elektrischen und leittechnischen Systemen nuklearer Anlagen. Sie legt Anforderungen fest für die

- Anlagenanalyse;
- Analyse und Vermeidung von CCF durch Gefährdungen;
- Analyse und Vermeidung von CCF durch systematische Fehler;
- Dokumentation der Maßnahmen gegen CCF, um deren Eignung zu beurteilen.

Diese Norm stellt keine detaillierten Auslegungsanforderungen zur Vermeidung von CCF in Systemen zur Verfügung; dafür sind die Normen von IEC/SC 45A/WG 11 bzw. IEC/SC 45A/WG 3 zuständig.

Die Anforderungen zur Bestimmung der Eignung von Maßnahmen zur Vermeidung von CCF liegen außerhalb des Anwendungsbereichs dieser Norm. Dies liegt an den Unterschieden der nationalen Vorgehensweisen gegenüber dem CCF; einige Länder behandeln CCF als Auslegungsstörfall, andere als auslegungsüberschreitende Anlagenbedingung und einige als eine deterministische Anforderung; und es liegt auch an der Abhängigkeit vom Anlagentyp und von anlagenspezifischen Details.

Diese Norm folgt den allgemeinen Prinzipien nach IAEA Safety Requirement SSR-2/1 und IAEA Safety Guides SSG-34 und SSG-39 für elektrische und leittechnische Systeme, und definiert eine strukturierte Methode zur Anwendung der Anleitung in diesen IAEA-Codes und -Standards auf die elektrischen und leittechnischen Systeme, die sicherheitstechnisch wichtige Funktionen in einem Kernkraftwerk ausführen. Diese Norm sollte in Zusammenhang mit diesen IAEA-Dokumenten sowie IEC 63046 und IEC 61513 angewendet werden, um die Anforderungen der grundlegenden Sicherheitsnorm IEC 61508 zu realisieren.

Abschnitt 5 dieser Norm enthält die gesamte Herangehensweise an den CCF und seine Analyse.

Abschnitt 6 dieser Norm enthält die Vorgehensweise bei der Anlagen- und Systemanalyse, die als Vorkehrung unternommen werden müssen, um CCF infolge Gefährdungen zu vermeiden.

Abschnitt 7 dieser Norm enthält die Herangehensweise an die Anlagen- und Systemanalysen, die durchzuführen sind, um CCF infolge Fehlerfortpflanzung zu vermeiden. Dies umfasst Fehlerfortpflanzung zwischen Strängen desselben Systems und zwischen Systemen verschiedener Schutzlinien.

Abschnitt 8 dieser Norm enthält die Vorgehensweise zur Vermeidung von CCF wegen systematischer Fehler durch Herstellungsgüte und Verwendung von Diversität.

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).

IAEA SSR-2/1 R1, *Safety of Nuclear Power Plants: Design*

IAEA SSG 34, *Design of Electrical Power Systems for Nuclear Power Plants*

IAEA SSG 39, *Design of Instrumentation and Control Systems for NPP*

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 – 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 60987, *Nuclear power plants – Instrumentation and control important to safety – Hardware design requirements for computer-based systems.*

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 important for safety – Software aspects for computer-based systems performing category B or C functions*

IEC 62340, *Nuclear power plants – Electrical equipment of the safety system – Requirements for coping with Common cause failure*

IEC 62566, *Nuclear power plants – Instrumentation and control important to safety – Development of HDL-programmed integrated circuits for systems performing category A functions*

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

IEC 62808, *Nuclear power plants – Instrumentation and control systems important to safety – Design and qualification of isolation devices*

IEC 63046 Ed. 1.0, *Nuclear power plants – Electrical systems – General requirements*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

ISO und IEC stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

– IEC Electropedia: verfügbar unter <http://www.electropedia.org/>

– ISO Online Browsing Platform: verfügbar unter <http://www.iso.org/obp>

3.1

Störfallbedingungen

(en: accident conditions)

Abweichungen vom Normalbetrieb, die weniger häufig und schwerwiegender sind als anzunehmende betriebliche Vorkommnisse, und die Auslegungsstörfälle und auslegungsüberschreitende Störfälle umfassen.

[IAEA SSR 2/1]

3.2

Versagen aufgrund gemeinsamer Ursache

CCF

(en: common cause failure; CCF)

Versagen von zwei oder mehreren Strukturen, Systemen oder Komponenten infolge eines einzigen Ereignisses oder Grundes

[IAEA Safety Glossary 2007, modifiziert]

3.3

Auslegungsstörfall

(en: design basis accident, DBA)

Störfallbedingungen, für die eine Anlage gemäß vorgegebener Auslegungskriterien und konservativer Methodologie konstruiert ist, und bei denen die Abgabe radioaktiver Stoffe innerhalb akzeptabler Grenzen liegt

[IAEA SSR-2/1]

3.4

Auslegungseignis

(en: design basis event, DBE)

Gruppe von Auslegungsstörfällen und anzunehmenden betrieblichen Vorkommnissen

[IAEA SSR-2/1]

Anmerkung 1 zum Begriff: Siehe auch Begriff 3.13.

3.5

auslegungsüberschreitende Bedingungen

(en: design extension conditions)

angenommene Störfallbedingungen, die nicht explizit als Auslegungsstörfälle betrachtet werden, aber die im Auslegungsprozess der Anlage in Übereinstimmung mit der „Methodik der besten Schätzung“ berücksichtigt werden und bei denen die Abgabe radioaktiver Stoffe innerhalb genehmigter Grenzen liegt. Auslegungsüberschreitende Bedingungen können Bedingungen von Ereignissen ohne signifikante Brennelementschäden und Bedingungen mit Kernschmelzen einschließen.

[IAEA SSR-2/1]

3.6

Diversität

(en: diversity)

Vorhandensein von zwei oder mehreren redundanten Systemen oder Komponenten zur Ausführung einer bestimmten Funktionen, wobei die verschiedenen Systeme oder Komponenten unterschiedliche Eigenschaften aufweisen, und zwar derart, dass die Möglichkeit von Versagen aufgrund gemeinsamer Ursache verringert wird, einschließlich common mode Versagen^{N1}

[IAEA Safety Glossary 2007]

Anmerkung 1 zum Begriff: Nach IEC 60880 ist Diversität folgend definiert: Vorhandensein von zwei oder mehreren unterschiedlichen Verfahren oder Mitteln, um ein bestimmtes Ziel zu erreichen. Diversität ist besonders geeignet als Schutzmaßnahme gegen Versagen aufgrund gemeinsamer Ursache (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. Die beiden Definitionen sind konsistent.

3.7

Gerät

Einrichtung

(en: equipment)

ein oder mehrere Teile eines Systems. Ein Gerät ist ein einzelnes, definierbares (und üblicherweise ausbaubares) Teil eines Systems

[IEC 61513, modifiziert]

3.8

Funktion

(en: function)

spezifische durchzuführende Aufgabe, die spezifiziert oder beschrieben werden kann, ohne Hinweis auf die physikalischen Mittel, mit denen sie zu erfüllen ist

^{N1} Nationale Fußnote: In Deutschland wird ein Versagen gemeinsamer Art (en: common mode failure) nicht separat betrachtet; diese Versagensart ist im Versagen gemeinsamer Ursache (CCF) integriert.

3.9

Funktionalität

(en: functionality)

Attribut einer Funktion, das die Operationen zur Umwandlung der Eingangsinformationen in die Ausgangsinformationen definiert

[IEC 61513]

3.10

HF-Engineering-Programm

Human-Factor-Engineering-Programm

(en: human factor engineering programme)

Programm, das wenigstens die HF-Organisation, die Rolle und Aufgabe der HF-Spezialisten, die HF-Aktivitäten und ihre Einbindung in die Auslegungs- und Validierungsvorgänge beschreibt und eine Liste der in jedem Schritt des Programms zu erledigenden Aufgaben umfasst

3.11

sicherheitstechnisch wichtige Gegebenheit

sicherheitstechnisch wichtiges leittechnisches System

(en: item important to safety, I&C system important to safety)

Gegebenheit/Maßnahme, die Teil einer Sicherheitsgruppe ist und/oder deren Fehlfunktion oder Versagen zur Strahlenbelastung des Anlagenpersonals oder der Öffentlichkeit führen könnte.

Sicherheitstechnisch wichtige Gegebenheiten/Maßnahmen umfassen:

- Strukturen, Systeme und Komponenten, deren Fehlfunktion oder Versagen zu unzulässiger Strahlenbelastung des Anlagenpersonals oder der Öffentlichkeit führen könnte;
- Strukturen, Systeme und Komponenten, die verhindern, dass anzunehmende betriebliche Vorkommnisse zu Störfallbedingungen führen;
- Merkmale, die dazu dienen, die Folgen von Fehlfunktion oder Versagen der Strukturen, Systeme oder Komponenten abzuschwächen

Anmerkung 1 zum Begriff: Die Betrachtungen in dieser Norm beziehen sich hauptsächlich auf sicherheitstechnisch wichtige leittechnische Systeme.

3.12

kontrollierter Zustand

(en: controlled state)

Anlagenzustand nach einem anzunehmenden betrieblichen Vorkommnis oder einem Auslegungsstörfall, in dem die fundamentalen Sicherheitsfunktionen sichergestellt werden können und der genügend lange beibehalten werden kann, um den Sicherheitszustand zu erreichen.

[IAEA SSR-2/1]

3.13

Leistungsfähigkeit

(en: performance)

Effizienz, mit der eine gewünschte Funktion ausgeführt wird (z. B. Antwortzeit, Genauigkeit, Empfindlichkeit gegenüber Parameteränderungen)

3.14

Anlagenzustände

(en: plant states)

Betriebszustände		Störfallbedingungen		
Normalbetrieb	Anzunehmende betriebliche Vorkommnisse	Auslegungsstörfälle	Auslegungsüberschreitende Bedingungen	
			Ohne signifikante Brennstoffschäden	Mit Kernschmelzen

[IAEA Safety Glossary 2016]

Anmerkung 1 zum Begriff: Diese Definition entspricht der in IAEA SSR-2/1 und dem Anhang DS 462; sie gibt lediglich die Position des Konzepts „Auslegungsereignisse“ im Vergleich zu anderen Konzepten an.

3.15

anzunehmendes Versagen auslösendes Ereignis

(en: postulated initiating event, PIE)

im Zuge der Auslegung ermitteltes Ereignis, das zu den anzunehmenden betrieblichen Vorkommnissen oder Störfallbedingungen führen kann

[IAEA Safety Glossary 2007]

3.16

Herstellungsgüte

(en: production excellence)

Geräte und Systeme, die in voller Übereinstimmung mit den IEC SC45A nuklearen Standards wie a) Maßnahmen für Fehleraufdeckung und Eliminierung sind während ihrer Auslegung, Herstellung, Installation und Inbetriebnahme verwendet worden; b) sie schließen Maßnahmen zu Fehleraufdeckung und Management während des Betriebs ein; und c) sie umfassen Maßnahmen zur Unterstützung von Fehlerentdeckung und Meldung und somit prompter Instandhaltung.

3.17

Redundanz

(en: redundancy)

Vorhandensein mehrerer (identischer oder unterschiedlicher) Strukturen, Systeme oder Komponenten, so dass jede Einheit (Struktur, System oder Komponente) unabhängig vom Betriebszustand oder Versagen irgendeiner anderen Einheit die geforderte Funktion ausführen kann.

[IAEA Safety Glossary 2007]

3.18

Sicherheitszustand

(en: safe state)

Anlagenzustand nach einem anzunehmendem betrieblichen Vorkommnis oder Störfallbedingungen, in dem der Reaktor unterkritisch ist und die fundamentalen Sicherheitsfunktionen sichergestellt und für lange Zeit stabil gehalten werden können.

3.19

Sicherheitsmerkmal für auslegungsüberschreitende Bedingungen

(safety feature for design extension conditions)

Auslegungsmerkmal zur Ausübung einer Sicherheitsfunktion unter auslegungsüberschreitenden Bedingungen.

[IAEA SSR-2/1]

3.20

Sicherheitsgruppe

(en: safety group)

Anordnung von Geräten, die dazu bestimmt ist, alle erforderlichen Aktionen durchzuführen, um sicherzustellen, dass die in der Auslegungsgrundlage für anzunehmende betriebliche Vorkommnisse und Auslegungsstörfälle festgelegten Grenzwerte nicht überschritten werden.

[IAEA Safety Glossary 2007]

3.21

sicherheitsrelevantes System

(en: safety related system)

sicherheitstechnisch wichtiges System, das nicht Teil eines Sicherheitssystems ist

[IAEA Safety Glossary 2007]

3.22

Sicherheitssystem

(en: safety system)

sicherheitstechnisch wichtiges System, das dazu dient, die sichere Abschaltung des Reaktors und die Restwärmeabfuhr aus dem Reaktorkern sicherzustellen, oder die Konsequenzen von anzunehmenden betrieblichen Vorkommnissen und Auslegungsstörfällen zu begrenzen

[IAEA Safety Glossary 2007]

3.23

Einzelausfall

Einzelversagen^{N2}

(en: single failure)

ein Ausfall mit dem Ergebnis, dass ein System oder eine Komponente die geplanten Sicherheitsfunktionen nicht ausführen kann, und alle daraus resultierenden Folgeausfälle

[IAEA Safety Glossary 2007]

3.24

System

(en: system)

Satz von Komponenten, die entsprechend der Auslegung zusammenarbeiten, wobei ein Element des Systems ein weiteres System, genannt Teilsystem, sein kann

[IEC 61513]

3.25

Typprüfung

(en: type testing)

Konformitätsprüfung, die an einem oder mehreren für die Produktion repräsentativen Stücken durchgeführt wird^{N3}

[IEV 394-40-02]

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

^{N3} Nationale Fußnote: Bei Typprüfungen nach KTA 3503 und KTA 3505 sind mindestens drei repräsentative Stücke vorgesehen.

4 Abkürzungen^{N4}

Deutsch	Englisch
CCF Fehler aufgrund gemeinsamer Ursache	CCF Common Cause Failure
DBA Auslegungsstörfall	DBA Design Basis Accident
DBE Auslegungsereignis	DBE Design Basis Event
DEC auslegungsüberschreitende Bedingung	DEC Design Extension Condition
FMEA Fehlermöglichkeits- und -einflussanalyse	FMEA Failure Modes and Effects Analysis
IAEA Internationale Atomenergie-Behörde	IAEA International Atomic Energy Agency
KKW Kernkraftwerk	NPP Nuclear Power Plant
AVE anzunehmendes Versagen auslösendes Ereignis	PIE Postulated Initiating Event
QS Qualitätssicherung	QA quality assurance
DiD Konzept gestaffelter Schutzmaßnahmen	DiD defence in depth

5 Fehler aufgrund gemeinsamer Ursache

5.1 Allgemeines

Von nuklearen Anlagen wird gefordert sicher zu sein, d. h. so ausgelegt und konstruiert zu sein, um Schutz von Öffentlichkeit, Anlagenpersonal und Anlage zu bieten. Im Sicherheitsbericht nuklearer Anlagen wird häufig auf die Redundanz zur Erreichung hoher Zuverlässigkeit und auf die Fehlerunabhängigkeit der verschiedenen Teile der Architektur der elektrischen und leittechnischen Systeme zur Erzielung von DiD nach IAEA SSR 2.1 R7 verwiesen. Der Fehler aufgrund gemeinsamer Ursache (CCF) stellt eine Herausforderung für diese Argumentation dar, da er die Verwendung folgender Maßnahmen paralysieren kann:

- 1) redundante, aber identische Stränge in elektrischen und leittechnischen Systemen zur Erzielung hoher Zuverlässigkeit (z. B. Sicherheitssysteme mit Auswahl-schaltungen); und
- 2) mehrfache elektrische und leittechnische Systeme in verschiedenen Linien eines DiD Konzepts, um die deterministischen und probabilistischen Zielvorgaben für die Sicherheit der Anlage zu erreichen.

Beispiele für 2) schließen als Alternative eine vom Netz unabhängige elektrische Versorgung mit lokaler Stromerzeugung und/oder Batterien sowie unabhängige Steuerungs-/Regelungs- und Sicherheitssysteme ein.

CCF ist für geraume Zeit als Bedrohung für die Anlagensicherheit betrachtet worden, daher die Anforderungen, Abweichungen des Anlagenverhaltens durch mehr als einen Parameter zu überwachen, Verwendung einer Hauptlogik und einer alternativen Logik zur Anregung von Sicherheitsfunktionen, und mehr als einen Mechanismus, um die Kettenreaktion in nuklearen Reaktoren zu beenden. Es wird jedoch empfunden, dass die steigende Verwendung und inhärente Komplexität der digitalen Leittechnik in elektrischen und leittechnischen Systemen die Empfänglichkeit für CCF verschärft.

IAEA SSR 2.1 R24 fordert die Berücksichtigung von CCF, dargelegt in IAEA SSG-34 (elektrische Systeme) und SSG-39 (Leittechnik). Es gibt auch eine umfangreiche Literatur über CCF und die Mittel, ihn zu analysieren und zu vermeiden, und es sind signifikante Untersuchungen zur Wirksamkeit einiger dieser Mittel unternommen worden.

CCF könnte auftreten wegen

- ungeeigneter Spezifikation von und Qualifizierung für sowie Schutz gegen interne(n) und externe(n) Gefährdungen;
- Fehlerfortpflanzung von einem Strang oder einem System oder einer Komponente zum/zur nächsten;

^{N4} Nationale Fußnote: Entgegen zur IEC 45A/1257/CD wurde die Nummerierung fortlaufend fortgeführt.

- menschliche Fehler im Entwicklungs- oder Herstellungsprozess, Wartungsfehler, Fehler in zur Entwicklung benutzten Software-Werkzeugen, d. h. Einbringen latenter oder systematischer Fehler.

Weitere Diskussion über Ursachen findet sich in Verweisungen von [Anhang B](#).

5.2 Anlagenanalyse

Die CCF-Bedrohung der Sicherheit einer Anlage und die Maßnahmen zu ihrer Vermeidung müssen über den gesamten Lebenszyklus der Anlage ein Anliegen sein, d. h. von der Konzeptphase der Anlage bis zu ihrer Außerbetriebsetzung, SSR 2.1 R3. Die funktionalen Folgen von CCF können das Nicht-Ansprechen oder das unerwünschte Ansprechen von Gerät sein, wobei beides zu adressieren ist. Die Maßnahmen zur Vermeidung von CCF umfassen physikalische und elektrische Trennung, ingenieurtechnische Barrieren und Diversität; sie sind fundamental für das Anlagenkonzept und die Systemarchitektur. Solche Maßnahmen sind teuer, folglich ist es wichtig, das Ausmaß der Konsequenzen (hoch, mittel, niedrig, siehe SSG 30) der verschiedenen CCF zu benennen und die Maßnahmen verhältnismäßig anzuwenden; d. h. sehr robuste Maßnahmen für solche, die zu hohen Konsequenzen führen. Folglich sollte die Bedeutung einer frühen Analyse nicht unterschätzt werden.

5.2.1 Die Strategien zum Schutz gegen CCF von sicherheitstechnisch wichtigen elektrischen und leittechnischen Systemen müssen bewertet werden, und die ausgewählte Vorgehensweise muss zu Beginn des Projekts spezifiziert und dokumentiert werden und über die Lebenszeit der Anlage beibehalten werden.

5.2.2 Die CCF-Analyse muss systematisch in einer Reihe von Schritten vorgenommen werden:

- die Folgen von CCF in elektrischen und leittechnischen Systemen, die eine Risikoreduzierung durch das DiD-Konzept und individuell für PIE bewirken, müssen festgestellt werden;
- die potenziellen Ursachen der anzunehmenden CCF müssen ermittelt werden (wobei es offensichtlich nicht möglich ist, alle potenziellen Ursachen zu identifizieren);
- die vorhandenen Abwehrmaßnahmen gegen die identifizierten Ursachen von CCF müssen identifiziert werden;
- die Robustheit dieser Abwehrmaßnahmen muss festgestellt werden;
- die Analyse muss dokumentiert werden.

Die Analyse zur Bestimmung der möglichen Folgen von CCF muss abgeschlossen werden sobald Anlagenkonzept und -architektur und die Systemarchitektur der elektrischen und leittechnischen Systeme erstellt sind.

5.2.3 Die Analyse muss von einem multidisziplinären Team durchgeführt werden und muss von der deterministischen und probabilistischen Sicherheitsanalyse der Anlage unterstützt werden bzw. diese unterstützen.

5.2.4 Die Analyse muss für alle PIE/DBE durchgeführt werden und die Schwere der Konsequenzen und den Einfluss auf deterministische und probabilistische Sicherheitsrechtfertigungen für jeden angenommenen CCF in individuellen Systemen und in Systemen, für die in der Sicherheitsanalyse Fehlerunabhängigkeit in Anspruch genommen wird.

5.2.5 Wenn ein anzunehmender CCF dazu führt, dass die Anlage die erklärten Sicherheitsziele nicht erfüllt, müssen die involvierten Systeme zusammen mit den möglichen Ursachen der angenommenen CCF identifiziert und dokumentiert werden. Typischerweise können das sein: Gefährdungen, Fehlerfortpflanzung und systematische Fehler, die sich gleichzeitig auf redundante Zweige eines einzelnen Systems und auf Systeme in verschiedenen CCF-Schutzlinien befinden.

5.2.6 In jedem Fall müssen in der Analyse die Maßnahmen gegen CCF identifiziert und die erforderlichen Merkmale der Maßnahmen festgelegt werden, um CCF zu vermeiden.

Die möglichen Ursachen von CCF und die Maßnahmen/Merkmale die zu ihrer Verhinderung eingesetzt werden, sind in [Abschnitt 6](#) (Gefährdungen), [Abschnitt 7](#) (Fehlerfortpflanzung) und [Abschnitt 8](#) (Systematische Fehler) weiter betrachtet.

5.2.7 Die Robustheit dieser Maßnahmen/Merkmale muss dann im Zusammenhang mit der Größe der Folgen und Auswirkungen für in Anspruch genommene probabilistische Sicherheitsargumente bezüglich CCF und die Wahrscheinlichkeit des Eintretens postulierter CCF bewertet werden.

5.2.8 Die Ergebnisse der Analyse müssen dokumentiert werden. Dabei sollte die Feststellung eingeschlossen werden, wo CCF eine Bedrohung ist, sowie die Maßnahmen zum Schutz gegen CCF und die Bewertung der Robustheit der Maßnahmen im Vergleich mit der Schwere der Folgen.

Bei CCF mit schwerwiegenden Folgen oder voraussichtlich großer Häufigkeit wären zum Schutz gegen dieses Ereignis sehr robuste Maßnahmen zu erwarten; ein Beispiel könnte Kernschmelzen als Ergebnis eines seismischen Ereignisses in einer Erdbebenzone sein. Wenn jedoch die Folgen weniger schwerwiegend wären und die voraussichtliche Häufigkeit des Ereignisses niedrig, könnten vergleichsweise schwache Maßnahmen eingesetzt werden; in diesem Fall könnten die Maßnahmen mittels einer Kosten/Nutzenanalyse bestimmt werden.

5.3 Timing der Analyse

Damit die Vorgehensweise zur Vermeidung von CCF effektiv ist, muss sie schon bei Beginn der Anlagenkonzeptionierung berücksichtigt werden und für die Lebenszeit der Anlage und der elektrischen und leittechnischen Systeme beibehalten werden (SSR 2.1 R3). Dies kann z. B. durch Aufsetzung einer Strategie zur Erfassung von Kriterien für eine effektive Vermeidung von CCF erreicht werden, die dann für alle Aktivitäten im Lebenszyklus beibehalten wird. Die Strategie und die Kriterien würden dann bei jedem Schritt des Anlagen-Lebenszyklus überprüft werden.

5.3.1 Bei Beginn des Anlagenprojekts muss eine Studie abgeschlossen sein, um festzustellen, wo eine CCF-Analyse der elektrischen und leittechnischen Systeme erforderlich ist, um zu bestätigen, dass die Fehlerunabhängigkeit, die in den deterministischen und probabilistischen Fehlerstudien angenommen wird, bei der Genehmigung der Anlage in Anspruch genommen werden kann; siehe 5.2.5. Die Analyse muss alle Phasen des Lebenszyklus der elektrischen und leittechnischen Systeme von der Indienststellung bis zur Außerbetriebsetzung abdecken. Das Ergebnis der Studie muss dokumentiert werden, um die Annahmen und Kriterien zur Erzielung des gewünschten Schutzes gegen CCF festzuhalten, z. B. als Teil eines Anhangs zum CCF-Strategiedokument.

Zusätzlich zu der in 5.2.5 identifizierten Analyse sind Analysen der folgenden Hauptpunkte und Schlüsselereignisse während der Lebensdauer der Anlage durchzuführen:

5.3.2 Eine Analyse muss bei Beginn der Auslegung der gesamten elektrischen und leittechnischen Systeme fertiggestellt sein; diese Analyse ist ein Zusatz zu der nach 5.2.5 und muss die Anforderungen an das Management, die Auslegungsprozesse, Personalangelegenheiten und auch alles mit Einfluss auf die Diversität umfassen, wenn diese im Sicherheitsbericht als Mittel gegen CCF von verschiedenen Systemen in Anspruch genommen wird.

5.3.3 Eine Analyse muss bei Abschluss der Auslegung fertiggestellt sein, um zu bestätigen, dass die physikalische Auslegung und Anforderungen zu Trennung, Isolation und Barrieren (physikalisch und administrativ) zum Schutz gegen CCF erfüllt worden sind. Zusätzlich muss die Analyse bestätigen, dass Anforderungen an Signale, Menschen, Verfahren, Technologie, Gerät sowie Herstellungsanforderungen für Diversität erfüllt worden sind.

5.3.4 Eine Analyse muss bei Abschluss der Herstellung der elektrischen und leittechnischen Geräte fertiggestellt sein, um zu bestätigen, dass die Anforderungen an Signale, Personal, Verfahren, Technologie, Gerät sowie Herstellungsanforderungen erfüllt worden sind.

5.3.5 Eine Analyse muss bei Abschluss der Inbetriebnahme der Elektro- und Leittechnik fertiggestellt sein, um zu bestätigen, dass Anforderungen zu Trennung, Isolation und Barrieren (physikalisch und administrativ) erfüllt worden sind.

5.3.6 Eine Analyse für Betriebs- und Wartungsaktivitäten muss fertiggestellt sein, um zu bestätigen, dass Maßnahmen zur Vermeidung einer möglichen Einschleppung von Möglichkeiten für CCF, z. B. durch Wartungsfehler, getroffen worden sind.

5.3.7 Eine Analyse muss bei einer Auslegungsänderung fertig gestellt sein, einschließlich jeglicher Änderungen wegen Zugeständnissen in der Herstellung, und für Gerät/Komponentenaustausch während des Betriebs, um zu bestätigen, dass die Änderung nicht die sicherheitstechnische Aussage bezüglich Schutz gegen CCF infrage stellt.

6 CCF infolge von Gefährdung

6.1 Allgemeines

IAEA SSR 2.1 R17 fordert, interne und externe Gefährdungen, die sich auf die Anlagensicherheit auswirken könnten, zu identifizieren und die Auswirkung zu bewerten. Eine Anzahl solcher von IAEA genannten Gefährdungen sind in [Anhang A](#) zusammengestellt. Bei der Betrachtung der möglichen Auswirkungen kann man sehen, dass sie nicht nur die Fähigkeit zu einem lokalen Effekt haben, sondern eine anlagenweite Auswirkung und folglich das Potenzial, zu einem CCF zu führen.

6.1.1 Jede festgestellte Gefährdung muss analysiert werden, um die physikalischen und Umgebungsbedingungen zu bestimmen, die sie hervorrufen können, und das physikalische Ausmaß hiervon bestimmt die Bedingungen, denen das elektrische und leittechnische Gerät ausgesetzt sein würde.

6.1.2 Das elektrische und leittechnische System muss untersucht werden, um festzustellen, wo die Gefährdung möglicherweise das Versagen multipler redundanter Abschnitte eines Systems und CCF in Systemen verursacht, die zu verschiedenen Schutzlinien gehören. Die festgestellten Lücken müssen dokumentiert werden.

6.1.3 Die Schwere der Folgen für die Anlagensicherheit eines in der Analyse festgestellten möglichen CCF, 6.1.1 und 6.1.3, muss bestimmt werden und die Notwendigkeit für Gegenmaßnahmen den elektrischen und leittechnischen Ingenieuren zur Kenntnis gebracht werden, um die Sicherheitsziele einzuhalten.

6.2 Schutz gegen Gefährdungen

Die Vorgehensweise, um Schutz gegen Gefährdungen zu erhalten, ist allgemein folgende:

- 1) Eliminierung der Gefährdung (z. B. zeigen, dass sie nicht auftreten kann);
- 2) Vorsehen von ingenieurtechnischem Schutz gegen die Gefährdung (z. B. durch physikalische Barrieren und räumliche Trennung);
- 3) administrativer Schutz (z. B. durch vor Ort verfügbare Betriebsprozeduren, so dass eine bestehende Gefährdung sich auf die in Betrieb befindliche Anlage nicht auswirken kann);
- 4) Abmilderung (z. B. durch Brandschutz).

Damit und mit der Liste von Gefährdungen in [Anhang A](#) wird offensichtlich, dass die elektrischen und leittechnischen Ingenieure beim Einrichten von Schutz gegen Gefährdungen nur begrenzt eine Rolle spielen; so haben sie keine größere Rolle bei Beurteilung und Bereitstellung von Schutz gegen CCF aufgrund von Gefährdungen. Tatsächlich wird aus der Liste der Gefährdungen klar, dass der Schutz gegen CCF mit Entscheidungen über den Anlagenstandort beginnt, und dass viele der Schutzmaßnahmen darin bestehen, elektrisches und leittechnisches Gerät von verschiedenen Strängen und unterschiedlichen Systemen an verschiedenen Einbauorten zu haben, z. B. an entgegengesetzten Seiten im Reaktorgebäude und umgeben von technischen Barrieren, z. B. in brand- und überflutungssicheren Umschließungen, die stark genug sind, Einwirkungen von fliegenden Teilen oder herabfallenden Lasten auszuhalten. Es ist Aufgabe der Bauingenieure und mechanischen Ingenieure, den Anlagenstandort und die Auslegung festzulegen sowie den ingenieurtechnischen Schutz vorzusehen (siehe 2) oben).

Nichtsdestoweniger gibt es eine Anzahl von Anforderungen, die dem Gebiet der Elektro- und Leittechnik zufallen, einschließlich Geräteauslegung und -auswahl sowie Gerätequalifizierung.

6.2.1 Die Intention von Entwurf und Qualifizierung des elektrischen und leittechnischen Geräts muss sein, dass es imstande ist, die physikalischen und Umgebungsbedingungen auszuhalten, die für jede Gefährdung festgestellt wurden, der es möglicherweise ausgesetzt wird, einschließlich

- Umgebung nach IEC 60780.
- Erdbeben nach IEC 60980.
- elektromagnetische Beeinflussung nach IEC 62003.

Diese Auslegungsmittel der Elektro- und Leittechnik umfassen Dinge wie tauchfeste und feuerfeste (Überflutung, Brand) Kabel, Faraday-Käfige, geschirmte Kabel und Filter (elektromagnetische Beeinflussung), starke Rückwände für Schalttafeln und fixierte Stecker und Buchsen (Erdbeben). Die Elektro- und Leittechnik muss auch Abmilderungs-Maßnahmen berücksichtigen, z. B. die Konsequenzen eines Brand-Unterdrückungssystems, indem Gerät in entsprechend ausgelegten Schränken untergebracht wird, um Zerstörung durch Sprinklersysteme zu vermeiden.

6.2.2 Die Fälle, in denen mehr als ein System sicherheitstechnisch in Anspruch genommen wird, um Schutz gegen die Gefährdungen zu bieten, müssen festgestellt werden. Die Fähigkeit dieser Systeme, den Gefährdungen zu widerstehen, muss bewertet werden, um zu bestimmen, ob die sicherheitstechnisch in Anspruch genommenen Systeme wegen der Gefährdungen CCF erleiden könnten. Diese Fälle müssen identifiziert und dokumentiert werden.

Es ist offensichtlich, dass einige der elektrischen und leittechnischen Geräte den Gefährdungen nicht widerstehen werden, um mögliche CCF allein durch elektrische und leittechnische Maßnahmen zu verhindern. Während z. B. einige elektrische und elektronische Komponenten das Untertauchen überstehen können, z. B. elektrische Unterwasserkabel, so können es doch nicht alle. In solchen Fällen wird physikalische Trennung und Platzierung des Geräts an gefährdungsresistenten Orten verwendet; z. B. an brand- oder überflutungsresistenten Orten oder in Faraday-Käfigen zur Verhinderung elektromagnetischer Beeinflussung.

6.2.3 Wenn ein alternatives Mittel verwendet wird, um das Überleben eines Geräts sicherzustellen und damit CCF zu verhindern, müssen elektrische, leittechnische und andere Ingenieure die Vorkehrung überprüfen und bestätigen, dass das gewünschte Ziel erreicht worden ist.

Wenn z. B. Gerät in einem überflutungs- oder brandsicheren Bereich platziert wird, müssen die elektrischen und leittechnischen Ingenieure bestätigen, dass durch Kabel und Kabeldurchführung nicht die Fähigkeit des Bereichs verlorengeht, der Gefährdung zu widerstehen.

6.2.4 Wenn der Widerstand von Barrieren oder Gerät begrenzt ist, z. B. in der Zeit durch die Verwendung von brandsicheren Kabeln und Brandbarrieren, müssen die elektrischen und leittechnischen Ingenieure die Wirkung davon auf die Fähigkeit der Systeme bestimmen, ihre Sicherheitsfunktion auszuüben. Die Sicherheitsingenieure müssen dann die Folgen für die Anlagensicherheit bewerten.

In der Definition des CCF wird das Konzept „zur selben Zeit“ eingeführt, das oft als „simultan“ verstanden wird. In diesem Zusammenhang sollte „simultan“ als Zeitspanne betrachtet werden, in der – wenn die Sicherheitsmaßnahmen nicht greifen – das Sicherheitsziel nicht erreicht wird. Bei Gefährdungen kann CCF über eine Reihe von Fehlern in einer größeren Zeitspanne auftreten; z. B. aufeinanderfolgende Brandbarrieren. Wenn alle Maßnahmen zur Erzielung des sicheren Zustands versagen bevor dieser erreicht ist, wird die Anlagensicherheit durch CCF paralysiert werden; folglich ist die Anforderung 6.2.4 essenziell, um sicherzustellen, dass Gefährdungen nicht zum Verlust der Anlagensicherheit infolge CCF führen.

Maßnahmen zur Abmilderung von Gefährdungen gehören nicht zum Anwendungsbereich dieser Norm; allerdings haben einige davon, wie etwa Sprinklersysteme und Brandbekämpfung, die Fähigkeit, CCF zu verursachen.

6.2.5 Die elektrischen und leittechnischen Ingenieure müssen in der Analyse von CCF-Ursachen die möglichen Auswirkungen bei der Verwendung von gefährdungsabmildernden Maßnahmen einschließen.

7 CCF infolge von Fehlerfortpflanzung

7.1 Allgemeines

Wenn mehrfache Stränge eines einzelnen Systems verbunden sind (z. B. Auswahlaltungen) oder Systeme in verschiedenen Schutzlinien verbunden sind (möglicherweise am Akteur) ist ein Potenzial für