

**DIN IEC 60709
(VDE 0491-7)**
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 27.120.10

Einsprüche bis 2016-06-15

Vorgesehen als Ersatz für
DIN EN 60709
(VDE 0491-7):2010-12

Entwurf

**Kernkraftwerke –
Elektrische und leittechnische Systeme mit sicherheitstechnischer
Bedeutung –
Physikalische und elektrische Trennung
(IEC 45A/1046/CD:2015)**

Nuclear power plants –
Instrumentation, control and electrical systems important to safety –
Separation
(IEC 45A/1046/CD:2015)

Centrales nucléaires de puissance –
Systèmes d'instrumentation, de contrôle-commande et électriques importants pour la sûreté –
Séparation
(IEC 45A/1046/CD:2015)

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2016-04-15 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 des DIN unter www.entwuerfe.din.de 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/stellungnahme 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 93 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE

Anwendungsbeginn

Anwendungsbeginn dieser Norm ist

Inhalt	Seite
Nationales Vorwort.....	5
Nationaler Anhang NA (informativ) Zusammenhang mit Europäischen und Internationalen Dokumenten	8
Nationaler Anhang NB (informativ) Literaturhinweise.....	9
Einleitung	11
1 Anwendungsbereich	13
2 Normative Verweisungen	13
3 Begriffe	14
4 Abkürzungen	17
5 Fehlerarten	17
5.1 Auslegungsfehler.....	17
5.2 Leittechnische und elektrotechnische Fehlerereignisse.....	18
5.2.1 Allgemeines	18
5.2.2 Einzelner Zufallsfehler	18
5.2.3 Mehrfache Fehler einer einzelnen gemeinsamen Ursache	18
5.3 Fehlerereignisse im Kraftwerk	18
5.3.1 Allgemeines	18
5.3.2 Umgebungsbedingungen	18
5.3.3 Elektromagnetische Beeinträchtigung.....	18
5.3.4 Fehler in Kraftwerkssystemen, Geräten oder Strukturen	19
5.3.5 Bedienungsfehler.....	19
5.4 Externe versagensauslösende Ereignisse	19
5.4.1 Allgemeines	19
5.4.2 Naturereignisse	19
5.4.3 Durch Menschen verursachte Ereignisse	19
5.5 Spezielle Betriebsbedingungen	19
6 Grundsätze (funktionaler und/oder räumlicher) Trennung	19
6.1 Allgemeines	19
6.2 Anforderungen an die Unabhängigkeit.....	20
6.3 Grundsätze	21
6.4 Räumliche Trennung	22
6.4.1 Allgemeines	22
6.4.2 Trennung durch Abstand	23
6.4.3 Trennung durch bauliche Maßnahmen	23
6.5 Elektrische Trennung.....	23
6.5.1 Allgemeines	23

6.5.2	Allgemeines.....	24
6.5.3	Kurzschluss-/Überstromschutz	24
6.5.4	Elektrische Rückwirkungsfreiheit	24
6.5.5	Galvanische Trennung (elektrische Isolation).....	24
6.6	Funktionale Unabhängigkeit.....	25
6.7	Unabhängigkeit der Kommunikation	25
6.8	Verbundene (Schalt-)kreise	26
6.9	Aspekte der Trennung in bestehenden Kraftwerken.....	27
7	Auslegungsgrundlagen der Trennung.....	28
7.1	Grundsätze.....	28
7.2	Brandschutz	28
7.3	Umgebungsbedingungen während und nach Störfällen.....	28
7.4	Elektrische Trennung	29
7.4.1	Allgemeines.....	29
7.4.2	Trennungseigenschaften.....	29
7.4.3	Priorisierung	30
7.4.4	Entkopplung	30
7.5	Elektromagnetische Verträglichkeit.....	30
7.6	Brüche hochenergetischer Rohrleitungen.....	31
7.7	Unabhängigkeit von Steuerungssystemen	31
8	Anforderungen zur Trennung von Kabeln und Gerät.....	32
8.1	Allgemeine Anforderungen.....	32
8.2	Trennung	33
8.2.1	Trennungskriterien	33
8.2.2	Trennungsanforderungen.....	33
8.2.3	Trennung von Kabeln und Kabeltragkonstruktionen innerhalb der leittechnischen und elektrischen Sicherheitssysteme.....	33
8.2.4	Trennung von Komponenten innerhalb leittechnischer und elektrischer Sicherheitssysteme	36
8.2.5	Wartenschränke, -pulte, -tafeln und zugehörige Kabel.....	37
8.3	Thermischer und physikalischer Schutz	38
8.4	Brandschutz	38
8.5	Identifikation	38
Anhang A (informativ) Bezug zu IAEA-Sicherheitsstandards und zur IEC 61226 (CD 2015)		40
A.1	Ziel dieses Anhangs	40
A.2	Anwendbarkeit dieser Norm	40
A.3	Für diese Norm anwendbare IAEA-Sicherheitsstandards	40
A.4	IEC-Normen, anwendbar für die Sicherheitskategorisierung und -klassifizierung.....	40
A.5	Barrieren des tief gestaffelten Schutzes, vereinfachte Definitionen	40
Anhang B (informativ) Beispiele ausgeführter Trennungen		42

	Seite
B.1 Ziel dieses Anhangs	42
B.2 Beispiele physikalischer Trennung	42
B.2.1 Beispiele physikalischer Trennung	42
B.2.2 Beispiele physikalischer Trennung durch Abstand	42
B.2.3 Beispiele physikalischer Trennung durch bauliche Maßnahmen	44
B.3 Beispiele elektrischer Trennung	45
B.3.1 Beispiele von Überspannungsbarrieren	45
B.3.2 Beispiele von Kurzschluss- und Überstromschutz	46
B.3.3 Beispiele galvanischer Trennung	47
B.4 Beispiele von EMV-Schutzmaßnahmen	48
B.5 Verbundene Schaltkreise	49
Literaturhinweise	51
Bilder	
Bild 1 – Maßnahmen elektrischer Trennung und Wahl der Komponenten	23
Bild B.2.1.a – Trennung der Kabeltragkonstruktionen durch Abstand	43
Bild B.2.1.b – Trennung der Kabelpritschen durch Abstand	43
Bild B.2.2 – Trennung der Kabelpritschen durch bauliche Strukturen	44
Bild B.3.1.a – Überspannungs-Schutzeinrichtung in der Leittechnik	45
Bild B.3.1.b – Überspannungs-Schutzeinrichtung in einem elektrischen Abzweig	46
Bild B.3.2 – Kurzschluss-Schutz im Falle einer Querverbindung	47
Bild B.3.3.a – Galvanische Trennung von Leittechniksystemen	47
Bild B.3.3.b – Galvanische Trennung in elektrischen Systemen	48
Bild B.4 – EMV-Schutz von Leittechnikkabeln	49
Bild B.5 – Beispiele verbundener Schaltkreise	50

Nationales Vorwort

Das internationale Dokument IEC 45A/1046/CD:2015 „Nuclear power plants – Instrumentation, control and electrical systems important to safety – Separation“ (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 systems of nuclear facilities“ der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet und den nationalen Komitees zur Stellungnahme vorgelegt.

Da der Abstimmungszeitraum für einen FDIS 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 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.

Das Original-Dokument enthält Bilder in Farbe, die in der Papierversion in einer Graustufen-Darstellung wiedergegeben werden. Elektronische Versionen dieses Dokuments enthalten die Bilder in der originalen Farbdarstellung.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. ISO [und/oder] IEC sind nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

In der Reihe VDE 0491 sind als Normen erschienen:

- DIN EN 61226 (VDE 0491-1):2010-08, *Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Kategorisierung leittechnischer Funktionen (IEC 61226:2009); Deutsche Fassung EN 61226:2010*
- DIN EN 61513 (VDE 0491-2):2013-09, *Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Allgemeine Systemanforderungen (IEC 61513:2011); Deutsche Fassung EN 61513:2013*
- DIN EN 60987 (VDE 0491-3-1):2015-06, *Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Anforderungen an die Hardwareauslegung rechnerbasierter Systeme (IEC 60987:2007 + A1:2013); Deutsche Fassung EN 60987:2015*
- DIN EN 60880 (VDE 0491-3-2):2010-03, *Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Softwareaspekte für rechnerbasierte Systeme zur Realisierung von Funktionen der Kategorie A (IEC 60880:2006); Deutsche Fassung EN 60880:2009*
- DIN EN 62138 (VDE 0491-3-3):2010-03, *Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Softwareaspekte für rechnerbasierte Systeme zur Realisierung von Funktionen der Kategorien B oder C (IEC 62138:2004); Deutsche Fassung EN 62138:2009*
- DIN EN 61500 (VDE 0491-3-4):2011-12, *Kernkraftwerke – Leittechnik mit sicherheitstechnischer Bedeutung – Datenkommunikation (IEC 61500:2009); Deutsche Fassung EN 61500:2011*
- DIN EN 62566 (VDE 0491-3-5):2015-02, *Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Entwicklung HDL-programmierter integrierter Schaltkreise für Systeme, die Funktionen der Kategorie A ausführen (IEC 62566:2012); Deutsche Fassung EN 62566:2014*
- DIN IEC 62117 (VDE 0491-4):2001-10, *Kernkraftwerke – Druckwasserreaktoren – Überwachung ausreichender Kühlung des Kerns im abgeschalteten Zustand des Reaktors (IEC 62117:1999)*

E DIN IEC 60709 (VDE 0491-7):2016-05

- DIN EN 61839 (VDE 0491-5):2015-01, *Kernkraftwerke – Auslegung von Warten – Analyse und Zuordnung der Funktionen (IEC 61839:2000); Deutsche Fassung EN 61839:2014*
- DIN EN 60964 (VDE 0491-5-1):2010-08, *Kernkraftwerke – Warten – Auslegung (IEC 60964:2009); Deutsche Fassung EN 60964:2010*
- DIN EN 62241 (VDE 0491-5-2):2015-06, *Kernkraftwerke – Warte – Funktionen zur Meldung und Anzeige von Störungen (IEC 62241:2004); Deutsche Fassung EN 62241:2015*
- DIN IEC 61227 (VDE 0491-5-3):2009-01, *Kernkraftwerke – Warten – Handbedienungen (IEC 61227:2008)*
- DIN EN 61772 (VDE 0491-5-4):2013-09, *Kernkraftwerke – Warten – Anwendung von Sichtgeräten (IEC 61772:2009); Deutsche Fassung EN 61772:2013*
- DIN EN 60965 (VDE 0491-5-5):2011-12, *Kernkraftwerke – Warten – Notsteuerstellen für das Abfahren des Reaktors ohne Verbindung zur Hauptwarte (IEC 60965:2009); Deutsche Fassung EN 60965:2011*
- DIN IEC 60568 (VDE 0491-6):2006-11, *Kernkraftwerke – Instrumentierung mit sicherheitstechnischer Bedeutung – Kerninstrumentierung zur Messung der Neutronenflussdichte in Leistungsreaktoren (IEC 60568:2006)*
- DIN EN 60709 (VDE 0491-7):2010-12, *Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Physikalische und elektrische Trennung (IEC 60709:2004); Deutsche Fassung EN 60709:2010*
- DIN EN 62340 (VDE 0491-10):2010-12, *Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Anforderungen zur Beherrschung von Versagen aufgrund gemeinsamer Ursache (IEC 62340:2007); Deutsche Fassung EN 62340:2010*
- DIN EN 60671 (VDE 0491-100):2011-12, *Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Prüfungen zur Sicherstellung der Funktionsfähigkeit (IEC 60671:2007); Deutsche Fassung EN 60671:2011*

Als Norm-Entwürfe liegen vor:

- E DIN IEC 61226 (VDE 0491-1):2015-08, *Kernkraftwerke – Leittechnische und elektrische Systeme mit sicherheitstechnischer Bedeutung – Kategorisierung von Funktionen und Klassifizierung von Systemen (IEC 45A/1018/CD::2015)*
- E DIN IEC 62138 (VDE 0491-3-3):2015-01, *Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Softwareaspekte für rechnerbasierte Systeme zur Realisierung von Funktionen der Kategorien B oder C (IEC 45A/962/CD:2014)*
- E DIN IEC 61500 (VDE 0491-3-4):2016-02, *Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Datenkommunikation in Systemen, die Funktionen der Kategorie A ausführen (IEC 45A/1044/CD:2015)*
- E DIN IEC 62988 (VDE 0491-3-6):2016-05, *Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Auswahl und Einsatz drahtloser Geräte (IEC 45A/1050/CD:2015)*
- E DIN IEC 62645 (VDE 0491-3-7):2013-04, *Kernkraftwerke – Leittechnische Systeme – Anforderungen an die IT-Sicherheitsplanung für rechnerbasierte Systeme (IEC 45A/890/CDV:2012)*
- E DIN IEC 62859 (VDE 0491-3-8):2015-10, *Kernkraftwerke – Leittechnische Systeme – Anforderungen bezüglich der Koordination von Sicherheit und Cyber-Security (IEC 45A/1014/CD:2015)*
- E DIN IEC 60965 (VDE 0491-5-5):2014-11, *Kernkraftwerke – Warten – Notsteuerstellen für das Abfahren des Reaktors ohne Verbindung zur Hauptwarte (IEC 45A/952/CD:2014)*
- E DIN IEC 62646 (VDE 0491-5-6):2011-09, *Kernkraftwerke – Warten – Rechnerunterstützte Prozeduren (IEC 45A/839/CDV:2011)*
- E DIN IEC 60709 (VDE 0491-07):2016-05, *Kernkraftwerke – Elektrische und leittechnische Systeme mit sicherheitstechnischer Bedeutung – Physikalische und elektrische Trennung (IEC 45A/1046/CD:2015)*
- E DIN IEC 61225 (VDE 0491-8):2012-06, *Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Anforderungen an die elektrische Energieversorgung (IEC 61225:2005)*
- E DIN IEC 62855 (VDE 0491-8-1):2014-11, *Kernkraftwerke – Elektrische Systeme – Analyse der Stromversorgung (IEC 45A/964/CD:2014)*

- E DIN IEC 60772 (VDE 0491-9-1):2014-11, *Kernkraftwerke – Sicherheitswichtige Instrumentierung – Elektrische Durchführungen für Sicherheitsbehälter (IEC 45A/966/CD:2014)*
- E DIN IEC 60744 (VDE 0491-9-2):2014-11, *Kernkraftwerke – Leittechnik mit sicherheitstechnischer Bedeutung – Sicherheitslogikanordnungen: Merkmale und Testverfahren (IEC 45A/946/CD:2014)*
- E DIN IEC 62808 (VDE 0491-9-3):2016-03, *Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Auslegung und Qualifizierung von Isolationseinrichtungen (IEC 62808:2015)*
- E DIN IEC 62887 (VDE 0491-9-4):2016-03, *Kernkraftwerke – Instrumentierung mit sicherheitstechnischer Bedeutung – Druckmessumformer: Eigenschaften und Prüfverfahren (IEC 45A/1045/CD:2015)*
- E DIN IEC 62003 (VDE 0491-11):2016-05, *Kernkraftwerke – Elektro- und leittechnische Systeme mit sicherheitstechnischer Bedeutung – Anforderungen für die Prüfung der Elektromagnetischen Verträglichkeit (IEC 45A/1052/CD:2015)*
- E DIN IEC 62705 (VDE 0491-15):2015-02, *Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Strahlungsüberwachungssysteme: Eigenschaften und Lebenszyklus (IEC 62705:2014)*
- E DIN IEC 61504 (VDE 0491-16):2015-10, *Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Zentralisierte Systeme zur kontinuierlichen Strahlungs- und/oder Radioaktivitätsüberwachung (IEC 45A/1016/CD:2015)*
- E DIN IEC 62342 (VDE 0491-20-1):2012-02, *Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Alterungsmanagement (IEC 62342:2007)*
- E DIN IEC/IEEE 62582-1 (VDE 0491-21-1):2015-06, *Kernkraftwerke – Leittechnik mit sicherheitstechnischer Bedeutung – Zustandsüberwachung elektrischer Geräte – Teil 1: Allgemeines (IEC/IEEE 62582-1:2011)*
- E DIN IEC/IEEE 62582-2 (VDE 0491-21-2):2015-08, *Kernkraftwerke – Leittechnik mit sicherheitstechnischer Bedeutung – Zustandsüberwachung elektrischer Geräte – Teil 2: Eindringprüfung (IEC/IEEE 62582-2:2011)*
- E DIN IEC/IEEE 62582-3 (VDE 0491-21-3):2015-07, *Kernkraftwerke – Leittechnik mit sicherheitstechnischer Bedeutung – Zustandsüberwachung elektrischer Geräte – Teil 3: Reißdehnung (IEC/IEEE 62582-3:2012)*
- E DIN IEC/IEEE 62582-4 (VDE 0491-21-4):2015-10, *Kernkraftwerke – Leittechnik mit sicherheitstechnischer Bedeutung – Zustandsüberwachung elektrischer Geräte – Teil 4: Oxidation (IEC/IEEE 62582-4: 2011)*
- E DIN IEC/IEEE 62582-5 (VDE 0491-21-5):2016-03, *Kernkraftwerke – Leittechnik mit sicherheitstechnischer Bedeutung – Zustandsüberwachung elektrischer Geräte – Teil 5: Optische Zeitbereichsreflektometrie (IEC/IEEE 62582-5: 2015)*
- E DIN IEC 62765-1 (VDE 0491-22-1):2015-06, *Kernkraftwerke – Leittechnik mit sicherheitstechnischer Bedeutung – Alterungsmanagement von Sensoren und Transmittern – Teil 1: Drucktransmitter (IEC 45A/1001/FDIS:2015)*
- E DIN IEC 60780-323 (VDE 0491-80):2014-03, *Kerntechnische Anlagen – Elektrisches Gerät mit sicherheitstechnischer Bedeutung – Qualifizierung (IEC 45A/940/CD:2013)*

Änderungen

Gegenüber DIN EN 60709 (VDE 0491-7):2010-12 wurden folgende Änderungen vorgenommen:

- a) Titel und Anwendungsbereich wurden auf alle elektrischen und leittechnischen Systeme mit sicherheitstechnischer Bedeutung erweitert, Anforderungen bezüglich der elektrischen Systeme neu aufgenommen;
- b) Trennungskriterien für elektrische und leittechnische Systeme werden in generischer Form beschrieben;
- c) die gegenseitige Beeinflussung elektrischer und leittechnischer Geräte unterschiedlicher Sicherheitsklassen wurde berücksichtigt;
- d) die Anforderungen wurden bezüglich neuer Technologien angepasst;
- e) die Rolle der Elektromagnetischen Verträglichkeit als Auslöser von Versagen aufgrund gemeinsamer Ursache (CCF) wurde aufgenommen;

- f) bezüglich Kabeln und Kabelanlagen wurden die Anforderungen präzisiert;
- g) das Konzept der "verbundenen Schaltkreise" wurde aus US-amerikanischer Praxis aufgenommen;
- h) die Behandlung des Themas "Brandschutz" wurde aufgenommen;
- i) es werden auch die Auswirkungen niederenergetischer Schaltkreise angesprochen;
- j) die bestehenden Anforderungen und Begriffe wurden einer kritischen Prüfung unterzogen;
- k) die Bezüge auf IEC- und IAEA-Dokumente wurden aktualisiert;
- l) eine Anleitung für die Anwendung der Norm auf bestehende Anlagen wurde aufgenommen;
- m) der Text wurde redaktionell überarbeitet;
- n) die deutsche Fassung wurde in den Abschnitten 2 und 3 an die aktuellen Standardsätze angepasst.

Nationaler Anhang NA (informativ)

Zusammenhang mit Europäischen und Internationalen Dokumenten

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.

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

Tabelle NA.1 (1 von 2)

Europäisches Dokument	Internationales Dokument	Deutsches Dokument	Klassifikation im VDE-Vorschriftenwerk
EN 60332 (alle Teile)	IEC 60332 (alle Teile)	DIN EN 60332 (VDE 0482-332) (alle Teile)	VDE 0482-332
HD 60364 (alle Teile)	IEC 60364 (alle Teile)	DIN VDE 0100 (VDE 0100) (alle Teile)	VDE 0100
HD 60364-5-52	IEC 60364-5-52	DIN VDE 0100-520 (VDE 0100-520)	VDE 0100-520
HD 60364-5-53	IEC 60364-5-53	DIN VDE 0100-534 (VDE 0100-534)	VDE 0100-534
EN 60880	IEC 60880	DIN EN 60880 (VDE 0491-3-2)	VDE 0491-3-2
EN 60964	IEC 60964	DIN EN 60964 (VDE 0491-5-1)	VDE 0491-5-1
EN 61000 (alle Teile)	IEC 61000 (alle Teile)	DIN EN 61000 (VDE 0838 / VDE 0839 / VDE 0847) (alle Teile)	VDE 0838 VDE 0839 VDE 0847
EN 61000-6-5	IEC 61000-6-5	DIN EN 61000-6-5 (VDE 0839-6-5) ^a	VDE 0839-6-5
EN 61226	IEC 61226	DIN EN 61226 (VDE 0491-1)	VDE 0491-1

Tabelle NA.1 (2 von 2)

Europäisches Dokument	Internationales Dokument	Deutsches Dokument	Klassifikation im VDE-Vorschriftenwerk
–	IEC/TR 61508	DIN EN 61508 Bbl 1 (VDE 0803 Bbl 1)	VDE 0803 Bbl 1
EN 61508-1	IEC 61508-1	DIN EN 61508-1 (VDE 0803-1)	VDE 0803-1
EN 61508-2	IEC 61508-2	DIN EN 61508-2 (VDE 0803-2)	VDE 0803-2
EN 61508-3	IEC 61508-3	DIN EN 61508-3 (VDE 0803-3)	VDE 0803-3
EN 61508-4	IEC 61508-4	DIN EN 61508-4 (VDE 0803-4)	VDE 0803-4
EN 61513	IEC 61513	DIN EN 61513 (VDE 0491-2)	VDE 0491-2
EN 61647 (alle Teile) ersetzt durch:	IEC 61647 (alle Teile) ersetzt durch:	DIN EN 61647 (VDE 0845) (alle Teile) ersetzt durch:	VDE 0845
EN 61643 (alle Teile)	IEC 61643 (alle Teile)	DIN EN 61643 (VDE 0675 / VDE 0845) (alle Teile)	VDE 0675 VDE 0845
–	IEC 62003	–	–
–	IEC/TR 62096	–	–
EN 62138	IEC 62138	DIN EN 62138 (VDE 0491-3-3)	VDE 0491-3-3
EN 62305 (alle Teile)	IEC 62305 (alle Teile)	DIN EN 62305 (VDE 0185-305) (alle Teile)	VDE 0185-305
–	IEC 62808	DIN IEC 62808 (VDE 0491-9-3) ^a	VDE 0491-9-3
^a In Vorbereitung.			

Nationaler Anhang NB (informativ)

Literaturhinweise

DIN EN 60332 (VDE 0482-332) (alle Teile), *Prüfungen an Kabeln, isolierten Leitungen und Glasfaserkabeln im Brandfall*

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

DIN EN 60964 (VDE 0491-5-1), *Kernkraftwerke – Warten – Auslegung*

DIN EN 61000 (VDE 0838/VDE 0839/VDE 0847) (alle Teile), *Elektromagnetische Verträglichkeit (EMV)*

DIN EN 61000-6-5 (VDE 0839-6-5) (in Vorbereitung), *Elektromagnetische Verträglichkeit (EMV) – Teil 6-5: Fachgrundnormen – Störfestigkeit von Betriebsmitteln, Geräten und Einrichtungen, die im Bereich von Kraftwerken und Schaltstationen verwendet werden*

DIN EN 61226 (VDE 0491-1), *Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Kategorisierung leittechnischer Funktionen*

E DIN IEC 60709 (VDE 0491-7):2016-05

DIN EN 61508 Beiblatt 1 (VDE 0803 Beiblatt 1), *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 0: Funktionale Sicherheit und die IEC 61508*

DIN EN 61508-1 (VDE 0803-1), *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 1: Allgemeine Anforderungen*

DIN EN 61508-2 (VDE 0803-2), *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 2: Anforderungen an sicherheitsbezogene elektrische/ elektronische/programmierbare elektronische Systeme*

DIN EN 61508-3 (VDE 0803-3), *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 3: Anforderungen an Software*

DIN EN 61508-4 (VDE 0803-4), *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 4: Begriffe und Abkürzungen*

DIN EN 61513 (VDE 0491-2), *Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Allgemeine Systemanforderungen*

DIN EN 61643 (VDE 0675/VDE 0845) (alle Teile), *Überspannungsschutzgeräte für Niederspannung / Bauelemente für Überspannungsschutzgeräte für Niederspannung*

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

DIN EN 62305 (VDE 0185-305) (alle Teile), *Blitzschutz*

DIN IEC 62808 (VDE 0491-9-3) (in Vorbereitung), *Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Auslegung und Qualifizierung von Isolationseinrichtungen*

DIN VDE 0100 (VDE 0100) (alle Teile), *Errichten von Niederspannungsanlagen*

DIN VDE 0100-520 (VDE 0100-520), *Errichten von Niederspannungsanlagen – Teil 5-52: Auswahl und Errichtung elektrischer Betriebsmittel – Kabel- und Leitungsanlagen*

DIN VDE 0100-534 (VDE 0100-534), *Errichten von Niederspannungsanlagen – Teil 5-53: Auswahl und Errichtung elektrischer Betriebsmittel – Trennen, Schalten und Steuern – Abschnitt 534: Überspannungsschutzeinrichtungen (ÜSE)*

**Kernkraftwerke –
Elektrische und leittechnische Systeme mit sicherheitstechnischer Bedeutung –
Physikalische und elektrische Trennung**

Einleitung

a) Hintergrund, hauptsächliche Inhalte und Organisation der Norm

Sicherheitstechnisch wichtige leittechnische und elektrische Systeme in Kernkraftwerken müssen fehlertolerant für Auswirkungen von Anlagen-/Gerätefehlern sowie internen und externen Störfällen sein. Es gibt verschiedene Techniken, um die Unempfindlichkeit von leittechnischen und elektrischen Systemen gegen solche Auswirkungen zu erhöhen, einschließlich der Planung unabhängiger Systeme, Teilsysteme und Geräte. Will man sich auf die Unabhängigkeit zwischen derartigen Systemen und Geräten berufen, sollte eine geeignete räumliche und elektrische Trennung ausgeführt und aufrechterhalten bleiben. Diese Norm enthält allgemeine technische Anforderungen und Empfehlungen für die Realisierung der Trennung bei der Auslegung leittechnischer und elektrischer Systeme.

Zweck dieser Norm ist,

- in Abschnitt 4 eine gewisse Zahl möglicher Ursachen für Fehler zu identifizieren und unter Berücksichtigung dieser Ursachen einen Satz von Anforderungen aufzustellen, die bei der Auslegung eines sicherheitstechnisch wichtigen leittechnischen und elektrischen Systems zu befolgen sind, um eine möglichst gute Erfüllung seiner Aufgaben sicherzustellen. Diese Anforderungen beziehen sich auf das leittechnische und das elektrische System insgesamt. Abschnitt 6 enthält auch Anleitungen zur Trennung, die bei der Modernisierung leittechnischer und/oder elektrischer Systeme in bestehenden Kernkraftwerken zu beachten sind
- in Abschnitt 7 Auslegungskriterien für sicherheitstechnisch wichtige leittechnische und elektrische Systeme festzulegen und damit die in Abschnitt 4 ermittelten Ausfallursachen zu berücksichtigen
- in Abschnitt 8 Anforderungen zu definieren, die für die Trennung von Verkabelung und Komponenten innerhalb sicherheitstechnisch wichtiger leittechnischer und elektrischer Systeme einzuhalten sind.

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

Die vorliegende Norm (IEC 60709) ist ein Dokument der zweiten Ebene und wird in IEC 61513 unmittelbar in Bezug auf die physikalische Trennung und die räumliche Trennung unterschiedlicher leittechnischer und elektrischer Teilsysteme unterschiedlicher Sicherheitsstränge angesprochen, sowie zwischen sicherheitstechnisch wichtigen und sicherheitstechnisch nicht wichtigen leittechnischen und elektrischen Systemen.

Aufsetzend auf IAEA SSG-30 beschreibt IEC 61226 die Grundsätze der Kategorisierung von leittechnischen und elektrischen Funktionen und die Klassifizierung der Strukturen, Systeme und Komponenten in Abhängigkeit ihrer sicherheitstechnischen Bedeutung. IEC 61226 bezieht sich wiederum auf IEC 60709 als normativen Standard bezüglich Anforderungen an funktionale und räumliche Trennung.

Weitere Details im Zusammenhang mit dieser Norm, können IAEA-Richtlinien und der IEC 61226 entnommen werden (siehe hierzu auch Anhang A dieser Norm).

c) Empfehlungen und Einschränkungen der Anwendung der Norm

Die vorliegende Norm gilt für sicherheitstechnisch wichtige leittechnische und elektrische Systeme. In ihr sind Anforderungen für die räumliche und elektrische Trennung als eines der Mittel zur Erzielung der Unabhängigkeit zwischen den in diesen Systemen und Geräten ausgeführten Funktionen zusammengestellt. Andere Gesichtspunkte der Unabhängigkeit, die etwa in Hinblick auf Fragen zum Versagen aufgrund gemeinsamer Ursache anzusprechen wären, sind in dieser Norm nicht behandelt. Ebenso werden keine Trennungskriterien aus Gründen der allgemeinen Sicherheit behandelt.

Die in dieser Norm genannten Regeln der Trennung von Sicherheitsklassen können auch bei der Befolgung anderer Zwänge angewendet werden, wie zum Beispiel beim „tief gestaffelten Schutz“-Konzept (en.: defence in depth) und sie sind zu Beginn eines Projektes zu definieren.

Einzelheiten dazu sind in Anhang A beschrieben.

d) Beschreibung der Struktur der Normen des IEC/SC 45A und deren Beziehungen zu anderen Dokumenten einschließlich der Dokumente anderer Organisationen (IAEA, ISO)

Das Eingangsdokument der Normen des IEC/SC 45A ist die IEC 61513. Diese enthält allgemeine Anforderungen an die leittechnischen Systeme und Geräte, die zur Ausführung sicherheitstechnisch wichtiger Funktionen in Kernkraftwerken genutzt werden. IEC 61513 gibt die Struktur der SC-45A-Normenreihe vor.

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

Für IEC 61513 wird ein Darstellungsformat verwendet, das dem der grundsätzlichen Sicherheitsnorm IEC 61508 ähnlich ist, mit einem Sicherheits-Lebenszyklus als Gesamtrahmen und einem System-Lebenszyklus als weiteren wichtigen Rahmen. Bezüglich der Sicherheit kerntechnischer Anlagen werden die allgemeinen Anforderungen der IEC 61508-1, IEC 61508-2 und IEC 61508-4 für den Bereich nuklearer Anwendungen interpretiert. In diesem Zusammenhang entsprechen IEC 60880 und IEC 62138 der IEC 61508-3 für den kerntechnischen Bereich. IEC 61513 bezieht sich auf ISO ebenso wie auf IAEA GS-R-3 und IAEA GS-G-3.1 und IAEA GS-G-3.5 auf Themen der Qualitätssicherung.

In den Normen des IEC/SC 45A werden die Prinzipien und grundsätzlichen Sicherheitsaspekte des IAEA-Codes für die Sicherheit von Kernkraftwerken und der IAEA-Sicherheitsserie, insbesondere die Anforderungen SSR-2/1, die sicherheitstechnische Anforderungen an die Auslegung von Kernkraftwerken festlegt und der Sicherheitsleitfaden SSG-39, der Anforderungen an die Sicherheitsleittechnik von Kernkraftwerken festlegt, umgesetzt. Terminologie und Definitionen in den Normen des IEC/SC 45A stimmen mit den von der IAEA verwendeten überein.

ANMERKUNG 1 Es wird angenommen, dass für die Auslegung von leittechnischen Systemen in Kernkraftwerken, die konventionelle Sicherheitsfunktionen ausführen (zum Beispiel betreffend Personenschutz, Investitionsschutz, chemische Gefahren, Energieprozessgefahren), internationale oder nationale Normen angewendet werden, die auf Anforderungen von Normen, wie die der IEC 61508, basieren.

ANMERKUNG 2 Der Bereich für den IEC/SC 45A Aussagen macht, wurde 2013 erweitert, um auch elektrische Systeme einzuschließen. In den Jahren 2014 und 2015 wurde in IEC/SC 45A diskutiert, um zu entscheiden, wie und wo allgemeine Anforderungen an die allgemeine Auslegung elektrischer Systeme zu berücksichtigen sind. IEC/SC-45A-Fachleute haben empfohlen, dazu eine eigenständige Norm auf gleichem Niveau wie IEC 61513 zu erstellen, um allgemeine Anforderungen (auch) an elektrische Systeme zu definieren. Dieses Vorhaben ist in naher Zukunft zu starten. IEC 61513 und diese neue Norm, die Anforderungen an elektrische Systeme definieren soll, wird im Zusammenhang zu lesen sein. Sie werden gemeinsam einen zusammenhängenden, einheitlichen und kompletten Rahmen für allgemeine Anforderungen an leittechnische und elektrische Systeme bilden. Wenn das Vorhaben der Entwicklung der Norm, die allgemeine Anforderungen an elektrische Systeme definiert, begonnen wird, wird dieser Abschnitt aus der Einleitung der IEC/SC-45A-Normen aktualisiert, um diese Entwicklung zu berücksichtigen.

1 Anwendungsbereich

Diese Internationale Norm ist bei leittechnischen und elektrischen Systemen einschließlich der zugehörigen Geräte und Kabel von Kernkraftwerken anzuwenden, deren Unabhängigkeit durch die Projektdaten aufgrund ihrer Beiträge zu

- redundanten oder diversitären Teilsystemen
- unterschiedlich tief gestaffelten Schutzeinrichtungen
- unterschiedlicher Stränge von Schutzeinrichtungen (Kombination oder Gruppen tief gestaffelter Schutz-einrichtungen).

Sie ist ebenso bei temporären Einrichtungen anzuwenden, die Teil sicherheitstechnisch wichtiger leittechnischer und elektrischer Systeme sind (zum Beispiel Hilfseinrichtungen für Inbetriebsetzung und Experimente oder mobile Stromversorgungen). Abschnitt 8 betrifft insbesondere die Verkabelung und die Anordnung von Gerät sicherheitstechnisch wichtiger Leit- und Elektrotechnik.

Diese Norm ist bei Leittechnik und Elektrotechnik neuer Kernkraftwerke sowie bei Leit- und Elektrotechnik zur Verbesserung oder Nachrüstung bestehender Kraftwerke anzuwenden. Bei bereits bestehenden Kraftwerken ist nur eine Teilmenge der Anforderungen anwendbar; diese Teilmenge ist zu Beginn eines jeden Projekts zu bestimmen.

Wird Unabhängigkeit durch allgemeine Sicherheitsnormen, wie die IAEA Sicherheitsregeln, IEC 61513 und oder durch Projekte gefordert, ist die räumliche Trennung zwischen den Systemen und ihren Geräten, die die sicherheitstechnisch wichtigen Funktionen ausführen, eine Möglichkeit, Unabhängigkeit zu erreichen.

Diese Norm definiert die erforderlichen Bewertungen und die einzuhaltenden technischen Anforderungen, die von sicherheitstechnisch wichtigen leittechnischen und elektrischen Systemen und Geräten oder zugeordnet zu einer entsprechenden Ebene einer tief gestaffelten Schutzeinrichtung (en: defense in depth) und ihrer Kabel einzuhalten sind, um eine ausreichende physikalische und elektrische Trennung zwischen den redundanten Scheiben eines Systems und zwischen höher und niedriger klassifizierten Systemen. Diese Trennung ist erforderlich, um entweder einen Einfluss auf die Sicherheit zu verhindern oder zu reduzieren, der das Ergebnis von Versagen oder Fehlern sein kann, der sich in seiner Wirkung ausbreiten oder mehrere Scheiben eines Systems oder mehrere Systeme beeinflussen kann.

Schaltkreise, die unabhängig sein sollen, sind in den Eingangsdaten zu definieren; ihre Definition ist nicht Gegenstand dieser Norm.

2 Normative Verweisungen

Die folgenden Dokumente, die in diesem Dokument teilweise oder als Ganzes zitiert werden, 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 60332 (alle Teile), *Tests on electric cables under fire conditions*

IEC 60364 (alle Teile), *Low-voltage electrical installation*

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

IEC 60964, *Design for control rooms of nuclear power plants*

IEC 61000 (alle Teile), *Electromagnetic compatibility (EMC)*

IEC 61000-6-5, *Electromagnetic compatibility (EMC) – Part 6-5: Generic standards – Immunity for power station and substation environments*

IEC 61226, *Nuclear power plants – Instrumentation, control and electrical systems important to safety – Categorization of functions and classification of systems*

IEC 61508, *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related 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 62096, *Nuclear power plants – Instrumentation and control – Guidance for the decision on modernisation*

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

IEC 62808, *Nuclear power plants – I&C systems important to safety – Design and qualification of isolation devices*

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

IAEA SSG-30, *Safety Classification of Structures, Systems and Components in Nuclear Power Plants*

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

IAEA SSG-39, *Design of Instrumentation and Control Systems for Nuclear Power Plants, (Under Revision Draft Safety Guide DS431 (Supersedes NS-G-1.1 and NS-G-1.3))*

ANMERKUNG Eine Norm, ähnlich der IEC 61513, wird erst noch für elektrische Systeme erstellt: Kernkraftwerke – Sicherheitstechnisch wichtige elektrische Systeme – Allgemeine Anforderungen für Systeme. Nach ihrer Fertigstellung ist diese Norm ebenfalls zu berücksichtigen.

3 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

3.1

„verbundener Schaltkreis“

(en: associated circuit)

Schaltkreis einer niedrigeren Sicherheitskategorie, der nicht physikalisch oder elektrisch von Schaltkreisen einer höheren Kategorie durch ausreichenden Trennungs-Abstand, Sicherheitsklasse-Baustrukturen, Barrieren oder elektrische Trenneinrichtungen separiert ist, aber ausreichende Sicherheitskriterien einhält

3.2

Barriere

(en: barrier)

Einrichtung oder Struktur, die zwischen sicherheitstechnisch wichtigen redundanten Geräten oder Schaltkreisen oder zwischen sicherheitstechnisch wichtigen Geräten oder Schaltkreisen und einer möglichen Gefahrenquelle angeordnet ist, um im Schadensfall die Beschädigung des sicherheitstechnisch wichtigen leittechnischen Systems auf ein akzeptables Maß zu beschränken

3.3

Kabeltrasse

(en: cable route)

physikalischer Weg durch die Anlage, auf dem mehrere Kabel verlegt werden können, wie durch einen Raum oder Gang in dem Anlagengebäude, oder eine metallische Führung, Pritschen oder Rohre oder eine Über- oder Unterführung von Straßen

3.4

Versagen aufgrund gemeinsamer Ursache

(en: common cause failure – CCF)

Versagen von zwei oder mehr Strukturen, Systemen oder Komponenten infolge eines einzelnen spezifischen Ereignisses oder einer spezifischen Ursache

[QUELLE: IAEA Safety Glossary 2007]

3.5

tief gestaffelter Schutz^{N1)}

(en: defense in depth)

hierarchische Anordnung verschiedener Ebenen unterschiedlichen Geräts oder Prozeduren, um die Ausbreitung betrieblicher Ereignisse zu verhindern und um die Wirksamkeit physikalischer Barrieren zwischen einer Strahlenquelle oder radioaktivem Material und Mitarbeitern, Personen der Öffentlichkeit oder der Umgebung während des Betriebs oder unter Störfallbedingungen zu erhalten

[QUELLE: IAEA Safety Glossary 2007]

3.6

Trennung durch Abstand

(en: distance (separation by))

Montage zu schützender Geräte derart weit voneinander, dass sie durch ein zu berücksichtigendes Ereignis nicht gleichzeitig zerstört werden können

3.7

Diversität

(en: diversity)

Vorhandensein von zwei oder mehreren redundanten Systemen oder Komponenten um die gleiche Funktion mit unterschiedlicher Hardware oder funktionalem Aufbau auszuführen, um die Möglichkeit von Fehlern gemeinsamer Ursache einschließlich Fehlern gleicher Art zu reduzieren

[QUELLE: IAEA Safety Glossary 2007]

3.8

baulich und funktional getrennter Teil

(en: division)

eine bauliche Teilung, dient der Aufnahme einer Teilsumme funktionaler Stränge, die verschiedene Sicherheitsfunktionen ausführen, und dabei sowohl mechanisch als auch elektrisch von anderen Divisionen getrennt sind. Die Trennung zwischen den Divisionen ist entweder räumlich ausgeführt oder durch physikalische Barrieren. Der Begriff Division ist Ausdruck für sicherheitstechnisch wichtige Raumbereiche des Kraftwerks

3.9

Elektromagnetische Verträglichkeit

(en: electromagnetic compatibility – EMC)

Fähigkeit eines Gerätes, einer Komponente, eines Systems oder einer Einrichtung auch in den beabsichtigten, elektromagnetischen, betrieblichen Umgebungsbedingungen wie erforderlich ohne Schwächung oder Fehler zu funktionieren

3.10

elektromagnetische Beeinträchtigung

(en: electromagnetic interference – EMI)

Störung eines elektrischen Schaltkreises durch elektrische Induktion oder Strahlung, die durch externe Quellen emittiert wird

^{N1)} Nationale Fußnote: Allgemeinsprachlich ins Deutsche übersetzt, könnte man von einer tief gestaffelten Verteidigung sprechen. Einer Verteidigung also, die aus mehreren Linien besteht und dadurch sicherstellen soll, dass ein Versagen durch die Hintereinanderschaltung mehrerer Verteidigungslinien verhindert werden soll.

3.11

funktionaler Strang

(en: functional train)

Teilmenge eines Systems, bestehend aus Komponenten, die insgesamt oder in Teilen eine oder mehrere Funktionen eines Systems durchführt. Ein Strang ist redundant zu einem oder mehreren funktionalen Strängen; jeder mit derselben Fähigkeit spezifizierte Funktion(en) auszuführen

3.12

Trennungselement

(en: isolation device)

Einrichtung in einer Schaltung, die verhindert, dass Fehler in einem Abschnitt der Schaltung unzulässige Einflüsse in anderen Abschnitten der Schaltung oder in anderen Schaltungen verursachen

3.13

physikalische Trennung

(en: physical separation)

Trennung durch Geometrie (Abstand, Ausrichtung usw.), durch geeignete Barrieren oder durch Kombinationen daraus

[QUELLE: IAEA Safety Glossary 2007]

3.14

anzunehmendes versagenauslösendes Ereignis

(en: postulated initiating event - PIE)

Ereignis, das während der Auslegung identifiziert wurde, anzunehmende betriebliche Ereignisse oder Störfallbedingungen auslösen zu können

[QUELLE: IAEA Safety Glossary 2007]

3.15

Redundanz

(en: redundancy)

Vorsehen alternativer (identischer oder unterschiedlicher) Strukturen, Systeme oder Komponenten, so dass jede(s) davon die geforderte Funktion unabhängig davon ausführen kann, welchen Betriebszustand oder Ausfall irgendein(e) andere(s) aufweist

[QUELLE: IAEA Safety Glossary 2007]

3.16

Sicherheits-Teilsystem

(en: safety group)

Funktionseinheit bestehend aus Gerät mit der Aufgabe alle erforderliche Maßnahmen für ein bestimmtes anzunehmendes versagenauslösendes Ereignis sicherzustellen, dass die spezifizierten Grenzen für anzunehmende betriebliche Ereignisse und Auslegungstörfälle nicht überschritten werden

[QUELLE: IAEA Safety Glossary 2007]

3.17

Sicherheitssystem

(en: safety system)

Vorsehen alternativer (identischer oder unterschiedlicher) Strukturen, Systeme oder Komponenten, so dass jede(s) davon die geforderte Funktion unabhängig davon ausführen kann, welchen Betriebszustand oder Ausfall irgendein(e) andere(s) aufweist

[QUELLE: IAEA Safety Glossary 2007]

3.18

Separierung

(en: separation)

Satz von Maßnahmen, um den Einfluss einer Funktionseinheit auf eine andere Funktionseinheit zu reduzieren und damit die Unabhängigkeiten der Funktionseinheiten zu verbessern

[QUELLE: IAEA Safety Glossary 2007]

3.19

räumliche Trennung

(en: structural separation)

Anordnung getrennter Komponenten in unterschiedlichen Gebäuden, Räumen oder Anordnung von Trennstrukturen zwischen Komponenten innerhalb desselben Raumes derart, dass sie nicht gleichzeitig durch zu berücksichtigende Gefährdungen zerstört werden können

3.20

Strukturen, Systeme und Komponenten

(en: structures, systems and components – SSC)

allgemeiner Ausdruck, der alle Elemente einer Einrichtung oder Maßnahmen umfasst, die zum Schutz und Sicherheit beitragen, mit Ausnahme menschlicher Einflüsse

[QUELLE: IAEA Safety Glossary 2007]

4 Abkürzungen

AC	Wechselstrom (en: alternating current)
CCF	Fehler gemeinsamer Ursache (en: common cause failure)
DC	Gleichstrom (en: direct current)
DiD	tief gestaffelter Schutz (en: defense in depth)
EMC	Elektromagnetische Verträglichkeit (en: electromagnetic compatibility)
EMI	Elektromagnetische Beeinträchtigung (en: electromagnetic interference)
HEPB	Bruch einer hochenergetischen Leitung (en: high energy pipe break)
HFE	systematische Berücksichtigung menschlicher Handlungen (en: human factor engeneering)
HSI	Mensch-Maschine-Schnittstelle (en: human system interface)
I&C	Leittechnik (en: instrumentation and control)
IAEA	International Atomenergiebehörde (en: International Atomic Energy Agency)
IEC	International Electrotechnical Commission
LV	Niederspannung (Spannungen kleiner/gleich 1000 V) (en: low voltage (≤ 1000 V))
HV	Mittelspannung (en: medium voltage)
NPP	Kernkraftwerk (en: nuclear power plant)
PIE	anzunehmendes versagenauslösendes Ereignis (en: postulated initiating event)
SSC	Strukturen, Systeme und Komponenten (en: structures, systems and components)

5 Fehlerarten

5.1 Auslegungsfehler

Das Fehlerpotential in den Spezifikationen der Anforderungen an sicherheitstechnisch wichtige leittechnische und elektrische Systeme, kann nicht ignoriert werden. Auslegungsfehler dieser Art können zur Ausbreitung von Fehlern zwischen Systemen führen, zum Beispiel ungenügende Isolierung von Kabeln, unpassende Wahl der Größe von Komponenten oder Leitungsquerschnitten, usw. Mittel diese Art von Fehlern zu berücksichtigen, sind grundsätzlich eine konservative Auslegung räumlicher und elektrischer Trennung.

5.2 Leittechnische und elektrotechnische Fehlerereignisse

5.2.1 Allgemeines

Versagensauslösende Ereignisse, die ihren Grund in jedem sicherheitstechnisch wichtigen System haben (können), sind zu berücksichtigen. Diese Ereignisse sind grundsätzlich durch räumlich begrenzte mechanische und elektrische Effekte, die unterschiedliche funktionale Folgen haben können, gekennzeichnet. Einzelne Fehler in Prozesseinheiten und mehrkanaligen Kommunikations-Schnittstellen können das Potential haben, mehrfache Fehler zu erzeugen. Leittechnische und elektrische Fehlerereignisse können wie folgt unterschieden werden.

5.2.2 Einzelner Zufallsfehler

Ein einzelner Zufallsfehler eines leittechnischen oder elektrischen Systems oder einer leittechnischen oder elektrischen Komponente, der zur Fehlfunktion einer Komponente, zu Kurzschlüssen, zur Unterbrechung eines Schaltkreises, zum Erdschluss, zur Änderung der Spannung oder Frequenz, zu einem mechanischen Fehler einer Komponente oder zu einem lokalen Feuer führen kann, ist zu berücksichtigen.

5.2.3 Mehrfache Fehler einer einzelnen gemeinsamen Ursache

Die Ursachen von Fehlern in zwei oder mehreren Komponenten, die aufgrund eines einzelnen gemeinsamen Fehlers, wie zum Beispiel Wartungsfehler, mechanische Zerstörung oder elektrische Beeinflussung, redundante Sicherheits-Funktionseinheiten beeinflussen, sind zu berücksichtigen. Einflüsse der Umgebung, Schädigung durch radioaktive Strahlung und andere potentielle gemeinsame physikalische Faktoren sind ebenfalls zu berücksichtigen.

5.3 Fehlerereignisse im Kraftwerk

5.3.1 Allgemeines

Versagensauslösende Ereignisse, die durch Betriebsbedingungen ausgelöst werden, können zu Ausfällen von leittechnischen und/oder elektrischen Komponenten führen. Solche Ereignisse sind gekennzeichnet durch mittlere bis starke Energiefreisetzung und durch einen Bereich von Folgen für einzelne Räume oder ganze Teile von Gebäuden. Diese Ereignisse können wie folgt unterteilt werden.

5.3.2 Umgebungsbedingungen

Veränderung der Umgebungsbedingungen, wie zum Beispiel Strahlung, Temperatur, Druck, Feuchte während des normalen Betriebs und unter Störfallbedingungen, sind zu berücksichtigen. Feuer oder Rauch, die einen Geräteraum oder eine Kabeltrasse beeinflussen, sind ebenfalls wesentliche Umgebungsbedingungen. Ebenso ist die Fehlauslösung von Feuerlöschsystemen, soweit installiert, zu berücksichtigen.

5.3.3 Elektromagnetische Beeinträchtigung

Leittechnisches und elektrisches Gerät schließt naturgegeben die Erzeugung und die Fortleitung elektromagnetischer Signale ein. Diese Signale können empfänglich sein für ungewollte Veränderungen oder Störungen durch externe Quellen. Technischer Fortschritt in leittechnischen und elektrischen Systemen, insbesondere die Verringerung der Signalspannung der Leittechnikssysteme und der Einsatz von Leistungselektronik, können Systeme noch empfindlicher gegenüber der Beeinflussung der Funktion und gegenüber Schädigung sein. Deshalb ist elektromagnetische Beeinflussung als potentielle Ursache redundanter Leittechnik-Sicherheitssysteme zu betrachten. Räumliche Trennung ist eine Möglichkeit, die Unabhängigkeit leittechnischer und/oder elektrischer Signale zu erhalten und gegen mögliche Fehler gemeinsamer Ursachen durch elektromagnetische Beeinflussung zu schützen.

Die IEC 61000 Normenserie enthält Anleitungen in der Auslegung und für das Testen möglicher Einflüsse durch elektromagnetische Beeinflussung.

5.3.4 Fehler in Kraftwerkssystemen, Geräten oder Strukturen

Versagensauslösende Ereignisse in Kraftwerkssystemen, Gerät oder Strukturen, wie zum Beispiel Feuer, umherfliegende Trümmer, schlagende Rohrleitungen, mechanische und thermische Auswirkungen, Explosion oder Leckagen von Wasser, Dampf oder flüssigem Metall, von Gasen, Öl und andere Ereignisse, die das Potential haben Gerät zu beschädigen, sind zu berücksichtigen.

5.3.5 Bedienungsfehler

Versagensauslösende Ereignisse, die ihren Ursprung in fehlerhafter Bedienung während des normalen Betriebs und besonders unter Störfallbedingungen haben, sind zu berücksichtigen.

5.4 Externe versagensauslösende Ereignisse

5.4.1 Allgemeines

Versagensauslösende Ereignisse, die Ihre Ursache außerhalb des Kraftwerks haben, können Fehler in leittechnischen und elektrischen Komponenten verursachen. Ereignisse dieser Art sind charakterisiert durch eine sehr große Energiefreisetzung und durch Einflüsse auf Teile von Gebäuden oder ganzen Gebäuden. Diese Ereignisse können wie folgt unterschieden werden.

5.4.2 Naturereignisse

Naturereignisse wie Erdbeben, Überschwemmungen, Wirbelstürme, Blitzschlag, Sturmflut oder Tsunami, soweit für den Standort des Kraftwerks zutreffend, sind zu berücksichtigen.

5.4.3 Durch Menschen verursachte Ereignisse

Ereignisse innerhalb oder außerhalb des Kraftwerks, verursacht durch Menschen, wie zum Beispiel Explosionen, Feuer, Flugzeugabsturz, Sabotage sind zu berücksichtigen.

5.5 Spezielle Betriebsbedingungen

Versagensauslösende Ereignisse, die ihre Ursache in speziellen Betriebsbedingungen haben, wie zum Beispiel Inbetriebsetzung, Umbauten, Wartung und Reparatur, Auslegungs- und formale Kontroll-Maßnahmen, sind bei Auslegung und Bau zu berücksichtigen, um ihren möglichen Umfang in einem akzeptablen Rahmen zu halten.

6 Grundsätze (funktionaler und/oder räumlicher) Trennung^{N2)}

6.1 Allgemeines

Leittechnische und elektrotechnische sicherheitstechnisch wichtige Systeme sind erforderlich, um versagensauslösende Ereignisse entsprechend Abschnitt 5 zu beherrschen. Um die Sicherheitsfunktionen des Kraftwerks zu erhalten, ist Redundanz für die gesamte Auslegung des Kraftwerks erforderlich. Redundanz stellt wiederum Unabhängigkeit zwischen Strukturen, Systemen und Komponenten sicher.

Unabhängigkeit ist eine Bedingung, die dann existiert, wenn die erfolgreiche Ausführungen von Funktionen eines Systems, unabhängig ist vom Betriebsverhalten, einschließlich Störungen und normalem Betrieb eines anderen Systems oder infolge von jedwedem Signal, Daten oder Information generiert vom anderen System.

^{N2)} Nationale Fußnote: An dieser Stelle wurde der sehr allgemeine Begriff „Trennung“ zumindest teilweise durch die Einfügung der Worte „funktional“ und „räumlich“ präzisiert. Wo erforderlich oder sinnvoll, werden abhängig vom Kontext, jeweils zutreffendere Benennungen wie „Trenneinrichtung“, „Entkopplungseinrichtung“, „Vorrangbildung“ usw. verwendet.

Mittel, um Unabhängigkeit zu erreichen oder zu unterstützen, sind tief gestaffelter Schutz, Diversität und räumliche Trennung. Kombinationen dieser Maßnahmen werden genutzt, die Ziele der Unabhängigkeit zu erreichen (IAEA SSG-39; 6.27). Dieser Abschnitt zeigt die wesentlichen Grundsätze der Trennung, einschließlich der dazu erforderlichen allgemeinen Maßnahmen.

Entsprechend der IAEA SSR 2/1, Anforderung 21, sind Wechselwirkungen zwischen Sicherheitssystemen oder zwischen redundanten Teilen eines Sicherheitssystems, durch Trennungsmaßnahmen zu vermeiden, wie zum Beispiel:

- Räumliche Trennung;
- Elektrische Trennung;
- Funktionale Unabhängigkeit;
- Unabhängigkeit von Kommunikationseinrichtungen.

Zur Trennung sind verschiedene Maßnahmen je nach Erfordernis anzuwenden.

Während der Auslegung der Leit- und der Elektrotechniksysteme, sind die Bedingungen zur Auslegung eines Kernkraftwerks, entsprechend IEC 61513, 5.2.4, zu berücksichtigen. In Abhängigkeit der Ergebnisse, sind geeignete Auslegungsmaßnahmen zu spezifizieren.

Abhängigkeiten zwischen leittechnischen und elektrischen Systemen kann es an bestehenden physikalischen Schnittstellen geben (wie zum Beispiel Stromversorgung, Signalaustausch): die konstruktive Auslegung innerhalb eines Raumes oder zwischen Gebäuden, Hilfssystemen (z. B. Klima, Lüftung) oder durch die Ausbreitung von Fehlern (wie Feuer, Flugzeugabsturz).

Die Notwendigkeit für Schnittstellen ergibt sich aus der gewählten Auslegung des Kraftwerks (zum Beispiel gemeinsame Nutzung von Gebern oder Antrieben) und/oder durch Anforderungen an die Beherrschung menschlicher Handlungen. Der Austausch von Informationen betrifft Mensch-Maschine-Schnittstellen, zum Beispiel Alarmer, Steuerungen, Informationen auf Anzeigen usw., um die Sicherheit des Kraftwerks zu erhöhen, die Verfügbarkeit, Leistung und Effektivität und der Einsatz neuer Technologien wegen ihres potentiellen Nutzens führt zu mehr Verbindungen in den Systemen, wodurch die Trennung komplizierter wird. Die Anforderung Strukturen, Systeme und Komponenten strikter zu trennen, kann Anforderungen an Mensch-Maschine-Schnittstellen widersprechen. Um beide Anforderungen in einem ausgewogenen Verhältnis zu halten, ist das Thema im Rahmen der Auslegung der Anlage zu spezifizieren.

In Abhängigkeit von den Trennungseinrichtungen, werden in diesem Abschnitt zu berücksichtigende Maßnahmen in der Auslegung von elektrischen und leittechnischen Systemen in allgemeiner Weise angesprochen.

Nachweis und Wertung der getroffenen Trennungsmaßnahmen sollen abschließend belegen, dass die Auslegung den Anforderungen entspricht.

6.2 Anforderungen an die Unabhängigkeit

Die allgemeinen Grundsätze für Trennungen sind im Wesentlichen beeinflusst durch die allgemeinen Sicherheitsgrundsätze des Kraftwerks:

- Unabhängigkeits-Anforderungen;
- Gefahren-Analysen und entsprechende Regeln für Schutzmaßnahmen;
- Deterministische Sicherheitsregeln;
- Brandanalyse und Brandschutz-Regeln.

Grundsätzlich sind Strukturen, Systeme und Komponenten entsprechend ihrer Sicherheitsklassifizierung getrennt.

Dennoch kann nicht ausgeschlossen werden, dass nationale kerntechnische Normen eine Trennung zwischen tief gestaffelten Ebenen verlangen, ein solches Vorgehen entspricht nicht genau den Anforderungen der Sicherheits-Klassifizierung.

Entsprechend können die allgemeinen Trennungsanforderungen an Sicherheitsklassen, die in dieser Norm formuliert sind, auch bei tief gestaffelten Ebenen angewendet werden.

IEC 61226 definiert wie Sicherheitsfunktionen entsprechend ihrer Bedeutung für die Sicherheit zu kategorisieren und physikalisch zu trennen sind, um einen Schutz vor der Ausbreitung von Fehlern durch physikalische Effekte sicherzustellen und um damit auch eine gleichzeitige Gefährdung redundanter Systeme zu verhindern.

Ein leittechnisches oder elektrisches System kann Funktionen von mehr als einer Kategorie ausführen. In solch einem Fall, ist die Kategorie des Systems der höchsten Funktions-Kategorie zuzuordnen, die vom System ausgeführt wird. Zum Beispiel, ein System, das Kategorie A- und Kategorie B-Funktionen ausführt, ist als Kategorie A-System zu definieren.

Des Weiteren enthält IEC 61226 Hinweise darauf, welche entsprechenden sicherheitstechnisch wichtigen System- und Komponenten-Klassen den Kategorien der Funktionen zuzuordnen sind.

In anderen anzuwendenden Normen zur Kategorisierung von Funktionen oder der Klassifizierung von Strukturen, Systemen und Komponenten, sollte grundsätzlich in gleicher Weise vorgegangen werden.

Als Auslegungsbasis für sicherheitstechnisch wichtige leittechnische und elektrische Systeme sind folgende allgemeine Prinzipien anzuwenden, um die Unabhängigkeit redundanter Systeme und zwischen unterschiedlichen Systemen aufrecht zu halten und sicherzustellen, dass Redundanz und Diversität (die für das Erreichen hoher Zuverlässigkeit sicherheitstechnisch wichtiger Systeme eingesetzt wird) wirksam sind. Die Gruppierungs- und die Trennungskriterien zwischen den unterschiedlichen Sicherheitsklassen sind zu Beginn des Projektes zu definieren.

- Systeme der Sicherheitsklasse 1, müssen vor Folgen physikalischer Effekte, verursacht durch Fehler und übliche Handlungen, geschützt werden, die auftreten können innerhalb von
 - a) redundanten Teilen solcher Systeme; und
 - b) Systemen einer niedrigeren Sicherheitsklasse.

Die in Betracht gezogenen Fehler müssen sowohl die innerhalb eines leittechnischen oder elektrischen Systems umfassen, als auch solche, die als Ergebnis von Ereignissen außerhalb des leittechnischen oder elektrischen Systems auftreten.

In manchen Fällen kann es erforderlich sein, eine physikalische Trennung zwischen unterschiedlichen Systemen der Sicherheitsklasse 1 vorzusehen, wenn Unabhängigkeit gefordert ist.

- Systeme der Sicherheitsklasse 2, vor Folgen physikalischer Effekte, verursacht durch Fehler und übliche Handlungen, geschützt werden, die auftreten können innerhalb von
 - a) redundanten Teilen solcher Systeme; und
 - b) Systemen einer niedrigeren Sicherheitsklasse.

Die in Betracht gezogenen Fehler müssen Fehler innerhalb des leittechnischen oder elektrischen Systems umfassen, dürfen aber Fehler als Folge von Ereignissen außerhalb der leittechnischen oder elektrischen Systeme ausschließen. Wenn Funktionen der Sicherheitsklasse 2 als Schutz für bestimmte versagensauslösende Ereignisse vorzusehen sind, müssen diese Systeme nach den Prinzipien der Sicherheitsklasse 1 ausgelegt sein. Zum Beispiel sind in einigen Ländern alle Systeme, die erforderlich sind eine sichere Langzeit-Abschaltung zu erreichen und langfristig sicherzustellen, gegen Feuer zu schützen, unabhängig von ihrer Sicherheitsklasse.

- Für einige Systeme der Sicherheitsklasse 3 kann es erforderlich sein, sie gegen Einflüsse von Fehlern in anderen Systemen zu schützen. Ob dies erforderlich ist, muss von Fall zu Fall entschieden werden.
- Nicht klassifizierte Systeme brauchen nicht gegen Einflüsse von Fehlern in anderen Systemen geschützt zu werden.

6.3 Grundsätze

Trennung verhindert

- a) Ausfallfortpflanzung von System zu System,

- b) Ausfallfortpflanzung zwischen redundanten Teilen innerhalb eines Systems,
- c) Ausfälle gemeinsamer Ursache infolge interner und einiger externer versagensauslösenden Ereignisse.

Wo physikalische Trennung verlangt wird, müssen Vorkehrungen gegen eine Ausfallfortpflanzung von Fehlern in Betracht gezogen werden, die auftreten können

- gleichzeitig an mehreren System-Komponenten als Folge von versagensauslösenden Ereignissen;
- zwischen Systemen der gleichen Sicherheitsklasse;
- zwischen redundanten Sicherheitsgruppen desselben sicherheitstechnisch wichtigen leittechnischen oder elektrischen Systems und;
- von Systemen mit Funktionen niedrigerer Sicherheitsklasse zu Systemen mit Funktionen höherer Sicherheitsklasse und in einigen speziellen Fällen, von Systemen mit Funktionen höherer Sicherheitsklasse zu Systemen mit Funktionen niedrigerer Sicherheitsklasse;
- entweder von Systemen die zu einem niedrigeren Grad des tief gestaffelten Schutzes gehören, zu Systemen die zu einem höheren Grad des tief gestaffelten Schutzes gehören, falls dies durch die Sicherheitsbestimmungen des Projektes gefordert wird oder durch eine nationale Norm.

Die Arten möglicher versagensauslösender Ereignisse, die in den folgenden Unterabschnitten enthalten sind, sind zu berücksichtigen (zum Beispiel benannt, dokumentiert und begründet). In den sicherheitstechnisch wichtigen leittechnischen und elektrischen Systemen, sind geeignete Maßnahmen vorzusehen, um die möglichen Auswirkungen dieser Ereignisse auf ein akzeptables Maß zu begrenzen. Auch die Folgen von Kombinationen versagensauslösender Ereignisse sollten berücksichtigt werden.

Die Grundsätze trennender Maßnahmen und die gewählten Mittel, die Trennung zu erreichen, sind in einem geeigneten Dokument für das Projekt zu beschreiben. In einem weiteren Schritt ist zu begründen, dass die Trennungsregeln eingehalten wurden.

6.4 Räumliche Trennung

6.4.1 Allgemeines

Die Konstruktion eines Kernkraftwerks besteht aus mehreren Verteidigungslinien, um externen Gefahren zu widerstehen, wie zum Beispiel Flugzeugabsturz, Wirbelstürme, Erdbeben oder Überflutung. Diese baulichen Verteidigungslinien bilden die Voraussetzung für leittechnische und elektrische Systeme, Betriebs- und Störfallbedingungen zu beherrschen.

Für die Auslegung der Strukturen der Leittechnik- und der Elektrotechniksysteme, ist die Auswirkung interner Gefahren durch räumliche Trennung in verschiedene Raumbereiche in Kombination mit elektrischer Trennung zu berücksichtigen.

Entsprechend dem IAEA Sicherheitsglossar, ist physikalische Trennung definiert als: „Trennung durch Geometrie (Abstand, Ausrichtung etc.), durch geeignete Barrieren oder einer Kombination daraus.“ Des Weiteren ist eine Barriere definiert als „Ein physikalisches Hindernis, das die Fortbewegung von Personen, Radionukliden oder irgendwelchen anderen Phänomenen (zum Beispiel Feuer) vermeidet oder verhindert oder das radioaktive Strahlung abschirmt.“

Räumliche Trennung kann erreicht werden durch Abstand, durch bauliche Trennung oder durch eine Kombination aus beidem. Sie ist eine Maßnahme, um die Wahrscheinlichkeit abhängiger Fehler (Fehler gemeinsamer Ursache) als Ergebnis von Fehlern in Folge von Auslegungsstörfällen (wie zum Beispiel Feuer, Flugkörper, Überflutung oder das Bersten hochenergetischer Rohrleitungen) zu reduzieren.

Die Wahl hängt von den Auslegungsstörfällen ab und kann von Ort zu Ort innerhalb des Kernkraftwerks unterschiedlich sein. Sie wird von den Auslegungsstörfällen, die in der Phase der Auslegung des Kraftwerks berücksichtigt wurden und für die entsprechende Schutzvorrichtungen vorgesehen sind, abhängen.

Physikalische Trennung ist eine Maßnahme zur Beherrschung mechanischer und umgebungsbedingter Auswirkungen.

6.4.2 Trennung durch Abstand

Physikalische Trennung verlangt nicht ausdrücklich strukturelle Barrieren zwischen zwei Komponenten, um zugrundeliegende Auslegungsstörfälle zu beherrschen (zum Beispiel Flugzeugabsturz).

Die Maßnahme Abstand, ist der Raum in dem keine dazwischen liegende Strukturen, Gerät oder Materialien vorhanden sind, die die Ausbreitung von Auswirkungen, verursacht durch Gefahren (zum Beispiel Feuer, Flugzeugabsturz etc.), unterstützen könnten oder die auf andere Weise die Funktion der Leittechnik oder Elektrotechnik verhindern könnten.

6.4.3 Trennung durch bauliche Maßnahmen

Im Zusammenhang mit Leittechnik und Elektrotechnik, ist eine strukturelle Barriere eine physikalische Trennung zweier unabhängiger Bereiche durch bauliche Maßnahmen. Diese Maßnahmen sollen die Ausbreitung von Auslegungsstörfällen und interne Gefährdungen verhindern. In Abhängigkeit des jeweiligen Auslegungsstörfalles, kann eine bauliche Barriere eine Wand als Brandschutz sein oder eine zu diesem Zweck vorgesehene Abschirmung, um gegen Auswirkungen, verursacht durch Störfälle, zu schützen.

6.5 Elektrische Trennung

6.5.1 Allgemeines

Die elektrische Trennung ist in IAEA SSG-34 und IAEA SSG-39 beschrieben.

Elektrische Trennung wird genutzt, um elektrische Fehler in einem System daran zu hindern, angeschlossene Systeme zu beeinflussen. Elektrische Trennung beherrscht oder verhindert nachteilige Wechselwirkungen zwischen Gerät und Komponenten, verursacht durch Faktoren wie elektromagnetische Interferenz, elektrostatische Übertragung, Kurzschlüsse, offene Schaltkreise, Erdschlüsse oder den Einfluss einer maximal möglichen elektrischen Spannung (Wechsel- oder Gleichstrom).

Das leittechnische oder elektrische System ist entweder zu schützen oder der Einfluss fehlerhaften Eintrags systemeigener/em oder fremder/dem Spannung oder Stroms muss zugelassen werden können (**Überspannungsschutz, Kurzschluss- / Überstromschutz**), um die Eigenständigkeit von Signalvervielfachung und von Signaltransfer sicherzustellen (**elektrisch rückwirkungsfrei, elektrische Isolation**). Die Maßnahmen der elektrischen Trennung (Entkopplungskonzept) setzen sich aus einer Auswahl / Kombination entsprechend Bild 1 zusammen.

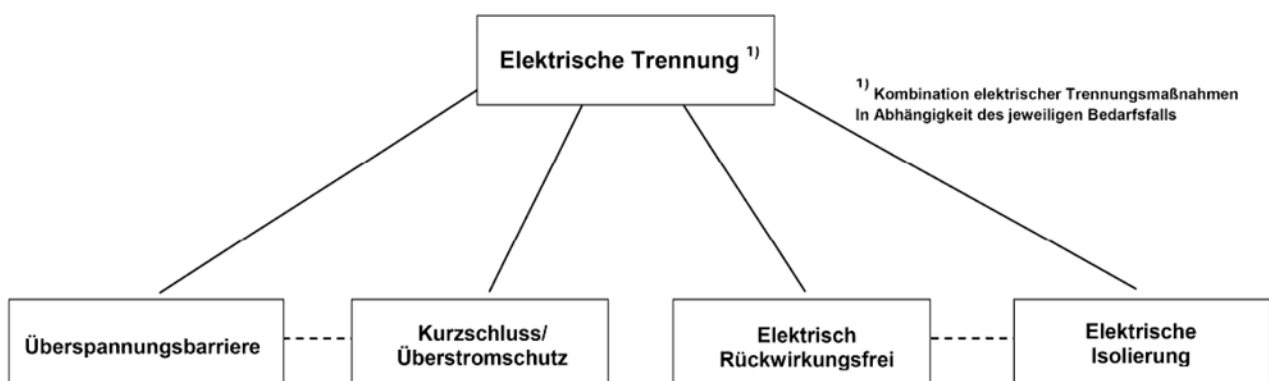


Bild 1 – Maßnahmen elektrischer Trennung und Wahl der Komponenten

In Abhängigkeit des geforderten Anwendungsfalls, ist die Kombination der Maßnahmen in der Auslegung zu spezifizieren. Das Fehlen einer einzigen Maßnahme kann dazu führen, dass die komplette elektrische Trennung unwirksam ist.

6.5.2 Allgemeines

Eine Überspannungsbarriere trennt entweder oder sie verhindert die Ausbreitung einer Überspannungs- oder Stromtransiente in einer gegebenen Richtung (abhängig vom Anwendungsfall). Überspannung, ist das Vorhandensein einer Spannung (Gleich- oder Wechselspannung) aus einer niederohmigen Quelle, die die Auslegungsnennspannung zwischen einem Teil der Schaltung und jedem anderen elektrischen Teil, einschließlich Erde, übersteigt.

Die Einspeisung einer Überspannung in ein System ist grundsätzlich zu berücksichtigen, sofern sie eine aus physikalischer Sicht realistische Fehlermöglichkeit ist.

Fremdspannung ist durch die Installation zugeordneter Trenneinrichtungen auf ein für das zu schützende System ungefährliches Niveau zu begrenzen. Abhängig vom Anwendungsfall, ist eine Kombination elektrischer Einrichtungen zu bestimmen, um die Komponenten gegen die zu unterstellenden maximalen Spannungstransienten und Belastungszeiten zu schützen.

Das elektrische System ist grundsätzlich durch verschiedene Ebenen zum Schutz gegen Überspannung geschützt. Die erste Ebene zum Schutz gegen Überspannung, ist in den Anschlusspunkten zum externen Netz und zu internen Energiequellen, wie Hauptgenerator und Notstromgeneratoren, installiert. Eine zweite Ebene zum Schutz gegen Überspannung, ist grundsätzlich in den Mittelspannungsschaltanlagen und den Komponenten der Unterbrechungslosen Stromversorgung, wie Gleich- und Wechselrichter, installiert. Eine dritte Ebene zum Schutz gegen Überspannung, ist in vielen Fällen auf der elektrischen Seite der Stromversorgung von Leittechnikschränken installiert.

Maßnahmen zur Bildung einer Überspannungsbarriere können die geplante Zerstörung eines kompletten, begrenzten Teils von Leittechnikkomponenten sein. Eine physikalische Zerstörung könnte ausgelöst werden durch Schmelzen, Brennen oder Platzen von Komponenten. Die Wirkungen der ausgelösten Überspannungsbarriere auf weitere Komponenten der Signalkette, ist in der Auslegung des leittechnischen und elektrischen Systems durch physikalische Trennung zu berücksichtigen (siehe 6.4).

6.5.3 Kurzschluss-/Überstromschutz

Zum Schutz vor Kurzschlüssen werden Geräte wie Sicherungen oder Leistungsschalter genutzt, um die Stromzufuhr zur Fehlerstelle zu unterbrechen. Überstrom wird durch geeignete Geräte, soweit sie installiert sind, detektiert und unterbrochen durch Geräte wie Schütze oder Leistungsschalter.

Die Schutzgeräte in der Notstromversorgung sind grundsätzlich so ausgelegt, dass Defekte oder Fehler zuverlässig erkannt werden, dass erforderliche Abschaltungen ausgeführt werden und dass fehlerhafte Auslösungen durch betriebliche Transienten vermieden werden. Betriebliche Ereignisse, wie Anlaufstromspitzen oder wiederholte Starts von Motoren, dürfen keine Schutzeinrichtungen auslösen. Grundsätzlich sind Überstrom-Schutzfunktionen so auszuwählen und so einzustellen, dass der kleinste Kurzschlussstrom noch erfasst wird, jedoch keine Auslösung durch betriebliche Stromtransienten zur Abschaltung führt.

6.5.4 Elektrische Rückwirkungsfreiheit

Elektrische Rückwirkung ist ein Effekt, bei dem ein Signalausgang durch einen Fehler im zu speisenden Signaleingang das Ausgangssignal verfälscht. Rückwirkungsfrei ist eine Eigenschaft einer Schnittstelle, die sicherstellt, dass Fehler im Zielsystem die Signalquelle nicht negativ beeinflusst.

Für einen rückwirkungsfreien Signalaustausch (oder Signalvervielfachung) kann der Ausgang einer rückwirkungsfreien Komponente durch ein Signal hoher Spannung oder niedriger Spannung beaufschlagt werden, ohne dass die Signalquelle negativ beeinflusst wird. Ein solcher Signalwert darf keine negative Auswirkung (rückwirkungsfrei) auf das Eingangssignal der elektrischen Entkopplungskomponente haben.

6.5.5 Galvanische Trennung (elektrische Isolation)

Zusätzlich zur rückwirkungsfreien Signalübertragung, müssen hochohmige Isolationsbauteile den Signalaustausch zwischen separaten Leittechniksystemen schützen (einschließlich Schnittstellen zwischen verschiedenen Leittechniksystemen).

Elektrische Isolierung ist das Prinzip, Stromfluss zwischen elektrischen Stromkreisen zu verhindern auch wenn Strom oder Signale ausgetauscht werden. Elektrische Isolierung ist erforderlich, wenn Informationen zwischen Leittechniksystemen zugehörig zu

- unterschiedlichen Systemspannungsebenen (zum Beispiel 110 V Wechselspannung ↔ 24 V Gleichspannung);
- verschiedenen Erdschleifen;
- unterschiedlichen Räumen (Gebäudeteile), wenn elektrische Schnittstellen vermieden werden sollen;
- langen Kabelwegen (abhängig vom Spannungsabfall über der Länge des Kabels)

ausgetauscht werden.

Die Eigenschaften der gewählten elektrischen Trennungsmaßnahmen sind bei der Auslegung der leittechnischen und elektrischen Systemstruktur zu berücksichtigen. Eine elektrische Schnittstelle kann rückwirkungs-frei sein und kann gegen Überspannung auf der Leittechnikseite schützen.

Auf der Seite der Elektrotechnik ist eine induktive Trennung mittels Transformator grundsätzlich eine galvanische Trennung. Eine galvanische Trennung auf Seiten der Elektrotechnik, ist jedoch allgemein kein ausreichender Schutz gegen Überspannung.

6.6 Funktionale Unabhängigkeit

Zwei Funktionen, Systeme oder Komponenten sind funktional unabhängig, wenn sie keine Informationen austauschen müssen um ihre Funktion ausführen zu können. Funktionale Unabhängigkeit kann beidseitig sein, wenn keinen Informationen ausgetauscht werden oder einseitig, wenn ein einseitig gerichteter Informationsaustausch erlaubt ist.

Die Ausführung von Sicherheits- und Betriebsfunktionen durch elektrische und leittechnische Systeme, kann unterbrochen werden durch:

- Entkopplung von Sicherheits- und Betriebsfunktionen (zum Beispiel weil sie zu unterschiedlichen Schutzebenen gehören);
- fehlerhafte Hilfssysteme (mit direktem oder verzögertem Auswirkung auf die Systemfunktion);
- Verriegelung automatischer Sicherheitsauslösung (zum Beispiel, um die Weiterentwicklung zu einem noch ernsteren Kraftwerkszustand zu verhindern);
- Beeinflussung durch Wartungsmaßnahmen (zum Beispiel durch Erhaltungsmaßnahmen und Wiederkehrende Prüfungen).

Entsprechend IAEA SSG-39, „6.46. Funktionelle Unabhängigkeit wird unterstützt durch bauliche Auslegung und sorgfältige Behandlung von Daten, die zwischen Funktionen geteilt werden (...).“

Maßnahmen betreffend funktionale Unabhängigkeit sind als Eingangsdaten für Trennungsmaßnahmen zu verwenden.

Für elektrische Systeme könnte dies die Einschaltung einer Stromversorgung sein, ohne Auswirkung auf andere Stromversorgungssysteme.

ANMERKUNG Die Anforderungen bezüglich funktionaler Diversität ist eine weitere Methode Unabhängigkeit zwischen Betriebs- und Sicherheitsfunktionen sicherzustellen. Eine Maßnahme zur Trennung ist dies jedoch nicht.

6.7 Unabhängigkeit der Kommunikation

Das Ziel einer Kommunikation ist es, Information von System A nach System B zu übertragen oder umgekehrt. Die Methoden der Kommunikation in Kernkraftwerken erfordern eine physikalische Verbindung durch die Information, basierend auf elektrischen Werten (binär / analog), verbreitet wird oder auf Basis von Datenprotokollen (nicht jedoch drahtlos).

Für jede Art der Kommunikation sollte berücksichtigt werden, dass entweder der Sender oder der Empfänger sein Gegenüber beeinflussen oder zerstören kann. Abhängig von der Art der Kommunikations-Methode können unterschiedliche Faktoren die Kommunikation beeinflussen.

Maßnahmen, die die Unabhängigkeit der Datenkommunikation sicherstellen sollen, sind nicht Gegenstand dieser Norm, einschließlich der zu berücksichtigenden Gefährdungen, die durch das IT-Sicherheitskonzept identifiziert werden sollten.

6.8 Verbundene (Schalt-)kreise

Sind Funktionen nach den Anforderungen der IEC 61226 kategorisiert und Systeme entsprechend IAEA-30 klassifiziert, wird es des Öfteren vorkommen, dass ein gegebenes System oder ein Satz von Geräten Funktionen unterschiedlicher Kategorien ausführen. Ebenso können gewisse Funktionen einer niedrigeren Kategorie eine sehr enge Beziehung zu einer Kategorie-A-Funktion haben. Zum Beispiel basiert die Prozessüberwachung auf denselben Messungen wie Sicherheitsfunktionen. Die Anforderungen, die eingangs in diesem Dokument formuliert wurden, zeigen generell, dass Schaltkreise einer niedrigeren Sicherheitsklasse von Schaltkreisen der Sicherheitsklasse 1 getrennt werden sollten. Jedoch, können alternativ Schaltkreise der niedrigeren Sicherheitsklasse als „verbundene Schaltkreise“ bezeichnet werden. Anforderungen an eine entsprechende Trennung sind in diesem Abschnitt beschrieben. Im Folgenden dieser Norm wird eine solche Trennung nur als Trennung oder Verbindung mit der Sicherheitsklasse 1 berücksichtigt. Dieses Prinzip mag in Abhängigkeit des Projekts auch auf andere Klassen angewendet werden.

ANMERKUNG Während Schaltkreise der Sicherheitsklasse 3 oder nicht klassifizierte Schaltkreise mit Schaltkreisen der Sicherheitsklasse 2 prinzipiell verbunden sein können, bringt dies in der Praxis wenig Gewinn, weil die Trennungskriterien zwischen Schaltkreisen dieser Kategorien nur geringfügig sind.

Nicht in Sicherheitsklasse 1 klassifizierte Komponenten und/oder Kabel werden (formal) „verbundene (Schalt-) kreise“ in einem oder mehreren der folgenden Fälle:

- a) elektrische Verbindung mit einer Sicherheitsklasse 1-Stromversorgung, ohne eine Trenneinrichtung;
- b) elektrische Verbindung zu einer verbundenen Stromversorgung eines Klasse 1-Systems, ohne eine Trenneinrichtung;
- c) Nähe zu Sicherheitsklasse 1-Schaltkreisen oder –Gerät, ohne die erforderliche Trennung (Abstand oder Barrieren);
- d) Nähe zu verbundenen (Schalt-) kreisen und Gerät, ohne die erforderliche Trennung (Abstand oder Barrieren)
- e) gemeinsame Nutzung eines Sicherheitsklasse 1- oder verbundenen Signals, ohne eine Trenneinrichtung.

Für die elektrische Stromversorgung niedrig klassifizierter Komponenten, gilt in den folgenden Fällen die Stromversorgungseinheit als „verbunden“ (zum Beispiel die Einheit in der Schaltanlage):

- f) Abhängigkeit zwischen einem niedrig sicherheitsklassifizierten System (zum Beispiel Notbeleuchtung) und höher klassifizierten Systemen (zum Beispiel Notstromversorgungs-System), rechtfertigt die Nutzung der „verbundenen“ Versorgung.
- g) die Stromversorgung niedriger klassifizierter Systeme oder Komponenten von höher klassifizierten Energiequellen aufgrund von Anforderungen an die Energieversorgungs-Systeme, rechtfertigt die Nutzung einer „verbundenen“ Versorgung. Der Einfluss dieser Fälle auf die höher klassifizierten Stromversorgungs-Systeme ist zu analysieren, zum Beispiel betreffend Energiebedarf und elektrischer Transienten.

„Verbundene Systeme“ müssen eine der folgenden Anforderungen erfüllen:

- 1) sie müssen eindeutig als solches oder als Klasse 1 identifizierbar sein und ihre Verlegung hat über den gesamten Verlauf gleich zu bleiben (verfolgbar bis zu dem Sicherheitsklasse 1-System) oder durch in gleicher Weise ausgeführte physikalische Trennung, wie die der Sicherheitsklasse 1-Schaltkreise mit denen sie verbunden sind. Sie sind Gegenstand der gleichen Anforderungen wie die der Sicherheitsklasse 1-Kreise, es sein denn, dass durch eine Analyse oder Test belegt werden kann, dass die Nichterfüllung solcher Anforderungen die Sicherheit der Sicherheitsklasse 1-Kreise auf ein nicht akzeptables Maß reduziert;

- 2) sie müssen die Anforderungen des vorangegangenen Absatzes 1) des Sicherheitsklasse 1-Systems bis zum und einschließlich des Trennungselements erfüllen. Nach dem Trennungselement, ist ein solcher Schaltkreis Nicht-Sicherheitsklasse 1, vorausgesetzt, dass das System nicht nochmals an ein Sicherheitsklasse 1-System anschließt;
- 3) sie sind zu analysieren oder zu testen, um zu belegen, dass die Sicherheit der Sicherheitsklasse 1-Kreise nicht auf ein nicht akzeptables Maß verringert wird.

Verbundene Systeme und Trenneinrichtungen sind ausreichend zu qualifizieren. Diese Qualifikation muss belegen, dass die höher qualifizierten Systeme weiterhin wie erforderlich funktionieren, auch wenn die Verbundenen Systeme oder Trennungseinrichtungen und ihre Kabel Gegenstand von elektrischen Betriebsbedingungen sind, bei denen die höher qualifizierten Kreise korrekt funktionieren sollten. An Stellen, an denen ein verbundener Stromkreis mit einem nicht der Sicherheitsklasse 1 angehörigen Gerät verbunden ist, ist dieses Gerät ebenso wie vorgenannt zu qualifizieren. Verbundene Stromkreise brauchen nicht für die Durchführung ihrer Funktion qualifiziert zu werden, weil ihre Funktion nicht der Kategorie A bzw. nicht der Sicherheitsklasse 1 zugeordnet ist.

Eine umfangreiche Anwendung des „verbundene Systeme“-Konzepts kann zu einer größeren Kombination von Schaltkreisen unterschiedlicher Sicherheitsklassen führen, vorausgesetzt, dass die allgemeinen Grundsätze der physikalischen Trennung eingehalten werden. Zum Beispiel brauchen Kabel unterschiedlicher Sicherheitsklassen innerhalb derselben Sicherheitsgruppe nicht voneinander getrennt zu werden, wenn die Sicherheitsfunktionen höherer Kategorie durch eine redundante Sicherheitsgruppe ausgeführt werden können, die von der Sicherheitsgruppe, die verbundene Systeme enthält, getrennt ist.

Trennungen innerhalb von Schalt- oder Leittechnikschränken sollten nicht erforderlich sein, wenn die Komponenten der niedriger klassifizierten Kreise genauso wie die höher klassifizierten Kreise qualifiziert sind.

6.9 Aspekte der Trennung in bestehenden Kraftwerken

Die physikalische Trennung sicherheitstechnisch wichtiger leittechnischer und elektrischer Systeme in bestehenden Kraftwerken, ist häufig unvollständig weil die Strukturen, Systeme und Komponenten, die ursprünglich nicht sicherheitsklassifiziert waren, höher klassifiziert werden müssen und weil die Normen zur Auslegung geändert wurden. Werden bestehende Kraftwerke aufgerüstet, sollten für den Fall, dass aus praktischen Erwägungen nicht alle Anforderungen dieser Norm erfüllt werden können, die möglichen Folgen gerechtfertigt werden, in dem dieser Nachteil dem Gewinn an Sicherheit durch die Summe der durchgeführt Verbesserungen aufgewogen wird. Die folgenden Rechtfertigungen mögen erlaubt sein:

- die baulichen Strukturen oder der im Kraftwerk verfügbare Raum mag die geforderte Trennung nicht erlauben. Physikalische Zwänge sollten vorm Einbau der verbesserten elektro- und leittechnischen Systeme überprüft werden;
- die wesentlichen Schwächen der ursprünglichen elektrischen und leittechnischen Systeme, sind im Vergleich mit den durch die Modernisierung gegebenen Verbesserungen in Trennungen und Sicherheit zu identifizieren;
- die vorhandene Trennung oder die machbare Verbesserung der Trennung, ist systematisch unter Anerkennung besonderer Verbesserungen oder Alternativen zu den Anforderungen dieser Norm zu bewerten;
- ein alternativer Satz von Trennungsregeln kann unter Würdigung und Rechtfertigung bestehender Bedingungen, bestätigt durch Aufzeichnungen des Kraftwerkbetriebs, etabliert werden;
- im Falle spezieller Situationen im Kraftwerk sind alternative Technologien aufzuzeigen und zu bewerten, zum Beispiel durch den Einsatz von Barrieren, Glasfaserkabel, räumliche Verteilung der Elektro- und der Leittechniksysteme.

Trennungsaspekte sind insbesondere bei der Ausführungsstrategie der Kraftwerksmodernisierung zu beachten. Themen, die zu berücksichtigen sind, beinhalten

- Trennung in Zwischenlösungen, wenn neue Leit- und/oder Elektrotechniksysteme in Teilschritten ausgetauscht werden;
- Bestimmung von Untereinheiten, die ohne die Notwendigkeit von Zwischenschnittstellen getrennt werden können;

- Eignung der bestehenden Trennung für die neue Elektro- oder Leittechniktechnologie (hauptsächlich Empfindlichkeit digitaler Leittechnik gegen elektromagnetische Beeinflussung, Leistungshalbleiter, besondere Anforderungen an die Umgebungstemperatur und Empfindlichkeit gegen radioaktive Strahlung);
- Grenzen der Kabelverlegung und Bewertung der Notwendigkeit spezieller Kabelpritschen, zum Beispiel für Glasfaserkabel, Kabelbusse und Anforderungen an eine entsprechende Trennung durch die Verwendung neuer Technologien.

Anleitung zur Entscheidungsfindung bei Aufrüstung und Modernisierung von Leittechniksystemen können IEC 62096 entnommen werden.

7 Auslegungsgrundlagen der Trennung

7.1 Grundsätze

Unter Berücksichtigung möglicher Fehler, definiert in Abschnitt 5, sind die folgenden Grundregeln bei der Auslegung des Aufbaus und der Struktur von Systemen sicherheitstechnisch wichtiger Elektro- und Leittechnik zu beachten.

7.2 Brandschutz

In der Auslegungsphase des Kernkraftwerks ist, basierend auf Überlegungen zur Reaktorsicherheit, die Analyse eines Brandstörfalls durchzuführen, um sicherzustellen, dass die aus Abschnitt 8 resultierenden Anforderungen zur physikalischen Trennung eingehalten werden.

Feuer- und Rauchdetektoren ausreichender Empfindlichkeit und Alarmmeldungen müssen für unbeaufsichtigte Bereiche, wo Kabel oder Systeme installiert sind, vorgesehen werden.

Redundantes Gerät leittechnischer und elektrischer Systeme muss zuweilen im Einflussbereich von fest installierten Brandschutzsystemen angeordnet werden. In diesen Fällen müssen das leittechnische und elektrische System und seine Geräte sowie das Brandschutzsystem so ausgelegt sein, dass der Betrieb des Brandschutzsystems die Unabhängigkeit redundanter Sicherheitsgruppen nicht beeinträchtigt.

Die Leistungsfähigkeit redundanter Sicherheitsgruppen darf durch Feuer und Rauch, die außerhalb eines sicherheitstechnisch wichtigen leittechnischen und elektrischen Systems entstehen, nicht negativ beeinflusst werden. Dieses muss durch räumliche Trennung, Barrieren oder eine Kombination von beiden sichergestellt werden, wobei folgende Anforderungen einzuhalten sind:

- a) der Raum zwischen redundanten Systemen oder Kabeln muss ausreichend sein und darf keine Strukturen, Geräte oder Materialien enthalten, die eine Ausbreitung des Feuers unterstützen könnten;
- b) wenn zwischen redundanten Systemen oder Kabeln Barrieren angeordnet sind, müssen diese eine Feuerfestigkeit entsprechend den Brandschutzbestimmungen haben.

7.3 Umgebungsbedingungen während und nach Störfällen

Das Gerät leittechnischer und elektrischer Systeme muss so ausgelegt, spezifiziert, qualifiziert und installiert sein, dass seine funktionale Fähigkeit während und nach den zu erwartenden Umgebungsbedingungen infolge von Ereignissen nach 5.4 und 5.5 sichergestellt ist.