

	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 27.120.20 Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Physikalische und elektrische Trennung (IEC 60709:2004) Nuclear power plants – Instrumentation and control systems important to safety – Separation (IEC 60709:2004) Centrales nucléaires de puissance – Systèmes d'instrumentation et de contrôle commande importants pour la sûreté – Séparation (CEI 60709:2004) Gesamtumfang 22 Seiten DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE		

Beginn der Gültigkeit

Diese Norm gilt ab 2006-05-01.

Nationales Vorwort

Vorausgegangener Norm-Entwurf: E DIN IEC 60709 (VDE 0491-7):2005-10.

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

Die enthaltene IEC-Publikation wurde vom SC 45A „Instrumentation and control of nuclear facilities“ erarbeitet. Die Internationale Norm wurde vom SC 45A „Instrumentation and control of nuclear facilities“ der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet und veröffentlicht. Diese Norm, deren Anwendung international empfohlen wird, gibt das höchstmögliche Maß internationaler Übereinstimmung für das behandelte Sachgebiet wieder. Die Auslegung kerntechnischer Anlagen in Deutschland wird wesentlich durch die Strahlenschutzverordnung, die BMI-Kriterien, die KTA-Regeln und die RSK-Leitlinien bestimmt.

Hinweise zur Anwendung der IEC-Publikation werden in Nationalen Fußnoten gegeben. Bei Fragen der Interpretation von Aussagen wird empfohlen, ergänzend auf die zugrunde liegende, in englischer und französischer Sprache erschienene IEC-Publikation zurückzugreifen.

Die Überarbeitung der ersten Ausgabe der IEC 60709 von 1981 erfolgte zu folgenden Zwecken:

- Anpassung an die in den aktuellen ISO/IEC-Direktiven festgelegte Gliederung;
- Ergänzung, um alle sicherheitstechnisch wichtigen Systeme sowie die Trennung zwischen und innerhalb von Systemen der Kategorien A, B, C sowie nicht klassifiziert abzudecken;
- Berücksichtigung der Neuauflagen von IAEA-Dokumenten (Ersatz für die IAEA Safety Guides D3 und D8) sowie Erweiterung des Anwendungsbereichs, um weitere Aspekte der Unabhängigkeit einzuschließen;
- Aufnahme von Verweisen auf relevante Normen;
- Berücksichtigung neuer Technik, die entweder einheitliche Trennungslösungen oder neue Möglichkeiten der Sicherstellung der Unabhängigkeit bietet;
- Aufnahme von Anforderungen aus IEC 60639 (die zurückgezogen werden wird), soweit diese in IEC 61513 nicht ausreichend abgedeckt oder zusätzliche Anforderungen erforderlich sind, z. B. Trennung, Zusammenwirken von Betriebs- und Schutzsystemen;
- Erweiterung des Begriffs der „Elektromagnetischen Beeinflussung“ als eine Ausfall-/Versagensursache mit CCF-Potenzial sowie der Anwendung räumlicher Trennung als Maßnahme zur Reduzierung des Risikos von Beeinflussungen;
- Verschärfung der Anforderungen und Empfehlungen für Bereiche mit Bündelung/Häufung von Kabeln, z. B. Warten, Kabeltrassen;
- Einführung des Begriffs der „Assoziierten Schaltung“ (aus der Praxis in USA) zur Behandlung nicht sicherheitsrelevanter Kabel und Leitungen, die nicht von sicherheitsrelevanten Kabeln oder Leitungen getrennt sind;
- Aufnahme der Empfehlung zur Anwendung von Brand-Qualifizierungsnormen (wie die Normen der Reihe IEC 60332) für sicherheitswichtige Kabel. Dieses schließt Folgendes ein:
 - Barrieren als Alternative zur räumlichen Trennung,
 - Verwendung der Kabel selbst als mögliche Barrieren,
 - ähnliche Konzepte wie die Verwendung von Glasfaserkabeln zum Schutz vor elektromagnetischer Beeinflussung, Bewehrung als Schutz vor physikalischer Beschädigung usw.
- Ansprechen der Folgerungen aus dem Einsatz von Schaltkreisen mit niedrigen Energien, wie die Möglichkeit der Verringerung der Mindestabstände auf Grundlage einer erfolgten Analyse;

- Überprüfung der bestehenden Anforderungen, Aktualisierung der Begriffe und Definitionen;
- Aufnahme einer Empfehlung zur Anwendung der Norm auf bestehende Anlagen.

Das IEC-Komitee hat entschieden, dass der Inhalt dieser Publikation bis zu dem auf der IEC-Website unter „<http://webstore.iec.ch>“ mit den Daten zu dieser Publikation angegebenen Datum (maintenance result date) unverändert bleiben soll. Zu diesem Zeitpunkt wird entsprechend der Entscheidung des Komitees die Publikation

- bestätigt,
- zurückgezogen,
- durch eine Folgeausgabe ersetzt oder
- geändert.

In der Reihe VDE 0491 sind als Normen erschienen:

- **DIN IEC 61226 (VDE 0491-1):2005-09**, *Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Kategorisierung leittechnischer Funktionen (IEC 61226:2005)*.
- **DIN IEC 61513 (VDE 0491-2):2002-10**, *Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Allgemeine Systemanforderungen (IEC 61513:2001)*.
- **DIN IEC 61513/A100 (VDE 0491-2/A100):2005-02**, *Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Allgemeine Systemanforderungen – Nationaler Anhang ND (informativ): Mitgeltende Festlegungen aus anderen IEC-Normen*.
- **DIN IEC 60880-2 (VDE 0491-3-2):2001-12**, *Kernkraftwerke – Software für Rechner mit sicherheitstechnischer Bedeutung – Teil 2: Vorkehrungen gegen Versagen aufgrund von Softwarefehlern, Verwendung von Software-Werkzeugen und von vorgefertigter Software (IEC 60880-2:2000)*.
- **DIN IEC 62138 (VDE 0491-3-3):2004-09**, *Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Softwareaspekte für rechnerbasierte Systeme zur Realisierung von Funktionen der Kategorien B oder C (IEC 62138:2004)*.
- **DIN IEC 62117 (VDE 0491-4):2001-10**, *Kernkraftwerke – Druckwasserreaktoren – Überwachung ausreichender Kühlung des Kerns im abgeschalteten Zustand des Reaktors (IEC 62117:1999)*.
- **DIN IEC 61839 (VDE 0491-5):2002-09**, *Kernkraftwerke – Auslegung von Warten – Analyse und Zuordnung der Funktionen (IEC 61839:2000)*.
- **DIN IEC 62241 (VDE 0491-5-2):2006-05**, *Kernkraftwerke – Hauptwarte – Funktionen zur Meldung und Anzeige von Störungen (IEC 62241:2004)*.
- **DIN IEC 60709 (VDE 0491-7):2006-05** *Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Physikalische und elektrische Trennung (IEC 60709:2004)*.

Als Norm-Entwürfe liegen vor:

- E DIN IEC 60880 (VDE 0491-3-2):2004-07, *Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Softwareaspekte für rechnerbasierte Systeme zur Realisierung von Funktionen der Kategorie A (IEC 45A/523/CD:2003)*.
- E DIN IEC 60568 (VDE 0491-6):2003-11, *Kernkraftwerke – Kern-Instrumentierung zur Messung der Neutronenflussdichte (IEC 45A/480/CD:2003)*.
- E DIN IEC 62340 (VDE 0491-10):2006-04, *Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Versagen gemeinsamer Ursache (CCF) (IEC 45A/601/CDV:2005)*.
- E DIN IEC 60674 (VDE 0491-100):2006-05, *Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Sicherstellung der Betriebsbereitschaft (IEC 45A/604/CDV:2005)*.

Nationaler Anhang NA (informativ)

Zusammenhang mit Europäischen und Internationalen Normen

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

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

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

Tabelle NA.1

Europäische Norm	Internationale Norm	Deutsche Norm	Klassifikation im VDE-Vorschriftenwerk
–	Normen der Reihe IEC 60332	Normen der Reihe DIN EN 60332 (VDE 0482-332)	VDE 0482-332
–	IEC 60880:2006	vorgesehen als DIN IEC 60880 (VDE 0491-3-2)	VDE 0491-3-2
–	IEC 60964:1989	–	–
Normen der Reihe EN 61000	Normen der Reihe IEC 61000	Normen der Reihe DIN EN 61000 (VDE 0839)	VDE 0839
–	IEC 61000-6-5:2001	–	–
–	IEC 61226:2005	DIN IEC 61226 (VDE 0491-1):2005-09	VDE 0491-1
EN 61508-1:2001	IEC 61508-1:1998 + Corr. 1:1999	DIN EN 61508-1 (VDE 0803-1):2002-11	VDE 0803-1
EN 61508-2:2001	IEC 61508-2:2000	DIN EN 61508-2 (VDE 0803-2):2002-12	VDE 0803-2
EN 61508-3:2001	IEC 61508-3:1998 + Corr. 1:1999	DIN EN 61508-3 (VDE 0803-3):2002-12	VDE 0803-3
EN 61508-4:2001	IEC 61508-4:1998 + Corr. 1:1999	DIN EN 61508-4 (VDE 0803-4):2002-11	VDE 0803-4
–	IEC 61513:2001	DIN IEC 61513 (VDE 0491-2):2002-10 und DIN IEC 61513/A100 (VDE 0491-2/A100):2005-02	VDE 0491-2 VDE 0491-2/A100
–	IEC 62138:2004	DIN IEC 62138 (VDE 0491-3-3):2004-09	VDE 0491-3-3
–	IEC 62096:2002	–	–
–	IAEA Safety Guide NS-G-1.3:2002	–	–

Nationaler Anhang NB (informativ)

Literaturhinweise

Normen der Reihe DIN EN 60332 (VDE 0482 Teil 332), *Prüfungen an Kabeln, isolierten Leitungen und LWL-Kabeln im Brandfall*.

Normen der Reihe DIN EN 61000 (VDE 0839), *Elektromagnetische Verträglichkeit (EMV)*.

DIN EN 61508-1 (VDE 0803-1):2002-11, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 1: Allgemeine Anforderungen (IEC 61508-1:1998 + Corrigendum 1999); Deutsche Fassung EN 61508-1:2001*.

DIN EN 61508-2 (VDE 0803-2):2002-12, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 2: Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme (IEC 61508-2:2000); Deutsche Fassung EN 61508-2:2001*.

DIN EN 61508-3 (VDE 0803-3):2002-12, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 3: Anforderungen an Software; (IEC 61508-3:1998 + Corrigendum 1999); Deutsche Fassung EN 61508-3:2001*.

DIN EN 61508-4 (VDE 0803-4):2002-11, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 4: Begriffe und Abkürzungen (IEC 61508-4:1998 + Corrigendum 1999); Deutsche Fassung EN 61508-4:2001*.

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

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

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

DIN IEC 62138 (VDE 0491-3-3):2004-09, *Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Softwareaspekte für rechnerbasierte Systeme zur Realisierung von Funktionen der Kategorien B oder C (IEC 62138:2004)*.

Kernkraftwerke

Leittechnische Systeme mit sicherheitstechnischer Bedeutung

Physikalische und elektrische Trennung

Inhalt

	Seite
Einleitung	7
1 Anwendungsbereich	9
2 Normative Verweisungen	9
3 Begriffe	10
4 Allgemeine Trennungsprinzipien innerhalb der sicherheitstechnisch wichtigen Leittechnik.....	11
4.1 Allgemeines	11
4.2 Auslegungsfehler	12
4.3 Versagensauslösende Ereignisse in leittechnischen Systemen	12
4.3.1 Einzelausfall	12
4.3.2 Mehrfachversagen aufgrund einer gemeinsamen Ursache	13
4.4 Versagensauslösende Ereignisse aus der Anlage.....	13
4.4.1 Umgebungsbedingungen	13
4.4.2 Elektromagnetische Beeinflussung	13
4.4.3 Versagen von Anlagensystemen, Geräten und Strukturen.....	13
4.4.4 Bedienungsfehler	13
4.5 Externe versagensauslösende Ereignisse	14
4.5.1 Natürliche Ereignisse	14
4.5.2 Externe menschliche Ursachen.....	14
4.6 Besondere Betriebsbedingungen	14
4.7 Gesichtspunkte der Trennung bei bestehenden Anlagen	14
5 Auslegungsbasis	15
5.1 Brandschutz.....	15
5.2 Umgebungsbedingungen während und nach Störfällen	15
5.3 Isolationseinrichtungen	16
5.3.1 Allgemeines	16
5.3.2 Isolationseigenschaften	16
5.3.3 Vorrangschaltungen	17
5.4 Unabhängigkeit von Regelungssystemen	17
6 Anforderungen für die Trennung von Kabeln	18
6.1 Allgemeine Anforderung	18
6.2 Trennung	18
6.2.1 Trennung von redundanten Kabeln in sicherheitstechnisch wichtigen leittechnischen Systemen ...	18
6.2.2 Kleinere Abstände	19
6.2.3 Assoziierte Schaltungen	19
6.2.4 Trennung von Systemkabeln unterschiedlicher Sicherheitsklassen	20

	Seite
6.2.5 Trennung von Signal- und Energiekabeln und -leitungen.....	20
6.2.6 Trennung von Kabeln und Rohrleitungen	21
6.2.7 Allgemeine Überlegungen zur Kabelführung	21
6.2.8 Schränke, Pulte, Tafeln und zugehörige Kabel in der Warte.....	21
6.3 Thermischer und physikalischer Schutz.....	22
6.4 Brandschutz	22
6.5 Kennzeichnung.....	22

Einleitung

Hintergrund, hauptsächliche Inhalte und Organisation der Norm

Sicherheitstechnisch wichtige leittechnische 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 Systemen gegen solche Auswirkungen zu steigern, einschließlich der Planung unabhängiger Systeme, Teilsysteme und Geräte. Will man sich auf die Unabhängigkeit zwischen derartigen Systemen und Geräten berufen, muss eine geeignete räumliche und elektrische Trennung durchgeführt und aufrechterhalten bleiben. Diese Norm enthält technische Anforderungen und Empfehlungen für die Realisierung der Trennung bei der Auslegung leittechnischer Systeme.

Zweck dieser Norm ist,

- in [Abschnitt 4](#) mögliche Ursachen von Ausfällen zu identifizieren und unter Berücksichtigung dieser Ursachen einen Satz von Anforderungen aufzustellen, die bei der Auslegung eines sicherheitstechnisch wichtigen leittechnischen Systems zu befolgen sind, um eine möglichst gute Erfüllung seiner Aufgaben sicherzustellen. Diese Anforderungen beziehen sich auf das leittechnische System insgesamt. [Abschnitt 4](#) enthält auch Anleitungen zur Trennung, die bei der Modernisierung leittechnischer Systeme in bestehenden Kernkraftwerken zu beachten sind;
- in [Abschnitt 5](#) Kriterien für die Auslegungsgrundlage sicherheitstechnisch wichtiger leittechnischer Systeme festzulegen und damit die in [Abschnitt 4](#) ermittelten Ausfallursachen zu berücksichtigen;
- in [Abschnitt 6](#) Anforderungen aufzustellen, die für die Trennung der Verkabelung innerhalb sicherheitstechnisch wichtiger leittechnischer Systeme einzuhalten sind.

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

Die vorliegende Norm (IEC 60709) ist ein Dokument der zweiten Ebene und wird in [IEC 61513](#) unmittelbar in Bezug auf die physikalische und elektrische Trennung zitiert, die zwischen Teilsystemen von unterschiedlichen Sicherheitssträngen sicherheitstechnisch wichtiger leittechnischer Systeme sowie zwischen sicherheitstechnisch wichtigen und sicherheitstechnisch nicht wichtigen leittechnischen Systemen gefordert wird.

In [IEC 61226](#) sind die Prinzipien der Kategorisierung leittechnischer Funktionen einschließlich der Klassifizierung leittechnischer Systeme und Geräte entsprechend ihrem Sicherheitsniveau dargelegt. Dort wird auch gefordert, dass eine geeignete Trennung zwischen den Funktionen verschiedener Kategorien vorgesehen wird, und die vorliegende Norm bezüglich der Anforderungen an die Trennung zitiert.

Näheres zur Struktur der Normen des IEC/SC 45A ist am Ende dieser Einleitung zu finden.