

	DIN IEC 60671 (VDE 0491-100)	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 – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Prüfungen zur Sicherstellung der Funktionsfähigkeit (IEC 60671:2007) Nuclear power plants – Instrumentation and control systems important to safety – Surveillance testing (IEC 60671:2007) Centrales nucléaires de puissance – Systèmes d'instrumentation et de contrôle-commande importants pour la sûreté – Essais de surveillance (CEI 60671:2007) Gesamtumfang 24 Seiten DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE		

Beginn der Gültigkeit

Diese Norm gilt ab 2007-12-01.

Nationales Vorwort

Vorausgegangener Norm-Entwurf: E DIN IEC 60671 (VDE 0491-100):2006-05.

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. Diese Norm, deren Anwendung international empfohlen wird, gibt das höchstmögliche Maß internationaler Übereinstimmung für das behandelte Sachgebiet wieder. Bei Fragen der Interpretation von Aussagen wird empfohlen, ergänzend auf die zugrunde liegende, in englischer und französischer Sprache erschienene IEC-Publikation zurückzugreifen. Die Auslegung kerntechnischer Anlagen in Deutschland wird wesentlich durch die Strahlenschutzverordnung, die BMI-Kriterien, die KTA-Regeln und die RSK-Leitlinien bestimmt.

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 (VDE 0491-3-2):2007-08**, *Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Softwareaspekte für rechnerbasierte Systeme zur Realisierung von Funktionen der Kategorie A (IEC 60880:2006).*
- **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 60568 (VDE 0491-6):2006-11**, *Kernkraftwerke – Instrumentierung mit sicherheitstechnischer Bedeutung – Kerninstrumentierung zur Messung der Neutronenflussdichte in Leistungsreaktoren (IEC 60568:2006).*
- **DIN IEC 60709 (VDE 0491-7):2006-05**, *Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Physikalische und elektrische Trennung (IEC 60709:2004).*
- **DIN IEC 60671 (VDE 0491-100):2007-12**, *Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Prüfungen zur Sicherstellung der Funktionsfähigkeit (IEC 60671:2007).*

Als Norm-Entwürfe liegen vor:

- E DIN IEC 60987 (VDE 0491-3-1):2006-09, *Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Anforderungen an die Hardware-Auslegung rechnerbasierter Systeme* (IEC 45A/623/CDV:2006).
- E DIN IEC 60964 (VDE 0491-5-1):2007-11, *Kernkraftwerke – Warten – Auslegung* (IEC 45A/652/CDV:2007).
- E **DIN IEC 61227 (VDE 0491-5-3)**:2007-08, *Kernkraftwerke – Warten – Handbedienungen* (IEC 45A/649/CDV:2007).
- E DIN IEC 62340 (VDE 0491-10):2006-04, *Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Versagen gemeinsamer Ursache (CCF)* (IEC 45A/601/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 in Tabelle NA.1 wiedergegeben.

Tabelle NA.1

Europäische Norm	Internationale Norm	Deutsche Norm	Klassifikation im VDE-Vorschriftenwerk
EN 61508-1:2001	IEC 61508-1:1998 + Corr.: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.:1999	DIN EN 61508-3 (VDE 0803-3):2002-12	VDE 0803-3
EN 61508-4:2001	IEC 61508-4:1998 + Corr.:1999	DIN EN 61508-4 (VDE 0803-4):2002-11	VDE 0803-4
–	IEC 60880:2006	DIN IEC 60880 (VDE 0491-3-2):2007-08	VDE 0491-3-2
–	IEC 60987 in Überarbeitung	DIN IEC 60987 (VDE 0491-3-1):200x zurzeit Norm-Entwurf	VDE 0491-3-1
–	IEC 61226:2005	DIN IEC 61226 (VDE 0491-1):2005-09	VDE 0491-1
–	IEC 61513:2001	DIN IEC 61513 (VDE 0491-2):2002-10	VDE 0491-2
–	IEC 62138:2004	DIN IEC 62138 (VDE 0491-3-3):2004-09	VDE 0491-3-3
–	IAEA NS-G-1.3	–	–

Nationaler Anhang NB (informativ)

Literaturhinweise

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 60880 (VDE 0491-3-2):2007-08, Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Softwareaspekte für rechnerbasierte Systeme zur Realisierung von Funktionen der Kategorie A (IEC 60880:2006)

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 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)

E DIN IEC 60987 (VDE 0491-3-1):2006-09, Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Anforderungen an die Hardware-Auslegung rechnerbasierter Systeme (IEC 45A/623/CDV:2006)

**Kernkraftwerke –
Leittechnik für Systeme mit sicherheitstechnischer Bedeutung –
Prüfungen zur Sicherstellung der Funktionsfähigkeit**

Inhalt

	Seite
Einleitung.....	7
1 Anwendungsbereich	8
2 Normative Verweisungen.....	9
3 Begriffe.....	10
4 Grundsätze für Funktionsfähigkeitsprüfungen	12
4.1 Allgemeines.....	12
4.2 Abstufung der Anforderungen entsprechend der Kategorie	12
4.3 Umfang der Funktionsfähigkeitsprüfungen	13
4.4 Selbstüberwachung statt wiederkehrender Prüfungen	13
4.5 Kontinuierlicher Betrieb statt wiederkehrender Prüfungen	13
5 Allgemeine Anforderungen für Funktionsfähigkeitsprüfungen.....	14
5.1 Auslegungsanforderungen	14
5.2 Vorgehensweise	15
5.3 Daten, die nach Aufdeckung eines Fehlers aufzuzeichnen sind	15
5.4 Andere aufzuzeichnende Daten.....	15
5.5 Prüfabstände.....	15
5.6 Verifizierung der Auslöse-Sollwerte	15
5.7 Bypass	16
5.8 Ansprechzeit	16
5.9 Wiederherstellen des Normalzustandes	16
6 Anforderungen für die Prüfungen der Messfühler und Signalverarbeitungseinrichtungen.....	17
6.1 Allgemeines.....	17
6.2 Ungeprüfte Teile	17
6.3 Prüfeinrichtung	17
6.4 Signale	17
6.5 Variieren von Signalen	17
6.5.1 Allgemeines	17
6.5.2 Sich langsam änderndes Signal	18
6.5.3 Sich schnell änderndes Signal.....	18
6.5.4 Große Änderung des Signals	18
6.6 Betriebsbereitschaft	18
6.7 Ansprechzeit der Messfühler	18
6.8 Prüfeinrichtung	18
6.9 Kalibrierung und Übertragungsfunktion	19
6.10 Überwachung	19

	Seite
7 Anforderungen für die Prüfung elektromechanischer Geräte	19
7.1 Allgemeines	19
7.2 Schnittstelle	19
7.3 Typische Funktionsprüfungen	20
7.4 Ständige Überwachung	20
7.5 Relais und Ventile	20
8 Anforderungen für das Prüfen von Logikschaltungen	20
8.1 Anwendungsbereich	20
8.2 Allgemeines	20
8.3 Schalten von Signalen	20
8.4 Prüfsignale	21
8.5 Schnittstelle	21
8.6 Anzuzeigende Daten	21
8.7 Aufzuzeichnende Daten	22
8.8 Detaillierte Anzeige	22
8.9 Prüfgerät	22
8.10 Geräteprüfung mit Pulsen	22
9 Selbstüberwachung bei rechnerbasierten leittechnischen Systemen	22
9.1 Abdeckungsmerkmale der Selbstüberwachung	23
9.2 Balance zwischen Selbstüberwachung und Funktionsausführung	23
9.3 Zykluszeitüberwachung	24
9.4 Maßnahmen nach Fehlerentdeckung	24
9.5 Kategorisierung der Selbstüberwachungssoftware	24
Bild 1 – Umfang der Funktionsfähigkeitsprüfungen für Leittechnik	9

Einleitung

a) Hintergrund, hauptsächliche Inhalte und Organisation der Norm

Eine fundamentale Anforderung an sicherheitstechnisch wichtige leittechnische Systeme in Kernkraftwerken besteht darin, dass die Fähigkeit, ihre Sicherheitsfunktionen zu erfüllen, wann immer benötigt, gezeigt werden kann. Prüfungen zur Sicherstellung der Funktionsfähigkeit (im Folgenden kurz: Funktionsfähigkeitsprüfungen) können mit Hilfe von Funktionsprüfungen oder Selbstüberwachung der sicherheitstechnisch wichtigen leittechnischen Systeme durchgeführt werden; sie werden durch diagnostische Funktionen und Sichtprüfungen der leittechnischen Systeme und ihrer Statusanzeigen von der Betriebsmannschaft unterstützt. Abhängig von den Zuverlässigkeitszielen und den Prüfbedingungen kann die Bestätigung der Funktionsbereitschaft entweder während des Betriebs oder einer Abschaltung der Anlage durchgeführt werden. Diese Norm enthält Anforderungen und Empfehlungen für die Realisierung von Funktionsfähigkeitsprüfungen für sicherheitstechnisch wichtige leittechnische Systeme.

Ziel dieser Norm ist es,

- in [Abschnitt 4](#)
die Prinzipien der Funktionsfähigkeitsprüfungen von sicherheitstechnisch wichtigen leittechnischen Geräten aufzuzeigen;
- in den [Abschnitten 5 bis 9](#)
die Anforderungen zu formulieren, die bei Auslegung und Betrieb sicherheitstechnisch wichtiger leittechnischer Geräte in Hinblick auf Funktionsfähigkeitsprüfungen zu erfüllen sind.

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

In [IEC 61513](#) sind die Anforderungen der höchsten Ebene für sicherheitstechnisch wichtige leittechnische Systeme und Geräte enthalten. Zu diesen Anforderungen gehört unter anderem der fortgesetzte Nachweis der Betriebsbereitschaft der Geräte und ihrer Fähigkeit, die sicherheitsbezogenen Funktionen auszuführen.

In [IEC 61226](#) finden sich die Prinzipien der Kategorisierung leittechnischer Funktionen entsprechend ihrer Bedeutung für die Sicherheit. Die von jeder Funktion geforderte Zuverlässigkeit in Kategorie A, B oder C sollte entweder durch eine quantitative probabilistische Sicherheitsanalyse des Kernkraftwerks oder durch eine qualitative ingenieurmäßige Beurteilung ermittelt werden und in die Spezifikation mit einfließen.

IEC 60671 enthält die Grundlagen und Anforderungen für die Funktionsfähigkeitsprüfungen, um die Betriebsfähigkeit dieser Systeme und Geräte unter Normalbedingungen während ihrer betrieblichen Lebenszeit nachweisen zu können.

IEC 60671 bietet Unterstützung für das Erreichen der Zuverlässigkeitsziele durch Aufdecken von Fehlern an den Geräten, wodurch die Einleitung geeigneter Maßnahmen ermöglicht wird (rechtzeitige Reparatur oder andere alternative Lösungen).

IEC 60671 ist ein IEC/SC-45A-Dokument der dritten Ebene und behandelt das Gebiet der Funktionsfähigkeitsprüfungen für sicherheitstechnisch wichtige leittechnische Systeme.

Näheres zur Struktur der Normen des IEC/SC 45A ist unter d) dieser Einleitung zu finden.

c) Empfehlungen und Einschränkungen der Anwendung der Norm

IEC 60671 gilt für sicherheitstechnisch wichtige leittechnische Systeme und Geräte. Sie enthält Anforderungen für Funktionsfähigkeitsprüfungen als Mittel, die ständige Bereitschaft von Systemen und Geräten zu zeigen, die sicherheitstechnisch wichtigen Funktionen auszuführen.

Zusätzliche Anforderungen bezüglich Zuverlässigkeit und detaillierte Angaben für Redundanz und Diversität sind in dieser Norm nicht enthalten, können jedoch in anderen SC-45A-Dokumenten gefunden werden.

Es wird darauf hingewiesen, dass in einigen Ländern Aufgabenbereich und Inhalt wiederkehrender Prüfungen durch Genehmigungsanforderungen bestimmt werden und daher von den Festlegungen in dieser Norm abweichen können.

Bei bestehenden Anlagen können möglicherweise nicht alle Anforderungen dieser Norm angewendet werden. Daher ist bei Beginn eines Modernisierungsprojekts für sicherheitstechnisch wichtige leittechnische Systeme die anzuwendende Teilmenge der Anforderungen in Hinblick auf den Gesamtbereich der anstehenden Modernisierung und ihrer Folgen zu ermitteln.

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 stellt die Norm **IEC 61513** dar. Diese Norm befasst sich mit Anforderungen an sicherheitstechnisch wichtige leittechnische Systeme von Kernkraftwerken und strukturiert die Normen des IEC/SC 45A.

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 gemeinsamer Ursache, Softwareaspekte rechnerbasierter Systeme, Hardwareaspekte 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 SC-45A-Normen der dritten Ebene, auf die in **IEC 61513** nicht direkt verwiesen wird, beziehen sich auf spezielles Gerät, technische Methoden oder spezifische Aktivitäten. Üblicherweise können diese Dokumente, in denen auf Normen der Ebene 2 verwiesen wird, für sich allein benutzt werden.

Auf der vierten Ebene finden sich als Erweiterung der SC-45A-Normenreihe Technische Berichte, die der Information dienen und keine Normen darstellen.

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. Mit **IEC 61513** werden die allgemeinen Anforderungen (für Sicherheitssysteme unterschiedlicher industrieller Anwendungen) von **IEC 61508-1**, **-2** und **-4** für die Anwendung auf nuklearem Sektor umgesetzt. Die Einhaltung der **IEC 61513** erleichtert die Übereinstimmung mit IEC 61508, weil die Anforderungen der **IEC 61513** aus den Anforderungen der IEC 61508 für die Anwendung in der nuklearen Industrie entwickelt wurden. In diesem Rahmen entsprechen **IEC 60880** und **IEC 62138** für den nuklearen Sektor der Norm **IEC 61508-3**.

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

In den Normen des IEC/SC 45A werden die Prinzipien und grundsätzlichen Sicherheitsaspekte des „IAEA Code for the safety of nuclear power plants“ und der „IAEA safety series“, insbesondere der Anforderungen des NS-R-1 „Safety of Nuclear Power Plants: Design“ und des Safety Guide NS-G-1.3 „Instrumentation and control systems important to safety in Nuclear Power Plants“, umgesetzt und detailliert. Terminologie und Definitionen in den Normen des IEC/SC 45A sind mit den von der IAEA verwendeten konsistent.

1 Anwendungsbereich

Wenn im Rahmen von allgemeinen Sicherheitsstandards funktionale Zuverlässigkeit gefordert wird, ist ein Gesichtspunkt die online durchgeführte Prüfung während des Anlagenbetriebs oder während der Abschaltung in Vorbereitung der Rückkehr zum Leistungsbetrieb.

In dieser Norm werden Prinzipien für Prüfungen leittechnischer Systeme, die Funktionen der Kategorien A, B und/oder C nach **IEC 61226** ausführen, während Leistungsbetrieb und Abschaltung festgelegt, um so die funktionale Verfügbarkeit, insbesondere in Hinblick auf die Entdeckung von Fehlern, die das einwandfreie Arbeiten sicherheitstechnisch wichtiger Funktionen verhindern könnten, zu überprüfen. Dabei wird die Möglichkeit von Prüfungen in kurzen Zeitabständen (oder von ständiger Überwachung) sowie von wiederkehrenden Prüfungen in längeren Zeitabständen behandelt. Weiter werden die grundsätzlichen Regeln für die Auslegung und Anwendung der Prüfgeräte und der Schnittstellen mit den sicherheitstechnisch wichtigen Systeme-