

**DIN IEC 61500
(VDE 0491-3-4)**
DIN

Diese Norm ist zugleich eine **VDE-Bestimmung** im Sinne von VDE 0022. Sie ist nach Durchführung des vom VDE-Präsidium beschlossenen Genehmigungsverfahrens unter der oben angeführten Nummer in das VDE-Vorschriftenwerk aufgenommen und in der „etz Elektrotechnik + Automation“ bekannt gegeben worden.

VDE

ICS 27.120.20

Einsprüche bis 2016-03-08

Vorgesehen als Ersatz für
DIN EN 61500
(VDE 0491-3-4):2011-12

Entwurf

**Kernkraftwerke –
Leittechnische Systeme mit sicherheitstechnischer Bedeutung –
Datenkommunikation in Systemen, die Funktionen der Kategorie A
ausführen
(IEC 45A/1044/CD:2015)**

Nuclear power plants –
Instrumentation and control systems important to safety –
Data communication in systems performing category A functions
(IEC 45A/1044/CD:2015)

Centrales nucléaires de puissance –
Systèmes d'instrumentation et de contrôle-commande importants pour la sûreté –
Communication de données dans les systèmes réalisant des fonctions de catégorie A
(IEC 45A/1044/CD:2015)

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2016-01-08 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 34 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE

Anwendungsbeginn

Anwendungsbeginn dieser Norm ist

Inhalt

Seite

Nationales Vorwort.....	3
Nationaler Anhang NA (informativ) Zusammenhang mit Europäischen und Internationalen Dokumenten	6
Nationaler Anhang NB (informativ) Literaturhinweise.....	7
Einleitung	7
1 Anwendungsbereich	11
2 Normative Verweisungen	11
3 Begriffe	12
4 Abkürzungen	13
5 Allgemeine Anforderungen	13
5.1 Auswahlprinzipien für Techniken und Geräte der Datenkommunikation	13
5.2 Funktionale Anforderungen	13
5.3 Anforderungen an die Leistungsfähigkeit	14
5.4 Ausfallerkennung	14
5.5 Datenkommunikation innerhalb von Teilsystemen.....	15
5.6 Schnittstellen mit Systemen von geringerer Bedeutung für die Sicherheit	15
6 Galvanische und physikalische Trennung.....	15
6.1 Galvanische Trennung	15
6.2 Physikalische Trennung	16
7 Funktionale Unabhängigkeit.....	16
8 Zuverlässigkeit.....	16
8.1 Selbstüberwachung und Ausfallminderung.....	16
8.1.1 Entdecken von Datenkommunikationsfehlern.....	16
8.1.2 Reaktion auf Ausfälle bei der Datenkommunikation	16
8.2 Prüfung	17
8.3 Vorsorge gegen Ausfälle (einschließlich CCF)	18
8.4 IT-Sicherheit	18
9 Qualifizierung.....	18
10 Wartung und Modifizierung	18
Literaturhinweise.....	20

Nationales Vorwort

Das internationale Dokument IEC 45A/1044/CD:2015 „Nuclear power plants – Instrumentation and control systems important to safety – Data communication in systems performing category A functions“ (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 bzw. Schluss-Entwurf prEN 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.

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.

Vorbemerkung

- a) Anlässlich der Übersetzung von Ed.2 gab es bereits Diskussionen über die nicht ihrer Definition entsprechende Verwendung der Begriffe fault, failure, error (besonders augenscheinlich wird das in Kapitel 8, Reliability). Nach IEC 61513 gilt

fault	Defect in a hardware, software or system component
failure	Deviation of the delivered service from the intended one
error	discrepancy between a computed, observed or measured value or condition, and the true, specified or theoretical value or condition
human error	human action that produces an unintended result

ANMERKUNG Ungeachtet dessen hat UK 967.1 seinerzeit in der Übersetzung der für die DIN EN 61500 (VDE 0491-3-4):2011-12 verwendeten Übersetzung der Ed.2 die jeweils zutreffenden/richtigen deutschen Benennungen verwendet.

- b) Der Zusatz „as applicable“, der im Zusammenhang mit einem „requirement“ schon per se etwas fragwürdig ist, wird häufig auch am Ende einer Aufzählung mehrerer Normen verwendet. Dabei bleibt unklar, ob sich der Zusatz auf die gesamte Aufzählung oder nur auf die letztgenannte Norm bezieht (siehe Abschnitt 9 und Abschnitt 10). Eine entsprechende Korrektur ist im Rahmen der deutschen Stellungnahme zum IEC-Entwurf vorgesehen.

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*

E DIN IEC 61500 (VDE 0491-3-4):2016-02

- 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)*
- 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 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 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 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 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, *Kernkraftwerke – Elektrisches Gerät mit sicherheitstechnischer Bedeutung – Qualifizierung (IEC 45A/940/CD:2013)*

Änderungen

Gegenüber DIN EN 61500 (VDE 0491-3-4):2011-12 wurden folgende Änderungen vorgenommen:

- a) Die Zugangsschutzplanung muss nach IEC 62645 erfolgen;
- b) Empfehlungen zu IT-Sicherheitsmerkmalen wurden in 5.6 aufgenommen;
- c) Unterabschnitt 8.4 „IT-Sicherheit“ wurde neu aufgenommen;
- d) Die Verweisungen wurden aktualisiert und ergänzt.

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
–	ISO/IEC 7498	–	–
EN 60068 (alle Teile)	IEC 60068 (alle Teile)	DIN EN 60068 (VDE 0468) (alle Teile)	VDE 0468
EN 60709	IEC 60709	DIN EN 60709 (VDE 0491-7)	VDE 491-7
EN 60721 (alle Teile)	IEC 60721 (alle Teile)	DIN EN 60721 (VDE 0468-721) (alle Teile)	VDE 0468-721
–	IEC/IEEE 60780-323 (zurzeit in Vorbereitung)	Zurzeit Norm-Entwurf E DIN IEC 60780-323 (VDE 0491-80):2014-04	VDE 0491-80
–	Noch gilt: IEC 60780:1998	DIN IEC 60780:2000-12	–
EN 60880:2009	IEC 60880:2006	DIN EN 60880 (VDE 0491-3-2):2010-03	VDE 0491-3-2
EN 60964	IEC 60964	DIN EN 60964 (VDE 0491-5-1)	VDE 0491-5-1
EN 60965	IEC 60965	DIN EN 60965 (VDE 0491-5-5)	VDE 0491-5-5
–	IEC 60980	–	–
EN 60987:2015	IEC 60987:2007 + A1:2013	DIN EN 60987 (VDE 0491-3-1):2015-06	VDE 0491-3-1
EN 61000 (alle Teile)	IEC 61000 (alle Teile)	DIN EN 61000 (VDE 0839) (alle Teile)	VDE 0839
EN 61158-3-19	IEC 61158-3-19	DIN EN 61158-3-19	–
EN 61226	IEC 61226	DIN EN 61226 (VDE 0491-1)	VDE 0491-1
EN 61508-1	IEC 61508-1	DIN EN 61508-1 (VDE 0803-1)	VDE 0803-1

Tabelle NA.1 (2 von 2)

Europäisches Dokument	Internationales Dokument	Deutsches Dokument	Klassifikation im VDE-Vorschriftenwerk
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 61784-3:2008 ersetzt durch: EN 61784-3:2010	IEC 61784-3:2007 ersetzt durch: EN 61784-3:2010	DIN EN 61784-3 (VDE 0803-500):2008-11 ersetzt durch: DIN EN 61784-3 (VDE 0803-500):2011-02	VDE 0803-500 VDE 0803-500
EN 61784-3-1	IEC 61784-3-1	DIN EN 61784-3-1	–
–	IEC 62003	–	–
EN 62138	IEC 62138	DIN EN 62138 (VDE 0491-3-3)	VDE 0491-3-3
EN 62241	IEC 62241	DIN EN 62241 (VDE 0491-5-2)	VDE 0491-5-2
EN 62340:2010	IEC 62340:2007	DIN EN 62340 (VDE 0491-10):2010-12	VDE 0491-10
EN 62566	IEC 62566	DIN EN 62566 (VDE 0491-3-5)	VDE 0491-3-5
–	IEC 62645	–	–
–	IEC 62859	–	–

Nationaler Anhang NB (informativ)

Literaturhinweise

DIN EN 60068 (VDE 0468) (alle Teile), *Umgebungseinflüsse*

DIN EN 60709 (VDE 0491-7), *Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Physikalische und elektrische Trennung*

DIN EN 60721 (VDE 0468-721) (alle Teile), *Klassifizierung von Umgebungsbedingungen*

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

E DIN IEC 61500 (VDE 0491-3-4):2016-02

DIN EN 60965 (VDE 0491-5-5), *Kernkraftwerke – Warten – Notsteuerstellen für das Abfahren des Reaktors ohne Verbindung zur Hauptwarte*

DIN EN 60987 (VDE 0491-3-1):2015-06, *Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Anforderungen an die Hardware-Auslegung rechnerbasierter Systeme (IEC 60987:2007 + A1:2013); Deutsche Fassung EN 60987:2015*

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

DIN EN 61158-3-19, *Industrielle Kommunikationsnetze – Feldbusse – Teil 3-19: Dienstfestlegungen des Data Link Layer (Sicherungsschicht) – Typ 19-Elemente*

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

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 61784-3 (VDE 0803-500):2011-02, *Industrielle Kommunikationsnetze – Profile – Teil 3: Funktional sichere Übertragung bei Feldbussen – Allgemeine Regeln und Profilverfestlegungen (IEC 61784-3:2010); Deutsche Fassung EN 61784-3:2010*

DIN EN 61784-3-1, *Industrielle Kommunikationsnetze – Profile – Teil 3-1: Funktional sichere Übertragung bei Feldbussen – Zusätzliche Festlegungen für die Kommunikationsprofilfamilie 1*

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 62241 (VDE 0491-5-2), *Kernkraftwerke – Warte – Alarmfunktionen und ihre Darstellung*

DIN EN 62340 (VDE 0491-10):2010-12, *Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Anforderungen zur Beherrschung von Versagen aufgrund gemeinsamer Ursache (IEC 62340:2007); Deutsche Fassung EN 62340:2010*

DIN EN 62566 (VDE 0491-3-5), *Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Entwicklung HDL-programmierter integrierter Schaltkreise für Systeme, die Funktionen der Kategorie A ausführen*

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

E DIN IEC 60780-323 (VDE 0491-80):2014-04, *Kerntechnische Anlagen – Elektrisches Gerät mit sicherheitstechnischer Bedeutung – Qualifizierung (IEC 45A/940/CD:2013)*

Einleitung

a) Technischer Hintergrund, hauptsächliche Inhalte und Organisation der Norm

Durch Verwendung von Datenkommunikationssystemen für Online-Anlagendaten können die Kabelverbindungen verteilter leittechnischer Systeme vereinfacht werden, ein wegen der Bedeutung der Leittechnik für den sicheren Betrieb eines Kernkraftwerks wichtiger Gesichtspunkt. Weitere Vorteile gegenüber direkten Kabelverbindungen können sich bei der galvanischen Trennung, durch Verringerung der Kabelbrandlasten oder aus anderen Gründen ergeben. In einem rechnerbasierten verteilten System stellen die Datenkommunikationseinrichtungen einen wesentlichen Teil dar. Die Datenkommunikation ist gewöhnlich bei der Realisierung sicherheitstechnisch wichtiger leittechnischer Systeme für Kernkraftwerke von großer Bedeutung.

Diese Norm ist zur Verwendung für Kraftwerksbetreiber (EVU), Hersteller von Datenkommunikationseinrichtungen, Systemgutachter und Genehmigungsbehörden vorgesehen.

b) Einordnung der vorliegenden Norm in die Struktur der IEC-SC45A-Normenreihe

Die vorliegende Norm ist ein IEC-SC45A-Dokument der dritten Ebene und behandelt die Datenkommunikation für Geräte, die Funktionen der Kategorie A ausführen.

Die vorliegende Norm ist in Verbindung mit folgenden einschlägigen IEC-Normen anzuwenden:

- IEC 61513 für allgemeine Anforderungen an sicherheitstechnisch wichtige leittechnische Geräte;
- IEC 60880 für Softwareaspekte rechnerbasierter Systeme, die Kategorie-A-Funktionen ausführen;
- IEC 60987 für Hardwareaspekte rechnerbasierter Systeme.

Mehr Details über die Struktur der IEC-SC45A-Normenreihe finden sich in Punkt d) dieser Einleitung.

c) Empfehlungen und Einschränkungen der Anwendung der Norm

Es ist wichtig, darauf hinzuweisen, dass in dieser Norm keine zusätzlichen funktionalen Anforderungen für Sicherheitssysteme definiert werden.

Spezielle Überlegungen wurden hinsichtlich folgender Punkte angestellt:

- Anforderungen zur Datenkommunikation in Systemen für Kategorie-A-Funktionen;
- Anforderungen zur Datenkommunikation zwischen Teilsystemen, die Kategorie-A-Funktionen ausführen;
- Anforderungen zur Datenkommunikation von Systemen für Kategorie-A-Funktionen mit Systemen geringerer sicherheitstechnischer Bedeutung;
- Zuverlässigkeitsanforderungen zur Datenkommunikation^{N1)}.

Um sicherzustellen, dass die Norm über längere Zeit gültig bleibt, wurde der Schwerpunkt auf Prinzipien und nicht auf spezielle Technologien gelegt.

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

Das Eingangsdokument zur IEC-SC45A-Normenreihe stellt die Norm IEC 61513 dar. Sie enthält allgemeine Anforderungen an die leittechnischen Systeme und Geräte, die zur Ausführung sicherheitstechnisch wichtiger Funktionen in Kernkraftwerken genutzt werden. Durch die IEC 61513 wird die SC45A-Normenreihe strukturiert.

In IEC 61513 wird direkt auf andere IEC-SC45A-Normen verwiesen, die allgemeine Themen wie die Kategorisierung von Funktionen und die Klassifizierung von Systemen, Qualifizierung, Trennung von Systemen, Maßnahmen gegen Versagen aufgrund gemeinsamer Ursache, Software-Aspekte rechnerbasierter Systeme,

^{N1)} Nationale Fußnote: Inklusive der Anforderungen an Datenintegrität.

Hardware-Aspekte rechnerbasierter Systeme sowie 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 IEC-SC45A-Normen, auf die in IEC 61513 nicht direkt verwiesen wird. Diese Normen behandeln spezielles Gerät, technische Methoden oder spezifische Aktivitäten. Sie beziehen sich hinsichtlich der allgemeinen Themen auf die Dokumente der zweiten Ebene, können jedoch im Allgemeinen für sich allein benutzt werden.

Eine vierte Ebene erweitert die SC45A-Normenreihe um Technische Berichte, die nicht normativ sind.

Für IEC 61513 wird ein Darstellungsformat verwendet, das dem der grundlegenden Sicherheitsnorm IEC 61508 ähnlich ist, mit einem Sicherheits-Lebenszyklus als Gesamtrahmen und zusätzlich einem System-Lebenszyklus. Hinsichtlich der nuklearen Sicherheit werden mit IEC 61513 die allgemeinen Anforderungen von IEC 61508-1, IEC 61508-2 und IEC 61508-4 für die Anwendung auf dem nuklearen Sektor umgesetzt. In diesem Rahmen entsprechen IEC 60880 und IEC 62138 für den nuklearen Sektor der Norm IEC 61508-3. IEC 61513 bezieht sich bei Themen der Qualitätssicherung (QS) sowohl auf ISO als auch auf IAEA GS-R-3.

In der IEC-SC45A-Normenreihe werden die Prinzipien und grundsätzlichen Sicherheitsaspekte des IAEA-Codes für die Sicherheit von Kernkraftwerken und der IAEA-Sicherheitsserie umgesetzt, insbesondere die Requirements SSR-2/1 bezüglich der Sicherheit bei der Auslegung von Kernkraftwerken und der Safety Guide SSG-39 bezüglich der leittechnischen Systeme mit Sicherheitsbedeutung in Kernkraftwerken. Terminologie und Definitionen in den IEC-SC45A-Normen stimmen mit den von der IAEA verwendeten überein.

ANMERKUNG 1 Für die Auslegung von leittechnischen Systemen in Kernkraftwerken, die der Realisierung konventioneller Sicherheitsfunktionen dienen (z. B. hinsichtlich Arbeitersicherheit, Schutz vor Sachschaden, chemischer Gefährdung, energetischer Gefährdung), wird die Anwendung internationaler oder nationaler Standards vorausgesetzt, die auf Anforderungen von Standards wie IEC61508 beruhen.

ANMERKUNG 2 Der Aufgabenbereich von IEC SC45A wurde in 2013 auf elektrische Systeme ausgedehnt. In den Jahren 2014 und 2015 wurden im SC45A Diskussionen geführt, in welcher Form die Anforderungen für die Auslegung elektrischer Systeme in Betracht gezogen werden sollen. Die SC45A-Experten empfahlen die Entwicklung einer eigenständigen Norm, die auf derselben Ebene wie IEC 61513 die allgemeinen Anforderungen für elektrische Systeme behandelt. Dieses Projekt soll in naher Zukunft in Angriff genommen werden. IEC 61513 und die neue Norm über Anforderungen für elektrische Systeme würden in engem Zusammenhang zu sehen sein, sie sollen miteinander ein kohärentes, konsistentes und komplettes Rahmenwerk für die Erstellung allgemeiner Anforderungen für leittechnische und elektrische Systeme bilden. Um dieser Entwicklung Rechnung zu tragen, erfolgt eine Anpassung dieses Abschnitts der Einleitung von IEC SC45A Standards, sobald das Projekt zur Erstellung von allgemeinen Anforderungen für elektrische Systeme in Gang gesetzt wird,

**Kernkraftwerke –
Leittechnische Systeme mit sicherheitstechnischer Bedeutung –
Datenkommunikation in Systemen, die Funktionen der Kategorie A ausführen**

1 Anwendungsbereich

Diese Internationale Norm enthält Anforderungen zur Datenkommunikation, die in Systemen für Funktionen der Kategorie A in Kernkraftwerken verwendet wird.

Sie umfasst auch Schnittstellenanforderungen zur Datenkommunikation von Geräten für Kategorie-A-Funktionen mit anderen Systemen einschließlich jenen für Kategorie-B- und -C-Funktionen und sicherheitstechnisch unwichtige Funktionen.

Der Anwendungsbereich dieser Norm beschränkt sich auf die Datenkommunikation innerhalb der leittechnischen Systeme der Anlage. Kommunikation über Telefon, Funk, Lautsprecher, Stimme, Fax, E-Mail usw. wird nicht behandelt.

Der interne Betrieb und die detaillierte technische Spezifikation der Geräte für Datenkommunikation liegen nicht im Anwendungsbereich dieser Norm. Sie ist auch nicht auf interne Verbindungen und Datenkommunikation eines Prozessors, seiner Speicher und Steuerungslogik anwendbar. Sie betrifft auch nicht die rechnerinterne Datenverarbeitung der Leittechnik.

Diese Norm enthält Anforderungen an Funktionen und Eigenschaften der Online-Anlagendaten-Kommunikation durch Verweisung auf die Normen IEC 60880 und IEC 60987, die im Rahmen der Aufgabenstellung von IEC 61513 erstellt worden sind. Weiterhin verlangt sie die Kategorisierung der Datenkommunikationsfunktionen nach IEC 61226, woraus sich die erforderliche Qualifizierung hinsichtlich Umgebungs- und seismischer Bedingungen nach IEC/IEEE 60780-323 und IEC 60980 ergibt (d. h. die Umgebungsbedingungen, unter denen die Sicherheitsfunktion ihre Aufgabe erfüllen muss).

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

IEC/IEEE 60780-323, *Nuclear power plants – Electrical equipment of the safety system – Qualification*

IEC 60880:2006, *Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category A functions*

IEC 60980, *Recommended practices for seismic qualification of electrical equipment of the safety system for nuclear generating stations*

IEC 60987:2013, *Nuclear power plants – Instrumentation and control important to safety – Hardware design requirements for computer-based systems*

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

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

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