

	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 2009-08-31		
Entwurf		
Kernkraftwerke – Leittechnik mit sicherheitstechnischer Bedeutung – Datenkommunikation (IEC 45A/714/CDV:2008) Nuclear Power Plants – Instrumentation and control important to safety – Data communication (IEC 45A/714/CDV:2008) Centrales nucléaires de puissance – Instrumentation et contrôle commande importants pour la sûreté – Communication de données (CEI 45A/714/CDV:2008)		
Anwendungswarnvermerk Dieser Norm-Entwurf mit Erscheinungsdatum 2009-06-15 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt. Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfes besonders zu vereinbaren. Stellungnahmen werden erbeten – vorzugsweise als Datei per E-Mail an dke@vde.com in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.dke.de/stellungnahme abgerufen werden – oder in Papierform an die DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE, Stresemannallee 15, 60596 Frankfurt am Main. Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevante Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.		
Gesamtumfang 27 Seiten		
DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE		

Beginn der Gültigkeit

Diese Norm gilt ab ...

Inhalt

	Seite
Einleitung.....	6
1 Anwendungsbereich	7
2 Normative Verweisungen.....	8
3 Begriffe.....	8
4 Symbole und Abkürzungen.....	9
5 Allgemeine Anforderungen	9
5.1 Auswahlprinzipien für Techniken und Geräte der Datenkommunikation.....	9
5.2 Funktionale Anforderungen	10
5.3 Anforderungen an die Leistungsfähigkeit	10
5.4 Ausfallerkennung	11
5.5 Kommunikation innerhalb von Teilsystemen	11
5.6 Schnittstellen mit Systemen von geringerer Bedeutung für die Sicherheit.....	11
6 Galvanische und physikalische Trennung	11
6.1 Galvanische Trennung.....	11
6.2 Physikalische Trennung.....	12
7 Funktionale Unabhängigkeit	12
8 Zuverlässigkeit	12
8.1 Selbstüberwachung und Ausfallminderung	12
8.2 Prüfung	13
8.3 Vorsorge gegen CCF	14
9 Qualifizierung	14
10 Wartung und Modifizierung	14

Nationales Vorwort

Das internationale Dokument IEC 45A/714/CDV:2008 „Nuclear Power Plants – Instrumentation and control important to safety – Data communication“ (CDV, en: Committee Draft for Vote) 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 CDV entsprechend der diesbezüglich durch die IEC erteilten Erlaubnis beigefügt. Die Nutzungsbedingungen für den deutschen Teil des Norm-Entwurfes gelten gleichermaßen auch für den englischen IEC-Text.

Das internationale Dokument wurde vom SC 45A „Instrumentation and control of nuclear facilities“ der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet und den nationalen Komitees zur Stellungnahme und Abstimmung vorgelegt. Es wird jedoch nicht zeitgleich (parallel) bei IEC und CENELEC zur Umfrage gestellt. Derzeit ist also nicht vorgesehen, dieses Dokument als Europäische Norm zu übernehmen.

Da der Abstimmungszeitraum für einen FDIS (en: Final Draft International Standard) 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 CDV als DIN-Norm-Entwurf veröffentlicht, um die Stellungnahmen aus der Öffentlichkeit noch vor der Abstimmung berücksichtigen zu können.

Für diesen Norm-Entwurf ist das nationale Arbeitsgremium UK 967.1 „Leittechnik für kerntechnische Anlagen“ der DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE (www.dke.de) zuständig.

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 60068	IEC 60068	DIN EN 60068	–
–	IEC 60709	DIN IEC 60709 (VDE 0491-7)	VDE 0491-7
EN 60721	IEC 60721	DIN EN 60721	–
–	IEC 60780:1998	DIN IEC 60780:2000-12	–
–	IEC 60880:2006	DIN IEC 60880 (VDE 0491-3-2):2007-08	VDE 0491-3-2
–	IEC 60964	Siehe Entwurf E DIN IEC 60964 (VDE 0491-5-1):2007-11	VDE 0491-5-1
–	IEC 60965	–	–
–	IEC 60980	–	–
–	IEC 60987:2007	DIN IEC 60987 (VDE 0491-3-1):2008-04	VDE 0491-3-1
Reihe EN 61000	Reihe IEC 61000	Reihe DIN EN 61000 (VDE 0839 bzw. 0847)	Reihen VDE 0839 bzw. 0847
–	IEC 61226	DIN IEC 61226 (VDE 0491-1)	VDE 0491-1
–	IEC 61513:2001	DIN IEC 61513 (VDE 0491-2):2002-10	VDE 0491-2
–	IEC 62003	Siehe Entwurf E DIN IEC 62003 (VDE 0491-8):2009-03	VDE 0491-8
–	IEC 62241	DIN IEC 62241 (VDE 0491-5-2)	VDE 0491-5-2
–	IEC 62340:2007	Siehe Entwurf E DIN 62340 (VDE 0491-10):2006-04	VDE 0491-10

Nationaler Anhang NB (informativ)

Literaturhinweise

DIN EN 60068, *Umweltprüfungen*

DIN EN 60721, *Klassifizierung von Umweltbedingungen*

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

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

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

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)*

E DIN IEC 60964 (VDE 0491-5-1):2007-11, *Kernkraftwerke – Warten – Auslegung (IEC 45A/652/CDV:2007)*

DIN IEC 60987 (VDE 0491-3-1):2008-04, *Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Anforderungen an die Hardwareauslegung rechnerbasierter Systeme (IEC 60987:2007)*

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

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

E DIN IEC 62003 (VDE 0491-8):2009-03, *Kernkraftwerke – Leittechnik mit sicherheitstechnischer Bedeutung – Anforderungen zur Prüfung elektromagnetischer Verträglichkeit (IEC 45A/725/FDIS:2008)*

DIN IEC 62241 (VDE 0491-5-2), *Kernkraftwerke – Hauptwarte – Funktionen zur Meldung und Anzeige von Störungen*

E DIN 62340 (VDE 0491-10):2006-04, *Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Versagen gemeinsamer Ursache (CCF) (IEC 45A/601/CDV:2005)*

Kernkraftwerke – Leittechnik mit sicherheitstechnischer Bedeutung – Datenkommunikation

Einleitung

a) Technischer Hintergrund, hauptsächliche Inhalte und Organisation der Norm

Diese Internationale Norm definiert die Anforderungen für Kommunikationssysteme, wie sie sich aus dem IAEA Safety Guide NS-G-1.3, Abschnitte 5.53 bis 5.59 und 5.3.1.3 der IEC 61513 ergeben. Sie liefert ebenso Herstellern Anleitungen zu Anforderungen für Kernkraftwerken.

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 anderen Gründen ergeben. In einem rechnerbasierten verteilten System stellen die Kommunikationsgeräte einen wesentlichen Teil dar. Die Datenkommunikation ist gewöhnlich bei der Realisierung sicherheitstechnisch wichtiger leittechnischer Systeme für Kernkraftwerke von großer Bedeutung. Die Anforderungen des IAEA Safety Guide NS-G-1.3 sind anwendbar und diese Norm gibt eine Anleitung für deren Anwendung.

Diese Norm ist zur Verwendung für KKW-Betreiber (EVUs), 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 zweiten Ebene und behandelt die Datenkommunikation für Geräte, die Funktionen der Kategorie A ausführen.

Die vorliegende Norm ist in Zusammenhang mit IEC 61513 anzuwenden, die das entsprechende SC45A-Dokument für allgemeine Anforderungen an sicherheitstechnisch wichtige leittechnische Geräte darstellt.

Mehr Details über die Struktur der IEC-SC45A-Normenreihe finden sich in Abschnitt 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 Funktionen der Kategorie A.
- Anforderungen zur Datenkommunikation zwischen Teilsystemen, die Funktionen der Kategorie A ausführen.
- Anforderungen zur Datenkommunikation von Systemen für Funktionen der Kategorie A mit Systemen geringerer sicherheitstechnischer Bedeutung.
- Zuverlässigkeitsanforderungen zur Datenkommunikation.

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 IEC-SC45A-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 KKW 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, 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 mit Technischen Berichten, 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. Mit IEC 61513 werden die allgemeinen Anforderungen von IEC 61508-1, -2 und -4, für die Anwendung auf dem nuklearen Sektor umgesetzt. Die Einhaltung der IEC 61513 erleichtert somit die Übereinstimmung mit der Norm IEC 61508, weil deren allgemeine Anforderungen für die nukleare Industrie berücksichtigt wurden. 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 sowohl auf ISO als auch auf IAEA 50-C-QA (inzwischen durch IAEA 50-C/SG-Q ersetzt).

In der IEC-SC45A-Normenreihe werden die Prinzipien und grundsätzlichen Sicherheitsaspekte des IAEA-Codes für die Sicherheit von KKW und der IAEA-Sicherheitsserie umgesetzt, insbesondere die Requirements NS-R-1 „Safety of Nuclear Power Plants: Design“ und der Safety Guide NS-G-1.3 „Instrumentation and control systems important to safety in Nuclear Power Plants“. Terminologie und Definitionen in den IEC-SC45A-Normen stimmen mit den von der IAEA verwendeten überein.

1 Anwendungsbereich

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

Sie umfasst Schnittstellenanforderungen zur Datenkommunikation von Geräten für Funktionen der Kategorie A mit anderen Systemen einschließlich jenen für Funktionen der Kategorien B und C und sicherheitstechnisch unwichtigen Funktionen.

Diese Norm enthält auch Anforderungen zur Datenkommunikation zwischen Teilsystemen oder Kanälen innerhalb von Systemen, die Funktionen der Kategorie A ausführen.

Diese Norm beschränkt sich auf Datenkommunikation innerhalb der leittechnischen Systeme der Anlage. Sie behandelt nicht Kommunikation über Telefon, Funk, Lautsprecher, Fax, E-Mail etc.

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 interne Datenverarbeitung in Rechnersystemen 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 in Ergänzung zu IEC 61513 speziell Hard- und Software-Anforderungen für rechnerbasierte Systeme behandeln. Weiterhin verlangt sie die Kategorisierung der Kommunikationsfunktionen nach IEC 61226, woraus sich die erforderliche Qualifizierung der diese Funktionen ausführenden Geräte hinsichtlich Umgebungs- und seismischer Bedingungen nach IEC 60780 und IEC 60980 ergibt.

2 Normative Verweisungen

Die folgenden zitierten Dokumente 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 60068, *Environmental testing*

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

IEC 60721, *Classification of environmental conditions*

IEC 60780:1998, *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 60964, *Nuclear Power Plants – Control rooms – Design*

IEC 60965, *Nuclear Power Plants – Control rooms – Supplementary control points for reactor shutdown without access to the main control room*

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

IEC 60987:2007, *Nuclear power plants – Instrumentation and control important to safety – Hardware design requirements for computer-based systems*

IEC 61000, *Electromagnetic compatibility (EMC)*

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

IEC 61513:2001, *Nuclear power plants – Instrumentation and control for systems important to safety – General requirements for systems*

IEC 62241, *Nuclear power plants – Main control room – Alarm functions and presentation*

IEC 62003, *Nuclear power plants – Instrumentation and control important to safety – Requirements for electromagnetic compatibility testing*

IEC 62340:2007, *Nuclear power plants – Instrumentation and control systems important to safety – Requirements for coping with common cause failure (CCF)*

IAEA safety guide No. NS-G-1.3, *Instrumentation and Control Systems Important to Safety in Nuclear Power Plants*

3 Begriffe

Für diese Norm gelten die in IEC 60880, IAEA safety glossary und IAEA safety guide NS-G-1.3 sowie die im Folgenden genannten Begriffe.

3.1

Kommunikationskanal

(en: communication channel)

logische Verbindung zwischen zwei Endpunkten innerhalb eines Kommunikationssystems

[IEC 61784-3, 2007]

3.2

Kommunikationsknoten

(en: communication node)

Verbindungspunkt an einem Kommunikations-Netzwerk, zu oder von dem Daten über Kommunikationskanäle von oder zu anderen Punkten im Netzwerk übertragen werden

3.3

Kommunikationssystem

(en: communication system)

Anordnung von Hardware, Software und Übertragungsmedien zur Nachrichtenübermittlung (ISO/IEC 7498 application layer) von einer zur anderen Anwendung

[IEC 61784-3, 2007]

3.4

Datenkommunikation

(en: data communication)

Austausch von Daten zwischen Kommunikationsknoten über Kommunikationskanäle

3.5

Datenkommunikationsgerät

(en: data communication equipment)

Sammelbegriff für die Medien, modulations- und codeabhängigen Teile einer mit dem Bus verbundenen Einrichtung, die den niedrigeren Bereich der physikalischen Ebene innerhalb der Einrichtung bilden

[IEC 61784-3, 2007, modifiziert]

3.6

Nachricht

(en: message)

geordnete Reihe von Achtbit-Zeichen zum Zweck der Informationsübermittlung

[IEC 61784-3, 2007]

3.7

Protokoll

(en: protocol)

Vereinbarung über Datenformate, Zeitfolgen und Fehlerkorrektur beim Datenaustausch von Kommunikationssystemen

[IEC 61158-3-19, 2007]

4 Symbole und Abkürzungen

CCF Versagen/Ausfall aufgrund gemeinsamer Ursache (en: common cause failure)

FMEA Fehlerart- und -effektanalyse (en: failure mode and effect analysis)

I&C Leittechnik

5 Allgemeine Anforderungen

5.1 Auswahlprinzipien für Techniken und Geräte der Datenkommunikation

Um die Akzeptanz für nukleare Anwendungen zu erreichen, sollte eines der folgenden Auswahlprinzipien für Techniken und Geräte der Datenkommunikation angewendet werden:

- Verwendung von Protokollen mit Sicherheitsmerkmalen;
- Verwendung industrieller Standardprotokolle, mit Ergänzung von Sicherheitsebenen;