

	DIN EN IEC 62138 (VDE 0491-3-3)	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
<p>ICS 27.120.20; 35.080</p> <p>Ersatz für DIN EN 62138 (VDE 0491-3-3):2010-03 Siehe Anwendungsbeginn</p> <p>Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Softwareaspekte für rechnerbasierte Systeme zur Realisierung von Funktionen der Kategorien B oder C (IEC 62138:2018); Deutsche Fassung EN IEC 62138:2019</p> <p>Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category B or C functions (IEC 62138:2018); German version EN IEC 62138:2019</p> <p>Centrales nucléaires de puissance – Systèmes d'instrumentation et de contrôle-commande importants pour la sûreté – Aspects logiciels des systèmes informatisés réalisant des fonctions de catégorie B ou C (IEC 62138:2018); Version allemande EN IEC 62138:2019</p> <p>Gesamtumfang 60 Seiten</p> <p>DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE</p>		

Anwendungsbeginn

Anwendungsbeginn für die von CENELEC am 2019-09-09 angenommene Europäische Norm als DIN-Norm ist 2020-07-01.

Für **DIN EN 62138 (VDE 0491-3-3):2010-03** besteht eine Übergangsfrist bis 2022-09-09.

Nationales Vorwort

Vorausgegangener Norm-Entwurf: E DIN IEC 62138 (VDE 0491-3-3):2015-01.

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.

Die enthaltene IEC-Publikation wurde vom SC 45A „Instrumentation, control and electrical power systems of nuclear facilities“ erarbeitet.

Das IEC-Komitee hat entschieden, dass der Inhalt dieses Dokuments bis zu dem Datum (stability date) unverändert bleiben soll, das auf der IEC-Website unter „<http://webstore.iec.ch>“ zu diesem Dokument angegeben ist. Zu diesem Zeitpunkt wird entsprechend der Entscheidung des Komitees das Dokument

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

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 IEC 62138 (VDE 0491-3-3):2020-07**, *Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Softwareaspekte für rechnerbasierte Systeme zur Realisierung von Funktionen der Kategorien B oder C (IEC 62138:2018)*; Deutsche Fassung **EN IEC 62138:2019**
- **DIN EN IEC 61500 (VDE 0491-3-4):2020-04**, *Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Datenkommunikation in Systemen, die Funktionen der Kategorie A ausführen (IEC 61500:2018)*; Deutsche Fassung **EN IEC 61500:2019**
- **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 62859 (VDE 0491-3-8):2017-12**, *Leittechnische Systeme – Anforderungen für die Koordinierung von Sicherheit und IT-Sicherheit (IEC 62859:2016)*
- **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 IEC 60964 (VDE 0491-5-1):2020-07, Kernkraftwerke – Warten – Auslegung (IEC 60964:2018); Deutsche Fassung EN 60964:2019
- DIN EN 62241 (VDE 0491-5-2):2015-06, Kernkraftwerke – Warte – Alarmfunktionen und ihre Darstellung (IEC 62241:2004); Deutsche Fassung EN 62241:2015
- DIN EN 61227 (VDE 0491-5-3):2016-11, Kernkraftwerke – Warten – Handbedienungen (IEC 61227:2008); Deutsche Fassung EN 61227:2016
- 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):2017-02, Kernkraftwerke – Warten – Notsteuerstellen für das Abfahren des Reaktors ohne Verbindung zur Hauptwarte (IEC 60965:2016); Deutsche Fassung EN 60965:2016
- DIN EN IEC 62646 (VDE 0491-5-6):2020-04, Kernkraftwerke – Warten – Rechnerunterstützte Prozeduren (IEC 62646:2016); Deutsche Fassung EN IEC 62646:2019
- 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 IEC 60709 (VDE 0491-7):2020-05, Kernkraftwerke – Leittechnik und elektrische Energieversorgungssysteme mit sicherheitstechnischer Bedeutung – Physikalische und elektrische Trennung (IEC 60709:2018); Deutsche Fassung EN IEC 60709:2019
- DIN EN IEC 61225 (VDE 0491-8) (in Vorbereitung), Kernkraftwerke – Leittechnische System und elektrische Stromversorgungssysteme – Anforderungen an statische unterbrechungsfreie Gleich- und Wechselstrom-Energieversorgungssysteme (IEC 61225:2018); Deutsche Fassung EN IEC 61225:2020
- DIN EN 62808 (VDE 0491-9-3):2020-06, Kernkraftwerke – Leittechnik mit sicherheitstechnischer Bedeutung – Auslegung und Qualifizierung von Isolationseinrichtungen (IEC 62808:2015 + A1:2018); Deutsche Fassung EN 62808:2016 + A1:2019
- 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 IEC/IEEE 62582-1 (VDE 0491-21-1):2020-03, Kernkraftwerke – Leittechnik mit sicherheitstechnischer Bedeutung – Zustandsüberwachung elektrischer Geräte – Teil 1: Allgemeines (IEC/IEEE 62582-1:2011)
- DIN IEC/IEEE 62582-2 (VDE 0491-21-2):2020-03, Kernkraftwerke – Leittechnik mit sicherheitstechnischer Bedeutung – Zustandsüberwachung elektrischer Geräte – Teil 2: Eindringmodul (IEC/IEEE 62582-2:2011)
- DIN IEC/IEEE 62582-3 (VDE 0491-21-3):2020-03, Kernkraftwerke – Leittechnik mit sicherheitstechnischer Bedeutung – Zustandsüberwachung elektrischer Geräte – Teil 3: Reißdehnung (IEC/IEEE 62582-3:2012)
- DIN IEC/IEEE 62582-4 (VDE 0491-21-4):2020-03, Kernkraftwerke – Leittechnik mit sicherheitstechnischer Bedeutung – Zustandsüberwachung elektrischer Geräte – Teil 4: Oxidation (IEC/IEEE 62582-4:2011)
- DIN IEC/IEEE 62582-5 (VDE 0491-21-5):2020-03, Kernkraftwerke – Leittechnik mit sicherheitstechnischer Bedeutung – Zustandsüberwachung elektrischer Geräte – Teil 5: Optische Zeitbereichsreflektometrie (IEC/IEEE 62582-5:2015)
- DIN IEC/IEEE 62582-6 (VDE 0491-21-6):2020-05, Kernkraftwerke – Leittechnik mit sicherheitstechnischer Bedeutung – Zustandsüberwachung elektrischer Geräte – Teil 6: Isolationswiderstand (IEC/IEEE 62582-6:2019)
- DIN EN 62765-1 (VDE 0491-22-1):2018-03, Kernkraftwerke – Leittechnik mit sicherheitstechnischer Bedeutung – Alterungsmanagement von Sensoren und Transmittern – Teil 1: Drucktransmitter (IEC 62765-1:2015); Deutsche Fassung EN 62765-1:2017
- DIN EN IEC 62465 (VDE 0491-22-10):2020-05, Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Alterungsmanagement von elektrischen Kabeln (IEC 62465:2010); Deutsche Fassung EN IEC 62465:2019

DIN EN IEC 62138 (VDE 0491-3-3):2020-07

- **DIN EN 60780-323 (VDE 0491-80):2018-03**, *Kerntechnische Anlagen – Elektrisches Gerät mit sicherheitstechnischer Bedeutung – Qualifizierung (IEC/IEEE 60780-323:2016)*; Deutsche Fassung **EN 60780-323:2017**
- **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**

Änderungen

Gegenüber **DIN EN 62138 (VDE 0491-3-3):2010-03** wurden folgende Änderungen vorgenommen:

- Änderung der Beschreibung des Anwendungsbereichs der Norm dahingehend, dass statt von „Systemen zur Realisierung von Funktionen der Kategorien B oder C“ künftig von „Systemen der Klassen 2 oder 3“ gesprochen wird;
- Harmonisierung der Begriffe mit dem IAEA Safety Glossary und nach der 1. Ausgabe der IEC 62138 erschienenen Ausgaben von relevanten IEC-Normen (**IEC 61513**, **IEC 60880**, **IEC 62566**, IEC 62671);
- Benummerung der Absätze, die Anforderungen oder Empfehlungen enthalten, um die Vergleichbarkeit mit anderen Normen wie z. B. **IEC 60880** zu erleichtern;
- Aufteilung von Anforderungen und Empfehlungen auf separate Absätze;
- Vermeidung von „hanging paragraphs“;
- Aufnahme von Verweisen auf IEC 62645 „Requirements for security programmes for computer-based systems“ anstelle der Unterabschnitte 5.1.6 und 6.1.6 zum Zugriffsschutz;
- Aufnahme von Verweisen auf IEC 62671 „Selection and use of industrial digital devices of limited functionality“ anstelle der Unterabschnitte 5.2.4 und 6.2.4 zur Auswahl und Verwendung spezieller Einrichtungen mit integrierter Software;
- Aktualisierung der normativen Verweisungen;
- Aktualisierung der Literaturhinweise;
- Aufnahme einer mit **IEC 60880** konsistenten Liste typischer Softwaredokumentation als **Anhang A**;
- Aufnahme einer Gegenüberstellung von **IEC 61513** und IEC 62138 nach dem Vorbild der **IEC 60880** als **Anhang B**;
- Aufnahme der Bezüge auf IEC 61508:2010 in einer mit **Anhang D** der **IEC 61513** vergleichbaren Form als **Anhang C**;
- Überarbeitung von **Unterabschnitt 5.2** zur Auswahl vorgefertigter Software
- Aufnahme des Unterabschnitts 5.11 zu Ausfällen gemeinsamer Ursache (CCF) zwecks Konsistenz mit **IEC 60880:2006**;
- redaktionelle Überarbeitung und Klarstellung zuvor nicht ausreichend präzise formulierter Textstellen.

Frühere Ausgaben

DIN IEC 62138 (VDE 0491-3-3): 2004-09

DIN EN 62138 (VDE 0491-3-3): 2010-03

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
–	IAEA SSR-2/1:2016	–	–
–	IAEA GS-R-3	–	–
–	IAEA GS-G-3.1	–	–
–	IAEA GS-G-3.5	–	–
–	IEEE Std 7-4.3.2:2010	–	–
–	DO-178 revision C :2012	–	–
EN ISO 9001:2015	ISO 9001:2015	DIN EN ISO 9001:2015-11	–
–	ISO/IEC 12207:2008 <i>ersetzt durch:</i>	–	–
–	ISO/IEC/IEEE 12207: 2017	–	–
EN ISO/IEC 27001	ISO/IEC 27001 + Cor. 1 + Cor. 2	DIN EN ISO/IEC 27001	–
EN ISO/IEC 27002	ISO/IEC 27002	DIN EN ISO/IEC 27002	–
EN 60671:2011	IEC 60671:2007	DIN EN 60671 (VDE 0491-100):2011-12	VDE 0491-100
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 60987:2015	IEC 60987:2007 + A1:2013	DIN EN 60987 (VDE 0491-3-1):2015-06	VDE 0491-3-1
EN 61131-3	IEC 61131-3	DIN EN 61131-3	–
EN 61226	IEC 61226	DIN EN 61226 (VDE 0491-1)	VDE 0491-1
EN 61508-1:2010	IEC 61508-1:2010	DIN EN 61508-1 (VDE 0803-1):2011-02	VDE 0803-1

Tabelle NA.1 (2 von 2)

Europäisches Dokument	Internationales Dokument	Deutsches Dokument	Klassifikation im VDE-Vorschriftenwerk
EN 61508-2:2010	IEC 61508-2:2010	DIN EN 61508-2 (VDE 0803-2):2011-02	VDE 0803-2
EN 61508-3:2010	IEC 61508-3:2010	DIN EN 61508-3 (VDE 0803-3):2011-02	VDE 0803-3
EN 61508-4:2010	IEC 61508-4:2010	DIN EN 61508-4 (VDE 0803-4):2011-02	VDE 0803-4
EN 61511-1	IEC 61511-1	DIN EN 61511-1 (VDE 0810-1):2011-02	VDE 0810-1
EN 61513:2013	IEC 61513:2011	DIN EN 61513 (VDE 0491-2):2013-09	VDE 0491-2
–	IEC 62342	DIN IEC 62342 (VDE 0491-20-1) zurückgezogen	VDE 0491-20-1
EN 62566	IEC 62566	DIN EN 62566 (VDE 0491-3-5)	VDE 0491-3-5
–	IEC 62645:2014 <i>ersetzt durch:</i>	–	–
EN IEC 62645 ^a	IEC 62645:2019	DIN EN IEC 62645 (VDE 0491-3-7) ^a	VDE 0491-3-7
–	IEC 62671:2013	–	–
–	IEC 63046	–	–
–	ISO 90003:2014 <i>ersetzt durch:</i> ISO/IEC/IEEE 90003: 2018	–	–
^a In Vorbereitung.			

Nationaler Anhang NB (informativ)

Literaturhinweise

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*

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*

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 61131-3, *Speicherprogrammierbare Steuerungen – Teil 3: Programmiersprachen*

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

DIN EN 61508-1 (VDE 0803-1):2011-02, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 1: Allgemeine Anforderungen (IEC 61508-1:2010); Deutsche Fassung EN 61508-1:2010*

DIN EN 61508-2 (VDE 0803-2):2011-02, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 2: Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme (IEC 61508-2:2010); Deutsche Fassung EN 61508-2:2010*

DIN EN 61508-3 (VDE 0803-3):2011-02, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 3: Anforderungen an Software (IEC 61508-3:2010); Deutsche Fassung EN 61508-3:2010*

DIN EN 61508-4 (VDE 0803-4):2011-02, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 4: Begriffe und Abkürzungen (IEC 61508-4:2010); Deutsche Fassung EN 61508-4:2010*

DIN EN 61511-1 (VDE 0810-1), *Funktionale Sicherheit – Sicherheitstechnische Systeme für die Prozessindustrie – Teil 1: Allgemeines, Begriffe, Anforderungen an Systeme, Software und Hardware*

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 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 EN IEC 62645 (VDE 0491-3-7) (in Vorbereitung); *Kernkraftwerke – Leittechnische Systeme – Anforderungen an die IT-Sicherheitsplanung für rechnerbasierte Systeme (IEC 62645:2019); Deutsche Fassung EN IEC 62645:202x)*

DIN EN ISO/IEC 27001, *Informationstechnik – Sicherheitsverfahren – Informationssicherheitsmanagementsysteme – Anforderungen*

DIN EN IEC 62138 (VDE 0491-3-3):2020-07

DIN EN ISO/IEC 27002, *Informationstechnik – Sicherheitsverfahren – Leitfaden für Informationssicherheitsmaßnahmen*

DIN EN ISO 9001:2015-11, *Qualitätsmanagementsysteme – Anforderungen (ISO 9001:2015); Deutsche und Englische Fassung EN ISO 9001:2015*

DIN IEC 62342 (VDE 0491-20-1) (zurückgezogen), *Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Alterungsmanagement*

**Kernkraftwerke –
Leittechnische Systeme mit sicherheitstechnischer Bedeutung –
Softwareaspekte für rechnerbasierte Systeme zur Realisierung von Funktionen
der Kategorien B oder C
(IEC 62138:2018)**

Nuclear power plants –
Instrumentation and control systems important to
safety –
Software aspects for computer-based systems
performing category B or C functions
(IEC 62138:2018)

Centrales nucléaires de puissance –
Systèmes d'instrumentation et de contrôle-
commande importants pour la sûreté –
Aspects logiciels des systèmes informatisés
réalisant des fonctions de catégorie B ou C
(IEC 62138:2018)

Diese Europäische Norm wurde von CENELEC am 2019-09-09 angenommen. CENELEC-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist.

Auf dem letzten Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim CEN-CENELEC Management Centre oder bei jedem CENELEC-Mitglied auf Anfrage erhältlich.

Diese Europäische Norm besteht in drei offiziellen Fassungen (Deutsch, Englisch, Französisch). Eine Fassung in einer anderen Sprache, die von einem CENELEC-Mitglied in eigener Verantwortung durch Übersetzung in seine Landessprache gemacht und dem CEN-CENELEC Management Centre mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

CENELEC-Mitglieder sind die nationalen elektrotechnischen Komitees von Belgien, Bulgarien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, der Republik Nordmazedonien, Rumänien, Schweden, der Schweiz, Serbien, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, der Türkei, Ungarn, dem Vereinigten Königreich und Zypern.



Europäisches Komitee für Elektrotechnische Normung
European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brüssel

© 2019 CENELEC – Alle Rechte der Verwertung, gleich in welcher Form und in welchem Verfahren, sind weltweit den Mitgliedern von CENELEC vorbehalten.

Ref. Nr. EN IEC 62138:2019 D

Europäisches Vorwort

Dieses Dokument (EN IEC 62138:2019) enthält den Text der IEC 62138:2018 die vom SC 45A „Instrumentation, control and electrical power systems of nuclear facilities“ des IEC/TC 45 „Nuclear instrumentation“ erarbeitet wurde.

Nachstehende Daten wurden festgelegt:

- spätestes Datum, zu dem dieses Dokument auf nationaler Ebene durch Veröffentlichung einer identischen nationalen Norm oder durch Anerkennung übernommen werden muss (dop): 2020-09-09
- spätestes Datum, zu dem nationale Normen, die diesem Dokument entgegenstehen, zurückgezogen werden müssen (dow): 2022-09-09

Dieses Dokument ersetzt **EN 62138:2009** und alle Änderungen und Berichtigungen (falls vorhanden).

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. CENELEC ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Wie in der Richtlinie zur nuklearen Sicherheit 2009/71/EURATOM, Kapitel 1, Artikel 2, Punkt 2 angegeben, werden die Mitgliedsstaaten nicht davon abgehalten, strengere Sicherheitsmaßnahmen in dem von der Richtlinie behandelten Gebiet zu fordern, entsprechend dem Gemeinschaftsrecht. In vergleichbarer Weise hält diese Europäische Norm die Mitgliedstaaten nicht davon ab, strengere als die in dieser Norm beschriebenen Maßnahmen zur nuklearen Sicherheit zu fordern.

Anerkennungsnotiz

Der Text der Internationalen Norm IEC 62138:2018 wurde von CENELEC ohne irgendeine Abänderung als Europäische Norm angenommen.

In der offiziellen Fassung sind unter „Literaturhinweise“ zu den aufgelisteten Normen die nachstehenden Anmerkungen einzutragen:

IEC 61508-3:2010	ANMERKUNG	Harmonisiert als EN 61508-3:2010 (nicht modifiziert).
IEC 61508-4:2010	ANMERKUNG	Harmonisiert als EN 61508-4:2010 (nicht modifiziert).
IEC 61511-1:2016	ANMERKUNG	Harmonisiert als EN 61511-1:2016 (nicht modifiziert).
ISO 9001:2015	ANMERKUNG	Harmonisiert als EN ISO 9001:2015 (nicht modifiziert).

Anhang ZA (normativ)

Normative Verweisungen auf internationale Publikationen mit ihren entsprechenden europäischen Publikationen

Die folgenden Dokumente werden im Text in solcher Weise in Bezug genommen, dass einige Teile davon oder ihr gesamter Inhalt Anforderungen des vorliegenden Dokuments darstellen. 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).

ANMERKUNG 1 Ist eine internationale Publikation durch gemeinsame Abänderungen modifiziert worden, gekennzeichnet durch (mod.), dann gilt die entsprechende EN oder das HD.

ANMERKUNG 2 Aktualisierte Informationen über die in diesem Anhang aufgeführten aktuellen Fassungen der Europäischen Normen sind hier verfügbar: www.cenelec.eu.

<u>Publikation</u>	<u>Jahr</u>	<u>Titel</u>	<u>EN/HD</u>	<u>Jahr</u>
IEC 60880	2006	Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category A functions	EN 60880	2009
IEC 61226	–	Nuclear power plants – Instrumentation and control important to safety – Classification of instrumentation and control functions	EN 61226	–
IEC 61513	2011	Nuclear power plants – Instrumentation and control important to safety – General requirements for systems	EN 61513	2013
IEC 62671	2013	Nuclear power plants – Instrumentation and control important to safety – Selection and use of industrial digital devices of limited functionality	–	–

Inhalt

Seite

Europäisches Vorwort.....	2
Anhang ZA (normativ) Normative Verweisungen auf internationale Publikationen mit ihren entsprechenden europäischen Publikationen	3
Einleitung	6
1 Anwendungsbereich	8
2 Normative Verweisungen	8
3 Begriffe	8
4 Symbole und Abkürzungen	17
5 Grundsätzliche Konzepte und Annahmen.....	18
5.1 Allgemeines	18
5.2 Arten von Software	18
5.3 Konfigurationsdatentypen.....	19
5.4 Software- und System-Sicherheitslebenszyklen	19
5.5 Abstufungsprinzipien	21
6 Anforderungen an die Software für leittechnische Systeme der Klassen 2 und 3	22
6.1 Anwendbarkeit der Anforderungen.....	22
6.2 Allgemeine Anforderungen	22
6.2.1 Software-Sicherheitslebenszyklus – Software-Qualitätssicherung	22
6.2.2 Verifizierung.....	23
6.2.3 Konfigurationsmanagement	24
6.2.4 Auswahl und Verwendung von Softwarewerkzeugen	25
6.2.5 Auswahl von Sprachen.....	27
6.3 Auswahl von vorgefertigter Software.....	27
6.3.1 Allgemeines	27
6.3.2 Sicherheitsdokumentation	27
6.3.3 Nachweis der Zuverlässigkeit.....	29
6.3.4 Funktionale Eignung.....	35
6.3.5 Auswahl und Verwendung von industriellen digitalen Geräten mit begrenzter Funktionalität	35
6.4 Softwareanforderungsspezifikation	35
6.4.1 Allgemeines	35
6.4.2 Ziele	35
6.4.3 Eingangsinformationen.....	35
6.4.4 Inhalt.....	36
6.4.5 Eigenschaften.....	37
6.5 Softwareauslegung.....	37
6.5.1 Ziele	37
6.5.2 Eingangsinformationen.....	38
6.5.3 Inhalt.....	38

	Seite
6.5.4 Eigenschaften	39
6.6 Implementierung von Software	40
6.6.1 Allgemeine Anforderungen.....	40
6.6.2 Konfiguration von Software und von Geräten mit Software.....	40
6.6.3 Realisierung in anwendungsorientierten Sprachen	40
6.6.4 Realisierung in allgemeinen Sprachen	41
6.7 Softwareaspekte der Systemintegration	42
6.7.1 Allgemeines.....	42
6.8 Softwareaspekte der Systemvalidierung.....	43
6.8.1 Allgemeines.....	43
6.9 Einrichtung der Software in der Anlage	45
6.9.1 Allgemeines.....	45
6.10 Anomalieberichte	45
6.11 Softwaremodifizierung.....	45
6.11.1 Allgemeines.....	45
6.12 Maßnahmen gegen Fehler aufgrund gemeinsamer Ursache (CCF) infolge Software	47
Anhang A (informativ) Typische Liste einer Softwaredokumentation	48
Anhang B (informativ) Entsprechungen zwischen IEC 61513:2011 und diesem Dokument.....	49
Anhang C (informativ) Zusammenhang dieses Dokuments mit IEC 61508.....	50
C.1 Allgemeines.....	50
C.2 Vergleich von Anwendungsbereich und Konzepten	50
C.3 Zusammenhang zwischen diesem Dokument und IEC 61508-3:2010.....	51
Literaturhinweise	52
Bilder	
Bild 1 – Typische Softwareteile in einem rechnerbasierten leittechnischen System	18
Bild 2 – Tätigkeiten im System-Sicherheitslebenszyklus (nach IEC 61513:2011).....	19
Bild 3 – Softwarebezogene Tätigkeiten im System-Sicherheitslebenszyklus	20
Bild 4 – Entwicklungstätigkeiten im Software-Sicherheitslebenszyklus nach IEC 62138	21
Bild 5 – Überblick über den typischen Qualifizierungsprozess von vorgefertigter kompletter Betriebssystemsoftware	30
Bild 6 – Überblick über den typischen Qualifizierungsprozess für vorgefertigte Softwarekomponenten	31
Tabellen	
Tabelle A.1 – Typische Liste einer Softwaredokumentation	48
Tabelle B.1 – Entsprechungen zwischen IEC 61513:2011 und diesem Dokument.....	49
Tabelle C.1 – Zusammenhang zwischen diesem Dokument und IEC 61508-3:2010	51

Einleitung

a) Technischer Hintergrund, hauptsächliche Inhalte und Organisation der Norm

Diese Internationale Norm enthält Anforderungen für die Software von rechnerbasierten leittechnischen Systemen, die Funktionen der Kategorien B oder C nach der IEC 61226 ausführen. Sie ergänzt IEC 60880, die Anforderungen für die Software von rechnerbasierten leittechnischen Systemen, die Kategorie-A-Funktionen ausführen, enthält.

Sie ist konsistent mit und ergänzend zu IEC 61513:2011. Hauptsächlich auf Systemebene ablaufende Tätigkeiten (z. B. Integration, Validierung, Errichtung) sind in dieser Norm nicht erschöpfend behandelt; bezüglich nicht softwarespezifischer Anforderungen wird auf IEC 61513:2011 verwiesen.

Dieses Dokument berücksichtigt die derzeitigen Praktiken für die Entwicklung von Software leittechnischer Systeme, insbesondere

- die Verwendung von vorgefertigter Software sowie vorgefertigten Geräten und Gerätefamilien, die nicht notwendigerweise entsprechend den Normen der Nuklearindustrie ausgelegt wurden;
- die Verwendung anwendungsorientierter Sprachen

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

IEC 61513 ist ein Dokument der ersten Ebene der Normen des IEC/SC 45A und gibt Anleitungen zur Leittechnik auf Systemebene.

IEC 62138 ist ein SC-45A-Dokument der zweiten Ebene, das IEC 61513 hinsichtlich Softwareentwicklung von rechnerbasierten leittechnischen Systemen, die Kategorie-B- oder -C-Funktionen ausführen, ergänzt.

Mehr Details über die Struktur der Normen des IEC/SC 45A finden sich in Abschnitt d) dieser Einleitung.

c) Empfehlungen und Einschränkungen betreffend die Anwendung dieser Norm

Es ist nicht beabsichtigt, dass dieses Dokument als allgemeine Software-Engineering-Anleitung Verwendung findet. Es gilt für Software von leittechnischen Systemen, die Kategorie-B- oder -C-Funktionen ausführen sowohl für neue Kernkraftwerke als auch für Um- und Nachrüstung von bestehenden Kraftwerken.

Für bestehende Kraftwerke ist nur eine Teilmenge der Anforderungen anwendbar, und diese Teilmenge ist am Anfang jedes Projekts zu ermitteln.

Der Zweck der Anleitung, die diese Norm vermittelt, ist es, soweit wie möglich das Potenzial für latente Softwarefehler, die entweder durch Einzelsoftwarefehler oder durch Mehrfachsoftwarefehler (d. h. gemeinsam verursachte Ausfälle infolge von Software) Systemversagen verursachen können, zu reduzieren.

Dieses Dokument behandelt nicht explizit, wie man Software gegen jene Bedrohungen, die aus böswilligen Angriffen auf rechnerbasierte Systeme entstehen, schützt, d. h. IT-Sicherheit. IEC 62645 enthält Anforderungen für IT-Sicherheitsprogramme von rechnerbasierten Systemen.

Um sicherzustellen, dass dieses Dokument über längere Zeit relevant bleibt, wurde der Schwerpunkt eher auf prinzipielle Themen gelegt und nicht auf spezifische Technologien.

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

Die Eingangsdokumente der Normen des IEC/SC 45A sind IEC 61513 und IEC 63046. IEC 61513 enthält allgemeine Anforderungen an die leittechnischen Systeme und Geräte, die zur Ausführung sicherheitstechnisch wichtiger Funktionen in Kernkraftwerken genutzt werden. IEC 63046 enthält allgemeine Anforderungen für elektrische Energiesysteme von Kernkraftwerken, sie umfasst Stromversorgungssysteme einschließlich der Versorgungssysteme für die Leittechnik. IEC 61513 und IEC 63046 sind miteinander und gleichrangig zu

berücksichtigen. Durch IEC 61513 und IEC 63046 werden die Normen des IEC/SC 45A strukturiert und ein komplettes Rahmenwerk allgemeiner Anforderungen für leittechnische und elektrische Systeme von Kernkraftwerken aufgebaut.

In IEC 61513 und IEC 63046 wird für allgemeine Themen direkt auf andere Normen des IEC/SC 45A verwiesen, dazu gehören die Kategorisierung von Funktionen und Klassifizierung von Systemen, Qualifizierung, Trennung, Maßnahmen gegen Ausfälle aufgrund gemeinsamer Ursache (CCF), Wartenauslegung, elektromagnetische Verträglichkeit, Cybersicherheit, Software- und Hardwareaspekte programmierbarer digitaler Systeme, Koordination von Maßnahmen zur Sicherheit und IT-Sicherheit sowie Alterungsmanagement. Die Normen, auf die direkt verwiesen wird, bilden die zweite Ebene und sollten zusammen mit IEC 61513 und IEC 63046 als ein in sich konsistenter Satz von Dokumenten betrachtet werden.

Die dritte Ebene bilden Normen des IEC/SC 45A, auf die in IEC 61513 oder IEC 63046 nicht direkt verwiesen wird, dazu gehören Normen für spezielles Gerät, technische Verfahren 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 um Technische Berichte, die nicht normativ sind.

In den Normen des IEC/SC 45A werden die Prinzipien und grundsätzlichen Aspekte der Sicherheit und IT-Sicherheit der IAEA-Sicherheitsstandards und der relevanten Dokumente der IAEA-Standards zur nuklearen IT-Sicherheit (NSS) umgesetzt und detailliert. Dies betrifft insbesondere Anforderungen des IAEA Safety Standards SSR-2/1, in dem die Sicherheitsanforderungen für die Auslegung von Kernkraftwerken festgeschrieben werden, und der IAEA Safety Guides SSG-30 für die Sicherheitsklassifikation der Strukturen, Systeme und Komponenten in Kernkraftwerken, SSG-39 für die Auslegung der Leittechnik in Kernkraftwerken und SSG-34 für die Auslegung der Stromversorgung in Kernkraftwerken und des IAEA Implementing Guides NSS 17 für die IT-Sicherheit von Rechnern in kerntechnischen Anlagen. Terminologie und Definitionen in den Normen des IEC/SC 45A sind konsistent mit denen, die von der IAEA verwendet werden.

Für IEC 61513 und IEC 63046 wird ein Darstellungsformat verwendet, das dem der grundlegenden Sicherheitsnorm IEC 61508 ähnlich ist, mit einem Lebenszyklus als Gesamtrahmen und einem Systemlebenszyklus. Mit IEC 61513 und IEC 63046 werden 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, IEC 62138 und IEC 62566 bezogen auf den nuklearen Sektor der IEC 61508-3. IEC 61513 und IEC 63046 beziehen sich bei den Themen der Qualitätssicherung (QS) sowohl auf ISO als auch auf IAEA GS-R-3, IAEA GS-G-3.1 und IAEA GS-G-3.5. Auf Ebene 2 ist IEC 62645 das Eingangsdokument für die Normen des IEC/SC 45A zur IT-Sicherheit. Es baut auf die übergeordneten Prinzipien und Hauptkonzepte der generischen IT-Sicherheitsstandards auf, insbesondere auf ISO/IEC 27001 und ISO/IEC 27002; wobei es jene für die Anwendung im nuklearen Kontext adaptiert und vervollständigt sowie mit IEC 62443 koordiniert. Auf Ebene 2 ist IEC 60964 das Eingangsdokument für die Normen des IEC/SC 45A zu Warten, und IEC 62342 das Eingangsdokument für die Normen des IEC/SC 45A zum Alterungsmanagement.

ANMERKUNG 1 Es wird angenommen, dass für die Auslegung von leittechnischen Systemen in Kernkraftwerken, die konventionelle Sicherheitsfunktionen enthalten (z. B. in Bezug auf Arbeitssicherheit, Schutz von Vermögenswerten, chemische und prozesstechnische Gefährdungen), internationale und nationale Normen angewendet werden.

ANMERKUNG 2 Der Arbeitsbereich des IEC/SC 45A wurde 2013 erweitert, um auch elektrische Systeme abzudecken. In den Jahren 2014 und 2015 wurde in IEC/SC 45A diskutiert, wie und wo allgemeine Anforderungen für die Auslegung elektrischer Systeme behandelt werden sollten. Die Experten des IEC/SC 45A empfahlen, eine selbständige Norm auf derselben Ebene wie IEC 61513 zu entwickeln und allgemeine Anforderungen für elektrische Systeme aufzustellen. Dazu wurde jetzt das Projekt IEC 63046 gestartet. Sobald IEC 63046 veröffentlicht wird, verliert diese Anmerkung 2 der Einleitung der Normen ihre Gültigkeit.

1 Anwendungsbereich

Dieses Dokument legt Anforderungen für die Software von rechnerbasierten leittechnischen Systemen, die Funktionen der Kategorien B oder C nach IEC 61226 ausführen, fest. Sie ergänzt IEC 60880, die Anforderungen an die Software von rechnerbasierten leittechnischen Systemen, die Kategorie-A-Funktionen ausführen, enthält.

Es ist konsistent mit und ergänzend zu IEC 61513. Hauptsächlich auf Systemebene ablaufende Tätigkeiten (z. B. Integration, Validierung, Errichtung) sind in dieser Norm nicht erschöpfend behandelt; bezüglich nicht softwarespezifischer Anforderungen wird auf IEC 61513 verwiesen.

Die Verbindung zwischen Funktionskategorien und Systemklassen ist in IEC 61513 festgelegt. Da ein gegebenes sicherheitsklassifiziertes Leittechniksystem Funktionen unterschiedlicher Sicherheitskategorien und sogar nichtklassifizierte Funktionen ausführen darf, sind die Anforderungen in diesem Dokument den Sicherheitsklassen eines Leittechniksystems (Klasse 2 oder 3) zugeordnet.

Es ist nicht beabsichtigt, dass dieses Dokument als allgemeine Software-Engineering-Anleitung Verwendung findet. Sie gilt für Software von leittechnischen Systemen der Sicherheitsklassen 2 oder 3 sowohl für neue Kernkraftwerke als auch für die Um- und Nachrüstung von bestehenden Kraftwerken.

Für bestehende Kraftwerke ist nur eine Teilmenge der Anforderungen anwendbar, und diese Teilmenge ist am Anfang jedes Projekts zu ermitteln.

Der Zweck der Anleitung, die dieses Dokument vermittelt, ist es, soweit wie möglich das Potenzial für latente Softwarefehler, die entweder durch Einzelsoftwarefehler oder durch Mehrfachsoftwarefehler (d. h. gemeinsam verursachte Ausfälle infolge von Software) Systemversagen verursachen können, zu reduzieren.

Dieses Dokument behandelt nicht explizit wie man Software gegen jene Bedrohungen, die aus böswilligen Angriffen auf rechnerbasierte Systeme entstehen, schützt, d. h. IT-Sicherheit. IEC 62645 enthält Anforderungen für IT-Sicherheitsprogramme von rechnerbasierten Systemen.

2 Normative Verweisungen

Die folgenden Dokumente werden im Text in solcher Weise in Bezug genommen, dass einige Teile davon oder ihr gesamter Inhalt Anforderungen des vorliegenden Dokuments darstellen. 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 60880:2006, *Nuclear power plants – Instrumentation and control systems important to safety – Requirements for computer-based systems performing category A functions*

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

IEC 61513:2011, *Nuclear power plants – Instrumentation and control systems important to safety – General requirements for systems*

IEC 62671:2013, *Nuclear power plants – Instrumentation and control systems important to safety – Selection and use of industrial digital devices of limited functionality*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

ISO und IEC stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

- IEC Electropedia: verfügbar unter <http://www.electropedia.org/>
- ISO Online Browsing Platform: verfügbar unter <http://www.iso.org/obp>

3.1

Animation

(en: animation)

Prozess, durch den das in einer Spezifikation festgelegte Verhalten mit aktuellen Werten angezeigt wird, abgeleitet aus den Gleichungen für dieses Verhalten und einigen Eingangswerten

[QUELLE: IEC 60880:2006, 3.1]

3.2

Anwendungsfunktion

(en: application function)

Funktion eines leittechnischen Systems, die eine Aufgabe in Verbindung mit dem gesteuerten Prozess und nicht mit dem Funktionieren des Systems selbst erfüllt

[QUELLE: IEC 61513:2011, 3.1]

3.3

Anwendungssoftware

(en: application software)

Teil der Software eines leittechnischen Systems, durch den Anwendungsfunktionen realisiert werden

Anmerkung 1 zum Begriff: Anwendungssoftware im Gegensatz zu Systemsoftware.

Anmerkung 2 zum Begriff: Anwendungssoftware ist anlagenspezifisch, daher wird sie nicht als vorgefertigte Software angesehen.

[QUELLE: IEC 61513:2011, 3.2 modifiziert (modifizierte Anmerkungen zum Begriff)]

3.4

anwendungsorientierte Sprache

(en: application-oriented language)

Rechnersprache, die speziell für bestimmte Anwendungsarten entwickelt und von Personen verwendet wird, die Spezialisten in diesen Anwendungsarten sind

Anmerkung 1 zum Begriff: Gerätefamilien verwenden üblicherweise anwendungsorientierte Sprachen, um damit eine leicht nutzbare Möglichkeit für die Anpassung des Geräts an spezifische Anforderungen zur Verfügung zu stellen.

Anmerkung 2 zum Begriff: Anwendungsorientierte Sprachen können verwendet werden, um spezielle funktionale Anforderungen an ein leittechnisches System festzulegen und/oder Anwendungssoftware zu spezifizieren und/oder zu entwickeln. Sie dürfen auf Text, Grafik oder beidem beruhen.

Anmerkung 3 zum Begriff: Beispiele: Sprachen für Funktionsblockdiagramme, Sprachen definiert nach IEC 61131-3.

Anmerkung 4 zum Begriff: Siehe auch „allgemeine Sprache“.

[QUELLE: IEC 60880:2006, 3.3 modifiziert (Anmerkung 4 zum Begriff wurde hinzugefügt)]

3.5

Ausfall aufgrund gemeinsamer Ursache

(en: common cause failure, CCF)

Versagen von zwei oder mehr Strukturen, Systemen oder Komponenten aufgrund eines einzelnen spezifischen Ereignisses oder Grunds

Anmerkung 1 zum Begriff: Gemeinsame Ursachen können innerhalb oder außerhalb eines leittechnischen Systems auftreten.

[QUELLE: IAEA Safety Glossary, Ausgabe 2016]

3.6

Komplexität

(en: complexity)

Schwierigkeitsgrad der Verständlichkeit und Verifizierbarkeit eines Systems oder einer Komponente aufgrund von Auslegung, Realisierung oder Verhalten

[QUELLE: IEC 61513:2011, 3.9]

3.7

Rechnerprogramm

(en: computer program)

Satz geordneter Instruktionen und Daten, in dem Rechengänge in einer für den Rechner geeigneten Form spezifiziert werden

Anmerkung 1 zum Begriff: Dies schließt traditionelle Programme ein, die in allgemeinen Sprachen geschrieben sind. Eingeschlossen sind auch Programme in anwendungsorientierten Sprachen.

[QUELLE: IEC 60880:2006, 3.10, modifiziert (Anmerkung 1 zum Begriff wurde hinzugefügt)]

3.8

rechnerbasierte Betrachtungseinheit

(en: computer-based item)

Betrachtungseinheit, die auf Softwareanweisungen beruht, die auf einem Mikroprozessor oder Mikrocontroller ablaufen

Anmerkung 1 zum Begriff: In dieser Definition kann die Benennung Betrachtungseinheit durch die Benennungen System, Ausrüstung oder Gerät ersetzt werden.

Anmerkung 2 zum Begriff: Eine rechnerbasierte Betrachtungseinheit ist eine Art von programmierbaren digitalen Betrachtungseinheiten.

Anmerkung 3 zum Begriff: Dieser Begriff ist gleichbedeutend mit softwarebasierter Betrachtungseinheit.

3.9

Konfigurationsmanagement

(en: configuration management)

Prozess, in dem die Eigenschaften von Strukturen, Systemen und Komponenten einer Anlage (einschließlich Rechnersysteme und Software) festgelegt und dokumentiert werden, und in dem sichergestellt wird, dass Änderungen dieser Eigenschaften in geeigneter Weise geplant, bewertet, bestätigt, ausgestellt, realisiert, verifiziert, dokumentiert und in die Anlagendokumentation integriert werden

[QUELLE: IAEA Safety Glossary, Ausgabe 2016]

3.10

IT-Sicherheit

(en: cybersecurity)

Satz von Tätigkeiten und Maßnahmen zur Vorbeugung, zum Erkennen und Reagieren auf digitale Angriffe, die die Absicht haben, Folgendes zu bewirken:

- Offenlegung von Informationen (Vertraulichkeit), die zur Ausführung von böswilligen Handlungen ausgenutzt werden könnten, was dann zu einem Störfall, einer unsicheren Situation oder der Verschlechterung der Leistungsfähigkeit der Anlage führen könnte,
- böswillige Modifikationen (Integrität) von Funktionen, was die Bereitstellung oder Integrität einer von den programmierbaren digitalen Leittechniksystemen (CB & HDP) geforderten Leistung (einschließlich des Verlustes der Steuerung) beeinträchtigen und dann zu einem Störfall, einer unsicheren Situation oder der Verschlechterung der Leistungsfähigkeit der Anlage führen könnte,
- böswilliges Zurückhalten oder Unterbinden eines Zugriffs auf oder eines Austauschs von Informationen, Daten oder Hilfsmitteln (einschließlich Verlust der Ansicht), was zur Beeinträchtigung einer von Leittechniksystemen geforderten Dienstleistung (Verfügbarkeit) und infolge dessen zu einem Störfall, einer unsicheren Situation oder der Verschlechterung der Leistungsfähigkeit der Anlage führen könnte.

Anmerkung 1 zum Begriff: Diese Definition ist auf den Anwendungsbereich der IEC 62645 zugeschnitten, die sich auf den Schutz vor, Entdeckung von und Reaktion auf böswillige Handlungen gegen leittechnische rechnerbasierte und HDL-programmierte Systeme durch digitale Mittel richtet. Es wird anerkannt, dass der Begriff „IT-Sicherheit“ in anderen Normen und Anleitungen eine umfassendere Bedeutung besitzt und oftmals nichtböswillige Bedrohungen, Bedienfehler und Schutz vor Naturkatastrophen einschließt, die alle außerhalb des Anwendungsbereichs der IEC 62645 liegen.

[QUELLE: IEC 62645:2014, 3.6, modifiziert (Anmerkung 2 zum Begriff wurde gestrichen)]