DIN EN IEC 62566-2 (VDE 0491-3-9)

DIN

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

VDE

ICS 27.120.20

Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Entwicklung HDL-programmierter integrierter Schaltkreise – Teil 2: HDL-programmierte integrierte Schaltkreise für Systeme, die Funktionen der Kategorie B oder C ausführen (IEC 62566-2:2020); Deutsche Fassung EN IEC 62566-2:2020

Nuclear power plants – Instrumentation and control systems important to safety – Development of HDL-programmed integrated circuits – Part 2: HDL-programmed integrated circuits for systems performing category B or C functions (IEC 62566-2:2020); German version EN IEC 62566-2:2020

Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Développement des circuits intégrés programmés en HDL – Partie 2: Circuits intégrés programmés en HDL pour les systèmes réalisant des fonctions de catégorie B ou C (IEC 62566-2:2020); Version allemande EN IEC 62566-2:2020

Gesamtumfang 70 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE

Documents
Document Sharing Hub

Full document details: DIN EN IEC 62566-2:2021-11

Anwendungsbeginn

Anwendungsbeginn für die von CENELEC am 2020-11-16 angenommene Europäische Norm als DIN-Norm ist 2021-11-01.

Nationales Vorwort

Vorausgegangener Norm-Entwurf: E DIN IEC 62566-2 (VDE 0491-3-9):2017-10.

Für dieses Dokument ist das nationale Arbeitsgremium DKE/UK 967.1 „Elektro- und Leittechnik für kerntechnische Anlagen“ der DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE (www.dke.de) zuständig.

Aktuelle Informationen zu diesem Dokument können über die Internetseiten von DKE (www.dke.de) und DIN (www.din.de) durch eine Suche nach der Dokumentennummer aufgerufen werden.

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

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 diesem Dokument werden folgenden Schriftarten verwendet:

- *Anforderungen und Empfehlungen, die speziell für Systeme der Klasse 3 oder der Klasse 2 gelten, sind in Kursivschrift*

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*

Documents
Document Sharing Hub

Full document details: DIN EN IEC 62566-2:2021-11

- DIN EN IEC 62645 (VDE 0491-3-7):2021-03, *Kernkraftwerke – Leittechnische und elektrische Systeme – Anforderungen an die IT-Sicherheit (IEC 62645:2019); Deutsche Fassung EN IEC 62645:2020*
- DIN EN IEC 62859 (VDE 0491-3-8):2021-07, *Kernkraftwerke – Leittechnische Systeme – Anforderungen für die Koordinierung von Sicherheit und IT-Sicherheit (IEC 62859:2016 + A1:2019); Deutsche Fassung EN IEC 62859:2020*
- DIN EN IEC 62566-2 (VDE 0491-3-9):2021-11, *Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Entwicklung HDL-programmierter integrierter Schaltkreise – Teil 2: HDL-programmierte integrierte Schaltkreise für Systeme, die Funktionen der Kategorie B oder C ausführen (IEC 62566-2:2020); Deutsche Fassung EN IEC 62566-2:2020*
- 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):2020-08, *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 0491-8-3):2020-11, *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 EN IEC 62003 (VDE 0491-11):2021-08, *Kernkraftwerke – Elektro- und leittechnische Systeme mit sicherheitstechnischer Bedeutung – Anforderungen für die Prüfung der elektromagnetischen Verträglichkeit (IEC 62003:2020); Deutsche Fassung EN IEC 62003:2020*
- 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)*

Documents
Document Sharing Hub
Full document details: DIN EN IEC 62566-2:2021-11

- 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 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*

Documents
Document Sharing Hub

Full document details: DIN EN IEC 62566-2:2021-11

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

Europäisches Dokument	Internationales Dokument	Deutsches Dokument	Klassifikation im VDE-Vorschriftenwerk
EN ISO/IEC 27001	ISO/IEC 27001	DIN EN ISO/IEC 27001	–
EN ISO/IEC 27002	ISO/IEC 27002	DIN EN ISO/IEC 27002	–
–	IEC 60050-521:2002	a	–
EN 60671:2011	IEC 60671:2007	DIN EN 60671 (VDE 0491-100):2011-12	VDE 0491-100
EN 60780-232:2017	IEC/IEEE 60780-323:2016	DIN EN 60780-323 (VDE 0491-80):2018-03	VDE 0491-80
EN 60880:2009	IEC 60880:2006	DIN EN 60880 (VDE 0491-3-2):2010-03	VDE 0491-3-2
EN IEC 60964	IEC 60964	DIN EN IEC 60964 (VDE 0491-5-1)	VDE 0491-5-1
EN 60987	IEC 60987	DIN EN 60987 (VDE 0491-3-1)	VDE 0491-3-1
EN 61131-3	IEC 61131-3	DIN EN 61131-3	–
–	–	DIN EN 61131-3 Bbl 1	–
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
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 61513:2013	IEC 61513:2011	DIN EN 61513 (VDE 0491-2):2013-09	VDE 0491-2
EN IEC 62138:2019	IEC 62138:2018	DIN EN IEC 62138 (VDE 0491-3-3):2020-07	VDE 0491-3-3

AVA Documents
Document Sharing Hub

Full document details: DIN EN IEC 62566-2:2021-11

Europäisches Dokument	Internationales Dokument	Deutsches Dokument	Klassifikation im VDE-Vorschriftenwerk
EN 62340	IEC 62340	DIN EN 62340 (VDE 0491-10)	VDE 0491-10
–	IEC 62342:2007	E DIN IEC 62342 (VDE 0491-20-1):2012-03 zurückgezogen	VDE 0491-20-1
EN IEC 62443 (alle Teile)	IEC 62443 (alle Teile)	DIN EN IEC 62443 (VDE 0802) (alle Teile)	VDE 0802
EN 62566:2014	IEC 62566:2012	DIN EN 62566 (VDE 0491-3-5):2015-02	VDE 0491-3-5
EN IEC 62645	IEC 62645	DIN EN IEC 62645 (VDE 0491-3-7)	VDE 0491-3-7
EN IEC 63046	IEC 63046	DIN EN IEC 63046 (VDE 0491-8-2)[b]	VDE 0491-8-2
[a] „Internationales Elektrotechnisches Wörterbuch – Deutsche Ausgabe“, Online-Zugang: https://www.dke.de/dke-iev.			
[b] In Vorbereitung.			

Documents
Document Sharing Hub

Full document details: DIN EN IEC 62566-2:2021-11

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 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 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 60987 (VDE 0491-3-1), *Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Anforderungen an die Hardware-Auslegung*

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

DIN EN 61131-3 Beiblatt 1, *Speicherprogrammierbare Steuerungen – Leitlinien für die Anwendung und Implementierung von Programmiersprachen für Speicherprogrammierbare Steuerungen*

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 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 62340 (VDE 0491-10), *Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Anforderungen zur Beherrschung von Versagen aufgrund gemeinsamer Ursache*

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

AVA Documents
Document Sharing Hub

Full document details: DIN EN IEC 62566-2:2021-11

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 62443 (VDE 0802) (alle Teile), *IT-Sicherheit für industrielle Automatisierungssysteme*

DIN EN IEC 62645 (VDE 0491-3-7), *Kernkraftwerke – Leittechnische und elektrische Systeme – Anforderungen an die IT-Sicherheit*

DIN EN IEC 63046 (VDE 0491-8-2) (in Vorbereitung), *Kernkraftwerke – Elektrische Systeme – Allgemeine Anforderungen*

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

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

Entwurf DIN IEC 62342 (VDE 0491-20-1):2012-03 (zurückgezogen), *Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Alterungsmanagement (IEC 62342:2007)*

Documents
Document Sharing Hub

Full document details: DIN EN IEC 62566-2:2021-11

EUROPÄISCHE NORM

EUROPEAN STANDARD

NORME EUROPÉENE

EN IEC 62566-2

November 2020

ICS 27.120.20

Deutsche Fassung

Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Entwicklung HDL-programmierter integrierter Schaltkreise – Teil 2: HDL-programmierte integrierte Schaltkreise für Systeme, die Funktionen der Kategorie B oder C ausführen (IEC 62566-2:2020)

Nuclear power plants – Instrumentation and control systems important to safety – Development of HDL-programmed integrated circuits – Part 2: HDL-programmed integrated circuits for systems performing category B or C functions
(IEC 62566-2:2020)

Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Développement des circuits intégrés programmés en HDL – Partie 2: Circuits intégrés programmés en HDL pour les systèmes réalisant des fonctions de catégorie B ou C
(IEC 62566-2:2020)

Diese Europäische Norm wurde von CENELEC am 2020-11-16 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.

CENELEC

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

© 2020 CENELEC Alle Rechte der Verwertung, gleich in welcher Form und in welchem Verfahren, sind weltweit den Mitgliedern von CENELEC vorbehalten.

Documents
Document Sharing Hub

Ref. Nr. EN IEC 62566-2:2020 D

Full document details: DIN EN IEC 62566-2:2021-11

Europäisches Vorwort

Dieses Dokument (EN IEC 62566-2:2020) enthält den Text der IEC 62566-2:2020, die vom IEC/SC 45A „Instrumentation and control 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):	2021-11-16
– spätestes Datum, zu dem nationale Normen, die diesem Dokument entgegenstehen, zurückgezogen werden müssen	(dow):	2023-11-16

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.

Auf vergleichbare Weise hindert diese Europäische Norm die Mitgliedsstaaten nicht daran, im Geltungsbereich dieser Europäischen Norm strengere Maßnahmen bezüglich der nuklearen Sicherheit zu fordern.

Anerkennungsnotiz

Der Text der Internationalen Norm IEC 62566-2:2020 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/IEEE 60780-323:2016	ANMERKUNG	Harmonisiert als EN 60780-323:2017 (nicht modifiziert)
IEC 61508-1:2010	ANMERKUNG	Harmonisiert als EN 61508-1:2010 (nicht modifiziert).
IEC 61508-2:2010	ANMERKUNG	Harmonisiert als EN 61508-2:2010 (nicht modifiziert).
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 62645	ANMERKUNG	Harmonisiert als EN IEC 62645.

Documents
Document Sharing Hub

Full document details: DIN EN IEC 62566-2:2021-11

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.

Publikation	Jahr	Titel	EN/HD	Jahr
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 60987	–	Nuclear power plants – Instrumentation and control important to safety – Hardware design requirements for computer-based systems	EN 60987	–
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 62138	2018	Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category B or C functions	EN IEC 62138	2019
IEC 62340	–	Nuclear power plants – Instrumentation and control systems important to safety – Requirements for coping with common cause failure (CCF)	EN 62340	–
IEC 62566	2012	Nuclear power plants – Instrumentation and control important to safety – Development of HDL-programmed integrated circuits for systems performing category A functions	EN 62566	2014

Documents
Document Sharing Hub
Full document details: DIN EN IEC 62566-2:2021-11

Inhalt

Seite

Europäisches Vorwort ... 10

Anhang ZA (normativ) Normative Verweisungen auf internationale Publikationen mit ihren entsprechenden europäischen Publikationen ... 11

Einleitung ... 16

1 Anwendungsbereich ... 19

2 Normative Verweisungen ... 19

3 Begriffe ... 20

4 Symbole und Abkürzungen ... 28

5 Allgemeine Anforderungen für HPD-Projekte ... 29

5.1 Allgemeines ... 29

5.2 Lebenszyklus ... 29

5.3 Abstufungsprinzipien ... 31

5.4 HPD-Qualitätssicherung ... 32

5.4.1 Allgemeines ... 32

5.5 Konfigurationsmanagement ... 33

5.5.1 Allgemeines ... 33

5.6 HPD-Verifizierung ... 34

6 HPD-Anforderungsspezifikation ... 35

6.1 Allgemeines ... 35

6.1.1 Überblick ... 35

6.2 Funktionale Aspekte der Anforderungsspezifikation ... 36

6.2.1 Allgemeines ... 36

6.3 Fehlerentdeckung und Fehlertoleranz ... 37

6.4 Anforderungserfassung unter Benutzung von ESL-Werkzeugen ... 37

6.4.1 Allgemeines ... 37

6.4.2 Anforderungen an den Formalismus von Werkzeugen, die auf ESL-Ebene verwendet werden ... 37

6.4.3 Schnittstellen mit Auslegungswerkzeugen ... 37

7 Annahmeverfahren für programmierbare integrierte Schaltkreise, interne Blöcke und vorentwickelte Blöcke ... 38

7.1 Allgemeines ... 38

7.2 Annahmeprozess für programmierbare integrierte Schaltkreise und eingeschlossene interne Blöcke ... 38

7.2.1 Allgemeines ... 38

7.2.2 Annahme integrierter Schaltkreise ... 39

7.3 Annahmeprozess für PDBs ... 39

7.3.1 Allgemeines ... 39

7.3.2 Funktionale Eignung von PDBs ... 40

7.3.3 Sicherheitsdokumentation von PDBs ... 40

Documents
Document Sharing Hub

Full document details: DIN EN IEC 62566-2:2021-11

7.3.4 Erstellung unterstützender Sicherheitsdokumentation 41
7.3.5 Ergänzende Mittel 43
7.3.6 Verwendungsregeln 43
7.3.7 Änderung für die Annahme 44
8 HPD-Auslegung und -Realisierung 44
8.1 Allgemeines 44
8.2 Hardware-Beschreibungssprachen (HDL) und zugehörige Werkzeuge 44
8.2.1 Allgemeines 44
8.3 Auslegung 45
8.3.1 Allgemeines 45
8.3.2 Fehlerentdeckung 46
8.3.3 Sprach- und Kodierungsregeln 46
8.3.4 Synchrone vs. asynchrone Auslegung 47
8.3.5 Management der Energieversorgung 48
8.3.6 Auslegungsdokumentation 48
8.4 Realisierung 48
8.4.1 Produkte 48
8.4.2 Dateien von Parametern und Randbedingungen 49
8.4.3 Post-route-Analyse 49
8.4.4 Durch Werkzeuge eingebrachte oder entfernte Redundanzen 49
8.4.5 Zustandsmaschinen 49
8.4.6 Statische Zeitanalyse 49
8.4.7 Dokumentation der Realisierung 50
8.5 Werkzeuge auf Systemebene und automatische Codeerzeugung 50
8.5.1 Allgemeines 50
9 Integration und Prüfung der HPD 51
9.1 Allgemeines 51
9.2 Testumgebungen für die funktionale Simulation der HPD 51
9.3 Testabdeckung 52
9.4 Testdurchführung 52
10 HPD-Aspekte der Systemintegration 53
10.1 Allgemeines 53
10.2 Anforderungen 53
11 HPD-Aspekte der Systemvalidierung 53
11.1 Allgemeines 53
11.2 Anforderungen 53
12 Änderungen 55
12.1 Änderung der Anforderungen, Auslegung oder Realisierung 55
12.1.1 Allgemeines 55

Documents
Document Sharing Hub
Full document details: DIN EN IEC 62566-2:2021-11

12.2 Änderung der mikroelektronischen Technologie ... 56
13 HPD-Produktion ... 56
13.1 Allgemeines ... 56
13.2 Produktionsprüfungen ... 57
13.3 Programmierungsdateien und -tätigkeiten ... 57
14 HPD-Aspekte von Installation, Abnahme und Betrieb ... 57
14.1 Allgemeines ... 57
14.1.1 Überblick ... 57
14.2 Anomalieberichte ... 58
15 Softwarewerkzeuge für die Entwicklung von HPDs ... 58
15.1 Allgemeines ... 58
15.1.1 Überblick ... 58
15.2 Zusätzliche Anforderungen für Werkzeuge zur Auslegung, Implementierung und Simulation ... 59
16 Segmentierung oder Aufteilung der Auslegung ... 59
16.1 Hintergrund ... 59
16.2 Hilfs- oder Unterstützungsfunktionen ... 60
16.2.1 Allgemeines ... 60
16.2.2 Aufteilung von Hilfs- oder Unterstützungsfunktionen oder Funktionen einer untergeordneten Sicherheitskategorie ... 60
17 Maßnahmen gegen Versagen aufgrund gemeinsamer Ursache (CCF) in HPD ... 61
Anhang A (informativ) Dokumentation ... 62
A.1 Allgemeines ... 62
A.2 Projekt ... 62
A.3 HPD-Anforderungsspezifikation ... 62
A.4 Annahme von blanken integrierten Schaltkreisen, internen Blöcken und PDBs ... 62
A.5 HPD-Auslegung und -Realisierung ... 62
A.6 HPD-Integration und -Test ... 63
A.7 HPD-Aspekte der Systemintegration ... 63
A.8 HPD-Aspekte der Systemvalidierung ... 63
A.9 Änderung ... 63
A.10 HPD-Produktion ... 63
A.11 Softwarewerkzeuge für die Entwicklung von HPDs ... 63
Anhang B (informativ) Entwicklung von HPDs ... 64
B.1 Allgemeines ... 64
B.2 Optionale Erfassung von Anforderungen auf Elektroniksystemebene ... 64
B.3 HPD und Systemlebenszyklus ... 64
B.4 Auslegung ... 65
B.5 Annahmeprozess für programmierbare integrierte Schaltkreise, interne Blöcke und vorentwickelte Blöcke ... 66
B.6 Realisierung ... 66

Documents
Document Sharing Hub
Full document details: DIN EN IEC 62566-2:2021-11

B.7 HPD-Integration und -Test 67
B.8 Arten spezifischer integrierter Schaltkreise 67
B.8.1 Allgemeines 67
B.8.2 Programmierbare Gatterlogik (PAL) 68
B.8.3 Programmierbare logische Baugruppe (PLD) und komplexe PLD (CPLD) 68
B.8.4 FPGA 68
B.8.5 Gatter-Array oder vor-diffundierter Schaltkreis 69
B.8.6 Standardzellen 69
B.8.7 Komplette kundenspezifische ASICs oder rohe ASICS 69
Literaturhinweise 70

Bilder

Bild 1 – System-Lebenszyklus (informativ, wie in IEC 61513 definiert) 30
Bild 2 – HPD-Lebenszyklus 31
Bild 3 – Überblick über den Auswahl- und Annahmeprozess für blanke integrierte Schaltkreise und interne Blöcke 38
Bild 4 – Überblick über den Auswahl- und Annahmeprozess für PDBs 40

Documents
Document Sharing Hub
Full document details: DIN EN IEC 62566-2:2021-11

Einleitung

a) Technischer Hintergrund, hauptsächliche Inhalte und Organisation der Norm

Die in Kernkraftwerken verwendeten elektronischen Systeme, die Funktionen der Kategorien B und C (nach IEC 61226) ausführen, benötigen eine vollständige Validierung und Qualifizierung entsprechend ihrer Sicherheitsklasse. Diese Internationale Norm enthält Anforderungen für die Entwicklung HDL-programmierter Gerätschaften (HPDs) der Klassen 2 und 3, die Funktionen der Klassen B oder C nach IEC 61226 ausführen. Sie ergänzt IEC 62566, in der Anforderungen zur Entwicklung von HPDs für Kategorie-A-Funktionen bereitgestellt werden.

In rechnerbasierten Systemen kann eine Trennlinie zwischen Hardware- und Softwareteilen gezogen werden. Die Hardware ist hauptsächlich aus standardisierten Komponenten mit vordefinierten elektronischen Funktionen wie Mikroprozessoren, Timern oder Netzwerk-Controllern aufgebaut, wogegen die Software zur Koordinierung der verschiedenen Hardwareteile und zur Realisierung von Anwendungsfunktionen eingesetzt wird.

Der Entwickler der Leittechnik kann Anwendungsfunktionen unter Nutzung integrierter Schaltkreise, wie z. B. FPGAs oder ähnliche Technologien, erstellen. Die Funktion eines solchen integrierten Schaltkreises wird nicht vom Lieferanten der physikalischen Komponente oder der mikroelektronischen Technologie festgelegt, sondern vom Entwickler der Leittechnik.

Die in dieser Norm speziell angesprochenen integrierten Schaltkreise sind:

a) basierend auf vor-entwickelten mikroelektronischen Technologien,

b) in einem Leittechnikprojekt entwickelt,

c) in Hardware-Beschreibungssprachen (HDL) unter Verwendung geeigneter und kompatibler Entwicklungswerkzeuge entwickelt.

Daher werden diese Schaltkreise „HDL-programmierte Baugruppen“ (en: HDL-Programmed Devices, HPD) genannt. Die HDL-Festlegungen, die eine HPD beschreiben, können die unmittelbare Verwendung von vorgefertigten Blöcken (en: Pre-Developed Blocks, PDB) mit einschließen, die typischerweise in Bibliotheken, Makros oder eigentumsgeschützten Kernen vorgehalten werden.

HPDs können eine effektive Lösung zur Realisierung von erforderlichen Funktionen in einem leittechnischen Projekt sein. Jedoch könnten Verifizierung und Validierung durch Punkte wie große Anzahl interner Pfade und begrenzter Beobachtbarkeit eingeschränkt sein, wenn bei der Entwicklung des HPD seine Verifizierbarkeit nicht mitbedacht wurde.

Um die hohe Zuverlässigkeit zu erreichen, die für Geräte der Sicherheitsleittechnik gefordert wird, muss die Entwicklung der HPDs strikten prozesstechnischen und technischen Anforderungen, so wie sie in dieser Norm zur Verfügung gestellt werden, entsprechen, einschließlich Anforderungsspezifikation, Auswahl der blanken integrierten Schaltkreise und PDBs, Auslegung und Realisierung, Verifizierung und Prozeduren für Betrieb und Instandhaltung.

Diese Norm ist zur Anwendung durch HPD-Entwickler, Kernkraftwerksbetreiber und Genehmigungsbehörden vorgesehen. Mit der Genehmigung befasste Institutionen finden Anleitungen zur Bewertung wichtiger Aspekte betreffend Auslegung, Realisierung, Verifizierung und Validierung von HPDs.

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

Das Eingangsdokument zu den Normen des IEC/SC 45A ist die IEC 61513. Sie enthält Anleitungen zur Leittechnik auf Systemebene und wird ergänzt durch Anleitungen für Hardware (IEC 60987) und Software (IEC 60880 und IEC 62138) sowie HPD (IEC 62566 und IEC 62566-2). IEC 62340 enthält Anforderungen zur Reduzierung und Vermeidung von CCF (en: common cause failure) bei Funktionen der Kategorie A.

IEC 62566-2 ist ein IEC/SC 45A-Dokument der zweiten Ebene, das sich auf die Aktivitäten bei der Entwicklung von HPDs für Funktionen der Kategorien B oder C konzentriert. Hinsichtlich HPDs für Funktionen der Kategorie B ergänzt sie IEC 60987, die sich mit generischen Fragen der Hardwareauslegung rechnerbasierter Systeme befasst.

Documents
Document Sharing Hub

Full document details: DIN EN IEC 62566-2:2021-11

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.

Im Hinblick auf folgende Aspekte wurden spezielle Anforderungen und Empfehlungen erarbeitet:

a) Eine Vorgehensweise zur Spezifikation von Anforderungen für Auslegung, Realisierung und Verifizierung von „HDL-programmierten Baugruppen“ (HPD, 3.20) und Behandlung der zugehörigen Aspekte der Systemintegration und -validierung;

b) eine Vorgehensweise zur Analyse und Auswahl blanker integrierter Schaltkreise, mikroelektronischer Technologien und vor-entwickelter Blöcke (PDB, 3.29), die zur Entwicklung von HPDs verwendet werden;

c) Prozeduren zur Änderungs- und Konfigurationskontrolle von HPDs;

d) Anforderungen bzgl. Auswahl und Verwendung von Softwarewerkzeugen für die Entwicklung von HPDs.

Es ist berücksichtigt, dass sich die digitale Technologie nach wie vor rasch entwickelt und dass es in einer Norm wie dieser nicht möglich ist, Verweisungen auf alle modernen Entwicklungstechniken mit einzuschließen.

Um sicherzustellen, dass die Norm über längere Zeit unverändert gültig bleibt, wurde der Schwerpunkt auf Prinzipien und nicht auf spezielle Technologien gelegt. Wenn neu entwickelte Techniken zur Verfügung stehen, sollte es möglich sein, ihre Eignung durch die in dieser Norm enthaltenen Sicherheitsprinzipien zu beurteilen.

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

IEC 61513 und IEC 63046 stellen die Eingangsdokumente zu den Normen des IEC/SC 45A dar. 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 Stromversorgungssysteme in Kernkraftwerken; sie deckt die elektrische Energieversorgung einschließlich der Versorgungssysteme für die Leittechnik ab. IEC 61513 und IEC 63046 sind zusammengehörend auf gleicher Ebene zu betrachten. Durch IEC 61513 und IEC 63046 werden die Normen des IEC/SC 45A strukturiert und ein komplettes Rahmenwerk für allgemeine Anforderungen zu leittechnischen und elektrischen Systemen in Kernkraftwerken geschaffen.

In IEC 61513 und IEC 63046 wird direkt auf andere Normen des IEC/SC 45A verwiesen, die allgemeine Themen behandeln, wie die Kategorisierung von Funktionen und die Klassifizierung von Systemen, Qualifizierung, Trennung, Maßnahmen gegen Versagen aufgrund gemeinsamer Ursache, Wartenauslegung, elektromagnetische Verträglichkeit, IT-Sicherheit, Software- und Hardwareaspekte programmierbarer digitaler Systeme, Koordinierung von Anforderungen zur Sicherheit und zur 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. 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 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 in den einschlägigen IAEA Safety Standards und den entsprechenden Dokumenten der IAEA Nuclear Security Series (NSS) umgesetzt und detailliert: Dies umfasst speziell die Requirements SSR-2/1 betreffend Sicherheitsanforderungen für die Auslegung von Kernkraftwerken, den Safety Guide SSG-30 bezüglich der Sicherheitsklassifizierung von Strukturen, Systemen und Komponenten in Kernkraftwerken, SSG-39 betreffend die Auslegung der Leittechnik in Kernkraftwerken, SSG-34 betreffend die Auslegung der Stromversorgung in Kernkraftwerken und die Implementierungsleitlinie NSS 17 für IT-Sicherheit von Rechnern in nuklearen Einrichtungen. Terminologie und Definitionen in den Normen des IEC/SC 45A stimmen mit den von der IAEA verwendeten überein.

AVA Documents
Document Sharing Hub
Full document details: DIN EN IEC 62566-2:2021-11

Für IEC 61513 und IEC 63046 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 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 für den nuklearen Sektor der IEC 61508-3. IEC 61513 und IEC 63046 beziehen sich bei Themen der Qualitätssicherung (QS) sowohl auf ISO als auch auf IAEA GS-R Part 2 und IAEA GS-G-3.1 und IAEA GS-G-3.5. Auf Ebene 2 ist in Hinblick auf IT-Sicherheit IEC 62645 das Eingangsdokument für die IT-Sicherheitsstandards des IEC/SC 45A. Es baut auf die übergeordneten Prinzipien und Hauptkonzepte der generischen IT-Sicherheitsstandards auf, insbesondere auf ISO/IEC 27001 und ISO/IEC 27002; es adaptiert sie und vervollständigt sie, um in den nuklearen Kontext zu passen, und koordiniert sie mit IEC 62443. Auf Ebene 2 ist in Hinblick auf Warten IEC 60964 das Eingangsdokument für die Wartennormen des IEC/SC 45A, und IEC 62342 ist das Eingangsdokument für die IEC/SC 45A-Normen 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 Das Arbeitsgebiet des IEC/SC 45A wurde 2013 erweitert, um auch elektrische Systeme abzudecken. In den Jahren 2014 und 2015 wurde in 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 zu erstellen. Dazu wurde das Projekt IEC 63046 begonnen. Sobald IEC 63046 veröffentlich wird, verliert diese Anmerkung 2 der allgemeinen Einleitung für die Normen des IEC/SC 45A ihre Gültigkeit[N1].

N1 Nationale Fußnote: IEC 63046 ist zwischenzeitlich erschienen, DIN EN IEC 63046 (VDE 0491-8-2) in Vorbereitung.

Documents
Document Sharing Hub

Full document details: DIN EN IEC 62566-2:2021-11

1 Anwendungsbereich

Dieser Teil der IEC 62566 stellt Anforderungen für hochzuverlässige „HDL-programmierte Baugruppen“ (en: HDL-Programmed Devices, HPD) für die Verwendung in leittechnischen Systemen von Kernkraftwerken, die Funktionen der Sicherheitskategorien B oder C nach IEC 61226 ausführen, zur Verfügung.

Die Programmierung von HPDs beruht auf Hardware-Beschreibungssprachen (en: Hardware Description Languages, HDL) und zugehörigen Softwarewerkzeugen. HPDs basieren typischerweise auf blanken feldprogrammierbaren logischen Gattern (en: Field Programmable Gate Arrays, FPGAs) oder ähnlichen mikroelektronischen Technologien wie programmierbaren logischen Baugruppen (en: Programmable Logic Devices, PLDs), komplexen programmierbaren logischen Baugruppen (en: Complex Programmable Logic Devices, CPLDs) usw. Universelle integrierte Schaltkreise für allgemeine Anwendungen wie Mikroprozessoren sind keine HPDs. Beschreibungen etlicher unterschiedlicher Arten integrierter Schaltkreise sind in Abschnitt B.8 zu finden.

Dieses Dokument enthält Anforderungen betreffend

a) eines fest zugeordneten HPD-Lebenszyklus, in dem jede Phase der HPD-Entwicklung angesprochen wird, einschließlich der Spezifikation der Anforderungen, Auslegung, Realisierung, Integration und Validierung sowie die Verifizierungsarbeiten im Zusammenhang mit jeder Phase;

b) Planung und ergänzenden Tätigkeiten wie Änderungen und Produktion;

c) Auswahl vor-entwickelter Komponenten. Diese schließt mikroelektronische Technologien und vor-entwickelte Blöcke (PDBs) ein;

d) Werkzeugen für Auslegung, Realisierung und Verifizierung von HPDs.

Dieses Dokument enthält keine Anforderungen zur Entwicklung der mikroelektronischen Technologien, die gewöhnlich kommerziell verfügbar sind und nicht unter nuklearen Qualitätssicherungsstandards entwickelt werden. Es spricht vielmehr die Entwicklungen an, die mit diesen mikroelektronischen Technologien in einem leittechnischen Projekt mit HDLs und zugehörigen Werkzeugen getätigt werden.

Dieses Dokument enthält Anleitungen, wie latente Fehler in HPDs so weit wie möglich vermieden werden können, und sich so die Empfindlichkeit für Einzelfehler und mögliche CCF (en: common cause failures) verringert.

Zuverlässigkeitsaspekte in Bezug auf Qualifizierung hinsichtlich Umgebungsbedingungen und Versagen aufgrund Alterung oder physikalischer Abnutzung werden hier nicht behandelt. Diese Themen werden in anderen Normen wie IEC 60987, IEC/IEEE 60780-323 und IEC 62342 angesprochen.

Aspekte der IT-Sicherheit für HDL-Aspekte der Leittechnik werden in diesem Dokument nicht behandelt. IEC 62645 enthält Anforderungen zur IT-Sicherheit für programmierbare digitale leittechnische Systeme.

Dieses Dokument enthält Anleitungen und Anforderungen für verifizierbare HPD-Auslegungen und -Realisierungen, für die Nachweise hinsichtlich ihrer Aufgabe bei der Erfüllung von Sicherheitsfunktionen der Kategorien B oder C erforderlich sind. Dieses Dokument beschreibt die Tätigkeiten zur Entwicklung von HPDs, die im Rahmen eines fest zugeordneten Lebenszyklus organisiert sind. Es beschreibt auch Tätigkeiten und gibt Anleitungen, die zusätzlich zu den Anforderungen in IEC 61226 für Systemklassifizierung und in IEC 61513 für Systemintegration und -validierung bei Verwendung von HPDs zu benutzen sind.

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 – Software aspects for computer-based systems performing category A functions*

Documents
Document Sharing Hub
Full document details: DIN EN IEC 62566-2:2021-11

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

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 important to safety – General requirements for systems*

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

IEC 62566:2012, *Nuclear power plants – Instrumentation and control important to safety – Development of HDL-programmed integrated circuits for systems performing category A functions*

3 Begriffe

Für die Anwendung dieser Norm gelten folgende 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
Anwendungsfunktion
en **application function**
Funktion eines leittechnischen Systems, die eine Aufgabe in Verbindung mit dem Prozess und nicht mit dem Funktionieren des Systems selbst erfüllt

[QUELLE: IEC 61513:2011, 3.1]

3.2
anwendungsorientierte Sprache
en **application-oriented language**
Rechnersprache, speziell entwickelt für ein bestimmtes Anwendungsgebiet und zur Verwendung für Personen, die Spezialisten auf diesem Anwendungsgebiet sind

Anmerkung 1 zum Begriff: Geräte-Plattformen bevorzugen gewöhnlich anwendungsorientierte Sprachen mit leicht zu nutzenden Fähigkeiten für die Anpassung des Geräts an spezifische Anforderungen.

Anmerkung 2 zum Begriff: Anwendungsorientierte Sprachen können verwendet werden, um funktionale Anforderungen eines leittechnischen Systems festzulegen und/oder Anwendungssoftware festzulegen oder zu entwickeln. Sie können auf Texten, auf Graphiken oder auf beiden basieren.

Anmerkung 3 zum Begriff: Beispiele: Sprachen basierend auf Funktionsblock-Diagrammen, nach IEC 61131-3 definierte Sprachen.

Anmerkung 4 zum Begriff: Siehe auch allgemeine Sprache.

[QUELLE: IEC 60880:2006, 3.3]

3.3
Anwendungssoftware
en **application software**
Teil der Software eines leittechnischen Systems, durch den Anwendungsfunktionen realisiert werden

Documents
Document Sharing Hub

Full document details: DIN EN IEC 62566-2:2021-11

Anmerkung 1 zum Begriff: Bei HPDs werden Anwendungsfunktionen nicht mit Software realisiert; somit könnte der Begriff „Anwendungssoftware“ ersetzt werden durch „Anwendungsfunktionen, implementiert in der HPD-Auslegung“.

Anmerkung 2 zum Begriff: Anwendungssoftware im Gegensatz zu Systemsoftware.

Anmerkung 3 zum Begriff: Siehe auch Systemsoftware.

[QUELLE: IEC 61513:2011, 3.2]

3.4
anwendungsspezifischer integrierter Schaltkreis
ASIC
en **application specific integrated circuit**
integrierter Schaltkreis, der für speszifische Anwendungen ausgelegt ist

Anmerkung 1 zum Begriff: Spezieller integrierter Schaltkreis, der für die von einer Firma festgelegten Zwecke ausgelegt wurde. Er realisiert also von dieser Firma vorab definierte Funktionen.

[QUELLE: IEC 60050-521:2002, 521-11-18]

3.5
Block
en **block**
einer der Teile, aus denen eine Auslegung besteht; ein Block kann in weitere Blöcke unterteilt sein

Anmerkung 1 zum Begriff: Ein Block ist entweder ein vor-entwickelter Block oder ein interner Block oder ein im Rahmen des in Rede stehenden Projekts entwickelter Block.

[QUELLE: IEC 62566:2012, 3.2]

3.6
Versagen/Ausfall aufgrund gemeinsamer Ursache
CCF
en **common cause failure**
Versagen von zwei oder mehr Strukturen, Systemen oder Komponenten infolge eines einzigen spezifischen Ereignisses oder Grunds

[QUELLE: IEA Safety Glossary, 2016]

3.7
Konfigurationsmangement
en **configuration management**
Prozess, in dem die Eigenschaften von Strukturen, Systemen und Komponenten einer Anlage (einschließlich Rechnersystemen und Software) festgelegt und dokumentiert werden, und in dem sichergestellt wird, dass Änderungen dieser Eigenschaften in geeigneter Weise geplant, analysiert, bestätigt, niedergelegt, realisiert, verifiziert, dokumentiert und in die Anlagendokumentation integriert werden

[QUELLE: IEA Safety Glossary, 2016]

3.8
IT-Sicherheit
en **cybersecurity**
Satz von Tätigkeiten und Maßnahmen zur Vorbeugung, zum Erkennen und Reagieren auf:

– böswillige 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 von Funktionen (Integrität), was die Bereitstellung oder Integrität einer von den programmierbaren digitalen Leittechniksystemen geforderten Leistung (einschließlich des Verlustes der Steuerung) beeinträchtigen kann, was 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 Leittech-

Documents
Document Sharing Hub
Full document details: DIN EN IEC 62566-2:2021-11