

	DIN EN IEC 62645 (VDE 0491-3-7)	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; 35.030</p> <p>Kernkraftwerke – Leittechnische und elektrische Systeme – Anforderungen an die Cybersicherheit (IEC 62645:2019); Deutsche Fassung EN IEC 62645:2020</p> <p>Nuclear power plants – Instrumentation, control and electrical power systems – Cybersecurity requirements (IEC 62645:2019); German version EN IEC 62645:2020</p> <p>Centrales nucléaires de puissance – Systèmes d'instrumentation, de contrôlecommande et d'alimentation électrique – Exigences relatives à la cybersécurité (IEC 62645:2019); Version allemande EN IEC 62645:2020</p> <p>Gesamtumfang 65 Seiten</p> <p>DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE</p>		

Anwendungsbeginn

Anwendungsbeginn für die von CENELEC am 2020-07-07 angenommene Europäische Norm als DIN-Norm ist 2021-03-01.

Nationales Vorwort

Vorausgegangener Norm-Entwurf: E DIN IEC 62645 (VDE 0491-3-7):2013-04.

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.

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 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.

Das Original-Dokument enthält Bilder in Farbe, die in der Papierversion in einer Graustufen-Darstellung wiedergegeben werden. Elektronische Versionen dieses Dokuments enthalten die Bilder in der originalen Farbdarstellung.

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 EN IEC 62645 (VDE 0491-3-7):2021-03**, *Kernkraftwerke – Leittechnische und elektrische Systeme – Anforderungen an die Cybersicherheit (IEC 62645:2019)*; Deutsche Fassung **EN IEC 62645:2020**

- **DIN IEC 62859 (VDE 0491-3-8):2017-12**, Kernkraftwerke – Leittechnische Systeme – Anforderungen für die Koordinierung von Sicherheit und IT-Sicherheit (**IEC 62859:2016**)
Der Ersatz durch DIN EN IEC 62859 (VDE 0491-3-8):2021-xx, Kernkraftwerke – Leittechnische Systeme – Anforderungen für die Koordinierung von Sicherheit und IT-Sicherheit (**IEC 62859:2016 + A1:2019**); Deutsche Fassung **EN IEC 62859:2020**, ist zurzeit in Vorbereitung.
- **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)** (in Vorbereitung), 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**)
- **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 EN IEC 62645 (VDE 0491-3-7):2021-03

- **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*

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
EN IEC 60709	IEC 60709	DIN EN IEC 60709 (VDE 0491-7)	VDE 0491-7
EN 60880:2009	IEC 60880:2006	DIN EN 60880 (VDE 0491-3-2):2010-03	VDE 0491-3-2
EN 61226	IEC 61226	DIN EN 61226 (VDE 0491-1)	VDE 0491-1
EN 61508-1	IEC 61508-1	DIN EN 61508-1 (VDE 0803-1)	VDE 0803-1
EN 61508-2	IEC 61508-2	DIN EN 61508-2 (VDE 0803-2)	VDE 0803-2
EN 61508-3	IEC 61508-3	DIN EN 61508-3 (VDE 0803-3)	VDE 0803-3
EN 61508-4	IEC 61508-4	DIN EN 61508-4 (VDE 0803-4)	VDE 0803-4
EN 61513:2013	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
EN IEC 62443 (alle Teile)	IEC 62443 (alle Teile)	DIN EN IEC 62443 (VDE 0802-4-1) (alle Teile)	VDE 0802-4-1
EN 62566:2014	IEC 62566:2012	DIN EN 62566 (VDE 0491-3-5):2015-02	VDE 0491-3-5
EN IEC 62859:2020	IEC 62859:2016 + A1:2019	DIN EN IEC 62859 (VDE 0491-3-8) ^a	VDE 0491-3-8
EN IEC 62988 ^a	IEC 62988:2018	DIN EN IEC 62988 (VDE 0491-3-6) ^a	VDE 0491-3-6
EN IEC 63046 ^a	IEC 63046	DIN EN IEC 63046 (VDE 0491-8-2) ^a	VDE 0491-8-2
–	IEC 63096	DIN IEC 63096 (VDE 0491-3-10) ^a	VDE 0491-3-10
EN ISO/IEC 27000:2020	ISO/IEC 27000:2018	DIN EN ISO/IEC 27000:2020-06	–

Tabelle NA.1 (2 von 2)

Europäisches Dokument	Internationales Dokument	Deutsches Dokument	Klassifikation im VDE-Vorschriftenwerk
EN ISO/IEC 27001:2017	ISO/IEC 27001:2013 + Cor. 1:2014 + Cor. 2:2015	DIN EN ISO/IEC 27001:2017-06	—
EN ISO/IEC 27002:2017	ISO/IEC 27002:2013 + Cor. 1:2014 + Cor. 2:2015	DIN EN ISO/IEC 27002:2017-06	—
—	ISO/IEC 27005:2018	—	—
^a In Vorbereitung.			

Nationaler Anhang NB (informativ)

Literaturhinweise

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

DIN EN 61508-1 (VDE 0803-1), *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 1: Allgemeine Anforderungen*

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

DIN EN 61508-3 (VDE 0803-3), *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 3: Anforderungen an Software*

DIN EN 61508-4 (VDE 0803-4), *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 4: Begriffe und Abkürzungen*

DIN EN 61513 (VDE 0491-2):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):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 60709 (VDE 0491-7), *Kernkraftwerke – Leittechnik und elektrische Energieversorgungssysteme mit sicherheitstechnischer Bedeutung – Physikalische und elektrische Trennung*

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 0802-4-1) (alle Teile), *IT-Sicherheit für industrielle Automatisierungssysteme – Teil 4-1: Anforderungen an den Lebenszyklus für eine sichere Produktentwicklung*

DIN EN IEC 62859 (VDE 0491-3-8) (in Vorbereitung), *Kernkraftwerke – Leittechnische Systeme – Anforderungen für die Koordinierung von Sicherheit und IT-Sicherheit*

DIN EN IEC 62988 (VDE 0491-3-6) (in Vorbereitung), *Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Auswahl und Einsatz drahtloser Geräte*

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

DIN EN ISO/IEC 27000:2020-06, *Informationstechnik – Sicherheitsverfahren – Informationssicherheitsmanagementsysteme – Überblick und Terminologie (ISO/IEC 27000:2018); Deutsche Fassung EN ISO/IEC 27000:2020*

DIN EN ISO/IEC 27001:2017-06, *Informationstechnik – Sicherheitsverfahren – Informationssicherheitsmanagementsysteme – Anforderungen (ISO/IEC 27001:2013 einschließlich Cor 1:2014 und Cor 2:2015); Deutsche Fassung EN ISO/IEC 27001:2017*

DIN EN IEC 62645 (VDE 0491-3-7):2021-03

DIN EN ISO/IEC 27002:2017-06, *Informationstechnik – Sicherheitsverfahren – Leitfaden für Informationssicherheitsmaßnahmen (ISO/IEC 27002:2013 einschließlich Cor 1:2014 und Cor 2:2015); Deutsche Fassung EN ISO/IEC 27002:2017*

DIN IEC 63096 (VDE 0491-3-10) (in Vorbereitung), *Kernkraftwerke – Leittechnische Systeme und elektrische Energiesysteme – IT-Sicherheitsmaßnahmen*

Kernkraftwerke –
Leittechnische und elektrische Systeme –
Anforderungen an die Cybersicherheit
(IEC 62645:2019)

Nuclear power plants –
Instrumentation, control and electrical power
systems –
Cybersecurity requirements
(IEC 62645:2019)

Centrales nucléaires de puissance –
Systèmes d'instrumentation, de
contrôlecommande et d'alimentation
électrique –
Exigences relatives à la cybersécurité
(IEC 62645:2019)

Diese Europäische Norm wurde von CENELEC am 2020-07-07 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

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

Ref. Nr. EN IEC 62645:2020 D

Europäisches Vorwort

Der Text des Dokuments 45A/1289/FDIS, zukünftige 2. Ausgabe der IEC 62645, erarbeitet vom SC 45A „Instrumentation, control and electrical power systems of nuclear facilities“ des IEC/TC 45 „Nuclear instrumentation“, wurde zur parallelen IEC-CENELEC-Abstimmung vorgelegt und von CENELEC als EN IEC 62645:2020 angenommen.

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): 2021-07-07
- spätestes Datum, zu dem nationale Normen, die diesem Dokument entgegenstehen, zurückgezogen werden müssen (dow): 2023-07-07

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 Anwendungsbereich dieser Europäischen Norm strengere Maßnahmen bezüglich der nuklearen Sicherheit zu fordern.

Anerkennungsnotiz

Der Text der Internationalen Norm IEC 62645:2019 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 60709	ANMERKUNG	Harmonisiert als EN IEC 60709 .
ISO/IEC 27000:2018	ANMERKUNG	Harmonisiert als EN ISO/IEC 27000:2020 (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 systems important to safety – Classification	– ^{N1}	–
IEC 61513	–	Nuclear power plants – Instrumentation and control for systems important to safety – General requirements for systems	– ^{N1}	–
IEC 62138	–	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	–
IEC 62566	–	Nuclear power plants – Instrumentation and control important to safety – Development of HDL-programmed integrated circuits for systems performing category A functions	EN 62566	–
IEC 62859	–	Nuclear power plants – Instrumentation and control systems – Requirements for coordinating safety and cybersecurity	– ^{N1}	–
ISO/IEC 27001	2013	Information technology – Security techniques – Information security management systems – Requirements	EN ISO/IEC 27001	2017
ISO/IEC 27002	2013	Information technology – Security techniques – Code of practice for information security controls	EN ISO/IEC 27002	2017
ISO/IEC 27005	2018	Information technology – Security techniques – Information security risk management	–	–

^{N1} Nationale Fußnote: IEC 61226:2009 wurde als EN 61226:2010 übernommen, IEC 61513:2011 als EN 61513:2013 und IEC 62859:2016 + A1:2019 als EN IEC 62859:2020.

Inhalt

Seite

Europäisches Vorwort.....	2
Anhang ZA (normativ) Normative Verweisungen auf internationale Publikationen mit ihren entsprechenden europäischen Publikationen	3
Einleitung	7
1 Anwendungsbereich	9
1.1 Allgemeines	9
1.2 Anwendung.....	10
1.3 Rahmen	10
2 Normative Verweisungen	13
3 Begriffe	13
4 Abkürzungen	18
5 Erstellung und Management einer IT-Sicherheitsplanung für nukleare programmierbare leittechnische Systeme.....	18
5.1 Kontext der Organisation.....	18
5.1.1 Verständnis der Organisation und ihres Kontexts.....	18
5.1.2 Verständnis der Erfordernisse und Erwartungen der interessierten Parteien.....	18
5.1.3 Festlegung des Anwendungsbereichs des Sicherheitsprogramms für die programmierbaren digitalen leittechnischen Systeme	19
5.2 Programm, Politik und Plan	19
5.2.1 IT-Sicherheitsprogramm für programmierbare digitale leittechnische Systeme	19
5.2.2 Politik	20
5.2.3 Plan	20
5.3 Leitung	20
5.3.1 Verpflichtung der Leitung	20
5.3.2 Rollen, Verantwortlichkeiten und Behörden	20
5.4 Planung des Programms.....	22
5.4.1 IT-Sicherheitsziele und Planung, um diese zu erreichen.....	22
5.4.2 Risiken und Chancen des Programms.....	22
5.4.3 Abgestuftes Vorgehen zu IT-Sicherheit und Risikobewertung der Leittechnik	22
5.5 Unterstützung	30
5.5.1 Ressourcen	30
5.5.2 Training, Befugnisse und Sensibilisierung	30
5.5.3 Kommunikation zur Cybersicherheit.....	30
5.5.4 Dokumentierte Informationen	31
5.6 Betrieb	31
5.6.1 Betriebsplanung und -kontrolle.....	31
5.6.2 Abgestufte Vorgehensweise zur Cybersicherheit, Risikobewertung und Risikobehandlung	31
5.7 Bewertung der Wirksamkeit	31
5.7.1 Überwachung, Messung, Analyse und Bewertung	31

5.7.2	Interne Audits	32
5.7.3	Managementreview	32
5.8	Verbesserung	33
5.8.1	Allgemeines	33
5.8.2	Nichtkonformität und Korrekturmaßnahmen	33
5.8.3	Kontinuierliche Verbesserung	33
6	Lebenszyklus-Realisierung für die IT-Sicherheit des programmierbaren digitalen leittechnischen Systems	33
6.1	Allgemeines	33
6.2	Systemanforderungsspezifikation	33
6.2.1	Allgemeines	33
6.2.2	Zuordnung der IT-Sicherheitsgrade	34
6.3	Systemspezifikation	34
6.3.1	Auswahl aus vorhandenen Komponenten	34
6.3.2	Systemarchitektur	34
6.4	Systemauslegung und -realisierung	34
6.4.1	Allgemeines	34
6.4.2	Risikobewertung in der Auslegungsphase	35
6.4.3	Projekt-IT-Sicherheitsplan der Auslegung	35
6.4.4	Kommunikationswege	35
6.4.5	Definition von Sicherheitszonen	36
6.4.6	IT-Sicherheitsbewertung der endgültigen Auslegung	36
6.4.7	Realisierungstätigkeiten	36
6.5	Systemintegration	36
6.6	Systemvalidierung	36
6.7	Systemerrichtung	37
6.8	Betriebs- und Wartungstätigkeiten	37
6.8.1	Änderungskontrolle während Betrieb und Wartung	37
6.8.2	Wiederkehrende Bewertung der Risiken und IT-Sicherheitsmaßnahmen	37
6.8.3	Änderungsmanagement	37
6.9	Außerbetriebsetzung	38
7	IT-Sicherheitsmaßnahmen	38
7.1	Allgemeines	38
7.2	Charakterisierung	38
7.3	Gestaffelte Verteidigung der IT-Sicherheit	39
7.4	Auswahl und Durchsetzung von Cybersicherheitsmaßnahmen	39
Anhang A (informativ)	Begründung für und Anmerkungen zum Anwendungsbereich dieses Dokuments	41
A.1	Ziele dieses Anhangs	41
A.2	Einbeziehung programmierbarer digitaler leittechnischer Systeme ohne sicherheitstechnische Bedeutung	41

	Seite
A.3 Ausschluss von Anlagensicherung, Zugangskontrolle zu Räumen und Überwachungssystemen der Anlagensicherung.....	41
A.4 Ausschluss von nicht böswilligen Handlungen und Ereignissen.....	41
A.5 Entwicklungswerkzeuge und Gerätefamilien.....	42
Anhang B (informativ) Allgemeine Überlegungen zu den IT-Sicherheitsgraden.....	43
B.1 Begründung der drei IT-Sicherheitsgrade	43
B.1.1 Allgemeines	43
B.1.2 Sicherheitskategorien als Eingangsgrößen für die Zuordnung von IT-Sicherheitsgraden.....	43
B.1.3 Einfluss auf die Anlagenverfügbarkeit und -leistungsfähigkeit als Eingangsgrößen für den IT-Sicherheitsgrad.....	44
B.1.4 Das sich ergebende Zuordnungsverfahren für die IT-Sicherheitsgrade	44
B.2 Überlegungen zu Werkzeugen für Online-Systeme	44
B.3 Praktische Auslegung und Implementierung.....	44
Anhang C (informativ) Zusammenhang mit ISO/IEC 27001:2013	45
Anhang D (informativ) Gesamtorganisation der Normen des IEC/SC 45A bezüglich Cybersicherheit	47
Anhang E (informativ) Auswahl von IT-Sicherheitsmaßnahmen.....	49
Anhang F (informativ) Überlegungen zur Anwendbarkeit der IEC 62645 auf andere kerntechnische Anlagen	51
F.1 Anwendbarkeit der abgestuften Vorgehensweise für die IT-Sicherheit nach IEC 62645 auf Forschungsreaktoren.....	51
F.1.1 Allgemeines	51
F.1.2 Kategorisierung von Forschungsreaktoren nach dem Gefährdungspotenzial	51
F.1.3 Sicherheitskategorien als Eingangsgrößen für die Zuordnung von IT-Sicherheitsgraden.....	52
F.1.4 Einfluss auf die Betriebskapazität als Eingangsgröße für IT-Sicherheitsgrade	53
F.1.5 Betrachtungen von Anforderungen, die mit IT-Sicherheitsgraden verbunden sind	53
F.2 Anwendbarkeit der abgestuften Vorgehensweise für die IT-Sicherheit nach IEC 62645 auf Anlagen des Brennstoffzyklus	54
F.3 Anwendbarkeit der abgestuften Vorgehensweise für die IT-Sicherheit nach IEC 62645 auf kleine modulare Reaktoren (SMR).....	54
F.4 Referenzdokumente	54
Anhang G (informativ) Übersicht des Zusammenhangs der Reihe IEC 62443 mit IEC 62645.....	55
Literaturhinweise.....	57
Bilder	
Bild 1 – Gesamtrahmen der IEC 62645.....	12
Bild 2 – E/E/PE-Einheiten	15
Bild D.1 – Überblick über die Normen des IEC/SC 45A mit Bezug zur Cybersicherheit.....	48
Bild E.1 – Auswahl von IT-Sicherheitsmaßnahmen	50
Tabellen	
Tabelle C.1 – Zusammenhang von ISO/IEC 27001:2013 und IEC 62645.....	45
Tabelle F.1 – Zusammenhang der Sicherheitskategorien und -klassen nach IEC 61513	52

Einleitung

a) Technischer Hintergrund, hauptsächliche Inhalte und Organisation der Norm

Diese Internationale Norm befasst sich speziell mit der Thematik der Cybersicherheitsanforderungen, um die Auswirkung von Angriffen auf programmierbare digitale leittechnische Systeme, auf die nukleare Sicherheit und auf die Anlagenleistung zu vermeiden und/oder zu minimieren. Sie behandelt Anforderungen für die Programmebene, die Architekturebene und die Systemebene.

Sie wurde basierend auf der Reihe ISO/IEC 27000 sowie IAEA- und länderspezifischen Richtlinien in diesem sich ausweitenden technischen Sicherheitsgebiet erarbeitet.

Diese Norm ist zur Anwendung durch Hersteller und Betreiber von Kernkraftwerken, Lizenznehmer, Gutachter, Lieferfirmen und Subunternehmen sowie Genehmigungsbehörden vorgesehen.

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

IEC 62645 ist ein IEC/SC 45A-Dokument der zweiten Ebene, das die allgemeine Thematik der Cybersicherheit in der Leittechnik von Kernkraftwerken behandelt.

IEC 62645 wird formal als Dokument der zweiten Ebene in Bezug auf **IEC 61513** betrachtet, obwohl **IEC 61513** einer Revision bedarf, um angemessene Bezüge auf und Übereinstimmung mit IEC 62645 sicherzustellen. IEC 62645 ist das Eingangsdokument in Bezug auf Cybersicherheit in der Reihe der Normen des IEC/SC 45A. Weitere Dokumente entstehen unterhalb von IEC 62645, die den Dokumenten der dritten Ebene innerhalb der Normen des IEC/SC 45A entsprechen.

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

c) Empfehlungen und Einschränkungen der Anwendung dieser Norm

Diese Norm legt Anforderungen an programmierbare digitale leittechnische Systeme in Hinblick auf die IT-Sicherheit von Rechnern fest und erläutert die Prozesse, unter denen programmierbare digitale leittechnische Systeme in Kernkraftwerken und nuklearen Einrichtungen ausgelegt, entwickelt und betrieben werden.

Es ist bekannt, dass wegen der ständig wechselnden Bedrohungen der IT-Sicherheit diese Norm ein laufend sich entwickelndes Feld genehmigungstechnischer Anforderungen anspricht. Daher definiert diese Norm, Rahmenvorgaben, innerhalb derer die aufkommenden länderspezifischen Anforderungen entwickelt und angewendet werden können.

Es ist weiterhin bekannt, dass Produkte zu dieser Thematik zu schützen sind. Die Freigabe der länderspezifischen Anforderungen zu dieser Norm sollte kontrolliert werden, um das Ausmaß des Nutzens für Organisationen oder Einzelpersonen zu begrenzen, die illegal, in unzulässiger Weise oder ohne Genehmigung auf nukleare Anlagensysteme zuzugreifen beabsichtigen.

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 die IEC 63046 stellen die Eingangsdokumente der 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 an elektrische Energiesysteme von Kernkraftwerken, sie deckt Energieversorgungen einschließlich der Versorgung leittechnischer Systeme ab. **IEC 61513** und IEC 63046 sind im Zusammenhang und auf gleichen Rang befindlich zu betrachten. Durch **IEC 61513** und IEC 63046 werden die Normen des IEC/SC 45A strukturiert und ein komplettes Rahmenwerk für allgemeine Anforderungen zu Leittechnik und elektrischen Systemen für Kernkraftwerke gebildet.

In **IEC 61513** und IEC 63046 wird direkt auf andere Normen des IEC/SC 45A verwiesen, die allgemeine Themen wie die Kategorisierung von Funktionen und die Klassifizierung von Systemen, Qualifizierung, Trennung von Systemen, Maßnahmen gegen Versagen aufgrund gemeinsamer Ursachen, Wartenauslegung,

elektromagnetische Verträglichkeit, Cybersicherheit, Software- und Hardwareaspekte programmierbarer digitaler Systeme, Koordination von Sicherheits- und IT-Sicherheitsanforderungen sowie das Alterungsmanagement behandeln. 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 Verfahren oder spezifische Aktivitäten. Sie beziehen sich hinsichtlich der allgemeinen Themen auf die Dokumente der zweiten Ebene, können jedoch im Allgemeinen für sich alleine 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 den Standard SSR-2/1, in dem die Sicherheitsanforderungen für die Auslegung von Kernkraftwerken festgeschrieben sind, und SSG-30 für die Sicherheitsklassifikation der Strukturen, Systeme und Komponenten in Kernkraftwerken, SSG-39 für die Auslegung der Leittechnik in Kernkraftwerken, SSG-34 für die Auslegung der Stromversorgung in Kernkraftwerken und NSS 17 für die IT-Sicherheit von Rechnern in Nuklearanlagen. Terminologie und Definitionen (zur IT- und funktionalen Sicherheit) in den Normen des IEC/SC 45A stimmen mit denen, die von der IAEA verwendet werden, überein.

Für IEC 61513 und IEC 63046 wird ein Darstellungsformat verwendet, das dem der grundlegenden Sicherheitsnorm IEC 61508 ähnlich ist, mit einem Sicherheitslebenszyklus als Gesamtrahmen und einem Systemlebenszyklus. Mit IEC 61513 und IEC 63046 werden die allgemeinen Anforderungen der IEC 61508-1, IEC 61508-2 und IEC 61508-4 für die Anwendung auf den nuklearen Sektor umgesetzt. In diesem Rahmen entsprechen IEC 60880, IEC 62138 und IEC 62566 bezogen auf den nuklearen Sektor 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 Part 2, IAEA GS-G-3.1 und IAEA GS-G-3.5. Auf der Ebene 2 ist IEC 62645 bezüglich der nuklearen IT-Sicherheit das Eingangsdokument der IT-Sicherheitsnormen des IEC/SC 45A. Sie baut auf den gültigen grundlegenden Prinzipien und Hauptkonzepten der generischen IT-Sicherheitsnormen, insbesondere ISO/IEC 27001 und ISO/IEC 27002, auf. Es passt sie an den kerntechnischen Zusammenhang an, vervollständigt sie und stimmt sie auf die Normenreihe IEC 62443 ab. Auf Ebene 2 ist IEC 60964 bezüglich Warten das Eingangsdokument der Wartennormen des IEC/SC 45A und IEC 62342 ist das Eingangsdokument der Alterungsmanagement Normen des IEC/SC 45A.

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 oder nationale Normen angewandt werden.

ANMERKUNG 2 Das Arbeitsgebiet des IEC SC 45A wurde im Jahr 2013 erweitert, um elektrische Systeme zu behandeln. In den Jahren 2014 und 2015 wurden im IEC/SC 45A Diskussionen geführt, um zu entscheiden wie und wo allgemeine Anforderungen an die Auslegung elektrischer Systeme berücksichtigt werden müssen. Die Experten des IEC/SC 45A empfahlen eine unabhängige Norm mit allgemeinen Anforderungen an elektrische Systeme auf der gleichen Ebene wie IEC 61513 zu entwickeln. Das Projekt IEC 63046 wurde zu diesem Zweck gestartet. Sobald IEC 63046 veröffentlicht wird, verliert diese Anmerkung 2 der Einleitung der Normen des IEC/SC 45A ihre Gültigkeit.

1 Anwendungsbereich

1.1 Allgemeines

Dieses Dokument enthält Anforderungen und Leitlinien für die Entwicklung und zum Management effektiver IT-Sicherheitsprogramme für programmierbare digitale leittechnische Systeme. Bei diesen Anforderungen und Leitlinien gilt als inhärentes Kriterium, dass die IT-Sicherheitsprogramme für die programmierbaren digitalen leittechnischen Systeme der Anlage mit den anwendbaren nationalen Anforderungen übereinstimmen.

Dieses Dokument legt angemessene Maßnahmen zur Verhinderung von, Erkennung von und Reaktion auf böswillige Handlungen, die auf digitalem Weg digitale programmierbare leittechnische Systeme angreifen (Cyberangriffe), fest. Dies beinhaltet alle unsicheren Situationen, Beschädigungen von Gerät oder Beeinträchtigungen der Leistungsfähigkeit der Anlage, die sich aus derartigen Handlungen ergeben könnten, wie z. B.:

- böswillige Änderungen, die die Systemintegrität beeinträchtigen;
- böswillige Wechselwirkungen mit Informationen, Daten oder Ressourcen, die die Ausführung oder die Leistungsfähigkeit einer angeforderten programmierbaren digitalen leittechnischen Funktion beeinträchtigen könnten;
- böswillige Wechselwirkungen mit Informationen, Daten oder Ressourcen, die die Bediendisplays beeinträchtigen oder zum Betriebsausfall der programmierbaren digitalen leittechnischen Systeme führen könnten;
- böswillige Änderungen der Hardware, Firmware oder Software auf der Ebene der speicherprogrammierbaren Steuerungen (SPS).

Bedienfehler, die zu einer Verletzung der Sicherheitspolitik führen und/oder die vorgenannten böswilligen Handlungen erleichtern, liegen ebenfalls im Anwendungsbereich dieses Dokuments.

Dieses Dokument beschreibt eine gestufte Vorgehensweise für schützenswerte Objekte (Assets), die Gegenstand digitaler Gefährdung sind, basierend auf der Bedeutung der Objekte für die gesamte Anlagensicherheit, Verfügbarkeit und den Schutz der Gerätschaften.

Im Anwendungsbereich dieser Norm nicht enthalten sind Überlegungen bezüglich:

- Handlungen und Ereignisse, die nicht in böswilliger Absicht zustande kommen, wie zufälliges Versagen, Bedienfehler (außer solchen, die die Leistungsfähigkeit der IT-Sicherheitsmaßnahmen beeinträchtigen) und Naturereignisse. Insbesondere liegen bewährte Praktiken für das Management von Anwendungen und Daten einschließlich Backup und Wiederherstellung im Zusammenhang mit zufälligen Ausfällen außerhalb des Anwendungsbereichs;

ANMERKUNG 1 Obwohl diese Gesichtspunkte oft auch durch IT-Sicherheitsprogramme im Kontext anderer Normen (z. B. in der Reihe ISO/IEC 27000 oder in der Reihe IEC 62443) behandelt werden, richtet sich dieses Dokument ausschließlich auf den Schutz gegen böswillige Handlungen, die auf digitalem Weg digitale programmierbare leittechnische Systeme angreifen (Cyberangriffe). Der Hauptgrund dafür liegt darin, dass auf dem Gebiet der nuklearen Energieerzeugung andere Normen und Vorgehensweisen zufällige Ausfälle, unbeabsichtigte Bedienfehler, Naturereignisse usw. abdecken. Der Schwerpunkt der IEC 62645 ist auf maximale Übereinstimmung und minimale Überlappungen mit diesen anderen nuklearen Normen und Vorgehensweisen gesetzt.

- physische IT-Sicherheit der Systeme der Anlagensicherung, wie (Raum-)Zugangskontrolle und Überwachungssystemen zur Anlagensicherung (Zaunüberwachung). Obwohl diese Themen in der vorliegenden Norm nicht angesprochen werden, müssen sie dennoch in Betriebsvorschriften und Programmen zur Cybersicherheit behandelt werden;

ANMERKUNG 2 Dieser Ausschluss stellt nicht in Abrede, dass Cybersicherheit direkte Abhängigkeiten von der physischen Umgebung besitzt (z. B. Objektschutz, Energieversorgungssysteme, Heizungs-, Lüftungs- und Klimatechnik usw.).

- der Gesichtspunkt der Vertraulichkeit der Informationen über digitale programmierbare leittechnische Systeme liegt nicht im Anwendungsbereich dieses Dokuments (siehe 5.4.3.2.3).

Anhang A liefert eine Begründung für und Kommentare zum Anwendungsbereich, zur Definition und zur Anwendung des Dokuments sowie zu den bereits genannten Ausschlüssen und Einschränkungen.

Normen wie ISO/IEC 27001 und ISO/IEC 27002 sind nicht direkt auf die Cybersicherheit nuklearer programmierbarer digitaler leittechnischer Systeme anwendbar. Das liegt hauptsächlich an den spezifischen Eigenheiten dieser Systeme, einschließlich der regulatorischen und (funktionalen) Sicherheitsanforderungen^{N2}, die kerntechnischen Einrichtungen innewohnen. Dennoch baut dieses Dokument auf den gültigen Grundsätzen und Hauptbegriffen der ISO/IEC 27001:2013 auf, gleicht sie an und ergänzt sie, um sie dem kerntechnischen Kontext anzupassen.

Dieses Dokument folgt den allgemeinen Grundsätzen, die im IAEA-Referenzhandbuch NSS17 vorgegeben sind.

1.2 Anwendung

Dieses Dokument ist auf die IT-Sicherheit programmierbarer digitaler leittechnischer Systeme (einschließlich betrieblicher Systeme) in einem Kernkraftwerk sowie zugehöriger rechnerbasierter Werkzeuge beschränkt. Dieses Dokument ist auf Teile elektrischer Systeme, die von IEC 63046 abgedeckt werden und auf digitaler programmierbarer Technik aufbauen, anwendbar.

ANMERKUNG 1 Der Einfachheit halber bezeichnet der Begriff „digitale programmierbare leittechnische Systeme“ sowohl die Leittechnik als auch die Teile der elektrischen Systeme, die von IEC 63046 abgedeckt werden und auf digitaler programmierbarer Technik aufbauen.

Dieses Dokument ist für die Verwendung bei der Bewertung oder Änderung eingeführter IT-Sicherheitsprogramme für digitale programmierbare leittechnische Systeme in Kernkraftwerken und für die Einführung neuer Programme vorgesehen. Dieses Dokument wird auf alle digitalen programmierbaren leittechnischen Systeme in Kernkraftwerken während des gesamten in diesem Dokument beschriebenen Lebenszyklus dieser Systeme angewandt. Es kann auch auf andere Arten kerntechnischer Einrichtungen anwendbar sein.

ANMERKUNG 2 Der Begriff Kernkraftwerk ist in seiner Bedeutung als „Standort“ zu verstehen, also die digitalen programmierbaren leittechnischen Systeme des Kernkraftwerks einschließlich der Systeme in den Kraftwerksgebäuden, aber auch in der Schaltanlage, der Wasseraufbereitungsanlage usw.

1.3 Rahmen

Die Anforderungen und Empfehlungen dieses Dokuments sind in drei normative Hauptabschnitte gegliedert.

Abschnitt 5 beschäftigt sich mit der Cybersicherheit der Lebenszyklus-Planungsebene; die Vorgehensweise stimmt mit ISO/IEC 27001:2013 überein. **Abschnitt 5** basiert auf Aufbau und Inhalt der ISO/IEC 27001:2013, die, wenn nötig, angepasst und komplettiert wurden, um sie an den spezifischen kerntechnischen Kontext anzupassen. **Anhang C** bietet eine abschnittsweise Vergleichstabelle zwischen dem Aufbau der IEC 62645 und dem Aufbau der ISO/IEC 27001:2013. In direkten Verweisungen auf den Inhalt der ISO/IEC 27001:2013 sind folgende Begriffsersetzungen vorzunehmen:

- Der in ISO/IEC 27001:2013 verwendete Begriff „Informationssicherheitsmanagementsystem“ entspricht „Cybersicherheitsprogramm für die digitalen programmierbaren leittechnischen Systeme“ in diesem Dokument (wie in **Abschnitt 3** festgelegt);

ANMERKUNG 1 Dieses Dokument ist auf den Teil des Programms oder auf den zugeordneten Teil des Programms gerichtet, der der Leittechnik zugeordnet ist. Dieser kann Teil eines größeren Programms auf gemeinsamer Ebene sein, die außerhalb des Anwendungsbereichs dieses Dokuments ist.

- der in ISO/IEC 27001:2013 verwendete Begriff „Informationssicherheit“ entspricht in diesem Dokument „Cybersicherheit“ (wie in **Abschnitt 3** festgelegt);

^{N2} Nationale Fußnote: Wo im IEC-Original nur „safety“ steht, nach Auffassung des DKE/UK 967.1 „Elektro- und Leittechnik für kerntechnische Anlagen“ aber „functional safety“ gemeint ist, wurde hier und im weiteren Text in der deutschen Übersetzung „(funktionale)“ vor „Sicherheit“ eingefügt.

- der in ISO/IEC 27001:2013 verwendete Begriff „Informationssicherheitspolitik“ entspricht in diesem Dokument „Sicherheitspolitik für die digitalen programmierbaren leittechnische Systeme“;

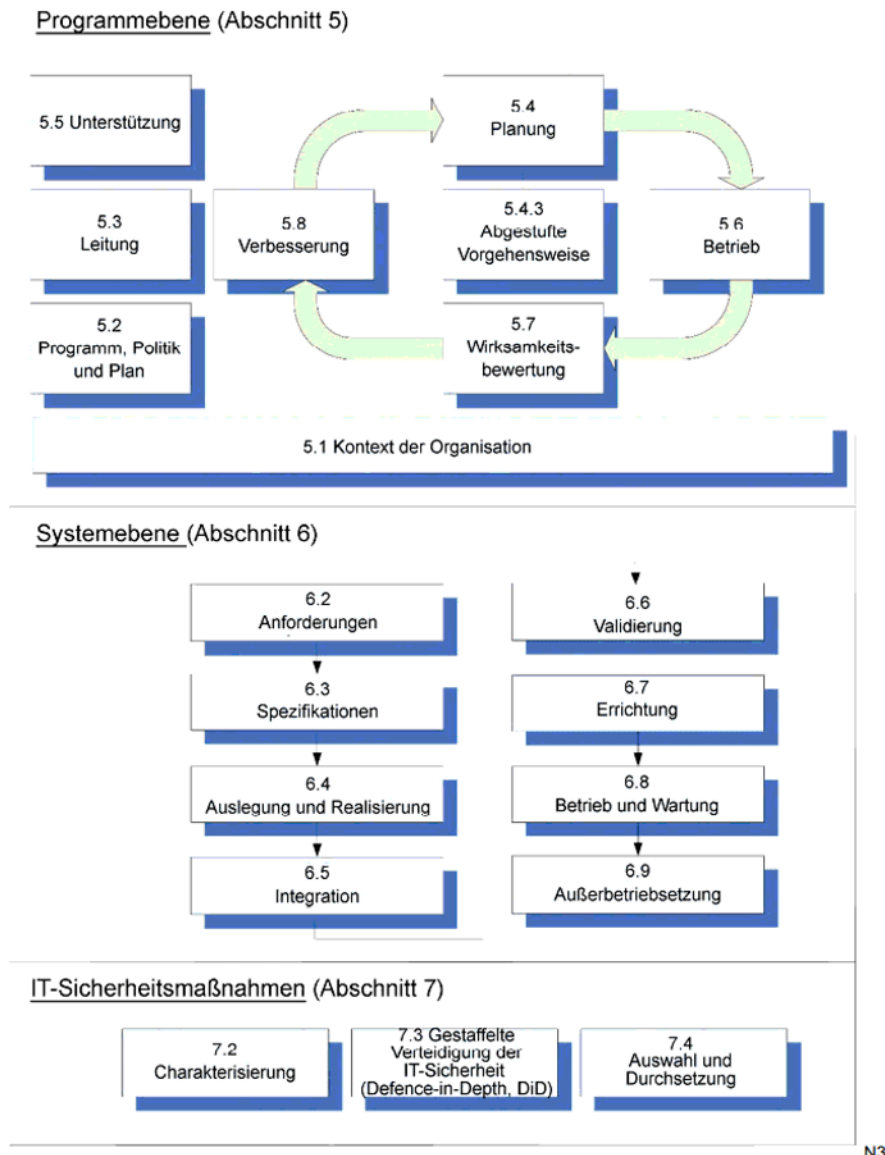
ANMERKUNG 2 Einige Unterabschnitte der ISO/IEC 27001:2013 enthalten interne Verweisungen auf andere Unterabschnitte der ISO/IEC 27001:2013. Falls zutreffend, sind die Verweisungen in den Unterabschnitten im Kontext der IEC 62645 zu berücksichtigen, jedoch verweisen sie nicht auf Unterabschnitte der IEC 62645. Siehe [Anhang C](#) als Hilfe bezüglich der Übereinstimmung.

Die Unterabschnitte für die abgestufte Vorgehensweise und die IT-Sicherheitskategorisierung sind auf ähnliche Art wie in [IEC 61226](#) organisiert.

[Abschnitt 6](#) enthält einen Sicherheitslebenszyklus auf Systemebene. Er ist wie der Systemlebenszyklus in [IEC 61513](#) strukturiert und an die speziellen Gesichtspunkte der Cybersicherheit angepasst.

[Abschnitt 7](#) behandelt Gesichtspunkte der Cybersicherheit auf der Ebene der IT-Sicherheitsmaßnahmen. Er stellt die Grundsätze einer mit ISO/IEC 27002:2013 übereinstimmenden Vorgehensweise dar, die in IEC 63096 weiter verfeinert werden.

[Bild 1](#) zeigt den Gesamtrahmen dieses Dokuments.



N3

Bild 1 – Gesamtrahmen der IEC 62645

In **IEC 61513** wird das Konzept eines Sicherheitslebenszyklus für die gesamte leittechnische Architektur und ein Sicherheitslebenszyklus für die einzelnen Systeme vorgestellt. Dabei wird als Teil des Gesamtrahmens die Erstellung eines IT-Sicherheitsplans angesprochen, in dem die vorzunehmenden prozeduralen und technischen Maßnahmen festgelegt werden, um die Architektur der leittechnischen Systeme vor digitalen Angriffen zu schützen, die sicherheitstechnisch wichtige Funktionen beeinträchtigen könnten. Die Vorkehrungen dieses Plans können, wie in **IEC 61226** beschrieben, zwischen Anforderungen für Systeme, die Funktionen der Kategorien A, B oder C ausführen, unterscheiden, und schließen die Einrichtung eines physischen und elektronischen Zugriffsschutzes mit ein. Dieses Dokument enthält detailliertere Anforderungen für den übergeordneten IT-Sicherheitsplan, wie er in **IEC 61513** angesprochen wird.

Zusätzliche Anforderungen für Software von Systemen, die Funktionen der Kategorie A ausführen, sind in **IEC 60880** und **IEC 62566** enthalten. Anforderungen für Software von Systemen mit Funktionen der Kategorie B und Systemen mit Funktionen der Kategorie C sind in **IEC 62138** zu finden.

Dieses Dokument ist auch für IT-Sicherheitsanforderungen an leittechnische Systeme anwendbar, die nicht im Anwendungsbereich der **IEC 61513**, **IEC 60880**, **IEC 62138** und **IEC 62566** liegen, jedoch das Potenzial haben, die Einrichtungen, Verfügbarkeit und Leistungsfähigkeit von Einrichtungen der Anlage zu beeinflussen.

^{N3} Nationale Fußnote: Der Kasten „5.4.3 Abgestufte Vorgehensweise“ ist im IEC-Original fälschlicherweise mit 5.4.2 bezeichnet.