

**DIN IEC 62954
(VDE 0491-5-7)**
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

ICS 27.120.20

Einsprüche bis 2016-07-13

Entwurf
**Kernkraftwerke –
Warten –
Anforderungen für Notfall-Reaktionseinrichtungen
(IEC 45A/1063/CD:2015)**

Nuclear power plants –
Control rooms –
Requirements for emergency response facilities
(IEC 45A/1063/CD:2015)

Centrales nucléaires de puissance –
Salles de commande –
Exigences relatives au Centre de Réponse d'Urgence (CRU)
(IEC 45A/1063/CD:2015)

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2016-05-13 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfs besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal des DIN unter www.entwuerfe.din.de bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an dke@vde.com möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/stellungnahme oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an die DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE, Stresemannallee 15, 60596 Frankfurt am Main.

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 50 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE

Anwendungsbeginn

Anwendungsbeginn dieser Norm ist ...

Inhalt

Seite

Nationales Vorwort.....	4
Nationaler Anhang NA (informativ) Zusammenhang mit Europäischen und Internationalen Dokumenten	6
Nationaler Anhang NB (informativ) Literaturhinweise.....	8
Einleitung	9
1 Zusammenhänge, Ziele und Anwendungsbereich.....	11
1.1 Zusammenhänge.....	11
1.2 Ziele	12
1.3 Anwendungsbereich	12
2 Normative Verweisungen	12
3 Begriffe	13
4 Abkürzungen	15
5 NRE-Auslegungsprinzipien	16
5.1 Allgemeines	16
5.2 Rolle und hauptsächliche Merkmale	16
5.2.1 Technisches Unterstützungszentrum (TUZ)	16
5.2.2 Notfall-Reaktionszentrum (NRZ)	16
5.2.3 Betriebliches Unterstützungszentrum (BUZ).....	17
5.3 Persönliche Sicherheits- und Zugangsschutz-Prinzipien	17
5.4 Verfügbarkeits-Prinzipien	17
5.5 Kommunikations-Prinzipien	18
5.6 Betriebserfahrung	18
6 NRE Lage und physikalische Merkmale.....	18
6.1 Lage und Zugang	18
6.2 Aufenthalt	19
6.3 Energieversorgungen	19
6.4 Dokumentation	19
7 Menschliche Einflussfaktoren	20
7.1 Allgemeines	20
7.2 Zusammensetzung der NRE-Teams.....	20
7.3 Lebensbedingungen	20
7.4 Arbeitsbereiche.....	20
7.5 Mensch-Maschine-Schnittstelle.....	21
8 Leittechnische Systeme.....	21
8.1 Sicherheits-Kategorisierung und Klassifizierung.....	21
8.2 Auslegung leittechnischer Systeme für NRE.....	21

8.3	Funktionen, die von innerhalb der NRE überwacht werden	22
8.4	Information	22
8.5	Funktionen im Zusammenhang mit NRE Aktivierung	22
8.6	Prüfbarkeit	22
8.7	Qualifizierung	22
9	Kommunikation.....	23
9.1	Art der Kommunikation.....	23
9.2	Datenkommunikation	23
9.3	Verbale Kommunikation	23
9.4	Nicht-verbale Kommunikationssysteme	24
9.5	Vertraulichkeit der Kommunikation	24
10	Wartung und Training.....	24
10.1	Wartbarkeit.....	24
10.2	Reparaturen	24
10.3	Periodische Nachprüfung von Geräten und verderblichem Gut	24
10.4	Training und Übungen.....	24
Anhang A (informativ) Für NRE relevante Auszüge aus IAEA Safety Guides.....		25
Anhang B (informativ) Literaturhinweise		27

Bilder

Bild 1 – NRE und Kommunikations-Einheiten in und außerhalb der Anlage	11
---	----

Tabellen

Tabelle NA.1	7
--------------------	---

Nationales Vorwort

Das internationale Dokument IEC 45A/1063/CD:2015 „Nuclear power plants – Control rooms – Requirements for emergency response facilities“ (CD, en: Committee Draft) ist unverändert in diesen Norm-Entwurf übernommen worden. Dieser Norm-Entwurf enthält eine noch nicht autorisierte deutsche Übersetzung.

Um Zweifelsfälle in der Übersetzung auszuschließen, ist die englische Originalfassung des CD entsprechend der diesbezüglich durch die IEC erteilten Erlaubnis beigelegt. Die Nutzungsbedingungen für den deutschen Text des Norm-Entwurfes gelten gleichermaßen auch für den englischen IEC-Text.

Das internationale Dokument wurde vom SC 45A „Instrumentation, control and electrical systems of nuclear facilities“ der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet und den nationalen Komitees zur Stellungnahme vorgelegt.

Da der Abstimmungszeitraum für einen FDIS bzw. Schluss-Entwurf prEN nur 2 Monate beträgt, und dann keine sachlichen Stellungnahmen mehr abgegeben werden können, sondern nur noch eine „JA/NEIN“-Entscheidung möglich ist, wobei eine „NEIN“-Entscheidung fundiert begründet werden muss, wird bereits der CD als DIN-Norm-Entwurf veröffentlicht, um die Stellungnahmen aus der Öffentlichkeit frühzeitig berücksichtigen zu können.

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

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.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. ISO [und/oder] IEC sind nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

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 62138 (VDE 0491-3-3):2010-03, *Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Softwareaspekte für rechnerbasierte Systeme zur Realisierung von Funktionen der Kategorien B oder C (IEC 62138:2004); Deutsche Fassung EN 62138:2009*
- DIN EN 61500 (VDE 0491-3-4):2011-12, *Kernkraftwerke – Leittechnik mit sicherheitstechnischer Bedeutung – Datenkommunikation (IEC 61500:2009); Deutsche Fassung EN 61500:2011*
- DIN EN 62566 (VDE 0491-3-5):2015-02, *Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Entwicklung HDL-programmierter integrierter Schaltkreise für Systeme, die Funktionen der Kategorie A ausführen (IEC 62566:2012); Deutsche Fassung EN 62566:2014*
- DIN IEC 62117 (VDE 0491-4):2001-10, *Kernkraftwerke – Druckwasserreaktoren – Überwachung ausreichender Kühlung des Kerns im abgeschalteten Zustand des Reaktors (IEC 62117:1999)*

- DIN EN 61839 (VDE 0491-5):2015-01, *Kernkraftwerke – Auslegung von Warten – Analyse und Zuordnung der Funktionen* (IEC 61839:2000); Deutsche Fassung EN 61839:2014
- DIN EN 60964 (VDE 0491-5-1):2010-08, *Kernkraftwerke – Warten – Auslegung* (IEC 60964:2009); Deutsche Fassung EN 60964:2010
- DIN EN 62241 (VDE 0491-5-2):2015-06, *Kernkraftwerke – Warte – Funktionen zur Meldung und Anzeige von Störungen* (IEC 62241:2004); Deutsche Fassung EN 62241:2015
- DIN IEC 61227 (VDE 0491-5-3):2009-01, *Kernkraftwerke – Warten – Handbedienungen* (IEC 61227:2008)
- DIN EN 61772 (VDE 0491-5-4):2013-09, *Kernkraftwerke – Warten – Anwendung von Sichtgeräten* (IEC 61772:2009); Deutsche Fassung EN 61772:2013
- DIN EN 60965 (VDE 0491-5-5):2011-12, *Kernkraftwerke – Warten – Notsteuerstellen für das Abfahren des Reaktors ohne Verbindung zur Hauptwarte* (IEC 60965:2009); Deutsche Fassung EN 60965:2011
- DIN IEC 60568 (VDE 0491-6):2006-11, *Kernkraftwerke – Instrumentierung mit sicherheitstechnischer Bedeutung – Kerninstrumentierung zur Messung der Neutronenflussdichte in Leistungsreaktoren* (IEC 60568:2006)
- DIN EN 60709 (VDE 0491-7):2010-12, *Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Physikalische und elektrische Trennung* (IEC 60709:2004); Deutsche Fassung EN 60709:2010
- DIN EN 62340 (VDE 0491-10):2010-12, *Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Anforderungen zur Beherrschung von Versagen aufgrund gemeinsamer Ursache* (IEC 62340:2007); Deutsche Fassung EN 62340:2010
- DIN EN 60671 (VDE 0491-100):2011-12, *Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Prüfungen zur Sicherstellung der Funktionsfähigkeit* (IEC 60671:2007); Deutsche Fassung EN 60671:2011

Als Norm-Entwürfe liegen vor:

- E DIN IEC 61226 (VDE 0491-1):2015-08, *Kernkraftwerke – Leittechnische und elektrische Systeme mit sicherheitstechnischer Bedeutung – Kategorisierung von Funktionen und Klassifizierung von Systemen* (IEC 45A/1018/CD:2015)
- E DIN IEC 62138 (VDE 0491-3-3):2015-01, *Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Softwareaspekte für rechnerbasierte Systeme zur Realisierung von Funktionen der Kategorien B oder C* (IEC 45A/962/CD:2014)
- E DIN IEC 61500 (VDE 0491-3-4):2016-02, *Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Datenkommunikation in Systemen, die Funktionen der Kategorie A ausführen* (IEC 45A/1044/CD:2015)
- E DIN IEC 62988 (VDE 0491-3-6):2016-04, *Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Auswahl und Einsatz drahtloser Geräte* (IEC 45A/1050/CD:2015)
- E DIN IEC 62645 (VDE 0491-3-7):2013-04, *Kernkraftwerke – Leittechnische Systeme – Anforderungen an die IT-Sicherheitsplanung für rechnerbasierte Systeme* (IEC 45A/890/CDV:2012)
- E DIN IEC 62859 (VDE 0491-3-8):2015-10, *Kernkraftwerke – Leittechnische Systeme – Anforderungen bezüglich der Koordination von Sicherheit und Cyber-Security* (IEC 45A/1014/CD:2015)
- E DIN IEC 60965 (VDE 0491-5-5):2014-11, *Kernkraftwerke – Warten – Notsteuerstellen für das Abfahren des Reaktors ohne Verbindung zur Hauptwarte* (IEC 45A/952/CD:2014)
- E DIN IEC 62646 (VDE 0491-5-6):2011-09, *Kernkraftwerke – Warten – Rechnerunterstützte Prozeduren* (IEC 45A/839/CDV:2011)
- E DIN IEC 62954 (VDE 0491-5-7):2016-06, *Kernkraftwerke – Warten – Anforderungen für Notfall-Reaktionseinrichtungen* (IEC 45A/1063/CD:2015)
- E DIN IEC 60709 (VDE 0491-07):2016-05, *Kernkraftwerke – Elektrische und leittechnische Systeme mit sicherheitstechnischer Bedeutung – Physikalische und elektrische Trennung* (IEC 45A/1046/CD:2015)
- E DIN IEC 61225 (VDE 0491-8):2012-06, *Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Anforderungen an die elektrische Energieversorgung* (IEC 61225:2005)

- E DIN IEC 62855 (VDE 0491-8-1):2014-11, *Kernkraftwerke – Elektrische Systeme – Analyse der Stromversorgung (IEC 45A/964/CD:2014)*
- E DIN IEC 60772 (VDE 0491-9-1):2014-11, *Kernkraftwerke – Sicherheitswichtige Instrumentierung – Elektrische Durchführungen für Sicherheitsbehälter (IEC 45A/966/CD:2014)*
- E DIN IEC 60744 (VDE 0491-9-2):2014-11, *Kernkraftwerke – Leittechnik mit sicherheitstechnischer Bedeutung – Sicherheitslogikanordnungen: Merkmale und Testverfahren (IEC 45A/946/CD:2014)*
- E DIN IEC 62808 (VDE 0491-9-3):2016-03, *Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Auslegung und Qualifizierung von Isolationseinrichtungen (IEC 62808:2015)*
- E DIN IEC 62887 (VDE 0491-9-4):2016-03, *Kernkraftwerke – Instrumentierung mit sicherheitstechnischer Bedeutung – Druckmessumformer: Eigenschaften und Prüfverfahren (IEC 45A/1045/CD:2015)*
- E DIN IEC 62003 (VDE 0491-11):2016-05, *Kernkraftwerke – Elektro- und leittechnische Systeme mit sicherheitstechnischer Bedeutung – Anforderungen für die Prüfung der Elektromagnetischen Verträglichkeit (IEC 45A/1052/CD:2015)*
- E DIN IEC 62705 (VDE 0491-15):2015-02, *Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Strahlungsüberwachungssysteme: Eigenschaften und Lebenszyklus (IEC 62705:2014)*
- E DIN IEC 61504 (VDE 0491-16):2015-10, *Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Zentralisierte Systeme zur kontinuierlichen Strahlungs- und/oder Radioaktivitätsüberwachung (IEC 45A/1016/CD:2015)*
- E DIN IEC 62342 (VDE 0491-20-1):2012-02, *Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Alterungsmanagement (IEC 62342:2007)*
- E DIN IEC/IEEE 62582-1 (VDE 0491-21-1):2015-06, *Kernkraftwerke – Leittechnik mit sicherheitstechnischer Bedeutung – Zustandsüberwachung elektrischer Geräte – Teil 1: Allgemeines (IEC/IEEE 62582-1:2011)*
- E DIN IEC/IEEE 62582-2 (VDE 0491-21-2):2015-08, *Kernkraftwerke – Leittechnik mit sicherheitstechnischer Bedeutung – Zustandsüberwachung elektrischer Geräte – Teil 2: Eindringprüfung (IEC/IEEE 62582-2:2011)*
- E DIN IEC/IEEE 62582-3 (VDE 0491-21-3):2015-07, *Kernkraftwerke – Leittechnik mit sicherheitstechnischer Bedeutung – Zustandsüberwachung elektrischer Geräte – Teil 3: Reißdehnung (IEC/IEEE 62582-3:2012)*
- E DIN IEC/IEEE 62582-4 (VDE 0491-21-4):2015-10, *Kernkraftwerke – Leittechnik mit sicherheitstechnischer Bedeutung – Zustandsüberwachung elektrischer Geräte – Teil 4: Oxidation (IEC/IEEE 62582-4:2011)*
- E DIN IEC/IEEE 62582-5 (VDE 0491-21-5):2016-03, *Kernkraftwerke – Leittechnik mit sicherheitstechnischer Bedeutung – Zustandsüberwachung elektrischer Geräte – Teil 5: Optische Zeitbereichsreflektometrie (IEC/IEEE 62582-5:2015)*
- E DIN IEC 62765-1 (VDE 0491-22-1):2015-06, *Kernkraftwerke – Leittechnik mit sicherheitstechnischer Bedeutung – Alterungsmanagement von Sensoren und Transmittern – Teil 1: Drucktransmitter (IEC 45A/1001/FDIS:2015)*
- E DIN IEC 60780-323 (VDE 0491-80):2014-03, *Kerntechnische Anlagen – Elektrisches Gerät mit sicherheitstechnischer Bedeutung – Qualifizierung (IEC 45A/940/CD:2013)*

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 Abschnichtsnummer, 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 11064	ISO 11064	DIN EN ISO 11064 (alle Teile)	
EN 60709	IEC 60709	DIN EN 60709 (VDE 0491-7)	VDE 0491-7
EN 60880	IEC 60880	DIN EN 60880 (VDE 0491-3-2)	VDE 0491-3-2
	IEC 60960		
EN 60964	IEC 60964	DIN EN 60964 (VDE 0491-5-1)	VDE 0491-5-1
EN 60965	IEC 60965	DIN EN 60965 (VDE 0491-5-5)	VDE 0491-5-5
EN 61226	IEC 61226	DIN EN 61226 (VDE 0491-1)	VDE 0491-1
EN 61227	IEC 61227	DIN IEC 61227 (VDE 0491-5-3)	VDE 0491-5-3
EN 61508 (alle Teile)	IEC 61508 (alle Teile)	DIN EN 61508 (VDE 0803) (alle Teile)	VDE 0803
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	IEC 61513	DIN EN 61513 (VDE 0491-2)	VDE 0491-2
	IEC 61771		
EN 61772	IEC 61772	DIN EN 61772 (VDE 0491-5-4)	VDE 0491-5-4
EN 61839	IEC 61839	DIN EN 61839 (VDE 0491-5)	VDE 0491-5
EN 62138	IEC 62138	DIN EN 62138 (VDE 0491-3-3)	VDE 0491-3-3
EN 62241	IEC 62241	DIN EN 62241 (VDE 0491-5-2)	VDE 0491-5-2
	IEC 62645	DIN IEC 62645 (VDE 0491-3-7) ^a	VDE 0491-3-7
	IEC 62859	DIN IEC 62859 (VDE 0491-3-8) ^a	VDE 0491-3-8
^a im Entwurfsstadium			

Nationaler Anhang NB (informativ)

Literaturhinweise

DIN EN ISO 11064 (alle Teile), *Ergonomische Gestaltung von Leitzentralen*

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

DIN EN 60880 (VDE 0491-3-2), *Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Softwareaspekte für rechnerbasierte Systeme zur Realisierung von Funktionen der Kategorie A*

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

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

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

DIN IEC 61227 (VDE 0491-5-3), *Kernkraftwerke – Warten – Handbedienungen*

DIN EN 61508 (VDE 0803) (alle Teile), *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme*

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

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

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

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

DIN EN 61513 (VDE 0491-2), *Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Allgemeine Systemanforderungen*

DIN EN 61772 (VDE 0491-5-4), *Kernkraftwerke – Warten – Anwendung von Sichtgeräten*

DIN EN 61839 (VDE 0491-5), *Kernkraftwerke – Auslegung von Warten – Analyse und Zuordnung der Funktionen*

DIN EN 62138 (VDE 0491-3-3), *Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Softwareaspekte für rechnerbasierte Systeme zur Realisierung von Funktionen der Kategorien B oder C*

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

DIN IEC 62645 (VDE 0491-3-7) (Entwurf), *Kernkraftwerke – Leittechnische Systeme – Anforderungen an die IT-Sicherheitsplanung für rechnerbasierte Systeme*

DIN IEC 62859 (VDE 0491-3-8) (Entwurf), *Kernkraftwerke – Leittechnische Systeme – Anforderungen bezüglich der Koordination von Sicherheit und Cyber-Security*

Einleitung

a) Technischer Hintergrund, hauptsächliche Inhalte und Organisation der Norm

Diese Norm wurde nach dem Fukushima-Daiichi-Störfall vorgeschlagen, um die Erfahrungen aus den dramatischen Ereignissen zu verarbeiten. Mehrere nach dem Vorfall auf nationaler Ebene (Bericht der japanischen Regierung) und internationaler Ebene (IAEA Fact Finding Mission) verfasste Berichte betonten die wichtige Rolle des Notfall-Reaktionszentrums (NRZ) während jener Ereignisse und hoben die Notwendigkeit hervor, die gewonnenen Erfahrungen zu berücksichtigen, um das Anforderungsprofil für eine solche Einrichtung zu schärfen.

Die Notwendigkeit für eine Norm wurde während des IEC/SC-45A-Treffens im Februar-März 2012 festgestellt. Im Juni 2013 wurde Einverständnis erzielt, dass IEC/SC 45A/WG 8 einen Projektvorschlag vorbereiten soll. Die Bestätigung des Projektvorschlags erfolgte im September 2014.

In verschiedenen Kommentaren der nationalen Komitees bezüglich des Projektvorschlags wurde die Intention deutlich, den Anwendungsbereich der vorgeschlagenen Norm zu konkretisieren. Diese Kommentare wurden anlässlich des IEC/SC-45A-Treffens im Oktober 2014 in der WG 8 diskutiert, mit folgenden Schlussfolgerungen:

- Der Anwendungsbereich soll dem der relevanten IAEA-Leitlinien entsprechen, wie in SSR-2/1 (dann als DS462 revidiert) und GSR Part 7 (dann als DS457 in Vorbereitung) angegeben;
- Im Anwendungsbereich sollen die in den IAEA-Leitlinien genannten auf die Notfallreaktionen bezogenen funktionalen Einrichtungen angesprochen werden (d.h. NRZ, TUZ und BUZ);
- Der Anwendungsbereich solle auf Einrichtungen beschränkt sein, die sich auf oder nahe dem Gelände des Kernkraftwerks befinden. Er sollte keine Aktivitäten enthalten, die im Verantwortungsbereich der lokalen für die Notfallreaktion zuständigen Stellen liegen;
- Die Anforderungen sollen in Form der auszuführenden Funktionen beschrieben werden;
- Die Norm soll die Art und Weise ansprechen, in der die Funktionen entsprechend unterschiedlicher Schwere von Störung oder Störfall ausgelöst werden, sowie alle Verantwortlichkeiten, die von der Hauptwarte auf die Notfall-Reaktionseinrichtungen (NRE) übertragen werden;
- Der Anwendungsbereich solle Überlegungen zu Anforderungen enthalten hinsichtlich Umgebungsüberwachung, Beleuchtung, Energieversorgungen, Zugangskontrolle der NRE usw., soweit notwendig, um die Durchführung der Notfall-Reaktionsfunktionen zu ermöglichen;
- Lediglich solche Bedienhandlungen sollen vorgesehen werden, die sich auf die o.g. Belüftung, Beleuchtung, Energieversorgungen, Zugangskontrolle der Notfall-Reaktionseinrichtung usw. beziehen;
- Die Norm solle berücksichtigen, dass es auf nationaler Ebene einen weiten Bereich von Bedingungen bezüglich Struktur und Vorkehrungen zur Notfall-Reaktionsunterstützung außerhalb der Anlage gibt.

Die vorliegende Norm befasst sich speziell mit den für Notfall-Reaktionseinrichtungen (NRE) relevanten Anforderungen.

Sie ist zur Verwendung durch Hersteller und Betreiber von Kernkraftwerken, Systemgutachter, Lieferfirmen und Unterlieferanten, und Genehmigungsbehörden vorgesehen.

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

IEC 62954 ist ein IEC/SC-45A-Dokument der dritten Ebene. Sie ist im Zusammenhang mit IEC 60964 zu sehen, dem Hauptdokument über Warten der Normen des IEC/SC 45A.

Eine allgemeine Beschreibung der Struktur der Normen des IEC/SC 45A findet sich in Abschnitt d) dieser Einleitung.

c) Empfehlungen und Einschränkungen der Anwendung der Norm

Es ist wichtig festzustellen, dass in dieser Norm die funktionalen Anforderungen für Notfall-Reaktionseinrichtungen behandelt und die Prozesse verdeutlicht werden, mit denen NRE Systeme geplant, entwickelt und betrieben werden, wenn Störfälle in Kernkraftwerken und/oder nuklearen Einrichtungen auftreten.

Es wird zur Kenntnis genommen, dass dies wegen der fortlaufenden Analyse der Fukushima Erfahrungen ein Entwicklungsgebiet für genehmigungstechnische Anforderungen ist. Daher ist das Ziel dieses Projekts eine Norm bereitzustellen, die den Rahmen absteckt, innerhalb dessen die landesspezifischen Anforderungen entwickelt und angewendet werden können.

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

Das Eingangsdokument zu den Normen des IEC/SC 45A stellt die Norm IEC 61513 dar. Diese enthält allgemeine Anforderungen an die leittechnischen Systeme und Geräte, die zur Ausführung sicherheitstechnisch wichtiger Funktionen in Kernkraftwerken genutzt werden. Durch die IEC 61513 werden die Normen des IEC/SC 45A strukturiert.

In IEC 61513 wird direkt auf andere Normen des IEC/SC 45A verwiesen, die allgemeinen Themen wie die Kategorisierung von Funktionen und die Klassifizierung von Systemen, Qualifizierung, Trennung von Systemen, Maßnahmen gegen Versagen aufgrund gemeinsamer Ursachen, Softwareaspekte rechnerbasierter Systeme, Hardwareaspekte rechnerbasierter Systeme, sowie die Auslegung von Warten behandeln. Die Normen, auf die direkt verwiesen wird, bilden die zweite Ebene und sollen zusammen mit IEC 61513 als ein in sich konsistenter Satz von Dokumenten betrachtet werden.

Die dritte Ebene bilden Normen des IEC/SC 45A, auf die in IEC 61513 nicht direkt verwiesen wird. Diese Normen behandeln spezielle Geräte, 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.

Für IEC 61513 wird ein Darstellungsformat verwendet, das dem der grundlegenden Sicherheitsnorm IEC 61508 ähnlich ist, mit einem Sicherheits-Lebenszyklus als Gesamtrahmen und zusätzlich einem System-Lebenszyklus. Mit IEC 61513 werden die allgemeinen nuklearen Sicherheitsanforderungen nach IEC 61508-1, IEC 61508-2 und IEC 61508-4 für die Anwendung auf dem nuklearen Sektor umgesetzt. In diesem Rahmen entsprechen IEC 60880 und IEC 62138 der Norm IEC 61508-3 für den nuklearen Sektor. IEC 61513 stützt sich für Themen der Qualitätssicherung (QS) sowohl auf ISO als auch auf IAEA GS-R-3 und IAEA GS-G-3.1.

In den Normen des IEC/SC 45A werden die Prinzipien und grundsätzlichen Sicherheitsaspekte des IAEA-Codes für die Sicherheit von Kernkraftwerken in der IAEA Sicherheitsserie umgesetzt, insbesondere die Requirements SSR-2/1, die die Sicherheitsanforderungen für die Auslegung von Kernkraftwerken festlegt, und die Safety Guide SSG-39, die die leittechnischen Systeme mit sicherheitstechnischer Bedeutung in Kernkraftwerken behandelt. Terminologie und Definitionen in den Normen des IEC SC 45A stimmen mit den von der IAEA verwendeten überein.

ANMERKUNG Für die Auslegung von leittechnischen Systemen in Kernkraftwerken, die der Realisierung konventioneller Sicherheitsfunktionen dienen (z.B. hinsichtlich Arbeitersicherheit, Schutz vor Sachschaden, chemischer Gefährdung, energetischer Gefährdung), wird die Anwendung internationaler oder nationaler Standards vorausgesetzt, die auf Anforderungen von Standards wie IEC 61508 beruhen.

Kernkraftwerke – Warten – Anforderungen für Notfall-Reaktionseinrichtungen

1 Zusammenhänge, Ziele und Anwendungsbereich

1.1 Zusammenhänge

Der Fukushima-Daiichi-Störfall hat gezeigt, dass extrem schwere Gefährdungen eintreten können, für die ein Kernkraftwerk nicht ausgelegt worden ist. In solchen Situationen ist man möglicherweise nicht nur mit einem oder mehreren beschädigten Reaktoren und der entsprechenden Freisetzung von radioaktiven Stoffen konfrontiert, sondern auch mit dem Verlust eines Großteils der elektrischen Energieversorgung, Kühlfunktionen und Leittechnik, gegebenenfalls einschließlich der Hauptwarte, sowie mit Schwierigkeiten bezüglich der Zugänglichkeit der Anlage. Es ist daher eine sehr große und wichtige Aufgabe, sichere Einrichtungen auf der Anlage zum Management eines derartigen Notfalls vorzusehen.

Infolge davon hat sich ein internationaler Konsens herausgebildet, die Auslegung und Einrichtung eines Satzes von Einrichtungen mit dem Ziel voranzutreiben, die Bemühungen des Personals zu koordinieren, das für die Steuerung der Notfallaktivitäten verantwortlich ist, und ebenso die Anstrengungen der Stellen außerhalb der Anlage, die mit dem Schutz der Bevölkerung und der Umgebung betraut sind. Diese Einrichtungen werden Notfall-Reaktionseinrichtungen (NRE) genannt.

Verschiedene Länder, Betreiber und Kernkraftwerke haben unterschiedliche geographische und infrastrukturelle Eigenheiten und somit unterschiedliche Anforderungen in Notfallsituationen. Es gelten jedoch dieselben Prinzipien hinsichtlich der Anforderungen innerhalb und außerhalb der Anlage.

Die IAEA Anforderungen zur Notfallreaktion sind in SSR-2/1 und GRS Teil 7 enthalten. Im informativen Anhang A sind die relevanten Auszüge dieser beiden IAEA-Veröffentlichungen zusammengestellt.

In Bild 1 sind die wichtigsten Überwachungsstellen, Notfall-Reaktionseinrichtungen und andere zugehörige Einrichtungen in und außerhalb der Anlage gezeigt. Einige der Einrichtungen in der Anlage könnten kombiniert werden, oder ihre Funktionen auf andere Einrichtungen in der Anlage aufgeteilt werden. Das Niveau von „Härtung“ und Autonomie der einzelnen Einrichtungen in der Anlage kann recht unterschiedlich sein.

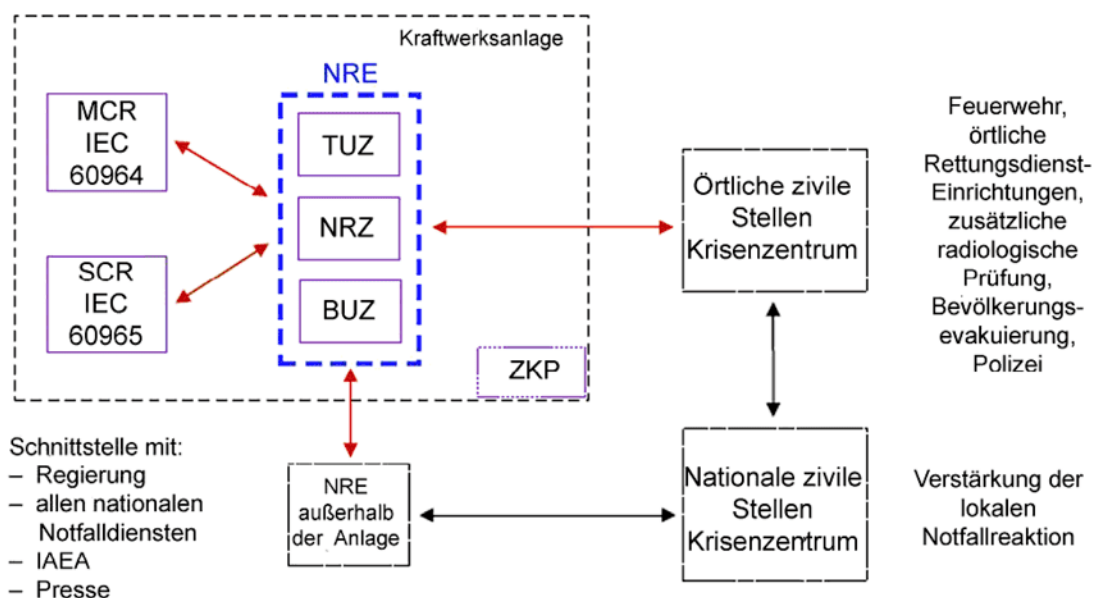


Bild 1 – NRE und Kommunikations-Einheiten in und außerhalb der Anlage

ANMERKUNG 1 Für die verschiedenen Notfall-Reaktionseinrichtungen in und außerhalb der Anlage hat sich noch keine allgemein anerkannte Terminologie herausgebildet. Die in dem Bild verwendeten Bezeichnungen entsprechen der für diese Norm gewählten Terminologie.

ANMERKUNG 2 Abhängig von örtlichen Zusammenhängen kann die „NRE in der Anlage“ auch nahe dem Kernkraftwerk realisiert werden.

ANMERKUNG 3 Die Rolle und Zusammensetzung der zivilen Stellen außerhalb der Anlage und der Notfall-Infrastruktur können bekannter Weise sehr variieren. Die entsprechenden Eintragungen im Bild sollten daher nur illustrativ verstanden werden.

1.2 Ziele

In dieser Norm werden die Anforderungen für die Notfall-Reaktionseinrichtungen in der Anlage (im Folgenden NRE genannt) behandelt.

Die Norm enthält Anforderungen für die NRE-Merkmale und NRE-Systeme, um

- die Auslegung und betrieblichen Bemühungen hinsichtlich Sicherheit und Strahlenschutz zu optimieren und zu koordinieren,
- die Feststellung und Lösung von möglichen Konflikten zwischen traditionellen betrieblichen Mitteln und Notfallmitteln zu verbessern (Hauptwarte/Notsteuerstelle und NRE, Betriebspersonal und Notfallteams, Betriebsprozeduren und Notfallprozeduren),
- die Feststellung und Verbesserung der potenziellen Synergien zwischen den traditionellen betrieblichen Mitteln und Notfallmitteln zu unterstützen.

1.3 Anwendungsbereich

Diese Norm ist für die Anwendung in neuen Kernkraftwerken gedacht, deren konzeptionelle Auslegung nach ihrer Veröffentlichung begonnen wird, sie kann aber auch für Auslegung und Realisierung von NRE in bestehenden Kernkraftwerken oder anderen nuklearen Einrichtungen verwendet werden.

Detaillierte Geräteauslegung liegt außerhalb des Anwendungsbereichs dieser Norm.

In dieser Norm werden nicht die Situationen definiert (Bedingungen, Gefährdungen und Größe der Gefährdungen), die zur Mobilisierung von Notfall-Reaktionsteams und Aktivierung/Verwendung der NRE führen. Solche Aspekte sollten im Notfallplan des Kernkraftwerks behandelt werden. Die notwendige Konsistenz von NRE-Auslegung und Betrieb mit dem Notfallplan liegt jedoch im Anwendungsbereich dieser Norm.

2 Normative Verweisungen

Die folgenden Dokumente, die in diesem Dokument teilweise oder als Ganzes zitiert werden, sind für die Anwendung dieses Dokuments erforderlich. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

IEC 60709, *Nuclear Power Plants – Instrumentation and control systems important to safety – Separation*

IEC 60960, *Functional design criteria for a safety parameter display system for nuclear power stations*

IEC 60964, *Nuclear Power Plants – Control rooms – Design*

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

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

IEC 61227, *Nuclear Power Plants – Control Rooms – Operator Controls*

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

IEC 61771, *Nuclear Power Plants – Main Control Room – Verification and Validation of design*

IEC 61772, *Nuclear Power Plants – Control rooms – Application of Visual Display Unit (VDU)*

IEC 61839, *Nuclear Power Plants – Design of Control Room – Functional Analysis & Assignments*

IEC 62241, *Nuclear Power Plants – Main Control Room – Alarm functions and presentation*

IEC 62645, *Nuclear Power Plants – Instrumentation and control systems – Requirements for security programmers for computer-based systems*

IEC 62859, *Nuclear Power Plants – Instrumentation and control systems – Requirements for coordinating safety and cybersecurity (currently at CDV)*

ISO 11064, *Ergonomic design of control centres; Parts 1-7*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

3.1

Zugangskontrollpunkt

(en: access control point)

einer oder mehrere der Bereiche innerhalb der Sicherungsgrenze der Anlage, um den Zutritt und Austritt von off-site-Personal zu kontrollieren, im speziellen Notfall-Teams

3.2

Störungsmeldung

(en: alarm)

diagnostische, prognostische oder hinweisende Information, die dazu dient, den Operateur auf eine Abweichung eines Systemzustandes oder eines Prozesses vom Soll-Zustand aufmerksam zu machen

ANMERKUNG Spezifische Informationen von Störungsmeldungen umfassen Angaben über das Bestehen einer Störung, für die eine korrigierende Maßnahme notwendig sein könnte, die Ursache und möglichen Folgen einer Störung, den allgemeinen Anlagenzustand, korrigierende Maßnahmen zur Behebung der Anomalie, und Rückmeldungen über korrigierende Maßnahmen.

Zwei Arten von Abweichungen können erkannt werden:

- ungeplante: unerwünschte Prozessabweichungen und Gerätefehler;
- geplante: Abweichungen von Prozessbedingungen oder des Gerätestatus, die der erwarteten Reaktion auf Anlagenzustände entsprechen, jedoch ein Anzeichen für unerwünschte Entwicklungen sein könnten.

[IEC 62241]

3.3

Sammelpunkt

(en: assembly point)

Ort (einer oder mehrere), an dem nicht essentielles Personal auf der Anlage gesammelt, registriert und geschützt oder evakuiert wird

3.4

Notfall

(en: emergency)

außergewöhnliche Situation oder Ereignis, die/das eine prompte Aktion erfordert, um vor allem eine Gefährdung oder schlimme Konsequenzen für Gesundheit und Sicherheit von Menschen, für Lebensqualität, Eigentum oder Umwelt abzumildern. Unter solchen Ereignissen werden nukleare und radiologische Notfälle und konventionelle Notfälle wie Feuer, Freisetzung gefährlicher Chemikalien, Sturm oder Erdbeben verstanden.

3.5

Notfallplan

(en: emergency plan)

Beschreibung von Zielen, Vorgehensweise und Konzept der Reaktionen auf einen Notfall und der Struktur, Institutionen und Verantwortlichkeiten für eine systematische, koordinierte und effektive Reaktion. Der Notfallplan dient als Basis für die Entwicklung weiterer Pläne, Prozeduren und Checklisten.

[IAEA GSR Teil 7 (DS457)]

3.6

Notfallreaktion

(en: emergency response)

Leistungsfähigkeit der Aktionen zur Abmilderung der Folgen eines Notfalls für Leben und Gesundheit des Menschen, Eigentum und Umwelt.

[IAEA GSR Teil 7 (DS457)]

3.7

Notfall-Reaktionszentrum (NRZ)

(en: emergency response center ERC)

Bereich neben oder in der Nähe der Anlage für den Stab, der aufgestellt wurde, um die Situation während eines Notfalls im Griff zu behalten.

3.8

Notfall-Reaktionseinrichtung (NRE) oder -Reaktionsstelle

(en: emergency response facility (ERF) or location)

Einrichtung oder Stelle zur Unterstützung einer Notfallreaktion, der im Bereitschaftsstatus bestimmte bei Notfallbedingungen einsatzfähige Funktionen zugeordnet sind.

[IAEA GSR Teil 7 (DS457)]

3.9

Betriebliches Unterstützungszentrum (BUZ)

(en: operational support center OSC)

Von der Hauptwarte getrennter Bereich, in dem sich der Stab zur Betriebsunterstützung des Kernkraftwerks in einer Notfallsituation einfindet, um verschiedene Aufgaben übernehmen zu können (z.B. Umgebungsüberwachung, Gesundheitsüberwachung, Schadenskontrolle, Brandbekämpfung).

3.10

Technisches Unterstützungszentrum (TUZ)

(en: technical support center TSC)

Von der Hauptwarte getrennter Bereich, in dem sich der Stab zur Betriebsunterstützung des Kernkraftwerks im Fall einer Reaktorstörung oder eines Reaktorstörfalles versammeln kann, um für die Wartenoperatoren eine technische Unterstützung bereitzustellen.

N1)

4 Abkürzungen

ACP	Access Control Point	ZKP	Zugangskontrollpunkt
ERC	Emergency Response Center	NRZ	Notfall-Reaktionszentrum
ERF	Emergency Response Facility	NRE	Notfall-Reaktionseinrichtung
HMI	Human Machine Interface	MMS	Mensch-Machine-Schnittstelle
I&C	Instrumentation and Control	LT	Leittechnik
MCR	Main Control Room		Hauptwarte
NPP	Nuclear Power Plant	KKW	Kernkraftwerk
PIE	Postulated Initiating Event	AAE	Anzunehmendes auslösendes Ereignis
PPE	Personal Protective Equipment		Persönliche Schutzausrüstung
OSC	Operational Support Center	BUZ	Betriebliches Unterstützungszentrum
SCR	Supplementary Control Room		Notsteuerstelle
TSC	Technical Support Center	TUZ	Technisches Unterstützungszentrum

N1) Nationale Fußnote: Weitere wichtige, aber im IEC-Dokument nicht enthaltene Definitionen sind:

3.N1

menschliche Einflussfaktoren

(en: human factors – HF)

Faktoren zur Berücksichtigung der menschlichen Fähigkeiten und Grenzen in Hinblick auf die Auslegung der Anlage, der Systeme und Geräte

3.N2

Auslegung unter Berücksichtigung des Faktors Mensch

(en: human factor engineering – HFE)

Anwendung des Wissens über die menschlichen Fähigkeiten und Grenzen in Hinblick auf die Auslegung der Anlage, der Systeme und Geräte. Damit wird sichergestellt, dass die Auslegung der Anlage, der Systeme und Geräte, die Aufgaben des Menschen und die Umgebungsbedingungen mit den Sinnes-, Wahrnehmungs-, kognitiven und physischen Merkmalen des Personals kompatibel sind, das Anlagen, Systeme und Geräte betreibt und wartet

[IEC 61226]

3.N3

Konzept der gestaffelten Verteidigung

(en: defence in depth – DiD)

Anwendung von mehr als einer Schutzmaßnahme zum Erreichen eines gegebenen Sicherheitsziels, so dass dieses erreicht wird, auch wenn eine der Schutzmaßnahmen versagt

ANMERKUNG Die Schutzmaßnahmen für DiD können eines oder mehrere der folgenden Elemente umfassen:

- das Bestehen mehrerer Gruppen von Sicherheitsfunktionen, wobei für jede Gruppe volle Übereinstimmung mit den Auslegungsspezifikationen sichergestellt ist;
- das parallele Bestehen von passiven und aktiven Systemen;
- das Bestehen gegenseitig unabhängiger Sicherheits- und Betriebssysteme, deren Aktionen im Anforderungsfall kumulativ sind;
- die parallele Anwendung unterschiedlicher Auslegungsmethoden, um die Robustheit und Fehlertoleranz der Systeme zu steigern.

[IEC 60880]