

	DIN IEC 60964 (VDE 0491-5-1)	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 2007-12-31		
Entwurf		
Kernkraftwerke – Warten – Auslegung (IEC 45A/652/CDV:2007) Nuclear power plants – Control rooms – Design (IEC 45A/652/CDV:2007) Centrales nucléaire de puissance – Salles de commande – Conception (CEI 45A/652/CDV:2007) Anwendungswarnvermerk Dieser Norm-Entwurf wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt. Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfes besonders zu vereinbaren. Stellungnahmen werden erbeten – vorzugsweise als Datei per E-Mail an dke@vde.com in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.dke.de/stellungnahme abgerufen werden – oder in Papierform an die DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE, Stresemannallee 15, 60596 Frankfurt am Main. Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevante Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen. Gesamtumfang 76 Seiten DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE		

Beginn der Gültigkeit

Diese Norm gilt ab ...

Nationales Vorwort

Das internationale Dokument IEC 45A/652/CDV:2007 „Nuclear power plants – Control rooms – Design“ (CDV, en: Committee Draft for Vote) ist unverändert in diesen Norm-Entwurf übernommen worden. Dieser Norm-Entwurf enthält eine noch nicht autorisierte deutsche Übersetzung.

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

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

Da der Abstimmungszeitraum für einen FDIS (en: Final Draft International Standard) nur 2 Monate beträgt, und dann keine sachlichen Stellungnahmen mehr abgegeben werden können, sondern nur noch eine „JA/NEIN“-Entscheidung möglich ist, wobei eine „NEIN“-Entscheidung fundiert begründet werden muss, wird bereits der CDV als DIN-Norm-Entwurf veröffentlicht, um die Stellungnahmen aus der Öffentlichkeit noch vor der Abstimmung berücksichtigen zu können.

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

In der Reihe VDE 0491 sind als Normen erschienen:

- DIN IEC 61226 (VDE 0491-1):2005-09, *Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Kategorisierung leittechnischer Funktionen (IEC 61226:2005)*.
- DIN IEC 61513 (VDE 0491-2):2002-10, *Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Allgemeine Systemanforderungen (IEC 61513:2001)*.
- DIN IEC 61513/A100 (VDE 0491-2/A100):2005-02, *Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Allgemeine Systemanforderungen – Nationaler Anhang ND (informativ): Mitgeltende Festlegungen aus anderen IEC-Normen*.
- DIN IEC 60880 (VDE 0491-3-2):2007-08, *Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Softwareaspekte für rechnerbasierte Systeme zur Realisierung von Funktionen der Kategorie A (IEC 60880:2006)*.
- DIN IEC 62138 (VDE 0491-3-3):2004-09, *Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Softwareaspekte für rechnerbasierte Systeme zur Realisierung von Funktionen der Kategorien B oder C (IEC 62138:2004)*.
- DIN IEC 62117 (VDE 0491-4):2001-10, *Kernkraftwerke – Druckwasserreaktoren – Überwachung ausreichender Kühlung des Kerns im abgeschalteten Zustand des Reaktors (IEC 62117:1999)*.
- DIN IEC 61839 (VDE 0491-5):2002-09, *Kernkraftwerke – Auslegung von Warten – Analyse und Zuordnung der Funktionen (IEC 61839:2000)*.
- DIN IEC 62241 (VDE 0491-5-2):2006-05, *Kernkraftwerke – Hauptwarte – Funktionen zur Meldung und Anzeige von Störungen (IEC 62241:2004)*.
- DIN IEC 60568 (VDE 0491-6):2006-11, *Kernkraftwerke – Instrumentierung mit sicherheitstechnischer Bedeutung – Kerninstrumentierung zur Messung der Neutronenflussdichte in Leistungsreaktoren (IEC 60568:2006)*.
- DIN IEC 60709 (VDE 0491-7):2006-05, *Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Physikalische und elektrische Trennung (IEC 60709:2004)*.

Als Norm-Entwürfe liegen vor:

- E DIN IEC 60987 (VDE 0491-3-1):2006-09, *Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Anforderungen an die Hardware-Auslegung rechnerbasierter Systeme (IEC 45A/623/CDV:2006)*.
- E DIN IEC 60964 (VDE 0491-5-1):2007-11, *Kernkraftwerke – Warten – Auslegung (IEC 45A/652/CDV:2007)*.
- E DIN IEC 61227 (VDE 0491-5-3):2007-08, *Kernkraftwerke – Warten – Handbedienungen (IEC 45A/649/CDV:2007)*.
- E DIN IEC 62340 (VDE 0491-10):2006-04, *Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Versagen gemeinsamer Ursache (CCF) (IEC 45A/601/CDV:2005)*.
- E DIN IEC 60671 (VDE 0491-100):2006-05, *Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Sicherstellung der Betriebsbereitschaft (IEC 45A/604/CDV:2005)*.

Nationaler Anhang NA (informativ)

Zusammenhang mit Europäischen und Internationalen Normen

Für den Fall einer undatierten Verweisung im normativen Text (Verweisung auf eine Norm ohne Angabe des Ausgabedatums und ohne Hinweis auf eine Abschnittsnummer, eine Tabelle, ein Bild usw.) bezieht sich die Verweisung auf die jeweils neueste gültige Ausgabe der in Bezug genommenen Norm.

Für den Fall einer datierten Verweisung im normativen Text bezieht sich die Verweisung immer auf die in Bezug genommene Ausgabe der Norm.

Eine Information über den Zusammenhang der zitierten Normen mit den entsprechenden Deutschen Normen ist in Tabelle NA.1 wiedergegeben.

Tabelle NA.1

Europäische Norm	Internationale Norm	Deutsche Norm	Klassifikation im VDE-Vorschriftenwerk
–	IEC 60709	DIN IEC 60709 (VDE 0491-7)	VDE 0491-7
–	IEC 60780	DIN IEC 60780	–
–	IEC 60960	–	–
–	IEC 60965	–	–
–	IEC 60980	–	–
–	IEC 61225	–	–
–	IEC 61226	DIN IEC 61226 (VDE 0491-1)	VDE 0491-1
–	IEC 61227 Zz. in Überarbeitung	Siehe Norm-Entwurf E DIN IEC 61227 (VDE 0491-5-3)	VDE 0491-5-3
–	IEC 61513	DIN IEC 61513 (VDE 0491-2)	VDE 0491-2
–	IEC 61771	–	–
–	IEC 61772	–	–
–	IEC 61839	DIN IEC 61839 (VDE 0491-5)	VDE 0491-5
–	IEC 62241	DIN IEC 62241 (VDE 0491-5-2)	VDE 0491-5-2
EN ISO 11064-1	ISO 11064	DIN EN ISO 11064-1	–

– Entwurf –

E DIN IEC 60964 (VDE 0491-5-1):2007-11

Nationaler Anhang NB (informativ)

Literaturhinweise

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

DIN IEC 60780, *Kernkraftwerke – Elektrisches Gerät des Sicherheitssystems – Qualifizierung*

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

E DIN IEC 61227 (VDE 0491-5-3):2007-08, *Kernkraftwerke – Warten – Handbedienungen (IEC 45A/649/CDV:2007)*.

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

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

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

DIN EN ISO 11064-1, *Ergonomische Gestaltung von Leitzentralen – Teil 1: Grundsätze für die Gestaltung von Leitzentralen*

Kernkraftwerke – Warten – Auslegung

Inhalt

	Seite
Einleitung	7
1 Anwendungsbereich	8
2 Normative Verweisungen	8
3 Begriffe	9
4 Anwendung der Norm.....	14
5 Auslegungsprinzipien für die Hauptwarte	14
5.1 Hauptaufgaben der Hauptwarte	14
5.2 Funktionales Auslegungsziel der Hauptwarte	14
5.3 Sicherheitsprinzipien	15
5.4 Verfügbarkeitsprinzipien	15
5.5 Human-Factor-Prinzipien.....	15
5.6 Betriebsprinzipien des Betreibers.....	16
5.7 Beziehung zu anderen Kontroll- und Managementzentren	16
5.8 Betriebserfahrung	16
6 Funktionale Auslegung der Hauptwarte	17
6.1 Allgemeines	17
6.2 Funktionsanalyse.....	17
6.2.1 Allgemeines	17
6.2.2 Festlegung von Funktionen	17
6.2.3 Anforderungen an Informationsfluss und -verarbeitung	17
6.3 Zuordnung von Funktionen.....	18
6.3.1 Allgemeines	18
6.3.2 Operateurfähigkeiten	18
6.3.3 Verarbeitungs-Fähigkeiten des leittechnischen Systems.....	19
6.4 Verifizierung der Funktionszuordnung.....	19
6.4.1 Allgemeines	19
6.4.2 Verifizierungsprozess	19
6.5 Validierung der Funktionszuordnung.....	20
6.5.1 Allgemeines	20
6.5.2 Validierungsprozess	20
6.5.3 Allgemeine Bewertungskriterien für die Validierung.....	20
6.6 Analyse der Arbeitsaufgabe	20
7 Funktionale Auslegungsspezifikation	21
7.1 Allgemeines	21
7.2 Erstellung einer Datenbasis über menschliche Fähigkeiten und Eigenschaften	21
7.3 Lage, Umgebung und Schutz.....	21
7.3.1 Lage.....	21
7.3.2 Umgebung	21
7.3.3 Schutz.....	22
7.4 Platzverhältnisse und Anordnung.....	23
7.4.1 Platzverhältnisse	23
7.4.2 Anordnung	23
7.5 Belegung von Schalttafeln.....	24
7.5.1 Prioritäten	24
7.5.2 Anordnung auf Schaltpulten und Schalttafeln	24

– Entwurf –

E DIN IEC 60964 (VDE 0491-5-1):2007-11

	Seite
7.5.3 Spiegelbildliche Anordnung	24
7.6 Lokalisierungshilfen	24
7.6.1 Gruppierung von Informationsanzeigen und Bediengeräten	24
7.6.2 Bezeichnungen und Kennzeichnung	25
7.6.3 Kodierung	26
7.6.4 Beschriftung	26
7.7 Leittechnische Systeme	26
7.7.1 Informationsfunktionen	27
7.7.2 Bedienfunktionen	30
7.8 Integration von Bedienung und Anzeige	31
7.9 Kommunikationssystem	32
7.9.1 Allgemeines	32
7.9.2 Verbale Kommunikationssysteme	32
7.9.3 Nicht verbale Kommunikationssysteme	33
7.10 Andere Anforderungen	33
7.10.1 Energieversorgung	33
7.10.2 Qualifizierung	33
7.10.3 Wartbarkeit	33
7.10.4 Reparaturen	34
7.10.5 Testbarkeit	34
8 Verifizierung und Validierung des integrierten Wartensystems	34
8.1 Allgemeines	34
8.2 Verifizierung des Wartensystems	34
8.2.1 Verifizierungsprozess	34
8.2.2 Allgemeine Bewertungskriterien für die Verifizierung des integrierten Systems	34
8.3 Validierung des Wartensystems	34
8.3.1 Validierungsprozess	34
8.3.2 Allgemeine Bewertungskriterien für die Validierung des Gesamtsystems	35
Anhang A (informativ) Erläuterung von Konzepten	38
 Bild 1 – Überblick über das Wartensystem	 36
Bild 2 – Gesamter Auslegungsprozess mit Bezügen zu den Abschnitten dieser Norm	37
 Tabelle A.1 – Mensch und Maschine in der funktionalen und der physikalischen Domäne	 39

Einleitung

a) Technischer Hintergrund, hauptsächliche Inhalte und Organisation der Norm

Die Norm IEC 60964:1989 ist entwickelt worden, um für die Auslegung von Hauptwarten von Kernkraftwerken relevante Anforderungen bereitzustellen. Die erste Ausgabe von IEC 60964 wurde von der Nuklearindustrie extensiv genutzt. Inzwischen aber ist klar geworden, dass neuere technische Entwicklungen, insbesondere die auf Software-Technologie basierenden, Eingang in die Norm finden sollten. Außerdem sollten die Beziehungen zu den mit IEC 60964 zusammenhängenden Normen (d. h. IEC 61227, IEC 61771, IEC 61772 IEC 61839 und IEC 62241) verdeutlicht und angepasst werden.

Diese Norm bezieht sich speziell auf die funktionale Auslegung von Hauptwarten für Kernkraftwerke. Sie ist zur Verwendung durch Kraftwerksbetreiber, Systemgutachter und Genehmigungsbehörden vorgesehen.

b) Einordnung der vorliegenden Norm in die Struktur der IEC-SC-45A-Normenreihe

Vorliegende Norm IEC 60964 ist ein IEC SC 45A Dokument der zweiten Ebene und behandelt generische Themen der Wartenauslegung.

Die Norm IEC 60964 ist in Verbindung mit den mit ihr zusammenhängenden oben genannten Normen anzuwenden, welche die zutreffenden IEC-SC-45A-Dokumente für Handbedienungen, Auslegungs-Verifizierung und -Validierung, Anwendung von Sichtgeräten, Funktionsanalyse und Funktionszuordnung sowie Funktionen zur Meldung und Anzeige von Störungen darstellen.

Mehr Details über die Struktur der IEC-SC-45A-Normenreihe finden sich im vierten Abschnitt dieser Einleitung.

c) Empfehlungen und Einschränkungen der Anwendung der Norm

Diese Norm ist zur Anwendung auf neue Warten gedacht, deren konzeptionelle Auslegung nach Veröffentlichung dieser Norm begonnen wurde. Die Anforderungen und Empfehlungen dieser Norm können auch für Verbesserungen, Modernisierungen und Modifizierungen bestehender Warten verwendet werden.

Hauptzweck der Norm ist die Bereitstellung von funktionalen Auslegungsanforderungen für Hauptwarten von Kernkraftwerken, um die betrieblichen und sicherheitstechnischen Anforderungen erfüllen zu können.

Diese Norm enthält auch funktionale Anforderungen für Schnittstellen, die sich auf die Zusammensetzung des Wartenpersonals, die Betriebsprozeduren und Trainingsprogramme beziehen, die zusammen mit der Mensch-Machine-Schnittstelle das Wartensystem bilden.

Um die zukünftige Relevanz dieser Norm sicherzustellen, wurde der Schwerpunkt der Ausführungen eher auf grundsätzliche Anforderungen und nicht auf spezielle Technologien gelegt.

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

Das Eingangsdokument zur IEC-SC-45A-Normenreihe stellt die Norm IEC 61513 dar. Sie enthält allgemeine Anforderungen an die leittechnischen Systeme und Geräte, die zur Ausführung sicherheitstechnisch wichtiger Funktionen in Kernkraftwerken genutzt werden. Durch die IEC 61513 wird die SC-45A-Normenreihe strukturiert.

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

E DIN IEC 60964 (VDE 0491-5-1):2007-11

Die dritte Ebene bilden IEC-SC-45A-Normen, auf die in IEC 61513 nicht direkt verwiesen wird. Diese Normen behandeln spezielles Gerät, technische Methoden oder spezifische Aktivitäten. Sie beziehen sich hinsichtlich der allgemeinen Themen auf die Dokumente der zweiten Ebene, können jedoch im Allgemeinen für sich alleine benutzt werden.

Eine vierte Ebene erweitert die SC-45A-Normenreihe 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 Anforderungen (für Sicherheitssysteme unterschiedlicher industrieller Anwendungen) von IEC 61508-1, -2 und -4, für die Anwendung auf dem nuklearen Sektor umgesetzt. Die Einhaltung der IEC 61513 erleichtert somit die Übereinstimmung mit IEC 61508, weil deren allgemeine Anforderungen für die nukleare Industrie berücksichtigt wurden. In diesem Rahmen entsprechen IEC 60880 und IEC 62138 für den nuklearen Sektor der IEC 61508-3.

IEC 61513 stützt sich für Themen der Qualitätssicherung sowohl auf ISO-Normen als auch auf IAEA 50-C-QA ab.

In der IEC-SC-45A-Normenreihe werden die Prinzipien und grundsätzlichen Sicherheitsaspekte des IAEA Codes für die Sicherheit von KKW und der IAEA Sicherheitsserie umgesetzt, insbesondere die Requirements NS-R-1 „Safety of Nuclear Power Plants: Design“ und der Safety Guide NS-G-1.3 „Instrumentation and control systems important to safety in Nuclear Power Plants“. Terminologie und Definitionen in den IEC-SC-45A-Normen stimmen mit den von der IAEA verwendeten überein.

1 Anwendungsbereich

Diese Norm legt Anforderungen für die Mensch-Maschine-Schnittstelle in Hauptwarten von Kernkraftwerken fest. Sie enthält auch Anforderungen zur Auswahl von Funktionen, Auslegungsüberlegungen und Organisation der Mensch-Maschine-Schnittstellen sowie Prozeduren, die systematisch verwendet werden müssen, um die funktionale Auslegung zu verifizieren und zu validieren. Die Anforderungen reflektieren die Human-Factor-Prinzipien, wie sie auf die Mensch-Maschine-Schnittstelle bei normalen und anomalen Anlagenzuständen anzuwenden sind. Diese Norm befasst sich nicht mit speziellen oder normalerweise unbeaufsichtigten Bedienstellen, wie sie zum Abfahren von außerhalb der Hauptwarte, für die Handhabung radioaktiver Abfälle oder Notfalleinrichtungen vorgesehen sind. Auch die detaillierte Geräte-Auslegung ist nicht Gegenstand dieser Norm.

Hauptzweck der Norm ist die Bereitstellung von funktionalen Auslegungsanforderungen für Hauptwarten von Kernkraftwerken, um die betrieblichen und sicherheitstechnischen Anforderungen erfüllen zu können. Diese Norm enthält außerdem funktionale Anforderungen für Schnittstellen, die sich auf die Zusammensetzung der Wartemannschaft, die Betriebsprozeduren und Trainingsprogramme beziehen, die zusammen mit der Mensch-Maschine-Schnittstelle das Wartensystem bilden.

Diese Norm ist zur Anwendung auf neue Warten gedacht, deren konzeptionelle Auslegung nach Veröffentlichung dieser Norm begonnen wurde. Wenn die Anwendung auf eine bestehende Warte gewünscht ist, muss dieses mit Bedacht erfolgen, um die Konsistenz der Auslegungsbasis beizubehalten.

2 Normative Verweisungen

Die folgenden zitierten Dokumente sind für die Anwendung dieses Dokuments erforderlich. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

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

IEC 60780, *Nuclear Power Plants – Electrical equipment of the safety system – Qualification.*

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

IEC 60965, *Supplementary control points for reactor shutdown without access to the main control room.*

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

IEC 61225, *Nuclear Power Plants – Instrumentation and Control Systems Important for Safety – Requirements for electrical supplies.*

IEC 61226, *Nuclear Power Plants – Instrumentation and Control Systems Important for Safety – Classification.*

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

IEC 61513, *Nuclear Power Plants – Instrumentation and Control 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 – Main Control Room – Application of Visual Display Units (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.*

ISO 11064, *Ergonomic design of control centres; Parts 1-4, 5-7.*

IAEA, 50-SG-D4, *Protection against internally generated missiles and their secondary effects in nuclear power plants.*

IAEA 50-SG-D6, *Ultimate heat sink and directly associated heat transport systems for nuclear power plants.*

3 Begriffe

Für diese Norm gelten die folgenden Definitionen. Zu weiteren Begriffe wird auf die allgemeine Terminologie nach IEC 61513 verwiesen, sowie auf die Publikationen des IAEA-NUSS-Programms, wie den Safety Guide NS-G-1.3.

3.1

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 könnten, 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]

3.2

Hilfsbediensysteme

(en: auxiliary control (operating) systems)

außerhalb der Warte installierte Bediensysteme, z. B. örtliche Bedienstellen für die Anlage oder für die Abschaltssysteme der Anlage

3.3

Bedienelemente

Bediengeräte

(en: controls)

vom Operateur verwendete Einrichtungen, um Befehlssignale an Steuerungssysteme und Anlagenkomponenten zu senden

3.4

Wartenpersonal

(en: control room staff)

in der Warte stationierte Gruppe von Anlagenpersonal, die für das Erreichen der betrieblichen Ziele verantwortlich ist, indem die Anlage über die Mensch-Maschine-Schnittstelle gesteuert wird. Üblicherweise besteht die Wartemannschaft aus übergeordneten Operateuren und Operateuren, die Bedienhandlungen durchführen. Sie kann aber auch Anlagenpersonal und Experten einschließen, die zur Anwesenheit in der Warte berechtigt sind, z. B. während lang andauernder Ereignisabläufe

3.5

Wartensystem

(en: control room system)

Zusammenfassung von Mensch-Maschine-Schnittstelle, Wartenpersonal, Betriebsprozeduren, Trainingsprogrammen und zugehörigen Einrichtungen, die insgesamt das einwandfreie Funktionieren der Warte ermöglichen

3.6

Anzeigegerät

(en: display)

Gerät zur Beobachtung von Anlagenzuständen, z. B. Prozesszustand, Zustand verfahrenstechnischer Einrichtungen

3.7

Format

Darstellungsformat

(en: format (display format))

bildliche Informationsdarstellung auf einem Sichtgerät, z. B. Meldetext, digitale Darstellung, Symbole, Fließbilder, Balkenanzeigen, Trendgraphiken, Zeiger, Polygon-Darstellungen

3.8

Funktion

(en: function)

dient einem bestimmten zu erreichenden Zweck oder Ziel, das spezifiziert oder beschrieben werden kann; auf die zum Erreichen des Ziels notwendigen physikalischen Mittel wird nicht näher eingegangen

[IEC 61226]

3.9

Funktionsanalyse

(en: functional analysis)

Untersuchung der funktionalen Ziele eines Systems in Hinblick auf verfügbares Personal, Technologie und andere Ressourcen, um die Grundlagen zu erarbeiten, wie die Funktion zugeordnet und durchgeführt werden kann

3.10

funktionales Ziel

(en: functional goal)

zu erreichenden Handlungsziele, um die entsprechende Funktion durchführen zu können

3.11

hierarchische Zielstruktur

(en: hierarchical goal structure)

Beziehung zwischen einem funktionalen Hauptziel und funktionalen Teilzielen, geordnet entsprechend einer hierarchischen Struktur

3.12

gehobene mentale Informationsverarbeitung

(en: high-level mental processing)

Denkprozess, bei dem Informationen verarbeitet und/oder interpretiert werden, um eine reduzierte abstrakte Information zu erhalten

3.13

Mensch-Maschine-Schnittstelle

(en: human-machine interface)

Schnittstelle zwischen dem Betriebspersonal und den mit der Anlage verbundenen Leittechnik- und Rechnersystemen. Diese Schnittstelle schließt Anzeigen, Bedienungen und die Schnittstelle zum Operateur-Unterstützungssystem mit ein.

3.14

leittechnisches System

(en: I&C system)

auf elektrischer und/oder programmierbarer elektronischer Technologie beruhendes System, das sowohl leittechnische Funktionen als auch auf sich selbst bezogene Dienstleistungs- und Überwachungsfunktionen ausführt

Der Begriff wird allgemein verwendet und umfasst alle Elemente des Systems wie interne Energieversorgung, Messfühler und andere Eingangsgeräte, Datenbusse und andere Kommunikationspfade, Schnittstellen zu den Betätigungsgliedern und andere Ausgangsgeräten. Die verschiedenen Funktionen in einem System können strikt zugeordnete und auch gemeinsame Ressourcen verwenden.

ANMERKUNG 1 Siehe auch „System“, leittechnische Funktion“.

ANMERKUNG 2 Die zu einem spezifischen leittechnischen System gehörenden Elemente sind durch die Spezifikation der Systemgrenzen definiert.

ANMERKUNG 3 Entsprechend ihrer typischen Funktionalität unterscheidet IAEA zwischen Automatisierungs- und Steuerungs-/Regelsystemen, MMK-Systemen, Verriegelungssystemen und Schutzsystemen.

[IEC 61513]

3.15

Gesamtaufgabe

(en: job)

eine Gesamtaufgabe besteht aus einem Satz von zusammenhängenden Einzelaufgaben. Diese Einzelaufgaben sollten in bezug auf geforderte Fertigkeit, Wissen und Verantwortlichkeit kohärent sein.

3.16

Analyse der Gesamtaufgabe

(en: job analysis)

Analyse zur Identifizierung der grundsätzlichen Anforderungen, die durch eine Gesamtaufgabe an die Struktur des Wartepersonals, an die Betriebsprozeduren und das Trainingsprogramm gestellt werden

3.17

örtliche Bedienstellen

(en: local control points (or facilities))

außerhalb der Warte befindliche Stellen oder Einrichtungen, wo örtliche Operateure ihre Bedientätigkeiten ausführen

3.18

örtliche Operateure

(en: local operators)

Betriebspersonal, das Aufgaben außerhalb der Warte durchführt

3.19

Betriebsprozeduren

(en: operating procedures)

Dokumentenreihe, in der die betrieblichen Aufgaben spezifiziert sind, deren Ausführung zur Erreichung funktionaler Ziele notwendig ist

3.20

Betriebspersonal

(en: operating staff)

Anlagenpersonal, das zum Betrieb der Anlage im Schichtbetrieb arbeitet. Das Betriebspersonal umfasst das Wartenpersonal, die Wartungstechniker usw.

3.21

Operateur-Wechselwirkung

(en: operator interaction)

Beziehung zwischen dem Operateur und dem leittechnischen System, speziell die Darstellung des Anlagenzustands durch das leittechnische System und die entsprechenden Operateurhandlungen

3.22

Operateur-Unterstützungssystem

Abkürzung: OÜS

(en: operator support system – OSS)

Systeme, die dem Wartenpersonal zugeordnete, gehobene mentale Informationsverarbeitungsaufgaben unterstützen

3.23

Leistungsanforderungen

(en: performance requirements)

quantitative Anforderungen an die Ausführung von Aufgaben, die das Erreichen funktionaler Ziele sicherstellen

3.24

Anlagenbetriebsziele

(en: plant operational goals)

letztendlicher Zweck der Anlagenauslegung, d. h. geregelte Erzeugung von Elektrizität und Begrenzung der Radioaktivitätsabgabe in die Umgebung

3.25

Stereotypie

(en: population stereotype)

Tendenz der meisten Personen in einer Gruppe oder Population, auf einen speziellen Stimulus in gleicher Art zu reagieren, auch wenn es alternative Möglichkeiten gibt. Die Stereotypie hängt von den Gepflogenheiten und Anlagen der untersuchten Population ab.

3.26

Analyse der Einzelaufgabe

(en: task analysis)

detaillierte Beschreibung der Einzelaufgabe eines Operateurs in Form ihrer Bestandteile, um die betroffenen detaillierten menschlichen Tätigkeiten und ihre funktionalen und zeitlichen Zusammenhänge zu spezifizieren

3.27

Aufgaben

Einzelaufgaben

(en: tasks)

entweder von Mensch oder Maschine ausgeführte Aktionen zum Erreichen eines funktionalen Ziels

3.28

Ausbildungsprogramm

(en: training programme)

zur Ausbildung des Wartenpersonals ausgelegtes Programm, um sich Fertigkeiten und Wissen für die nötigen betrieblichen Aktivitäten anzueignen.

3.29

Validierung

(en: validation)

Verfahren der Feststellung, ob ein Produkt oder eine Dienstleistung geeignet ist, die gewünschte Funktion zufriedenstellend auszuführen.

Validierung betrifft einen breiteren Bereich und kann einen größeren Bewertungsumfang annehmen als Verifizierung.

[IAEA Safety Glossary]

3.30

Verifizierung

(en: verification)

Verfahren zur Feststellung, ob die Qualität oder Leistungsfähigkeit eines Produkts oder einer Dienstleistung wie festgesetzt, gewünscht oder gefordert ist

[IAEA Safety Glossary]

3.31

Sichtgerät

(en: visual display unit – VDU)

Anzeigegerät mit Bildschirm zur Darstellung rechnergestützter Bilder

3.N1^{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^{N1)}

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^{N1)}

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 folgender 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 Ed. 2]

^{N1)} Nationale Fußnote: Die Definitionen 3.N1, 3.N2 und 3.N3 sind im IEC-Dokument nicht enthalten, hier im nationalen Norm-Entwurf zur besseren Verständlichkeit ergänzt.

4 Anwendung der Norm

Dieser Abschnitt soll den Leser auf die Organisation und die Schwerpunkte der Norm hinführen. Bild 1 zeigt einen Überblick über das Wartensystem. Das Ziel eines Auslegungsteams ist die erfolgreiche komplette Herstellung eines integrierten Wartensystems. Bestandteile dieses Systems sind das Wartenpersonal, die Mensch-Maschine-Schnittstelle, die Betriebs- und Sicherheitsleittechnik, die Betriebsprozeduren und das Ausbildungsprogramm. Anhang A gibt eine zusätzliche Erläuterung zum Begriff des Wartensystems.

Schwerpunkt dieser Norm ist die Ausbildung der Mensch-Maschine-Schnittstelle bei der Wartenauslegung. Die Norm legt auch Mittel zur Entwicklung von Personalanforderungen, Betriebsprozeduren und Trainingsprogrammen dar, gibt aber keine detaillierte Methodik für solche Entwicklungen an. Die Beziehungen zwischen den verschiedenen Abschnitten dieser Norm sind in Bild 2 gezeigt.

Nach dem Umfang, den Festlegungen und Spezifikationen der Auslegungsprinzipien wird in dem Bild gezeigt, dass der Auslegungsvorgang die Funktionsanalyse, Funktionszuordnung, Verifizierung und Validierung der Funktionszuordnung und die Analyse der Gesamtaufgabe umfasst. Danach werden, wie in Bild 2 gezeigt, die Spezifikationen der funktionalen Auslegung entwickelt.

Aus diesen Spezifikationen schließlich werden die detaillierte Auslegung, Betriebsprozeduren und Trainingsprogramme entwickelt. Zuletzt werden die resultierenden Systembestandteile verifiziert und das integrierte Wartensystem wird validiert.

Diese Norm richtet sich an die Verantwortlichen für die Wartenauslegung. Dies ist üblicherweise ein Auslegungsteam, das eine Vielzahl von Kompetenzen und Disziplinen aus wenigstens folgenden Bereichen umfasst:

- nukleares Ingenieurwesen;
- Architektur und Bauingenieurwesen;
- Systemtechnik;
- Leittechnik;
- Informations- und Rechnersysteme;
- Human-Factor-Prinzipien (Auslegung unter Berücksichtigung des Faktors Mensch);
- Anlagenbetrieb;
- Schulung.

Diese Kompetenzen können durch ständige oder temporäre Teammitglieder oder auch durch Berater zur Verfügung gestellt werden.

5 Auslegungsprinzipien für die Hauptwarte

5.1 Hauptaufgaben der Hauptwarte

Es ist eine Warte vorzusehen, von der aus das Kernkraftwerk in allen Betriebszuständen und unter Störfallbedingungen sicher und effizient betrieben werden kann. In der Warte werden dem Wartenpersonal die Mensch-Maschine-Schnittstellen samt zugehörigen Informationen und Geräten (z. B. die Kommunikationschnittstelle) zur Verfügung gestellt, die für das Erreichen der Anlagenbetriebsziele notwendig sind. Zusätzlich wird eine Umgebung geschaffen, in der das Wartenpersonal seine Aufgaben bequem, ohne exzessiven Stress oder körperliche Gefahr durchführen kann.

5.2 Funktionales Auslegungsziel der Hauptwarte

Prinzipielle Ziele der Wartenauslegung bestehen darin, den Operateur mit genauer, vollständiger, betrieblich relevanter und zeitgerechter Information bezüglich des funktionalen Zustandes von Anlagengeräten und Systemen zu versorgen.

Die Auslegung muss alle Betriebszustände einschließlich Wiederbelastung des Kerns und Störfallbedingungen berücksichtigen, die Aufgaben optimieren und die für Überwachung und Kontrolle der Anlagensicherheit erforderliche Arbeitsbelastung auf ein vernünftiges Maß reduzieren, sowie notwendige Informationen an andere Einrichtungen außerhalb der Warte vorsehen.

Die Wartenauslegung muss für eine optimale Zuordnung der Funktionen und damit für eine maximale Nutzung der Fähigkeiten von Operateur und System sorgen.

Ein zusätzliches Ziel der Wartenauslegung besteht darin, eine effektive Durchführung der Inbetriebnahme der Anlage sowie Änderungen und Wartung zu unterstützen.

5.3 Sicherheitsprinzipien

Eine Warte muss so ausgelegt werden, dass sie einen sicheren Betrieb der Anlage in allen Betriebszuständen und eine Rückkehr in den sicheren Zustand nach einsetzenden Störfallbedingungen erlaubt. Derartige Ereignisse müssen bei der Auslegung der Warte berücksichtigt werden.

Von der Warte aus gesteuerte Geräte sollten soweit praktikabel so ausgelegt sein, dass ein unsicherer Handbefehl nicht ausgeführt werden kann, z. B. durch Verwendung einer vom Anlagenzustand abhängigen logischen Verriegelung.

Beachtet werden muss auch die Notwendigkeit funktionaler Isolierung und räumlicher Trennung, wenn redundante Sicherheitssysteme, oder Sicherheitssysteme und sicherheitstechnisch nicht relevante Systeme, nahe beieinander liegen. Anforderungen für solche Fälle sind in IEC 60709 enthalten. Weiter muss für Sicherheit gesorgt werden, wenn die Warte und ihre Systeme von Feuer bedroht werden, und es muss, wie in IEC 60709 ausgeführt, die Brandmöglichkeit auf ein praktikables Minimum reduziert werden.

Geeignete Maßnahmen müssen zum Schutz der Anwesenden in der Warte gegen mögliche Gefahren getroffen werden; das sind unautorisierter Zugang, unzulässige Radioaktivität infolge Störfallbedingungen, toxische Gase und alle Folgen von Brand, die notwendige Operateurhandlungen beeinträchtigen könnten.

Es muss Fluchtwege geben, auf denen das Wartpersonal unter Notfallbedingungen die Warte verlassen oder erreichen kann oder Zugang zu anderen Bedienstellen hat.

5.4 Verfügbarkeitsprinzipien

Mit Blick auf die Maximierung des Kapazitätsfaktors der Anlage muss bei der Auslegung der Warte folgendes beachtet werden:

- Erleichterung von geplanten Lastwechseln, Anfahren und Abschalten;
- Minimierung des Auftretens ungewünschter Leistungsreduktion oder Anlagenabschaltung infolge irrtümlicher Entscheidungen und Handlungen der Operateure, oder durch Störungen in Verbindung mit Fehlfunktionen oder Ausfällen der leittechnischen Systeme;
- Erreichen der Nennleistung und Leistungsfähigkeit der Anlage entsprechend der Auslegung.

Die auf die Verfügbarkeit bezogenen Auslegungsspezifikationen dürfen die eingeplanten Sicherheitsprinzipien nicht beeinträchtigen.

5.5 Human-Factor-Prinzipien

Um eine optimale Zuordnung der Funktionen zu erreichen, die eine maximale Ausnützung der Fähigkeiten von Mensch und Maschine sicherstellt und auf das Erreichen höchster Anlagensicherheit und -verfügbarkeit abzielt, muss bei der Auslegung den Human-Factor-Prinzipien und den Eigenschaften des Personals in Hinblick auf Anthropometrie, Wahrnehmung, kognitiver, physiologischer und motorischer Fähigkeiten und Grenzen besondere Beachtung geschenkt werden.

5.6 Betriebsprinzipien des Betreibers

Ein integraler Teil der Warte und Betriebsphilosophie ist die Festlegung der Wartenmannschaft und ihre Ausbildung. Um die Sicherheit und Effizienz des Kraftwerksbetriebs zu maximieren, muss die Warte mit einer genügenden Anzahl von hochwertigen Fachkräften besetzt sein.

Das Wartenpersonal muss sowohl für die Bedienung der Warte praktisch trainiert und in den auf Kraftwerksbetrieb und -Sicherheit bezogenen ingenieurtechnischen Prinzipien geschult sein, als auch ein tiefes Wissen der Teilsysteme und Komponenten der Anlage, ihrer Funktion, Leistungsfähigkeit und örtlichen Anordnung haben.

Von Operateuren außerhalb der Warte wahrgenommene Aufgaben der Bedienung von Anlagengeräten müssen von der Warte aus administrativ kontrolliert und überwacht werden.

Um die Qualität des Kraftwerksbetriebs sicherzustellen, sollte die für den Anlagenbetrieb verantwortliche Stelle bei der personellen Besetzung der Warte folgende Faktoren in Betracht ziehen:

- die Anforderungen an Personalauswahl und Qualifikation;
- die Anforderungen an Anfangs- und Wiederholungstraining für normale, anomale und Störfallbedingungen;
- periodisches Wiederholungstraining der betrieblichen Fertigkeiten und Gelegenheit, das Wissen über die ingenieurtechnischen Prinzipien zu erweitern;
- Verantwortlichkeiten des Wartenpersonals und der Einzelpersonen bei Normalbetrieb und Stör- und Notfällen;
- physische Anforderungen an das Personal hinsichtlich Seh- und Hörvermögen; Personengröße, etwaige physische Schwächen;
- Management und Beaufsichtigungs-Strukturen und Verantwortlichkeiten;
- Schichteinteilung und Personalbelastung.

5.7 Beziehung zu anderen Kontroll- und Managementzentren

Zur Unterstützung des Wartenpersonals bei anomalen Betriebsbedingungen müssen Notfallstellen zur Verfügung stehen, um bei Notfallsituationen tätig werden zu können.

Zusätzliche Bedienstellen zur Überwachung und Steuerung müssen vorhanden sein, die zur Bewahrung der Sicherheit ausreichen, sollte die Warte beschädigt oder nicht betriebsfähig sein. Die Anforderungen für solche zusätzlichen Bedienstellen sind in IEC 60965 zu finden.

Es müssen Einrichtungen für den Wechsel der Überwachung und Steuerung von der Hauptwarte zu den zusätzlichen Bedienstellen vorgesehen werden. Diese Einrichtungen müssen unabhängig von den anderen in der Hauptwarte arbeiten.

5.8 Betriebserfahrung

Wenn verfügbar, sollte die Betriebserfahrung bestehender Kernkraftwerke gesammelt, analysiert und, wo anwendbar, bei der Auslegung neuer Kernkraftwerke berücksichtigt werden. Eine derartige Erfahrung kann den Einsatz oder die Optimierung bewährter Lösungen empfehlenswert machen oder die Berücksichtigung von Prinzipien in Bereichen, die im Folgenden genannt sind, beeinflussen:

- personelle Besetzung;
- Organisation der Betriebsmannschaft und Aufgabendefinition;
- Funktionszuordnung zwischen Hauptwarte und örtlichen Bedienstellen;
- Automatisierung;
- Auslegung der Informationsverarbeitung, Informationsdarstellung und Bedieneinrichtungen.

6 Funktionale Auslegung der Hauptwarte

6.1 Allgemeines

Es muss ein systembasiertes Vorgehen zur funktionalen Auslegung einer Warte angewendet werden, das die Warte und die zugehörigen Themen gemäß Bild 1 abdeckt. Diese Vorgehensweise muss folgende in Bild 2 gezeigten fünf Schritte umfassen:

- Funktionsanalyse;
- Funktionszuordnung;
- Verifizierung der Funktionszuordnung;
- Validierung der Funktionszuordnung;
- Aufgabenanalyse.

6.2 Funktionsanalyse

6.2.1 Allgemeines

Es muss eine Analyse der Funktionen durchgeführt werden, die vom KKW zur Erreichung der Ziele nach 5.1 und 5.2 in Übereinstimmung mit den Prinzipien nach 5.3 bis 5.8 auszuführen sind.

In dieser Analyse sollte eine Hierarchie von Zielen für die Wartenauslegung festgelegt werden, die alle Betriebszustände und Störfallbedingungen abdeckt. Diese Ziele müssen die Produktion von Elektrizität und die Minimierung der Radioaktivitätsabgabe als grundsätzliche Ziele mit einschließen. Die Ziele können in Form von Teilzielen weiterentwickelt und in den Entscheidungsprozessen der Auslegung verwendet werden.

Für detailliertere Beschreibungen und Anforderungen bezüglich des Vorgehens bei der Funktionsanalyse sei auf die Norm IEC 61839 verwiesen.

6.2.2 Festlegung von Funktionen

In Hinblick auf die hierarchischen Zielstrukturen müssen alle Anlagenfunktionen, die mit den auf die Warte bezogenen Zielen in Verbindung stehen, identifiziert und dokumentiert werden. Ein Weg zur Identifizierung dieser Ziele ist in IEC 61839 angegeben. Bei der Definition der Funktionen sollte die Analyse umfassend sein und die Wechselwirkungen zwischen Warte und Einrichtungen und Systemen außerhalb der Warte berücksichtigen.

6.2.3 Anforderungen an Informationsfluss und -verarbeitung

Analysen müssen durchgeführt werden, um den grundlegenden betrieblichen Informationsfluss und die Informationsverarbeitung zu bestimmen, die zur Ausführung der Anlagenfunktionen einschließlich Entscheidungsfindung und Handlungen erforderlich sind. Diese Analysen sind in IEC 61839 beschrieben.

Bei Festlegung der Anforderungen an Informationsfluss und -verarbeitung sollten bei der Auslegung mehrere repräsentative Auslegungsbasis-Ereignisse und alle normalen Betriebsformen zugrundegelegt werden.

Folgende Ereignisse sollten mit eingeschlossen werden:

- Ereignisse, die subjektiv als schwierig einzustufende Handlungen erfordern, wobei unter schwierig die Komplexität der Dateninterpretation oder der Bedienhandlungen, Bediengeschwindigkeit, etc. verstanden wird;
- Ereignisse, die höchste Gewissheit für ein korrektes Reagieren des Operators verlangen, z. B. bestimmte Störfallbedingungen;
- Ereignisse, die in Hinblick auf die probabilistische Risikoanalyse wichtig sind;
- Ereignisse, bei denen automatische Anlagenabschaltung höchstwahrscheinlich ist, wenn nicht rechtzeitig korrektive Maßnahmen ergriffen werden;

E DIN IEC 60964 (VDE 0491-5-1):2007-11

- Ereignisse mit hoher Eintrittshäufigkeit.

Es muss eine ausreichend große Anzahl von Ereignissen berücksichtigt werden, um die zur hierarchischen Aufgabenstruktur gehörenden Funktionen angemessen abzudecken.

6.3 Zuordnung von Funktionen

6.3.1 Allgemeines

Es muss eine Aufgabenanalyse durchgeführt werden, um zu bestimmen, welche Funktionen dem Menschen und welche Funktionen der Maschine zugeordnet werden sollten.

Nach Anhang A, Tabelle A.1 dem Menschen zugeordnete Funktionen sind:

- Handbedienung einschließlich Backup-Steuerung von automatischen Steuerungen;
- Überwachung in Zusammenhang mit Handbedienung und automatischer Steuerung;
- gehobene mentale Verarbeitungsaufgaben, wie die Diagnose zur Bestimmung der Ursache anomaler und unvorhergesehener Betriebsbedingungen und Ereignisse und das Festlegen der korrigierenden Eingriffe.

Der Maschine zugeordnete Funktionen beziehen sich, wie in Tabelle A.1 gezeigt, auf automatische Steuerungen.

In genannter Analyse müssen die Human-Factor-Prinzipien und Auslegungskriterien angewendet werden (ISO 11064-1, 7.3).

Die in der Analyse verwendeten Prinzipien und Kriterien müssen dokumentiert werden und müssen Gesichtspunkte einschließen, die sich mit Fähigkeiten und Beschränkungen sowohl des Wartenpersonals als auch der automatischen Steuerungssysteme befassen.

Bezüglich detaillierterer Anforderungen für den Prozess zur Zuordnung von Funktionen sei auf IEC 61839 verwiesen.

6.3.2 Operateurfähigkeiten

Bei der Zuordnung von Funktionen an den Operateur sollte zwischen Situationen unterschieden werden, in denen er tatsächlich eine Bedienaufgabe wahrnimmt, in denen er ein automatisches System überwacht, das die Steuerungsaufgaben durchführt, und in denen er komplexe mentale Verarbeitungsaufgaben (z. B. Diagnosen) ausführt. Diese Analyse sollte die Information erbringen, die für das Konzept der Informationssystem-Struktur und die funktionale Organisation der Ressourcen zur Durchführung jedes Entscheidungsprozesses und jeder Bedienaufgabe notwendig ist.

Für mögliche Operateur-Funktionen müssen Abschätzungen der geforderten Verarbeitungskapazität in Form von Arbeitsbelastung, Genauigkeit, Häufigkeit und Zeitfaktor für jeden Aspekt der Informationsverarbeitung und jede Bedienhandlung durchgeführt werden. Diese Abschätzungen müssen für eine erste Zuordnung der Funktionen verwendet werden. Die Abschätzungen sollten auf der Basis der Verifizierungsergebnisse angepasst und dazu verwendet werden, die Zuordnung der Funktion nochmals zu überdenken sowie eine detailliertere Definition der geforderten Operateur-Fähigkeiten auszuarbeiten.

Diese Anforderungen zusammen mit denen für Anzeigen, Steuerung und Kommunikation müssen konsistent mit den Aufgaben sein, die für die Ausführung der Funktion nötig sind. Die allgemeinen Aufgaben sollten Anforderungen zu Anzeige, Steuerung und Kommunikation mit einschließen.

Die verschiedenen Arten von Daten, die dem Operateur zur Verfügung stehen, sollten in Hinblick auf die Aufgaben und nicht in Hinblick auf die Datenquellen gruppiert werden. Zweck ist die Information verschiedener Quellen hinsichtlich jeder Entscheidungsaufgabe zu organisieren, um so ein umfassendes Informationssystem angepasst an die Fähigkeiten des Operateurs zu erhalten.

6.3.3 Verarbeitungs-Fähigkeiten des leittechnischen Systems

Die Analyse der Verarbeitungsmöglichkeiten des leittechnischen Systems muss mit einer Definition der funktionalen Anforderungen und Randbedingungen der Systeme und Geräte beginnen, gefolgt von einer detaillierteren Beschreibung der betrieblichen Ereignis-Abfolgen und Anforderungen an die Mensch-Maschine-Schnittstelle. Zweck ist die Organisation von Maschineninformation und Maschinenfähigkeit in Hinblick auf die Aufgaben, die für einen Operateur-Eingriff vorgesehen sind.

Diese Organisation erleichtert die Beurteilung der Fähigkeiten von automatischen Steuerungen und menschlichen Bedienhandlungen für jede Entscheidungsfindung und Steuerungsaufgabe. Verarbeitungsfähigkeiten des leittechnischen Systems sollten letztlich Aspekte wie Forderungen zu Umfang, Antwortzeit und Genauigkeit einschließen, die das System und/oder Gerät erfüllen muss, sowie Anforderungen aus den Human-Factor-Prinzipien, durch die für jeden Komponententyp die Mensch-Maschine-Schnittstelle definiert wird.

Um die Wahrscheinlichkeit von Operateur-Irrtümern zu reduzieren, sollten die Steuerungssysteme so ausgelegt sein, dass die Anlage nach Beginn einer gewissen anomalen Betriebsbedingung über eine spezifizierte Zeitspanne ohne irgendeinen Operateureingriff in sicheren Grenzen gehalten werden kann. Diese Zeitspanne muss in den funktionalen Anforderungen für die automatischen Steuerungssysteme berücksichtigt werden.

6.4 Verifizierung der Funktionszuordnung

6.4.1 Allgemeines

Eine akzeptierte Zuordnung von Wartenfunktionen an Mensch oder Maschine muss wie in Bild 2 gezeigt verifiziert werden. Es muss belegt werden, dass die vorgeschlagene Funktionszuordnung den maximalen Vorteil aus den Fähigkeiten von Mensch und Maschine zieht, ohne unzumutbare Anforderungen an Mensch oder Maschine zu stellen.

Bezüglich detaillierterer Anforderungen für die Verifizierung der Funktionszuordnung sei auf die Norm IEC 61771 verwiesen.

6.4.2 Verifizierungsprozess

Der für die Verifizierung entwickelte Prozess muss Vorbereitungs-, Bewertungs- und Lösungsphasen umfassen.

Allgemeine Bewertungskriterien zur Verifizierung:

Vor der Verifizierung der vorgeschlagenen Funktionszuordnung muss bestätigt werden, dass die für die Zuordnung verwendeten Kriterien in sich konsistent sind.

Anschließend muss durch die Verifizierungen bestätigt werden, dass

- a) alle für die Erreichung der Betriebs- und Sicherheitsziele der Anlage notwendigen Funktionen identifiziert sind;
- b) die vorgeschlagene Funktionszuordnung mit den für die Zuordnung aufgestellten Kriterien übereinstimmt;
- c) für jede Funktion ausreichende Anforderungen festgelegt sind. Diese Anforderungen umfassen Aspekte der Leistungsfähigkeit (z. B. Zeitkonstanten, Genauigkeit), aus Sicherheitsprinzipien und Verfügbarkeitsprinzipien sowie aus Prinzipien des Anlagenbetriebs abgeleiteten Gesichtspunkten, die in dieser Norm spezifiziert sind, und solchen, die auf andere Normen, Regeln und Leitlinien zurückgehen;
- d) Anforderungen von Funktionszielen höherer Ebenen, die bei allen Betriebsarten ohne Konflikte für eine niederere Funktionsebene passen.

Änderungen (d. h. Verbesserung von Fehlern oder Neuordnung) und Verifizierung müssen iterativ durchgeführt werden, bis alle diese Kriterien erfüllt sind.

6.5 Validierung der Funktionszuordnung

6.5.1 Allgemeines

Die vorgeschlagene Funktionszuordnung muss validiert werden, um zu zeigen, dass das System alle Funktionsziele erreicht. Im Speziellen muss die Leistungsfähigkeit der in 6.2 identifizierten Funktionen bei allen normalen Betriebsformen und mehreren repräsentativen Ereignissen bewertet werden.

Bezüglich detaillierterer Anforderungen für die Validierung der Funktionszuordnung sei auf die Norm IEC 61771 verwiesen.

6.5.2 Validierungsprozess

Der für die Validierung entwickelte Prozess muss Vorbereitungs-, Bewertungs- und Lösungsphasen umfassen.

Es müssen Auswahlkriterien entwickelt werden, um sicherzustellen, dass die für die Beurteilung gewählten Ereignisse repräsentativ sind. Zusätzlich zu allen in 6.2.3 spezifizierten normalen Betriebszuständen und Ereignissen, sollten von Mehrfachausfällen verursachte Ereignisse für die Beurteilung der dem Menschen zugeordneten Funktionen betrachtet werden.

Nach Abschluss der Auswahl repräsentativer Ereignisse müssen die für jedes Ereignis erforderlichen Funktionen ermittelt und geordnet in zeitlicher Abfolge zusammengestellt werden.

6.5.3 Allgemeine Bewertungskriterien für die Validierung

Die Leistungsfähigkeit der Funktionen muss für alle normalen Betriebsformen und die repräsentativen Ereignisse bewertet werden. Die allgemeinen Validierungskriterien müssen einschließlich folgender Punkte erfüllt werden:

- a) die Anzahl der Funktionsziele und die Arbeitsbelastung, die vom Wartenpersonal gefordert werden, darf seine Leistungsfähigkeit nicht überschreiten;
- b) die Zuordnung der Funktionen an das Wartenpersonal und die örtlichen Operateure ist akzeptabel. Insbesondere sollte nicht von ihnen verlangt werden, gemeinsam wechselseitig voneinander abhängige Aufgaben zur Ausübung einer Funktion durchzuführen, die entweder zeitkritisch oder für die Anlagensicherheit oder Anlagenverfügbarkeit wichtig ist.
- c) die Zuordnung von Funktionen an die Automatisierung ist zufriedenstellend und machbar.

6.6 Analyse der Arbeitsaufgabe

Um die grundsätzlichen Anforderungen für die Struktur des Wartenpersonals, die Betriebsprozeduren und das Schulungsprogramm weiter auszuarbeiten, sollte das Auslegungsteam eine Aufgabenanalyse der verifizierten und validierten Funktionszuordnung und der funktionalen Anforderungen durchführen.

Der erste Schritt dieser Analyse ist die Ermittlung der Hauptmerkmale und Anzahl der dem Menschen zugeordneten Teilaufgaben. Darauf basierend kann das Auslegungsteam die Organisation und Anzahl der Operateure definieren, unter Beachtung des Rahmens für die Wartenpersonal-Struktur, der von der Behörde verlangt wird und/oder sich aus der normalen Praxis des Betreibers ergibt.

Einem Operateur zugeordnete Aufgaben sollten ihn nicht überlasten und sollten konsistent mit seinen Verantwortlichkeiten sein, wie sie von der Wartenpersonal-Struktur vorgegeben sind. Weiterhin sollte das Auslegungsteam die Kommunikation zwischen den Operateuren und/oder zwischen den Wartenoperateuren ermitteln, die zur Erfüllung der Aufgaben notwendig ist.

Das Auslegungsteam sollte auch nichtbetriebliche Tätigkeiten ermitteln (z. B. Berichte für Behörden), die einigen Aufgaben insofern inhärent sind, da auf entsprechende Dokumente verwiesen werden kann.

Wenn die Analyse fertiggestellt ist, sollte folgendes klargestellt sein:

- Organisation und Anzahl der Operateure
- notwendige Operateur-Kompetenz;
- betriebliche Verantwortlichkeiten der Operateure;
- administrative Pflichten der Operateure;
- betriebliche Wechselwirkungen zwischen den Operateuren;
- Wechselwirkung zwischen Operateuren und Anlage;
- Kommunikation zwischen Operateuren und Anlagenpersonal, das außerhalb der Warte stationiert ist;
- Kommunikation mit Management und Vorgesetzten.

Zusammen mit den Ergebnissen der Analyse für die Funktionszuordnung (z. B. Konzept der Informationsstruktur) sollten die o. g. Punkte die Basis der Wartenpersonal-Struktur, der Betriebsprozeduren und des Schulungsprogramm bilden.

7 Funktionale Auslegungsspezifikation

7.1 Allgemeines

In diesem Abschnitt werden die funktionalen Auslegungsanforderungen für das Wartensystem und die Geräte festgelegt, welche die ihnen zugeordneten Beobachtungs- und Steuerungsfunktionen ausführen. Außerdem wird die Schnittstelle zwischen dem Menschen und den Wartengeräten definiert.

Grundlage der Auslegung muss eine integrierte ingenieurmäßige Vorgehensweise bezüglich des Systems Mensch-Maschine sein.

7.2 Erstellung einer Datenbasis über menschliche Fähigkeiten und Eigenschaften

Für die Durchführung der detaillierten Auslegung einer Warte muss eine Datenbasis über menschliche Fähigkeiten und Eigenschaften zur Verwendung als HF-Auslegungsdaten zur Verfügung stehen.

Die Datenbasis muss umfassen:

- anthropometrische Betrachtungen;
- Populations-Stereotypen;
- Hör- und Sehfähigkeiten und Eigenschaften;
- menschliche Fähigkeit der Informationsverarbeitung;
- Umgebungsfaktoren.

Da einige dieser Daten von den Gepflogenheiten im jeweiligen Land abhängen, kann die Datenbasis länderspezifisch oder betreiberspezifisch sein.

7.3 Lage, Umgebung und Schutz

7.3.1 Lage

Die Lage der Warte muss für den Anlagenbetrieb passend sein, die Warte muss die Sicherheitsprinzipien in 5.3 erfüllen.

7.3.2 Umgebung

Die Umgebungsbedingungen in der Warte müssen so sein, dass die Operateure ihre Aufgaben effektiv und komfortabel wahrnehmen können.

– Entwurf –

E DIN IEC 60964 (VDE 0491-5-1):2007-11

Die Umgebungsspezifikation muss Anforderungen für folgende Punkte umfassen:

a) Klimatisierung

Die Hauptwarte muss klimatisiert sein. Die Klima-Anlage muss so ausgestattet sein, um auf Unfallbedingungen der Anlage entsprechend reagieren zu können, z. B. durch Anwendung von Filtern oder Isolationsmaßnahmen. Die Luftzutritts-Schächte müssen mit einem Aktivitätsüberwachungssystem ausgestattet sein.

b) Beleuchtung

Die Auslegung des Beleuchtungssystems muss eine gleichmäßige Beleuchtung sicherstellen sowie Blendung, Spiegelungen und störende Schatten vermeiden.

c) Akustik

Die akustische Auslegung muss eine leicht Kommunikation unter den Operateuren und minimale Störung durch Geräusche der Umgebung sicherstellen, sowie zuverlässige Aufnahme von akustischen Informationen, Störungsmeldungen und Notfallsignalen ermöglichen.

Anleitungen für Umgebungsspezifikationen bei Normalbedingungen sind in ISO 11064 zu finden.

Es kann angebracht sein, in diese Spezifikation Anforderungen über Größe und Form der Warte mit vorläufiger Gestaltung, Kabelzugängen, seismischen Bedingungen, Raum- und Schalttafelanordnungen und anderen Details zur Oberflächen-Gestaltung aufzunehmen, um Abstimmung in baulichen Angelegenheiten zu erzielen, die später im Detail zu bestätigen sind.

Die Auslegung hat durch geeignete Maßnahmen sicherzustellen, dass die Betriebsfähigkeit der Warte und die Überwachung der Anlage auch während Notfallbedingungen der Anlage beibehalten werden können.

7.3.3 Schutz

Durch die Auslegung der Warte muss im Rahmen der Auslegungsbasis für Schutz gegen Brand, Strahlung, interne und externe fliegende Teile, Erdbeben und Fremdeinwirkung gesorgt werden. Die Geräte müssen in Übereinstimmung mit der Auslegungsbasis qualifiziert werden.

Durch die Auslegung muss sichergestellt werden, dass solche Ereignisse nicht gleichzeitig die Hauptwarte und die ergänzenden, in 5.7 genannten Bedienstellen beeinträchtigen können.

Im einzelnen ist zu beachten:

a) Brandschutz

Es sollte darauf geachtet werden, nur nicht entflammbares Material zu verwenden. Der Wartebereich muss mit einer Brandmeldeeinrichtung und einem Brandbekämpfungssystem ausgestattet sein.

Elektrische Geräte in der Warte müssen so ausgelegt sein, dass sie soweit möglich weder Brand verursachen noch unterstützen.

Zur Warte gehörende Kabel- und Schaltkreise müssen gegen Brandfolgen geschützt sein. Kabelisolierungen und Beschichtungsmaterial sollten feuerresistent sein und nationale Prüfkriterien für Feuerausbreitung und Freisetzung von Verbrennungsstoffen erfüllen.

b) Strahlenschutz

Das Wartepersonal sollte in jeder Störfall-Situation gegen direkte Strahlung geschützt sein. Die Luftzutritts-Schächte müssen mit einem Radioaktivitätsüberwachungssystem ausgestattet sein. Wenn es die Umstände erfordern, muss das Warten-Lüftungssystem die Fähigkeit haben, sich selbst zu isolieren. Für das Personal müssen Atmungsgeräte zur Verfügung stehen.

c) Schutz vor fliegenden Teilen

Die Wartenauslegung muss auch die Beurteilung von fliegenden Teilen, die ihren Ursprung in oder außerhalb der Warte haben, und Schutz davor mit einschließen. Anleitungen zum Schutz in solchen Situationen sind im IAEA Safety Guide 50-SG-D4 zu finden.

d) Erdbebenschutz

Das für Sicherheitsfunktionen vorgesehene Warten-Gerät, das Klimatisierungs-System und das Notbeleuchtungs-System müssen für dieselben Erdbebenanforderungen ausgelegt sein wie das sicherheitstechnisch wichtige leittechnische Gerät. Detaillierte Anforderungen sind in IEC 60980 enthalten.

e) Fremdeinwirkung

Es sollten Maßnahmen ergriffen werden, um den Zugang zur Warte zu beschränken und die Warte gegen Fremdeinwirkung zu schützen.

Die Planung des Zugriffsschutzes muss den Anforderungen und Regelungen des jeweiligen Landes entsprechen.

7.4 Platzverhältnisse und Anordnung

7.4.1 Platzverhältnisse

In der Warte muss genügend Platz zur Verfügung stehen, um dem Wartenpersonal die Durchführung aller notwendigen Tätigkeiten zu erlauben, wobei anomale Bewegungsbedingungen der Operateure zu minimieren sind.

Besondere Beachtung sollte der Bereitstellung von Arbeitsbereichen, ausreichendem Platz zum Schreiben und Aufbewahren von Dokumenten geschenkt werden:

- Kontinuierlich besetzte Arbeitsbereiche müssen für sitzende Tätigkeiten ausgelegt und geeignete Sitzgelegenheiten müssen bereitgestellt sein, jedoch sollte auch eine stehende Ausübung der Tätigkeiten möglich sein.
- Wenn Schreiben und Zugang zu Dokumenten einen normalen Teil der Wartentätigkeit ausmacht, muss ausreichender Schreibplatz verfügbar gemacht werden.
- Aufbewahrungsplatz für Dokumente muss nahe der Arbeitsposition zur Verfügung stehen, um das Ablegen der Dokumente auf Konsolen, Pulten etc. zu vermeiden.
- Einiger Platz kann für etwa in Zukunft gewünschte Erweiterungen vorgesehen werden (während Planungsphasen oder der Lebenszeit der Hauptwarte).

7.4.2 Anordnung

Bei der Gestaltung der Warte muss auf folgendes geachtet werden:

- Betriebs-Prinzipien des Betreibers;
- Zuordnung der Funktionen an Operateure und das leittechnische System;
- Zentralisierte oder lokale Bedien-Philosophie, woraus sich der Umfang der in der Warte vorhandenen Bedienmöglichkeiten ergibt;
- Überwachungskriterien, wodurch die Verwendung von Übersichtsdarstellungen, die Anzahl der Sichtgeräte, Anzeige-Instrumente, Schreiber, Störungsmeldungen und Anzeigelampen auf den Tafeln bestimmt wird;
- Festlegungen bezüglich der Bedien- und Beobachtungstechnologie, wodurch der Umfang von direkt zugeordneten (z. B. festverdrahteten) Bedienelementen und Anzeigen im Vergleich zur Bildschirmbedienung einschließlich Großbildschirmen bestimmt wird;
- Festlegungen der Anlagenauslegung und der verwendeten Technologien (Trennung zwischen verschiedenen Redundanten, Verwendung automatischer Steuerungen, Abmessungen der Instrumente und Bediengeräte, Ausmaß der Automatisierung und/oder Mehrfachsteuerungen);
- Anforderungen des Betreibers und gesetzliche Anforderungen, wie z. B. die Anzahl von Operateuren in der Warte als Forderung von Betriebsprinzipien oder der Genehmigungsbehörden;
- Installation von nicht-betrieblichen Systemen, wie z. B. Brandmelde- und Brandbekämpfungssysteme, und andere blockübergreifende Systeme;
- Platz für administrative Tätigkeiten.