

	Kernkraftwerke Auslegung von Warten Analyse und Zuordnung der Funktionen (IEC 61839:2000)	DIN IEC 61839
VDE	Diese Norm ist zugleich eine VDE-Bestimmung im Sinne von VDE 0022. Sie ist nach Durchführung des vom VDE-Vorstand beschlossenen Genehmigungsverfahrens unter nebenstehenden Nummern in das VDE-Vorschriftenwerk aufgenommen und in der etz Elektrotechnische Zeitschrift bekannt gegeben worden.	Klassifikation VDE 0491 Teil 5
ICS 27.120.20 Nuclear power plants Design of control-rooms Functional analysis and assignment (IEC 61839:2000) Centrales nucléaires de puissance Conception des salles de commande Analyse fonctionnelle et affectation des fonctions (CEI 61839:2000) Die Internationale Norm IEC 61839:2000 „Nuclear power plants – Design of control-rooms – Functional analysis and assignment“ ist unverändert in diese Deutsche Norm übernommen worden. Beginn der Gültigkeit Diese Norm gilt ab 01. September 2002. Nationales Vorwort Für die vorliegende Norm ist das nationale Arbeitsgremium GUK 967.1 „Reaktorinstrumentierung“ der DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE zuständig. Bei Fragen der Interpretation von Aussagen wird empfohlen, ergänzend auf die zugrunde liegende, in englischer und französischer Sprache erschienene IEC-Publikation zurückzugreifen. Norm-Inhalt war veröffentlicht als E DIN IEC 61839 (VDE 0491 Teil 5):2001-11. Die Internationale Norm wurde vom SC 45A „Reactor instrumentation“ des TC 45 „Nuclear instrumentation“ der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet. Diese Norm, deren Anwendung international empfohlen wird, gibt das höchstmögliche Maß internationaler Übereinstimmung für das behandelte Sachgebiet wieder. Die Auslegung kerntechnischer Anlagen in Deutschland wird wesentlich durch die Strahlenschutzverordnung, die BMI-Kriterien, die KTA-Regeln und die RSK-Leitlinien bestimmt. Fortsetzung Seite 2 bis 20 DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE		

DIN IEC 61839 (VDE 0491 Teil 5):2002-09

In KTA 3904 sind die Grundsätze des Planungsvorgangs für die Auslegung von Kernkraftwerkswarten festgelegt, allerdings in geringerer Tiefe bezüglich der Funktionsanalyse und Funktionszuweisung.

Insofern kann diese Norm als Ergänzung zur KTA 3904 angesehen werden. Sie kann sinngemäß auch auf die Nachrüstung und Modernisierung existierender Warten angewendet werden.

In der Reihe VDE 0491 sind erschienen:

- **DIN IEC 61226 (VDE 0491 Teil 1)**, *Kernkraftwerke – Sicherheitsleittechnik – Kategorisierung* (IEC 61226:1993).
- **DIN IEC 60880-2 (VDE 0491 Teil 3-2)**, *Kernkraftwerke – Software für Rechner mit sicherheitstechnischer Bedeutung – Teil 2: Vorkehrungen gegen Versagen aufgrund von Softwarefehlern, Verwendung von Software-Werkzeugen und von vorgefertigter Software* (IEC 60880-2:2000).
- **DIN IEC 62117 (VDE 0491 Teil 4)**, *Kernkraftwerke – Druckwasserreaktoren – Überwachung ausreichender Kühlung des Kerns im abgeschalteten Zustand des Reaktors* (IEC 62117:1999).
- DIN IEC 61839 (VDE 0491 Teil 5), *Kernkraftwerke – Auslegung von Warten – Analyse und Zuordnung der Funktionen* (IEC 61839:2000).

Als weitere Teile der Reihe VDE 0491 sind derzeit vorgesehen:

- **DIN IEC 61513 (VDE 0491 Teil 2)**, *Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Allgemeine Systemanforderungen* (IEC 61513:2001).
- DIN IEC 60880 (VDE 0491 Teil 3-1), *Kernkraftwerke – Software für Rechner mit sicherheitstechnischer Bedeutung – Anforderungen an Software für Funktionen der Kategorie A* (IEC 60880:xxxx).
- DIN IEC 62138 (VDE 0491 Teil 3-3), *Kernkraftwerke – Software für Rechner mit sicherheitstechnischer Bedeutung – Anforderungen an Software für Funktionen der Kategorien B und C* (IEC 62138:xxxx).

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 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.

Der Zusammenhang der zitierten Normen mit den entsprechenden Deutschen Normen ist nachstehend wiedergegeben. Zum Zeitpunkt der Veröffentlichung dieser Norm waren die angegebenen Ausgaben gültig.

IEC hat 1997 die Benummerung der IEC-Publikationen geändert. Zu den bisher verwendeten Normnummern wird jeweils 60000 addiert. So ist zum Beispiel aus IEC 68 nun IEC 60068 geworden.

Tabelle NA.1

Europäische Norm	Internationale Norm	Deutsche Norm	Klassifikation im VDE-Vorschriftenwerk
–	IEC 60964:1989	–	–
–	IEC 61226:1993	DIN IEC 61226 (VDE 0491 Teil 1):1997-07	VDE 0491 Teil 1
–	IEC 61771:1995	–	–

Nationaler Anhang NB (informativ)

Literaturhinweise

DIN IEC 61226 (VDE 0491 Teil 1), *Kernkraftwerke - Sicherheitsleittechnik - Kategorisierung* (IEC 61226:1993)

Deutsche Übersetzung

Kernkraftwerke Auslegung von Warten Analyse und Zuordnung der Funktionen

Inhalt	Seite
Vorwort	4
1 Anwendungsbereich	5
2 Normative Verweisungen	5
3 Begriffe	5
4 Vorgehensweise zur Analyse und Zuordnung der Funktionen	6
4.1 Allgemeine Beschreibung	6
4.1.1 Analyse der Funktionen	6
4.1.2 Zuordnung der Funktionen	7
4.2 Zentrale Arbeitsgruppe für die Analyse und Zuordnung der Funktionen	7
5 Analyse der Funktionen	8
5.1 Allgemeines	8
5.2 Bestimmung der Funktionen	8
5.3 Bestimmung der grundlegenden Anforderungen hinsichtlich Informationsaufnahme und -verarbeitung	9
5.3.1 Analyse der einzelnen Funktionen	9
5.3.2 Bestimmung der zeitlichen Anforderungen und repräsentativen Ereignisse	10
6 Zuordnung der Funktionen	10
6.1 Allgemeines	10
6.2 Analyse der Steuer- und Regelungsfunktionen	11
6.2.1 Bestimmung der Funktionseinheiten	11
6.2.2 Beschreibung der Funktionseinheiten	11
6.2.3 Bestimmung der Beurteilungskriterien für die Steuer- bzw. Regelungsfunktion	11
6.3 Entwicklung der Zuordnungskriterien	12
6.3.1 Eigenschaften und Mensch-Maschine-Fähigkeiten	12
6.3.2 Nationale Gesetze, national und international anerkannte Regeln und Leitlinien	14
6.3.3 Regeln und Interessen von Betreiber und Lieferanten	14
6.4 Zuordnungsprozess	14
Anhang A (informativ) Beispiele zur Aufgliederung in Ziele und Teilziele	18
Anhang B (informativ) Ansatz der Analyse von Funktionen für einen Druckwasserreaktor	19
Literaturhinweise	20
 Bild 1 – Darstellung der Maßnahmen zur Analyse und Zuordnung der Funktionen nach IEC 60964	 16
 Tabelle 1 – Mensch und Maschine im funktionalen und physikalischen Bereich	 17
Tabelle 2 – Zuordnung von Funktionen zu Menschen und Maschinen – Allgemeine Struktur	17

Vorwort

- 1) Die IEC (Internationale Elektrotechnische Kommission) ist eine weltweite Normungsorganisation, die alle Nationalen Elektrotechnischen Komitees (Nationale Komitees der IEC) umfasst. Die IEC hat das Ziel, die internationale Zusammenarbeit in allen Fragen der Normung auf dem Gebiet der Elektrotechnik und Elektronik zu fördern. Zu diesem Zweck und neben anderen Aktivitäten veröffentlicht die IEC Internationale Normen. Mit der Vorbereitung sind die Technischen Komitees beauftragt. Jedes Nationale Komitee der IEC, das an dem behandelten Thema interessiert ist, darf an dieser Vorbereitungsarbeit teilnehmen. Internationale Organisationen, Regierungs- und Nichtregierungsstellen, die mit der IEC in Verbindung stehen, nehmen ebenfalls an diesen Vorbereitungsarbeiten teil. Die IEC arbeitet eng mit der Internationalen Organisation für Normung (ISO) nach den in der Vereinbarung zwischen beiden Organisationen festgelegten Bedingungen zusammen.
- 2) Die offiziellen Beschlüsse oder Vereinbarungen der IEC über technische Fragen, die in Technischen Komitees von Vertretern aller an dem behandelten Thema besonders interessierten Nationalen Komitees erarbeitet werden, bringen das höchstmögliche Maß internationaler Übereinstimmung für das behandelte Sachgebiet zum Ausdruck.
- 3) Sie stellen Empfehlungen zur internationalen Anwendung dar, die als Normen, Fachberichte oder Leitlinien veröffentlicht werden und als solche von den Nationalen Komitees angenommen sind.
- 4) Um die internationale Vereinheitlichung zu fördern, verpflichten sich die Nationalen Komitees der IEC, Internationale Normen der IEC so durchschaubar wie möglich in ihren nationalen und regionalen Normen anzuwenden. Jede Abweichung zwischen der IEC-Norm und der entsprechenden nationalen oder regionalen Norm muss in dieser deutlich gekennzeichnet werden.
- 5) Die IEC hat kein Verfahren für die Kennzeichnung der Konformität festgelegt und übernimmt keine Verantwortung, wenn ein Gegenstand als konform mit einer ihrer Normen erklärt wird.
- 6) Es besteht die Möglichkeit, dass Bestandteile dieser Internationalen Norm Gegenstand von Patentrechten sind. Die IEC hat nicht die Verantwortung, das Vorhandensein solcher Patentrechte festzustellen und auf deren Existenz hinzuweisen.

Die Internationale Norm IEC 61839 wurde vom Unterkomitee 45A „Reactor instrumentation“ des Technischen Komitee Nr. 45 „Nuclear Instrumentation“ der IEC ausgearbeitet.

Der Text dieser Norm basiert auf den folgenden Dokumenten:

FDIS	Abstimmungsbericht
IEC 45A/382/FDIS	IEC 45A/389/RVD

Ausführliche Auskunft über die Abstimmung zur Genehmigung dieser Norm gibt der in obiger Tabelle zitierte Abstimmungsbericht.

Diese Norm wurde entsprechend ISO/IEC-Direktiven, Teil 3 erstellt.

Die Anhänge A und B dienen nur zur Information.

Das Komitee hat entschieden, dass diese Publikation bis 2006 unverändert gültig sein soll. Dann wird die Publikation entsprechend der Entscheidung des Komitees

- bestätigt,
- zurückgezogen,
- durch eine überarbeitete Ausgabe ersetzt oder
- geändert.

1 Anwendungsbereich

Diese Internationale Norm legt Vorgehensweisen für die Analyse und Zuordnung von Funktionen bei der Auslegung von Systemen für die Warte von Kernkraftwerken fest und gibt Anleitungen für die Entwicklung der Zuordnungskriterien.

Diese Norm ergänzt IEC 60964:1989 ^{N1)}, die für die Auslegung von Warten von Kernkraftwerken gilt.

Zweck dieser Norm ist, besondere Anforderungen für die Durchführung der Analyse und Zuordnung der Funktionen anzugeben, wie sie in 3.1 und 3.2 von IEC 60964:1989 gefordert werden, und ersetzt somit die in A.3.1 und A.3.2 von IEC 60964:1989 angegebene Anleitung.

Diese Norm ist sowohl für die Auslegung neuer Warten als auch für Nachrüstungen existierender Warten (bei Neuauslegung und bei Änderungen) anwendbar. Im zweiten Fall ist neben den direkt betroffenen Bereichen auch der Identifizierung von indirekt betroffenen Bereichen besondere Aufmerksamkeit zu widmen.

2 Normative Verweisungen

Die folgenden normativen Dokumente enthalten Festlegungen, die durch Verweisung in diesem Text Bestandteil dieser Internationalen Norm sind. Bei datierten Verweisungen gelten spätere Änderungen oder Überarbeitungen dieser Publikationen nicht. Anwender dieser Internationalen Norm werden jedoch gebeten, die Möglichkeit zu prüfen, die jeweils neuesten Ausgaben der nachfolgend angegebenen normativen Dokumente anzuwenden. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen normativen Dokuments. Mitglieder von ISO und IEC führen Verzeichnisse der gültigen Internationalen Normen.

IEC 60964:1989, *Design for control rooms of nuclear power plants*.

IEC 61771:1995, *Nuclear power plants – Main control-room – Verification and validation of design*.

3 Begriffe

Für die Anwendung dieser Norm gelten die in IEC 60964:1989 angegebenen und folgende Begriffe:

3.1

Störfallbedingungen

(en: **accident conditions**)

Satz von Bedingungen, welche in dem Bericht über die Sicherheits- oder Transientenanalyse und/oder den Störfallanweisungen festgelegt sind

3.2

Zuordnung von Funktionen

(en: **functional assignment**)

Verteilung von Funktionen auf die menschlichen und die automatisierten Bestandteile eines Systems

3.3

Mensch-Maschine-Schnittstelle

(en: **human machine interface**)

Schnittstelle zwischen Bedienpersonal (Operateure) und leittechnischem System, wie auch mit dem mit der Anlage verbundenen Computersystem. Die Schnittstelle umfasst Anzeigen, Steuerungen und das Bediener-Führungssystem

(siehe „man/machine interface“ in IEC 60964:1989)

^{N1)} Nationale Fußnote: Im Text der IEC 61839:2000 wird immer nur undatiert auf IEC 60964 verwiesen, gemeint ist aber immer die Ausgabe 1989. Die Verweisungen im Text sind in der deutschen Übersetzung entsprechend korrigiert.

3.4

probabilistische Risikobewertung

(en: probabilistic risk assessment)

methodischer Ansatz zur Bestimmung von Störfallabläufen, welche in Folge einer Vielzahl von auslösenden Ereignissen auftreten können; dieser schließt die systematische und realistische Bestimmung von Störfallhäufigkeit und -folgen ein ^{N2)}

3.5

Steuerfunktion

Regelungsfunktion ^{N3)}

(en: control function)

Steuer- und Regelhandlungen, die von Menschen oder Maschinen zur Erreichung eines funktionalen Ziels wahrgenommen werden, einschließlich der erforderlichen Informationsgewinnung und -verarbeitung ¹⁾

3.6

Aufgaben

(en: tasks)

Steuer- und Regelhandlungen, die von Menschen zur Erreichung eines funktionalen Ziels wahrgenommen werden ¹⁾

4 Vorgehensweise zur Analyse und Zuordnung der Funktionen

4.1 Allgemeine Beschreibung

Die Analyse und Zuordnung von Funktionen werden in Abschnitt 3 von IEC 60964:1989 als erster Schritt bei der Auslegung einer Warte gefordert (siehe [Bild 1](#)). Sie erfordern, zunächst alle für den Betrieb der Anlage erforderlichen Funktionen zu bestimmen und diese dann den Menschen oder den Maschinen zuzuordnen.

Zwei grundlegende Schritte sind erforderlich:

- a) Analyse der Funktionen;
- b) Zuordnung der Funktionen.

Diese sind in den Abschnitten [5](#) und [6](#) beschrieben.

4.1.1 Analyse der Funktionen

Die Bestimmung der Funktionen (siehe [5.2](#)) besteht zunächst in der Festlegung allgemeiner oder grundlegender Ziele des Betriebs der Anlage, insbesondere sichere und effektive Erzeugung elektrischer Energie, Schutz der Öffentlichkeit vor radiologischer Belastung, gefolgt von der Einteilung der für die Erfüllung dieser Ziele erforderlichen höchstrangigen Funktionen in eine Funktionshierarchie, deren niedrigste Funktionen die Steuer- oder Regelungsfunktion sind, welche den Menschen und Maschinen zuzuordnen sind. Die allgemeine Funktionsanalyse des Kernkraftwerks ist ein Mittel zur Bestimmung aller Funktionen, die von der Hauptwarte aus überwacht und gesteuert werden.

Die Aufstellung der Funktionen der verschiedenen Ebenen, die in dem obigen Schritt erstellt wurde, wird durch die Festlegung der grundlegenden Anforderungen an den betrieblichen Informationsfluss und -austausch vervollständigt (siehe [5.3.1](#)).

^{N2)} Nationale Fußnote: Die Probabilistische Risikobewertung (PRB) ist nicht mit der in Deutschland üblichen PSA „Probabilistische Sicherheitsanalyse“ gleichzusetzen. Die PRB entspringt der in Großbritannien eingeführten Risikobewertung als Grundlage für Sicherheitsbewertungen von Kernkraftwerken.

^{N3)} Nationale Fußnote: „Steuerfunktion“, wenn das Einstellen eines gewünschten Betriebszustands im offenen Wirkungsablauf (Signalführung in einer Richtung), „Regelfunktion“, wenn das Einstellen eines gewünschten Betriebszustands im geschlossenen Wirkungsablauf (eine Abweichung vom Sollwert wirkt über eine Stellgröße zurück auf die Regelgröße) gemeint ist.

¹⁾ Diese Definition weicht von der der IEC 60964:1989 ab und berücksichtigt das heutige Verständnis.