

|  |                                                                                                                                                                                                                                                                                                        |            |
|--|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
|  | <b>DIN IEC 63260<br/>(VDE 0491-60)</b>                                                                                                                                                                                                                                                                 | <b>DIN</b> |
|  | 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. | <b>VDE</b> |

ICS 27.120.20

**Leitfaden zur Berücksichtigung der Analyse menschlicher  
Zuverlässigkeit bei der probabilistischen Risikobewertung von nuklearen  
Energieerzeugungsanlagen und anderen kerntechnischen Anlagen  
(IEC 63260:2020)**

Guide for incorporating human reliability analysis into probabilistic risk assessments for nuclear power generating stations and other nuclear facilities  
(IEC 63260:2020)

Guide pour la prise en compte de l'analyse de la fiabilité humaine dans l'évaluation probabiliste de risque pour les centrales nucléaires de puissance et autres installations nucléaires  
(IEC 63260:2020)

Gesamtumfang 34 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE

## Anwendungsbeginn

Anwendungsbeginn dieser Norm ist 2022-01-01.

| Inhalt                                                                                                           | Seite |
|------------------------------------------------------------------------------------------------------------------|-------|
| Nationales Vorwort.....                                                                                          | 4     |
| Einleitung .....                                                                                                 | 7     |
| 1 Überblick.....                                                                                                 | 9     |
| 1.1 Anwendungsbereich .....                                                                                      | 9     |
| 1.2 Ziel .....                                                                                                   | 9     |
| 2 Begriffe und Abkürzungen .....                                                                                 | 9     |
| 2.1 Begriffe .....                                                                                               | 9     |
| 2.2 Abkürzungen .....                                                                                            | 12    |
| 3 Überblick über eine integrierte Analyse menschlicher Zuverlässigkeit .....                                     | 13    |
| 3.1 Allgemeines .....                                                                                            | 13    |
| 3.1.1 Bedeutung menschlicher Zuverlässigkeit.....                                                                | 13    |
| 3.1.2 Bedeutung integrierter Analysen menschlicher Zuverlässigkeit und probabilistischer Risikobewertungen ..... | 13    |
| 3.2 Übergeordnete Entwicklungsthemen .....                                                                       | 13    |
| 3.2.1 Vereinbarkeit der probabilistischen Risikobewertung .....                                                  | 13    |
| 3.2.2 Qualitative Analyse menschlicher Zuverlässigkeit .....                                                     | 14    |
| 3.2.3 Beziehung des Ansatzes zu seinen Ergebnissen .....                                                         | 14    |
| 3.2.4 Abstimmung der Methode auf die Anwendung .....                                                             | 14    |
| 3.2.5 Grenzen.....                                                                                               | 14    |
| 3.3 Prozess zur Analyse menschlicher Zuverlässigkeit .....                                                       | 15    |
| 3.3.1 Allgemeines .....                                                                                          | 15    |
| 3.3.2 Bestehende im Vergleich zu neuen Analysen menschlicher Zuverlässigkeit .....                               | 16    |
| 3.3.3 Struktur der Analyse menschlicher Zuverlässigkeit .....                                                    | 16    |
| 3.3.4 Zusammenfassung der Schritte der Analyse menschlicher Zuverlässigkeit.....                                 | 16    |
| 3.3.5 Ergebnisse.....                                                                                            | 17    |
| 4 Einzelheiten des Prozesses zur Analyse menschlicher Zuverlässigkeit.....                                       | 17    |
| 4.1 Allgemeines .....                                                                                            | 17    |
| 4.2 Schritte im Prozess zur Analyse menschlicher Zuverlässigkeit .....                                           | 18    |
| 4.2.1 Schritt 1: Das HRA-PRA-Team zusammenstellen und ausbilden.....                                             | 18    |
| 4.2.2 Schritt 2: Das Team mit der Anlage vertraut machen .....                                                   | 19    |
| 4.2.3 Schritt 3: Ein Anfangsmodell für die Anlage aufstellen .....                                               | 20    |
| 4.2.4 Schritt 4: Eine Durchsicht der Bedienereingriffe durchführen .....                                         | 21    |
| 4.2.5 Schritt 5: Die Bedienereingriffe charakterisieren .....                                                    | 23    |
| 4.2.6 Schritt 6: Die Bedienereingriffe wertmäßig beschreiben .....                                               | 24    |
| 4.2.7 Schritt 7: Das Anlagenmodell mit seiner Abhängigkeit und Wiederherstellbarkeit aktualisieren .....         | 25    |

|                       |                                                                                              |    |
|-----------------------|----------------------------------------------------------------------------------------------|----|
| 4.2.8                 | Schritt 8: Die Ergebnisse überprüfen .....                                                   | 26 |
| 5                     | Dokumentation .....                                                                          | 27 |
| 5.1                   | Ziel.....                                                                                    | 27 |
| 5.2                   | Aufbau .....                                                                                 | 27 |
| Anhang A (informativ) | Beispiel für die Dokumentation von Daten einer Analyse menschlicher<br>Zuverlässigkeit ..... | 29 |
| Anhang B (informativ) | Literaturhinweise .....                                                                      | 33 |

## **Bilder**

|                                                                             |    |
|-----------------------------------------------------------------------------|----|
| Bild 1 – Allgemeiner Prozess zur Analyse menschlicher Zuverlässigkeit ..... | 15 |
|-----------------------------------------------------------------------------|----|

## **Tabellen**

|                                                                                   |    |
|-----------------------------------------------------------------------------------|----|
| Tabelle 1 – Ergebnisse der Schritte zur Analyse menschlicher Zuverlässigkeit..... | 17 |
| Tabelle A.1 – Datenelemente der Analyse menschlicher Zuverlässigkeit .....        | 32 |

## Nationales Vorwort

Vorausgegangener Norm-Entwurf: E DIN IEC 63260 (VDE 0491-60):2020-11.

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

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

Das internationale Dokument wurde vom IEC/SC 45A „Instrumentation, control and electrical power systems of nuclear facilities“ der Internationalen Elektrotechnischen Kommission (IEC) und von IEEE veröffentlicht und unterliegt dem Copyright von IEEE. Sie wurde zugleich als IEEE Std 1082-2017 veröffentlicht. In die vorliegende DIN IEC 63260 (VDE 0491-60) wurde allerdings der in IEC 63260:2020 und IEEE Std 1082-2017 enthaltene Anhang C mit der Liste der auf IEEE-Seite an der Erarbeitung der Norm beteiligten Personen nicht mit übernommen.

Das IEC-Komitee hat entschieden, dass der Inhalt dieses Dokuments bis zu dem Datum (stability date) unverändert bleiben soll, das auf der IEC-Website unter „<http://webstore.iec.ch>“ zu diesem Dokument angegeben ist. Zu diesem Zeitpunkt wird entsprechend der Entscheidung des Komitees das Dokument

- bestätigt,
- zurückgezogen,
- durch eine Folgeausgabe ersetzt oder
- geändert.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. IEC ist 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 IEC 62138 (VDE 0491-3-3):2020-07**, Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Softwareaspekte für rechnerbasierte Systeme zur Realisierung von Funktionen der Kategorien B oder C (IEC 62138:2018); Deutsche Fassung **EN IEC 62138:2019**
- **DIN EN IEC 61500 (VDE 0491-3-4):2020-04**, Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Datenkommunikation in Systemen, die Funktionen der Kategorie A ausführen (IEC 61500:2018); Deutsche Fassung **EN IEC 61500:2019**
- **DIN EN 62566 (VDE 0491-3-5):2015-02**, Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Entwicklung HDL-programmierter integrierter Schaltkreise für Systeme, die Funktionen der Kategorie A ausführen (IEC 62566:2012); Deutsche Fassung **EN 62566:2014**
- **DIN EN IEC 62645 (VDE 0491-3-7):2021-03**, Kernkraftwerke – Leittechnische und elektrische Systeme – Anforderungen an die IT-Sicherheit (IEC 62645:2019); Deutsche Fassung **EN IEC 62645:2020**

- **DIN EN IEC 62859 (VDE 0491-3-8):2021-07**, Kernkraftwerke – Leittechnische Systeme – Anforderungen für die Koordinierung von Sicherheit und IT-Sicherheit (IEC 62859:2016 + A1:2019); Deutsche Fassung **EN IEC 62859:2020**
- **DIN EN IEC 62566-2 (VDE 0491-3-9):2021-11**, Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Entwicklung HDL-programmierter integrierter Schaltkreise – Teil 2: HDL-programmierte integrierte Schaltkreise für Systeme, die Funktionen der Kategorie B oder C ausführen (IEC 62566-2:2020); Deutsche Fassung **EN IEC 62566-2:2020**
- **DIN IEC 62117 (VDE 0491-4):2001-10**, Kernkraftwerke – Druckwasserreaktoren – Überwachung ausreichender Kühlung des Kerns im abgeschalteten Zustand des Reaktors (IEC 62117:1999)
- **DIN EN 61839 (VDE 0491-5):2015-01**, Kernkraftwerke – Auslegung von Warten – Analyse und Zuordnung der Funktionen (IEC 61839:2000); Deutsche Fassung **EN 61839:2014**
- **DIN EN IEC 60964 (VDE 0491-5-1):2020-08**, Kernkraftwerke – Warten – Auslegung (IEC 60964:2018); Deutsche Fassung **EN 60964:2019**
- **DIN EN 62241 (VDE 0491-5-2):2015-06**, Kernkraftwerke – Warte – Alarmfunktionen und ihre Darstellung (IEC 62241:2004); Deutsche Fassung **EN 62241:2015**
- **DIN EN 61227 (VDE 0491-5-3):2016-11**, Kernkraftwerke – Warten – Handbedienungen (IEC 61227:2008); Deutsche Fassung **EN 61227:2016**
- **DIN EN 61772 (VDE 0491-5-4):2013-09**, Kernkraftwerke – Warten – Anwendung von Sichtgeräten (IEC 61772:2009); Deutsche Fassung **EN 61772:2013**
- **DIN EN 60965 (VDE 0491-5-5):2017-02**, Kernkraftwerke – Warten – Notsteuerstellen für das Abfahren des Reaktors ohne Verbindung zur Hauptwarte (IEC 60965:2016); Deutsche Fassung **EN 60965:2016**
- **DIN EN IEC 62646 (VDE 0491-5-6):2020-04**, Kernkraftwerke – Warten – Rechnerunterstützte Prozeduren (IEC 62646:2016); Deutsche Fassung **EN IEC 62646:2019**
- **DIN IEC 60568 (VDE 0491-6):2006-11**, Kernkraftwerke – Instrumentierung mit sicherheitstechnischer Bedeutung – Kerninstrumentierung zur Messung der Neutronenflussdichte in Leistungsreaktoren (IEC 60568:2006)
- **DIN EN IEC 60709 (VDE 0491-7):2020-05**, Kernkraftwerke – Leittechnik und elektrische Energieversorgungssysteme mit sicherheitstechnischer Bedeutung – Physikalische und elektrische Trennung (IEC 60709:2018); Deutsche Fassung **EN IEC 60709:2019**
- **DIN EN IEC 63046 (VDE 0491-8-2):2022-01**, Kernkraftwerke – Elektrische Stromversorgungssysteme – Allgemeine Anforderungen (IEC 63046:2020); Deutsche Fassung **EN IEC 63046:2021**
- **DIN EN IEC 61225 (VDE 0491-8-3):2020-11**, Kernkraftwerke – Leittechnische System und elektrische Stromversorgungssysteme – Anforderungen an statische unterbrechungsfreie Gleich- und Wechselstrom-Energieversorgungssysteme (IEC 61225:2018); Deutsche Fassung **EN IEC 61225:2020**
- **DIN EN 62808 (VDE 0491-9-3):2020-06**, Kernkraftwerke – Leittechnik mit sicherheitstechnischer Bedeutung – Auslegung und Qualifizierung von Isolationseinrichtungen (IEC 62808:2015 + A1:2018); Deutsche Fassung **EN 62808:2016 + A1:2019**
- **DIN EN 62340 (VDE 0491-10):2010-12**, Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Anforderungen zur Beherrschung von Versagen aufgrund gemeinsamer Ursache (IEC 62340:2007); Deutsche Fassung **EN 62340:2010**
- **DIN EN IEC 62003 (VDE 0491-11):2021-08**, Kernkraftwerke – Elektro- und leittechnische Systeme mit sicherheitstechnischer Bedeutung – Anforderungen für die Prüfung der elektromagnetischen Verträglichkeit (IEC 62003:2020); Deutsche Fassung **EN IEC 62003:2020**
- **DIN IEC/IEEE 62582-1 (VDE 0491-21-1):2020-03**, Kernkraftwerke – Leittechnik mit sicherheitstechnischer Bedeutung – Zustandsüberwachung elektrischer Geräte – Teil 1: Allgemeines (IEC/IEEE 62582-1:2011)
- **DIN IEC/IEEE 62582-2 (VDE 0491-21-2):2020-03**, Kernkraftwerke – Leittechnik mit sicherheitstechnischer Bedeutung – Zustandsüberwachung elektrischer Geräte – Teil 2: Eindringmodul (IEC/IEEE 62582-2:2011)
- **DIN IEC/IEEE 62582-3 (VDE 0491-21-3):2020-03**, Kernkraftwerke – Leittechnik mit sicherheitstechnischer Bedeutung – Zustandsüberwachung elektrischer Geräte – Teil 3: Reißdehnung (IEC/IEEE 62582-3:2012)

## DIN IEC 63260 (VDE 0491-60):2022-01

- **DIN IEC/IEEE 62582-4 (VDE 0491-21-4):2020-03**, Kernkraftwerke – Leittechnik mit sicherheitstechnischer Bedeutung – Zustandsüberwachung elektrischer Geräte – Teil 4: Oxidation (IEC/IEEE 62582-4:2011)
- **DIN IEC/IEEE 62582-5 (VDE 0491-21-5):2020-03**, Kernkraftwerke – Leittechnik mit sicherheitstechnischer Bedeutung – Zustandsüberwachung elektrischer Geräte – Teil 5: Optische Zeitbereichsreflektometrie (IEC/IEEE 62582-5:2015)
- **DIN IEC/IEEE 62582-6 (VDE 0491-21-6):2020-05**, Kernkraftwerke – Leittechnik mit sicherheitstechnischer Bedeutung – Zustandsüberwachung elektrischer Geräte – Teil 6: Isolationswiderstand (IEC/IEEE 62582-6:2019)
- **DIN EN 62765-1 (VDE 0491-22-1):2018-03**, Kernkraftwerke – Leittechnik mit sicherheitstechnischer Bedeutung – Alterungsmanagement von Sensoren und Transmittern – Teil 1: Drucktransmitter (IEC 62765-1:2015); Deutsche Fassung **EN 62765-1:2017**
- **DIN EN IEC 62465 (VDE 0491-22-10):2020-05**, Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Alterungsmanagement von elektrischen Kabeln (IEC 62465:2010); Deutsche Fassung **EN IEC 62465:2019**
- **DIN IEC 63260 (VDE 0491-60):2022-01**; Leitfaden zur Berücksichtigung der Analyse menschlicher Zuverlässigkeit bei der probabilistischen Risikobewertung von nuklearen Energieerzeugungsanlagen und anderen kerntechnischen Anlagen (IEC 63260:2020)
- **DIN EN 60780-323 (VDE 0491-80):2018-03**, Kerntechnische Anlagen – Elektrisches Gerät mit sicherheitstechnischer Bedeutung – Qualifizierung (IEC/IEEE 60780-323:2016); Deutsche Fassung **EN 60780-323:2017**
- **DIN EN 60671 (VDE 0491-100):2011-12**, Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Prüfungen zur Sicherstellung der Funktionsfähigkeit (IEC 60671:2007); Deutsche Fassung **EN 60671:2011**

## Einleitung

Jeder Vorgang, der eine Regelung von Hand erfordert, um das Risiko für die Öffentlichkeit zu minimieren, erfordert ein hohes Maß an menschlicher Zuverlässigkeit. Diese Zuverlässigkeit lässt sich mit der systematischen Anwendung einer probabilistischen Risikobewertung (PRA, en: probabilistic risk assessment) bewerten. Eine derartige Bewertung erfordert jedoch ein genaues Verständnis der Verfahren für menschliche Leistungsfähigkeit und Zuverlässigkeit, um eine begründete Zuverlässigkeitsbewertung zu gestalten.

Die anfängliche Risikobewertung, die von der nuklearen Energiebranche durchgeführt wurde, WASH-1400 [B17], erkannte die Notwendigkeit für ein Fachgebiet der Analyse menschlicher Zuverlässigkeit (HRA, en: human reliability analysis), das systematisch innerhalb des PRA-Projekts einzugliedern ist<sup>1</sup>. Die Vorgehensweise – sowohl in der Analyse der Ereignisse aufgrund von menschlichem Versagen als auch, sie zu ermitteln und in geeigneter Weise in die probabilistische Risikobewertung einzufügen – war jedoch neu und auf mehrfache Weise unzulänglich.

Die Beschränkungen im Verständnis von menschlicher Zuverlässigkeit Mitte der 1970er Jahre traten anschaulich beim Störfall in Three-Mile-Island (TMI)<sup>N1</sup> zutage. Die nukleare Aufsichtsbehörde der USA (NRC) berief gemeinsam mit dem Institute for Electrical and Electronics Engineers (IEEE) direkt nach TMI eine Konferenz über die Probleme der menschlichen Einflüsse, die in TMI aufgetreten waren, ein<sup>2</sup>. Aus dieser Konferenz entwickelte sich anschließend eine Konferenzfolge. Zeitgleich mit der Einberufung dieser Konferenz begann das Unterkomitee 7 „Human Factors and Control Facilities“ des Komitees für nukleare Energietechnologie (NPEC) der IEEE eine Diskussion, die HRA-Technologie zu vereinheitlichen. Die Nahtstelle von PRA und HRA, das Einfügen und Durchführen einer Analyse menschlicher Zuverlässigkeit im Zusammenhang mit einer probabilistischen Risikobewertung, wurde als der am weitesten entwickelte Ansatz der Analyse menschlicher Zuverlässigkeit anerkannt. Ein Leitfaden, das am wenigsten verpflichtende Dokument der IEEE-Normen, wurde im Jahr 1984 als IEEE-Normprojekt genehmigt. Der Leitfaden wurde im Jahr 1997 überarbeitet.

Dieser Leitfaden behandelt die erforderlichen Schritte zur Erfassung der menschlichen Zuverlässigkeit bei der Risikobewertung. Die Absicht dieses Leitfadens ist nicht die Beschreibung eines spezifischen Verfahrens der Analyse menschlicher Zuverlässigkeit im Einzelnen, sondern es geht eher darum, eine methodenunabhängige Rahmenstruktur zu bestätigen, um einen weiten Bereich von Verfahren der Analyse menschlicher Zuverlässigkeit zur Unterstützung der probabilistischen Risikobewertung zu verwenden. Da sich Bedienerfehler als wesentliche Beitragsgröße zum Risiko herausgestellt haben, unterstreicht dieser Leitfaden die systematische Integration der Analyse menschlicher Zuverlässigkeit im frühesten Stadium und über die ganze probabilistische Risikobewertung hinweg.

Seit der Überarbeitung der IEEE Std 1082<sup>TM</sup> in 1997 wurden die Verfahren der Analyse menschlicher Zuverlässigkeit, die Theorie und Handhabungen wesentlich weiterentwickelt. Eine Arbeitsgruppe fand sich im Jahr 2012 zusammen, um diesen Leitfaden zu bestätigen. Die Arbeitsgruppe fand zahlreiche Beispiele, in denen die Norm von 1997 veraltete Bezüge enthielt oder Gesichtspunkte der Analyse menschlicher Zuverlässigkeit, die inzwischen allgemein anerkannt waren, nicht berücksichtigte. Die Arbeitsgruppe bestätigte jedenfalls die in der Fassung IEEE Std 1082-1997 eingeführte, der Analyse menschlicher Zuverlässigkeit zugrunde liegende Praxis als zeitgemäß und für die Anwendung bei der Analyse menschlicher Zuverlässigkeit zutreffend. Die Arbeitsgruppe aktualisierte im erforderlichen Maß den Leitfaden, um wichtige Fortschritte in der Analyse menschlicher Zuverlässigkeit wiederzugeben. Die Rahmenstruktur zur Ausführung einer Analyse menschlicher Zuverlässigkeit, wie sie sich in IEEE Std. 1082-1997 findet, verbleibt in dieser Fassung unberührt, wurde aber um Bezüge zu gegenwärtigen Problemen und Vorgehensweisen bereichert.

IEEE Std 1082 bleibt ein einzigartiger, kurzgefasster Leitfaden zur Beschreibung der Rahmenstruktur für die Durchführung einer Analyse menschlicher Zuverlässigkeit als Bestandteil einer PRA. Jenseits der IEEE Std 1082 gibt es noch weitere Unterlagen zur einheitlichen Anleitung. Das Institut für elektrische Energieforschung (EPRI) veröffentlichte zum Beispiel ein systematisches Verfahren für die Zuverlässigkeit menschlicher Hand-

<sup>1</sup> Die Angaben in eckigen Klammern bezeichnen die in [Anhang B](#) aufgeführten Literaturhinweise.

<sup>N1</sup> Nationale Fußnote: Auch bekannt als Unfall von Harrisburg.

<sup>2</sup> Veröffentlichungen der NUREG sind erhältlich bei der U.S. Nuclear Regulatory Commission (<http://www.nrc.gov>).

lungen (SHARP) und überarbeitete den SHARP-1-Ansatz [B4], der die Vorgehensweise zur Einfügung einer wertmäßigen Analyse menschlicher Zuverlässigkeit in eine PRA im Einzelnen beschreibt und dabei Teile der IEEE Std 1082 wiedergibt<sup>3</sup>. Die American Society of Mechanical Engineers (ASME) hat die Norm für Level 1/ „Wahrscheinlichkeitsbezogene Risikobewertungen für große Störfälle mit frühzeitiger Auslösehäufigkeit zur Anwendung in Kernkraftwerken“ [B1] erstellt, die hohe Anforderungen an das Niveau für HRAS, um in PRAs eingefügt zu werden, beschreibt. Die NRC veröffentlichte Handlungsempfehlungen für die Ausführung von Analysen zur menschlichen Zuverlässigkeit [B13]. Diese drei Anleitungen und zahlreiche Umsetzungsempfehlungen, die man in speziellen Verfahren und Texten zur Analyse menschlicher Zuverlässigkeit findet, ergänzen IEEE Std 1082, ersetzen diese jedoch nicht. SHARP 1 [B14] zum Beispiel beschäftigt sich mit der Wertbestimmung der Analysen zur menschlichen Zuverlässigkeit zum Einbau in die PRA, enthält aber nicht das vollständige HRA-Verfahren der IEEE Std 1082. Die PRA-Norm der ASME [B1] stellt Qualitätsanforderungen für Analysen zur menschlichen Zuverlässigkeit auf, beschreibt aber nicht, wie die Analyse zur menschlichen Zuverlässigkeit durchzuführen ist<sup>4</sup>. Die Umsetzungsempfehlungen der NRC sind bei mehreren Gesichtspunkten gleichlautend wie IEEE Std 1082, bieten aber keinen gesamten Verfahrensablauf, um die Analyse zur menschlichen Zuverlässigkeit durchzuführen. IEEE Std 1082 behält als übergeordnete Rahmennorm für die Durchführung einer Analyse zur menschlichen Zuverlässigkeit ihre Gültigkeit.

IEEE Std 1082 bietet einen verfahrensunabhängigen Ansatz. Die Auflistung, wie sich die Anleitung in die einzelnen HRA-Verfahren einbinden lässt, liegt außerhalb des Anwendungsbereichs dieses Leitfadens. Aktuelle Übersichten von HRA-Verfahren sind in [B1], [B3], [B14], [B15] und [B16] zu finden. Die Entwicklung von HRA-Verfahren verlief umfangreich, mit neuen Ansätzen zur Erfassung von Erkennungsvermögen, Zusammenhängen, Inbetriebnahmefehlern sowie Ansätzen, die die vereinfachte wertmäßige Bestimmung bei Analysen zur menschlichen Zuverlässigkeit bis zu Modellen für die Dynamik menschlicher Leistungsfähigkeit umfassen. Die Rahmenstruktur zum Einbau von HRAs in PRAs, wie sie in diesem Leitfaden dargestellt wird, bezieht sich auf alle HRA-Verfahren, obwohl einige Anpassungen notwendig sein dürften, um individuelle Anforderungen von speziellen Verfahren zu erfassen. Solche Anpassungen sollten, besonders bei der Verwendung vereinfachter HRA-Verfahren, nicht als Wirtschaftlichkeitsgewinn zulasten der Durchführung eines umfassenden und vollständigen HRA-Prozesses gewertet werden.

<sup>3</sup> Veröffentlichungen der EPRI sind erhältlich beim Electric Power Research Institute (<http://epri.com>).

<sup>4</sup> Veröffentlichungen der ASME sind erhältlich bei American Society of Mechanical Engineers (<http://www.asme.org/>).

# 1 Überblick

## 1.1 Anwendungsbereich

Dieser Leitfaden bietet einen strukturierten Rahmen für die Berücksichtigung der Analyse menschlicher Zuverlässigkeit (HRA) in probabilistischen Risikobewertungen.

## 1.2 Ziel

Ziel dieses Leitfadens ist es, die Analyse der Wechselwirkungen zwischen Bedienern und Systemen bei probabilistischen Risikobewertungen zu verbessern, um die Absicherung nachvollziehbarer Schlussfolgerungen zu unterstützen und die Dokumentierung solcher Bewertungen zu vereinheitlichen. Um dies zu verwirklichen, wird ein spezielles Grundgerüst aus gängigen Anwendungen entwickelt, das als Maßstab zur Bewertung alternativer Verfahren zur Berücksichtigung von Analysen menschlicher Zuverlässigkeit in probabilistischen Risikobewertungen dient.

# 2 Begriffe und Abkürzungen

## 2.1 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe<sup>N2</sup>. Für Begriffe, die nicht in diesem Abschnitt definiert sind, sollte das *IEEE Standards Dictionary Online* zu Rate gezogen werden<sup>5</sup>.

**ANMERKUNG** Mehrere Begriffe, die in diesem Leitfaden und im Bereich der Analyse menschlicher Zuverlässigkeit verwendet werden, sind wichtig, werden jedoch im allgemeinen Gebrauch nicht eindeutig oder nicht häufig genug verwendet, um geläufig zu sein. Sie werden in diesem Abschnitt zum Zweck des Verständnisses und der Nachvollziehbarkeit dieses Leitfadens definiert<sup>6</sup>.

### 2.1.1

**Basisereignis**  
en **basic event**

Bestandteil des Modells der probabilistischen Risikobewertung, das nicht weiter untergliedert wird, da es sich an der Auflösungsgrenze im Einklang mit den verfügbaren Daten bewegt

### 2.1.2

**Auswirkungen**  
en **consequences**

Ergebnis(se) eines bestimmten Ereignisses (d. h. Ereignisse, die einem bestimmten Ereignis folgen und von diesem abhängig sind)

### 2.1.3

**Schnittmenge**  
en **cutset**

Gruppe von Ereignissen, die, sofern alle eintreten, das übergeordnete Ereignis auslösen (das Ergebnis der Untersuchung, das mit Hilfe eines Fehlerbaums analysiert wird)

<sup>N2</sup> Nationale Fußnote: Abweichend von der mit IEEE Std. 1082-2017 identischen IEC-Publikation sind die Begriffe in diesem Abschnitt so formatiert und nummeriert wie in den ISO/IEC Directives gefordert.

<sup>5</sup> Das *IEEE Standards Dictionary Online* ist verfügbar unter <http://dictionary.ieee.org>.

<sup>6</sup> Anmerkungen in Text, Tabellen und Bildern einer Norm dienen nur zur Information und enthalten keine Anforderungen, die im Rahmen dieser Norm angewendet werden müssen.

#### 2.1.4

**Abhängigkeit**  
en **dependence**

Beziehung zwischen zwei oder mehr Ereignissen aufgrund von menschlichem Versagen, die zu einer Anpassung des Modells oder der Wahrscheinlichkeit menschlicher Fehler führen kann

#### 2.1.5

**Auslegungsstörfall**  
en **design-basis accident**

anzunehmender Störfall, für den eine nukleare Einrichtung ausgelegt und gebaut sein muss, um ihn ohne Verlust an Systemen, Gebäuden und Komponenten, die für die Gesundheit und Sicherheit der Öffentlichkeit benötigt werden, zu überstehen

#### 2.1.6

**herausragender Ablauf**  
en **dominant sequence**

Ablauf von Ereignissen, der einen herausragenden Beitrag zum Gesamtrisiko darstellt

#### 2.1.7

**Ereignis<sup>7</sup>**  
en **event**

- (A) jegliche Änderung im Zustand oder der Leistungsfähigkeit von Interesse
- (B) Erscheinung zu einem bestimmten Zeitpunkt

#### 2.1.8

**Ereignisbaum**  
en **event tree**

graphische Darstellung des logischen Ablaufs möglicher Szenarien durch mehrfache Ereignisserien, die eintreten oder nicht eintreten

#### 2.1.9

**Fehlerbaum**  
en **fault tree**

graphische Darstellung einer analytischen Technik, bei der ein unerwünschter Zustand eines Systems festgelegt wird und die Strukturen, die zu diesem Zustand führen, bewertet werden können, um zu bestimmen, wie die unerwünschte Systemfehlfunktion auftreten kann

#### 2.1.10

**Bedienerhandlung**  
en **human action**

erkennbares Ergebnis der Absicht einer Person (oftmals eine körperliche Bewegung)

#### 2.1.11

**Bedienerfehler**  
en **human error**

Scheitern bei der Ausführung einer Tätigkeit durch eine Person, um festgelegte Kriterien von Genauigkeit, Vollständigkeit, Fehlerfreiheit, Eignung oder Rechtzeitigkeit zu erfüllen

#### 2.1.12

**Wahrscheinlichkeit eines Bedienerfehlers**  
en **HEP, human error probability**

quantitative Schätzung der Wahrscheinlichkeit eines Bedienerfehlers

---

<sup>7</sup> Diese Definition weicht von denen in früheren IEEE-Leitfäden ab. Die hier vorliegende Definition wurde auf die besondere Verwendung in der Analyse menschlicher Zuverlässigkeit zugeschnitten.

**2.1.13****Ereignis aufgrund von menschlichem Versagen**en **HFE, human failure event**

Basisereignis, das auf einen Bedienerfehler zurückgeht

**2.1.14****Bedienereingriff**en **human interaction**

Handlung oder Folge von menschlichen Handlungen, die die Geräte, die Reaktion von Systemen oder andere Bedienerhandlungen beeinflusst

**2.1.15****Analyse menschlicher Zuverlässigkeit**en **HRA, human reliability analysis**

beliebige Anzahl von formalen Vorgehensweisen oder Verfahren, um die Quellen von Bedienerfehlern festzustellen und die damit verbundenen Wahrscheinlichkeiten für Bedienerfehler zu bemessen

**2.1.16****auslösendes Ereignis**en **initiating event**

anlageninternes oder -externes Ereignis, das den Dauerbetrieb der Anlage stört, indem es die Anlagenüberwachung und Sicherheitssysteme auslöst, deren Versagen möglicherweise zu einer Kernschmelze oder der Freisetzung von Zerfallsprodukten führen könnte

**2.1.17****Betriebspersonal****Betriebsmannschaft**en **operating crew**

Anlagenpersonal, das im Schichtbetrieb arbeitet, um die Anlage zu betreiben

Anmerkung 1 zum Begriff: Dieses umfasst das Personal in der Warte und solches Hilfspersonal, das das Wartenpersonal beim Betrieb der Anlage direkt unterstützt.

**2.1.18****Leistungsbeeinflussungsfaktor****Formfaktor für die Leistungsfähigkeit**en **PSF, performance shaping factor**

Faktor, der die menschliche Zuverlässigkeit durch seine Auswirkungen auf die Leistungsfähigkeit beeinflusst

Anmerkung 1 zum Begriff: Dies schließt Einflüsse durch die Umgebungsbedingungen, die Auslegung der Schnittstellen zwischen Bedienern und Systemen, Verfahrensregeln, Ausbildung und Überwachung ein.

**2.1.19****probabilistische Risikobewertung****wahrscheinlichkeitsbezogene Risikobewertung**en **PRA, probabilistic risk assessment**

qualitative und wertmäßige Bestimmung des Risikos in Verbindung mit dem Anlagenbetrieb und der Wartung, die anhand der Häufigkeit des Auftretens von Risikokennzahlen, wie Kernschmelze oder Freisetzung von radioaktivem Material und seine Auswirkungen auf die öffentliche Gesundheit gemessen wird

Anmerkung 1 zum Begriff: Auch als wahrscheinlichkeitsbezogene Sicherheitsbewertung (en: probabilistic safety assessment, PSA) bezeichnet.

**2.1.20****Wiederherstellung**en **recovery**

Folge von Eingriffen, mit der Zielsetzung, die ausgefallene Gerätschaft wiederherzustellen oder Alternativen zu finden, um ihre Funktion abzudecken