KTA 3501

Reaktorschutzsystem und Überwachungseinrichtungen des Sicherheitssystems

Fassung 2015-11

Frühere Fassungen der Regel: 1985-06 (BAnz. Nr. 203a vom 29. Oktober 1985)
1977-03 (BAnz. Nr. 107 vom 11. Juni 1977)

Inhalt

Grundlagen

(1) Die Regeln des Kerntechnischen Ausschusses (KTA) haben die Aufgabe, sicherheitstechnische Anforderungen anzugeben, bei deren Einhaltung die nach dem Stand von Wissenschaft und Technik erforderliche Vorsorge gegen Schäden durch die Errichtung und den Betrieb der Anlage (§ 7 Abs. 2 Nr. 3 AtG) getroffen ist, um die im Atomgesetz und in der Strahlenschutzverordnung (StrlSchV) festgelegten sowie in den „Sicherheitsanforderungen an Kernkraftwerke“ (SiAnf) und den „Interpretationen zu den Sicherheitsanforderungen an Kernkraftwerke“ weiter konkretisierten Schutzziele zu erreichen.

(2) Die Aufgabenstellung für die Leittechnik wird aus den Anforderungen der Systemtechnik abgeleitet. Die Anforderungen an die Systemtechnik und deren Kategorisierung leiten sich aus den Sicherheitsebenen ab. Eine Zuordnung der Kategorien von Leittechnikfunktionen zu den Sicherheitsebenen wird in den Interpretationen zu den SiAnf vorgenommen.

(3) Basierend auf den SiAnf und deren Interpretationen wird in dieser Regel festgelegt, welche Anforderungen an das Reaktorschutzsystem, die Schutzbegrenzungen, die Zustandsbegrenzungen und an die Überwachungseinrichtungen des Sicherheitssystems zu stellen sind.

(4) Im atomrechtlichen Genehmigungsverfahren zur Prüfung erforderliche Unterlagen über das Reaktorschutzsystem und die Überwachungseinrichtungen des Sicherheitssystems sind in der Zusammenstellung der in atomrechtlichen Genehmigungs- und Aufsichtsverfahren für Kernkraftwerke zur Prüfung erforderlichen Informationen (ZPI) aufgeführt.

(5) Die leittechnischen Funktionen des Reaktorschutzsystems, der Schutzbegrenzungen, der Zustandsbegrenzungen und der Überwachungseinrichtungen des Sicherheitssystems sind in dieser Regel gemäß der Definition in Abschnitt 2.2 kategorisiert.

(6) Die vorliegende Regel wird durch die Regeln KTA 3503, KTA 3504, KTA 3505, KTA 3506 und KTA 3507 ergänzt.

(7) Zusätzlich zu Abschnitt 8 wird die elektrische Energieversorgung in den Regeln KTA 3701 bis KTA 3705 geregelt.

(8) Zusätzlich zu Abschnitt 7 sind Anforderungen an lüftungstechnische Anlagen zur Kühlung der Sicherheitsleittechnik in KTA 3601 enthalten.

(9) Die Anforderungen an den Nachweis der Beständigkeit von elektrischen Einrichtungen unter Störfallbedingungen werden in KTA 2101.3, KTA 2201.4 und KTA 3706 behandelt.

(10) Weiter gilt zur Erfüllung der Anforderungen an die Qualitätssicherung übergeordnet die Regel KTA 1401. Anforderungen an das Alterungsmanagement sind in der KTA 1403 enthalten.

(11) In dieser Regel wird vorausgesetzt, dass die konventionellen Vorschriften und Normen (z. B. Unfallverhütungsvorschriften, DIN-Normen und VDE-Bestimmungen) unter Beachtung kernkraftwerkspezifischer Sicherheitsanforderungen eingehalten werden.

1 Anwendungsbereich

(1) Diese Regel gilt für Einrichtungen der Sicherheitsleittechnik in ortsfesten Kernkraftwerken, die leittechnische Funktionen der Kategorie A und B nach 2.2 ausführen.

(2) Diese Regel enthält Anforderungen an Aufbau, Ausführung, Gerätequalität, Einbau und Prüfung der Sicherheitsleittechnik für Einrichtungen, die leittechnische Funktionen der Kategorie A und B nach 2.2 ausführen. Sie enthält eine Zusammenstellung von Auslegungskriterien, Anforderungen an die Qualität und Qualitätssicherung und Anforderungen an die Funktionsweise der Sicherheitsleittechnik für Einrichtungen, die leittechnische Funktionen der Kategorie A und B nach 2.2 ausführen.

Hinweis:

Anforderungen an Sicherheitsgefahrenmeldungen (Klasse S) sowie an Aggregateschutzeinrichtungen, deren Signale Vorrang vor den Signalen von A-Funktions-Einrichtungen haben, werden in eigenständigen Abschnitten behandelt.

(3) Zusätzlich werden in dieser Regel auch Anforderungen an Protokolliereinrichtungen und Serviceeinrichtungen, die für A- und B-Funktions-Einrichtungen sowie Gefahrenmeldeeinrichtungen der Klasse I verwendet werden, gestellt.

(4) Nicht zum Anwendungsbereich dieser Regel gehören die elektrischen Antriebe, die Leistungskabel und die Schaltanlagenabzweige einschließlich der Steuerstromkreise.

Hinweis:

Anforderungen an diese Einrichtungen werden in den Regeln KTA 3504 und KTA 3701 bis KTA 3705 behandelt.

2 Begriffe

2.1 Definitionen

(1) A-Funktions-Einrichtungen

A-Funktions-Einrichtungen sind Einrichtungen zur Ausführung von Leittechnikfunktionen der Kategorie A.

(2) Aggregateschutz

Der Aggregateschutz ist eine Einrichtung, die einem Aggregat zugeordnet ist und dieses vor Betriebsbedingungen, für die das Aggregat nicht ausgelegt und bestimmt ist, schützen soll.

(3) Anregeebene

Die Anregeebene ist der Teil von A-, B-, C-Funktions-Einrichtungen, in dem alle Anregekanalgruppen zusammengefasst sind.

(4) Anregekanal

Der Anregekanal ist eine Einrichtung, die zur Erfassung und Aufbereitung von Prozessvariablen und zur Bildung eines Anregesignals notwendig ist. Ein Anregekanal umfasst alle Geräte, beginnend bei den Messwertgebern und endend bei einem Grenzsignalgeber-Ausgang.

(5) Anregekanalgruppe

Die Anregekanalgruppe ist ein System von mehreren Anregekanälen zur redundanten Erfassung von Prozessvariablen und zur Bildung redundanter Anregesignale.

(6) Anregekriterium

Das Anregekriterium ist die Bedingung, unter der eine Schutzaktion ausgelöst wird.

(7) Anregesignal

Das Anregesignal ist das Ausgangssignal eines Anregekanals und das Eingangssignal in die Logikebene.

(8) Ansprechverzögerung

Die Ansprechverzögerung ist die Gesamtheit der Eigenschaften eines Systems, die die Verzögerung vom Anstehen des Eingangssignals bis zur Ausgabe des Ausgangssignals bestimmen.

(9) Antivalenzüberwachung

Die Antivalenzüberwachung ist eine Einrichtung, die binäre Signale auf Eindeutigkeit überwacht.

(10) Ausfall

Verlust der Fähigkeit einer Einrichtung die geforderte Funktion zu erfüllen.

Hinweis:

Das Ereignis Ausfall markiert den Zeitpunkt des Übergangs von der Korrektheit zu einem fehlerhaften Zustand. Mit einem Ausfall kann gleichzeitig ein Versagen auftreten, muss aber nicht. Zum Beispiel

kann ein Aggregat, das nicht angefordert wird, ausgefallen sein, versagen wird es erst, wenn es angefordert wird und seine Funktion nicht mehr erbringt.

(11) Ausfall, systematischer

Ausfall aufgrund der gleichen Ursache.

Hinweis:

(1) Ein systematischer Ausfall von leittechnischen Einrichtungen kann sich als gleichzeitiger oder in kurzer zeitlicher Abfolge auftretender Ausfall mehrerer Einrichtungen aufgrund der gleichen Ursache zeigen.

(2) Er kann z. B. durch falsche Auslegung, Fehler in einer Fertigungsserie, falsche Betriebsweise, Wassereinbruch oder Brand in der Anlage hervorgerufen werden.

(12) Auslösesignal

Das Auslösesignal ist ein Ausgangssignal der Logikebene oder der Steuerebene, das Schutzaktionen auslöst.

(13) Bestimmungsgemäßer Betrieb

Der Betrieb, für den eine Anlage nach ihrem technischen Zweck bestimmt, ausgelegt und geeignet ist, umfasst die Betriebszustände und Betriebsvorgänge

a) bei funktionsfähigem Zustand der Einrichtungen, (ungestörter Betriebszustand, Normalbetrieb),

b) des anomalen Betriebs (gestörter Betriebszustand, Störung) sowie

c) bei Instandhaltungsvorgängen (Inspektion, Wartung, Instandsetzung).

(14) Betriebsbegrenzung

Die Betriebsbegrenzung ist eine Einrichtung zur Begrenzung von Prozessvariablen auf vorgegebene Werte, um die Verfügbarkeit der Anlage zu erhöhen.

(15) Betriebsverriegelung

Die Betriebsverriegelung ist eine Einrichtung zur betrieblichen Steuerung oder zum betrieblichen Schutz von Komponenten oder Systemen.

(16) B-Funktions-Einrichtungen

B-Funktions-Einrichtungen sind Einrichtungen zur Ausführung von Leittechnikfunktionen der Kategorie B.

(17) Dissimilare leittechnischen Einrichtungen

Dissimilare leittechnischen Einrichtungen besitzen die Eigenschaft hinsichtlich Hardware, Software, Entwicklungswerkzeugen, Entwicklungsteams, Fertigung, Test und Instandhaltung hinreichend unähnlich bzw. ungleichartig zu anderen leittechnischen Einrichtungen zu sein. Dissimilarität ist ein Teilaspekt der Diversität, der sich auf rechnerbasierte oder programmierbare Geräte bezieht.

Hinweise:

(1) Ziel ist es, unabhängige Systeme oder Teilsysteme so aufzubauen, dass deren sicherheitstechnisch unverzichtbare Funktionen auch beim postulierten systematischen Versagen von einem der unabhängigen Systeme oder Teilsysteme erhalten bleiben. Dazu muss die Dissimilarität in den zur Fehlerbeherrschung wichtigen Eigenschaften aufgezeigt werden.

(2) Die Bewertung der hinreichenden Dissimilarität kann auch die Zulässigkeit der Gleichheit einzelner Aspekte ergeben.

(18) Diversitäre leittechnische Einrichtungen

Vorhandensein von zwei oder mehr funktionsbereiten Einrichtungen zur Erfüllung der vorgesehenen Funktion, die physikalisch oder technisch verschiedenartig ausgelegt sind.

(19) Einzelantriebssteuerung

Die Einzelantriebssteuerung ist die einem einzelnen Antrieb zugeordnete Steuereinrichtung.

Hinweis:

In dieser Regel werden die Anforderungen an Einzelantriebssteuerungen von A- und B-Funktions-Einrichtungen behandelt (einschließlich Koppelrelais). Die Anforderungen an die anschließenden Steuerstromkreise werden in KTA 3705 behandelt.

(20) Fehlauslösung

Die Fehlauslösung ist die Auslösung eines Signals, die aufgrund des Anlagenzustands nicht gerechtfertigt war.

(21) Firmware

In ein Gerät fest eingebaute Software (embedded Software), die nicht frei programmierbar ist und definierte gerätespezifische Funktionen erbringt. Wird die Firmware modifiziert, handelt es sich um ein modifiziertes Gerät.

(22) Folgeausfall

Der Folgeausfall ist der von einem Störfall oder einem versagensauslösenden Ereignis verursachte nachfolgende Ausfall.

(23) Funktionsgruppensteuerung

Die Funktionsgruppensteuerung ist eine automatische Steuereinrichtung von funktionell zusammengehörigen Teilabschnitten eines bestimmten Prozesses, bei dem die Antriebe mit ihren Einzelantriebssteuerungen zum Ablauf dieses Prozesses gemeinsam erforderlich sind.

Hinweis:

Dieser Begriff wurde in der Fassung 1985-04 verwendet. Durch die neu eingeführte Kategorisierung nach 2.2 wird dieser Begriff in der vorliegenden Fassung obsolet. Zum besseren Verständnis wird er in diesem Abschnitt weitergeführt.

(24) Gefahrenmeldung der Klasse S

Die Gefahrenmeldung der Klasse S (Sicherheitsgefahrenmeldung) ist eine Meldung eines Schutzuntersystems, bei deren Auftreten dem zuständigen Betriebspersonal zwingend vorgeschrieben ist, eine Schutzaktion in einem vorgegebenen Zeitraum einzuleiten.

(25) Gefahrenmeldung der Klasse I

Die Gefahrenmeldung der Klasse I ist eine Meldung, die das Betriebspersonal auf eine Störung im Sicherheitssystem hinweist.

(26) Gefahrenmeldung der Klasse II

Die Gefahrenmeldungen der Klasse II umfassen alle Meldungen, die das Betriebspersonal auf Störungen hinweisen und die nicht zu den Gefahrenmeldungen der Klasse S und Klasse I gehören.

(27) Gerät / Baugruppe

Anordnung von Komponenten/Bauelementen, durch die eine bestimmte Funktion ausgeführt wird.

Hinweis:

Geräte bestehen aus Hardware und ggf. Software. Eine leittechnische Baugruppe ist ein austauschbares Gerät mit standardisierter Schnittstelle.

(28) Gerät, nichtprogrammierbar

Gerät bestehend aus diskreten, nichtprogrammierbaren Bauelementen.

(29) Gerät, programmierbar

Gerät bestehend aus mindestens einem programmierbaren Bauelement.

Hinweise:

Zu den programmierbaren Bauelementen zählen z. B. FPGA's, PLD's und ASIC's.

(30) Gerät, rechnerbasiert

Gerät bestehend aus mindestens einem Prozessor.

Hinweis:

Die Gerätfunktion ist im Speicher hinterlegt.

(31) Grenzbelastungsprüfung

Die Grenzbelastungsprüfung ist eine Prüfung, bei der das Verhalten des Geräts bei der ungünstigsten Kombination der Betriebs- und Umgebungsbedingungen, für die das Gerät ausgelegt ist, ermittelt wird.

(32) Grenzsignalgeber

Der Grenzsignalgeber ist eine Einrichtung, die den Wert einer Sicherheitsvariablen mit einem festen oder variablen Grenzwert vergleicht. Wird der Grenzwert über- oder unterschritten, ändert sich das Ausgangssignal sprunghaft.

(33) Grenzwert des Grenzsignalgebers

Der Grenzwert des Grenzsignalgebers ist der in einem Grenzsignalgeber eingestellte Wert.

(34) Inspektion

Inspektionen sind Maßnahmen zur Feststellung und Beurteilung des Ist-Zustandes von Einrichtungen. (s. a. DIN 31051)

(35) Instandhaltung

Die Instandhaltung ist die Gesamtheit der Maßnahmen zur Bewahrung und Wiederherstellung des Soll-Zustandes sowie zur Feststellung und Beurteilung des Ist-Zustandes. Die Instandhaltung gliedert sich in die vorbeugende Instandhaltung mit den zugehörigen Elementen, Inspektionen (insbesondere Wiederkehrende Prüfungen) und Wartung, sowie Instandsetzung (Austausch und Reparatur).

(36) Komponente

Eine Komponente ist ein nach baulichen oder funktionellen Gesichtspunkten abgegrenzter Teil eines Systems, der noch selbstständige Teilfunktionen erfüllt.

(37) Leittechnik

Gesamtheit der leittechnischen Einrichtungen zum Ausführen von Leittechnik-Funktionen.

(38) Leittechnische Einrichtungen

Leittechnische Einrichtungen sind Geräte und Systeme zur Ausführung von Leittechnik-Funktionen vom Messwertgeber bis zu den den Einzelantrieben zugeordneten Teilen der Steuerung zur Auslösung von Schutzaktionen. Leittechnische Einrichtungen umfassen sowohl automatische Einrichtungen als auch die Einrichtungen zur Prozessführung durch einen Operator.

(39) Leittechnik-Funktion

Funktion zum Messen, Steuern, Regeln, Überwachen, Aufzeichnen und Schützen eines Prozesses oder einer Einrichtung.

(40) Logikebene

Die Logikebene ist der Teil der A-Funktions-Einrichtungen, in dem die Verknüpfung der Anregesignale und die Wertung der Anregekriterien vorgenommen werden.

(41) Logische Verknüpfung

Die logische Verknüpfung ist ein Verfahren, mehrere binäre Signale zu einer Aussage zu verbinden.

Hinweis:

Logische Verknüpfungen sind z. B. UND, ODER.

(42) Logische Wertung

Die logische Wertung ist ein Verfahren, redundante Signale so miteinander zu verknüpfen, dass eine Aussage erreicht wird, die zuverlässiger ist als die des einzelnen Signals.

Hinweis:

Eine logische Wertung ist z. B. eine 2 von 3-Wertung.

(43) Phasenmodell

In einem Phasenmodell erfolgen die Definition und Strukturierung der aufeinander folgenden Abschnitte eines Entwicklungsprozesses mit Darstellung der Zusammenhänge zwischen den Abschnitten (Phasen), einschließlich Verifikation und Validierung.

(44) Prozessvariable

Die Prozessvariable ist eine unmittelbar im Prozess messbare chemische oder physikalische Größe.

(45) Reaktorschutzsystem

Das Reaktorschutzsystem ist der Teil des Sicherheitssystems, welcher die für die Sicherheit wesentlichen Prozessvariablen zur Verhinderung von unzulässigen Einwirkungen und zur Erfassung von Störfällen überwacht, verarbeitet und Schutzaktionen auslöst, um den Zustand der Reaktoranlage in sicheren Grenzen zu halten. Das Reaktorschutzsystem umfasst als Teil des Sicherheitssystems alle Einrichtungen der Messwerterfassung, der Signalaufbereitung, der Logikebene und die den Einzelantrieben zugeordneten Teile der Steuerung zur Auslösung von Schutzaktionen. Die Leittechnik-Funktionen des Reaktorschutzsystems sind typischerweise der Kategorie A zugeordnet.

Hinweis:

Die Festlegungen der Anzahl und der Art der vom Reaktorschutzsystem zu erfassenden Prozessvariablen und der daraus zu bildenden Sicherheitsvariablen, die Festlegung ihrer Grenzwerte sowie die Festlegung der Anzahl und der Art der Schutzaktionen erfolgen aufgrund der Störfallanalyse.

(46) Rechenschaltung

Die Rechenschaltung ist eine Einrichtung, mit deren Hilfe aus den Werten einer oder mehrerer Prozessvariablen eine nicht unmittelbar messbare Sicherheitsvariable ermittelt wird.

Hinweis:

Eine Rechenschaltung ist z. B. die Schaltung zur Bestimmung der Reaktorperiode aus der Neutronenflussdichte oder des Siedeabstandes aus Druck und Temperatur.

(47) Redundanz

Die Redundanz ist das Vorhandensein von mehr funktionsbereiten Einrichtungen, als zur Erfüllung der vorgesehenen Funktion notwendig ist.

Hinweis:

In dieser Regel wird die Forderung nach Redundanz als erfüllt angesehen, wenn gleichartige Einrichtungen eingesetzt werden.

(48) Redundanzgruppe

Die Redundanzgruppe ist eine Zusammenfassung von Einrichtungen mit der Zuordnung zu einer Redundanz unter Wahrung einer ausreichenden Unabhängigkeit zueinander redundanter Einrichtungen.

(49) Rückwirkungsfreiheit

Die Rückwirkungsfreiheit eines Geräts ist dessen Eigenschaft, das Eingangssignal des Geräts bei Störungen am Ausgang nicht unzulässig zu beeinflussen.

Hinweis:

(1) Störungen können zum Beispiel Kurzschluss, Überspannung, Erdschluss, Unterbrechung sein.

(2) Eine nicht unzulässige Beeinflussung bedeutet, dass trotz einer möglicherweise vorliegenden Rückwirkung die geforderte Aufgabe weiterhin erfüllt wird.

(50) Schutzaktion

Eine Schutzaktion ist die Betätigung oder der Betrieb von aktiven Sicherheitseinrichtungen, die zur Beherrschung von Störfällen erforderlich sind.

(51) Schutzaktion, eindeutig sicherheitsgerichtete

Die eindeutig sicherheitsgerichtete Schutzaktion ist eine Schutzaktion, die bei Auslösung keine andere Schutzaktion verhindern kann und immer in einen verfahrenstechnisch sicheren Zustand führt.

Hinweis:

Eine Reaktorschnellabschaltung ist in diesem Sinne eine eindeutig sicherheitsgerichtete Schutzaktion.

(52) Schutzaktion, nicht eindeutig sicherheitsgerichtete

Die nicht eindeutig sicherheitsgerichtete Schutzaktion ist eine Schutzaktion, die bei Auslösung andere Schutzaktionen verhindern kann oder abhängig vom Anlagenzustand nicht immer in einen verfahrenstechnisch sicheren Zustand führt.

(53) Schutzbegrenzung

Die Schutzbegrenzung ist eine Einrichtung zur Auslösung von solchen Schutzaktionen, die überwachte Sicherheitsvariablen auf einen Wert zurückführen, bei dem eine Fortführung des bestimmungsgemäßen Betriebs zulässig ist.

Hinweis:

Dieser Begriff wurde in der Fassung 1985-04 verwendet. Durch die neu eingeführte Kategorisierung nach 2.2 wird dieser Begriff in der vorliegenden Fassung obsolet. Zum besseren Verständnis wird er in diesem Abschnitt weitergeführt.

(54) Schutzteilaktion

Die Schutzteilaktion ist die Betätigung oder der Betrieb von einer oder mehreren zueinander redundanten Komponenten einer aktiven Sicherheitsteileinrichtung, die zur Beeinflussung von Störfallabläufen und zur Minderung von Schadensauswirkungen erforderlich sind.

(55) Schutzteilsystem

Das Schutzteilsystem ist der Teil der A-Funktions-Einrichtungen, der zur Auslösung einer Schutzteilaktion benötigt wird.

Hinweis:

Ein Schutzteilsystem ist z. B. der Teil der A-Funktions-Einrichtungen, der zum Einschalten einer von mehreren zueinander redundanten Pumpen benötigt wird.

(56) Schutzüberbrückung

Die Schutzüberbrückung ist die Maßnahme, durch die eine Funktion der A-Funktions-Einrichtungen in Abhängigkeit vom Betriebszustand geändert wird.

Hinweis:

Die Schutzüberbrückungen werden in der Logikebene oder in der Steuerebene vorgenommen. Ein Beispiel für eine Schutzüberbrückung ist die Anfahrüberbrückung (RESA bei nicht zulässigen Neutronenflussmesssignalen im Anfahrbereich).

(57) Schutzuntersystem

Das Schutzuntersystem ist ein Teil der A-Funktions-Einrichtungen, der aufgrund seiner Wirkungsweise eine Einheit bildet.

Hinweis:

Hierzu gehören z. B. Anregeebene, Logikebene, Steuerebene.

(58) Schutzvollaktion

Die Schutzvollaktion ist die Betätigung oder der Betrieb einer aktiven Sicherheitseinrichtung, die für sich allein die erforderliche sicherheitstechnische Aufgabe erfüllt.

Hinweis:

Hierzu gehört z. B. die Reaktorschnellabschaltung.

(59) Selbstüberwachung

Selbstüberwachung ist die Eigenschaft von Komponenten oder Systemen, ihre Ausfälle selbsttätig erkennbar zu machen.

(60) Sicherheitsabstand

Der Sicherheitsabstand ist die Differenz zwischen dem am Grenzsignalgeber eingestellten Auslösewert und dem bei der Störfallanalyse festgelegten Gefährdungsgrenzwert.

(61) Sicherheitseinrichtung, aktive

Die aktive Sicherheitseinrichtung ist eine technische Einrichtung des Sicherheitssystems, die Schutzaktionen ausführt.

Hinweis:

Aktive Sicherheitseinrichtungen sind z. B. Einrichtungen zur Abschaltung des Reaktors, zur Nachwärmeabfuhr, zum Durchdringungsabschluss des Reaktorsicherheitsbehälters. Sicherheitseinrichtungen, die eine Schutzfunktion ohne Stellglieder oder ohne Aggregate ausüben, z. B. Kernkühlmitteleinschluss, Sicherheitsbehälter, Abschirmung, werden als passive Sicherheitseinrichtungen bezeichnet.

(62) Sicherheitssystem

Das Sicherheitssystem ist die Gesamtheit aller Einrichtungen einer Reaktoranlage, die die Aufgabe haben, die Anlage vor unzulässigen Beanspruchungen zu schützen und bei auftretenden Störfällen deren Auswirkungen auf das Betriebspersonal, die Anlage und die Umgebung in vorgegebenen Grenzen zu halten.

(63) Sicherheitsteileinrichtung

Die Sicherheitsteileinrichtung ist der Teil einer Sicherheitseinrichtung, der zur Verwirklichung einer Schutzteilaktion benötigt wird.

(64) Sicherheitsvariable

Die Sicherheitsvariable ist eine aus einer oder mehreren Prozessvariablen gewonnene Größe, deren Wert die Sicherheit der Anlage kennzeichnet und die zur Auslösung von Schutzaktionen benötigt wird.

(65) Steuerebene

Die Steuerebene ist ein Schutzuntersystem, in dem Auslösesignale der Logikebene an die schaltungstechnischen Gegebenheiten der aktiven Sicherheitseinrichtungen angepasst werden.

(66) Störfall

Ein Störfall ist ein Ereignis bzw. Ereignisablauf, dessen Eintreten während der Betriebsdauer der Anlage nicht zu erwarten ist, gegen den die Anlage dennoch so auszulegen ist, dass die Auslegungsgrundsätze, Nachweisziele und Nachweiskriterien für die Sicherheitsebene 3 eingehalten werden und bei dessen Eintreten der Betrieb der Anlage oder die Tätigkeit aus sicherheitstechnischen Gründen nicht fortgeführt werden kann.

(67) Validierung

Validierung ist die Bestätigung durch Prüfung und Nachweis, dass die Anforderungsspezifikation wie vorgesehen erfüllt ist.

(68) Verifikation

Verifikation ist die Bestätigung durch Prüfung und Nachweise, dass die Resultate einer Tätigkeit die Ziele und Anforderungen erfüllen, die für diese Tätigkeit definiert wurden.

Hinweis:

Im Rahmen des Phasenmodells werden die einzelnen Phasen durch die Verifikation abgeschlossen.

(69) Vergleicher

Der Vergleicher ist eine Einrichtung, die die Messwerte zweier Sicherheits- oder Prozessvariablen miteinander vergleicht und bei vorgegebener Abweichung ein Binärsignal ausgibt.

(70) Versagen

Versagen ist die Nicht- oder Fehlfunktion bei Anforderung aktiver Systeme.

Hinweis:

Ursache des Versagens einer Funktion können Ausfälle von Komponenten oder Geräten sein, aber auch latente Fehler, die unter besonderen Randbedingungen wirksam werden.

(71) Vorrangsteuerung

Die Vorrangsteuerung ist eine Steuereinrichtung, die den Vorrang eines Steuersignals vor einem oder mehreren anderen bewirkt.

(72) Wächter

Der Wächter ist eine binäre Messeinrichtung, die aus einer Prozessvariablen ohne Zwischenschaltung eines Grenzsignalgebers eine binäre Information ausgibt.

Hinweis:

Ein Beispiel für einen Wächter ist ein Druckwächter.

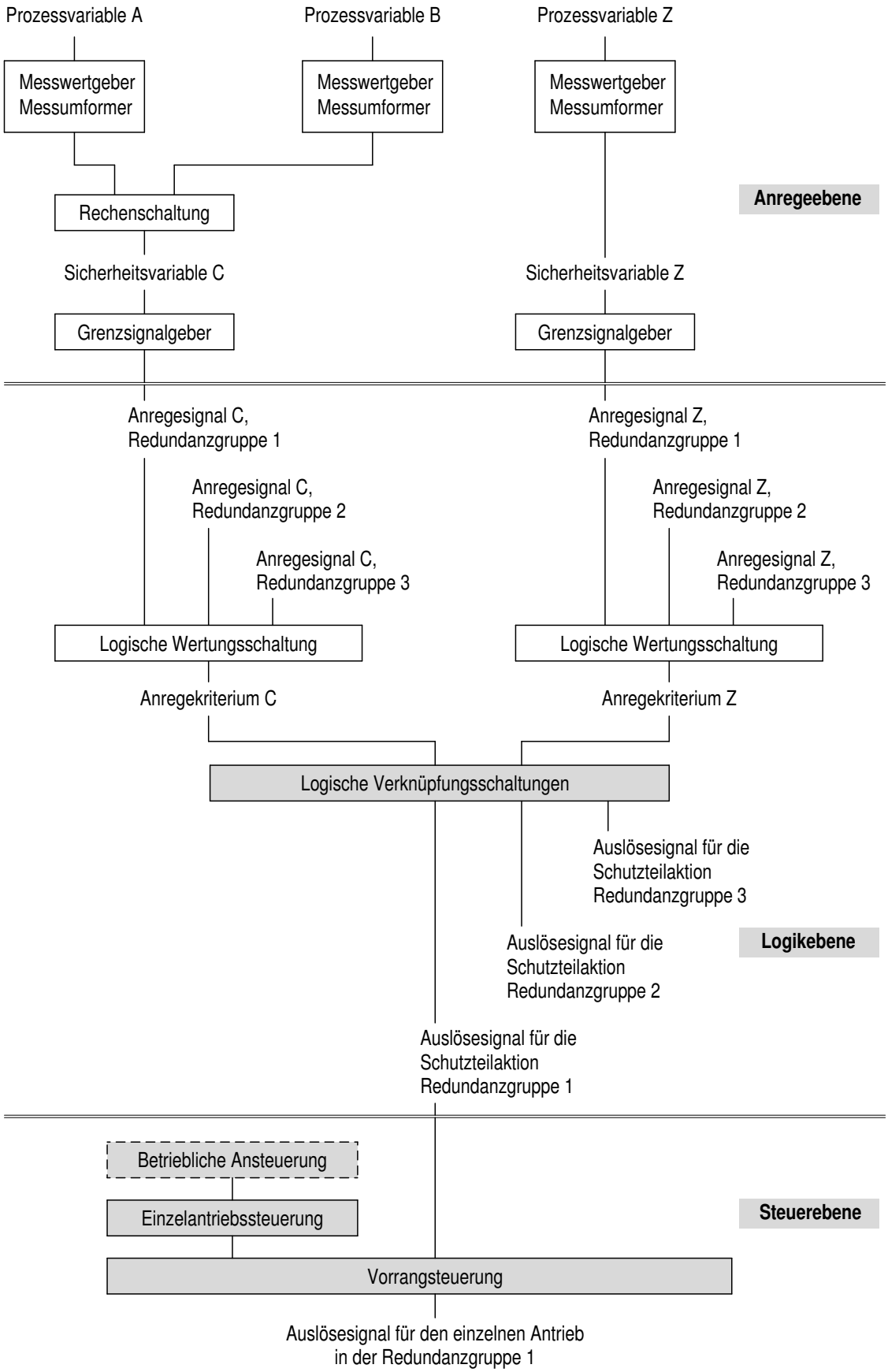

Bild 2-1: Beispielhafte Zuordnung von Begriffen zum funktionellen Aufbau von A-Funktions-Einrichtungen

(73) Werkssachverständiger

Der Werkssachverständige ist ein vom Werk ernannter Fachmann, der von der Fertigung im herstellenden oder verarbeitenden Werk unabhängig ist.

(74) Zufallsausfall

Der Zufallsausfall ist ein Ausfall, dessen Eintreten statistisch unabhängig von Ausfällen anderer gleichartiger Einrichtungen ist.

(75) Zustandsbegrenzungen

Die Zustandsbegrenzung ist eine Einrichtung zur Begrenzung der Werte von Prozessvariablen, um Ausgangszustände für zu berücksichtigende Störfälle einzuhalten.

Hinweise:

(1) Hierunter fällt z. B. die Begrenzung der Reaktorleistung auf einen Wert, der als Ausgangszustand für die Analyse des Kühlmittelverluststörfalls zugrunde gelegt wurde.

(2) Dieser Begriff wurde in der Fassung 1985-04 verwendet. Durch die neu eingeführte Kategorisierung nach 2.2 wird dieser Begriff in der vorliegenden Fassung obsolet. Zum besseren Verständnis wird er in diesem Abschnitt weitergeführt.

2.2 Kategorisierung der Funktionen der Sicherheitsleittechnik

(1) Entsprechend ihrer sicherheitstechnischen Bedeutung müssen Leittechnik-Funktionen, einschließlich Leittechnik-Funktionen der Störfallinstrumentierung, in unterschiedliche Kategorien eingeordnet werden, für die abgestufte Anforderungen gelten.

a) Kategorie A
Die Leittechnik-Funktionen der Kategorie A umfassen alle Funktionen, die erforderlich sind, um Störfälle zu beherrschen.

b) Kategorie B
Die Leittechnik-Funktionen der Kategorie B umfassen alle Funktionen, die erforderlich sind, um anomale Betriebszustände (vgl. SiAnf Anhang 1) zu beherrschen, so dass das Eintreten von Störfällen vermieden wird.

c) Kategorie C
Die Leittechnik-Funktionen der Kategorie C umfassen alle übrigen sicherheitstechnisch wichtigen Funktionen.

(2) Nicht kategorisiert sind Leittechnik-Funktionen, die keine sicherheitstechnisch wichtigen Funktionen ausführen.

3 Ermittlung der Aufgabenstellung

3.1 Grundsätzliche Anforderungen

(1) Zur Ermittlung der Aufgaben, die die A- und B-Funktions-Einrichtungen zu erfüllen haben, ist eine Analyse gemäß der in 3.2 genannten Ereignisabläufe der Anlage vorzunehmen. Die für die Analyse getroffenen Annahmen müssen begründet werden. Das Ergebnis der Analyse muss eine vollständige Auflistung, Kategorisierung und Beschreibung der verfahrenstechnischen Aufgabenstellung der A- und B- Leittechnikfunktionen, einschließlich erforderlicher Handmaßnahmen liefern. Bei dieser Analyse sind auch die Auswirkungen der Fehlauslösungen nach 4.1.3.4 zu beachten.

Hinweis:

Durch technische Maßnahmen außerhalb der A-Funktions-Einrichtungen kann die Eintrittswahrscheinlichkeit bestimmter Ereignisabläufe so weit herabgesetzt werden, dass sie zur Auslegung der A-Funktions-Einrichtungen und der aktiven Sicherheitseinrichtungen nicht herangezogen werden müssen.

(2) Die leittechnischen Funktionen, (z. B. basierend auf Prozessvariablen, Sicherheitsvariablen, Algorithmen, Grenzwerten, Kennlinien, Zeitverhalten) sind durch Analysen zu ermitteln, bei denen betrieblich bedingte Anlagentransienten, die Dynamik der Ereignisabläufe, die Messfehler und die Ansprechverzögerung der A- und B-Funktions-Einrichtungen und der zugeordneten Systeme zu betrachten sind.

(3) Durch die verfahrenstechnische Auslegung der Reaktoranlage sollen nicht eindeutig sicherheitsgerichtete Schutzaktionen bei A-Funktions-Einrichtungen vermieden werden. Erforderliche nicht eindeutig sicherheitsgerichtete Schutzaktionen sind zu begründen.

(4) Die den leittechnischen Funktionen der Kategorie A zugeordneten Sicherheitsabstände sind anzugeben.

3.2 Ereignisabläufe und ihre Auswirkungen

(1) Es sind Ereignisabläufe für den Leistungsbetrieb und Nichtleistungsbetrieb von Kernkraftwerken gemäß SiAnf Anhang 2 Tabelle 5.1 und 5.2 in Betracht zu ziehen

(2) Neben den Ereignisabläufen aus den SiAnf sind auch Störungen in Betracht zu ziehen, die die Funktionstüchtigkeit von aktiven Sicherheitseinrichtungen einschränken oder aufheben.

3.3 Ausgangszustand der Anlage

Als Ausgangszustand der Anlage ist bei den Analysen der Ereignisabläufe vom Normalbetrieb der Anlage auszugehen. Für jeden Ereignisablauf ist bezüglich der Auswirkungen des angenommenen Ereignisses zunächst vom wahrscheinlichsten Betriebszustand der Anlage auszugehen. Zusätzlich sind Analysen für ungünstige Ausgangszustände anzufertigen. Dazu sind bei quasistationären Betriebszuständen aus leittechnischer Sicht toleranzbedingte Abweichungen der Messwerte der Prozessvariablen vom Sollwert sowie Abweichungen der Prozessvariablen infolge eines einzelnen Zufallsausfalls innerhalb der Gesamtheit des Mess-, Steuer- oder Regelsystems zu berücksichtigen.

3.4 Erfassung der Störfälle

(1) Bei der Analyse der Ereignisabläufe müssen für die Störfallerfassung repräsentative Sicherheitsvariablen ausgewählt werden.

(2) Für jeden von den A-Funktionen zu beherrschenden Störfall sollen mindestens zwei physikalisch unterschiedliche Anregekriterien herangezogen werden. Für jedes Anregekriterium ist eine eigene Analyse der Ereignisabläufe nach 3.1 durchzuführen.

Hinweis:

Dies dient zur Abdeckung von Unsicherheiten bei der Analyse des Störfallablaufs und zur Beherrschung von Ausfällen mit gemeinsamer Ursache in der Messwerterfassung.

(3) Ist die Forderung nach (2) nicht oder technisch nicht sinnvoll zu erfüllen, so müssen bei der Messwerterfassung der Einsatz unterschiedlicher Messverfahren, unterschiedlicher Messgeräte in den entsprechenden Anregekanalgruppen sowie Fehlerselbsterkennung, verkürzte Prüfzyklen oder gleichwertige Maßnahmen vorgesehen werden.

(4) Der Ablauf der Schutzaktionen ist einschließlich der Ansprechverzögerung und der Genauigkeit der Anregekanäle für das erste und zweite Anregekriterium zu analysieren und die Auswirkungen auf den Ablauf der Störfälle sind aufzuzeigen.

(5) Bei Verwendung gemeinsamer Prozessvariablen für A-Funktions-Einrichtungen und Einrichtungen mit sicherheitstechnisch geringerer Bedeutung sind Analysen für Störungen in der Messwerterfassung unter Berücksichtigung von (1) und (2) durchzuführen.

Hinweis:

Bei diesen Analysen wird betrachtet, dass als Folge eines systematischen Ausfalls alle gleichartigen Geräte eines Fabrikats in den Signalkanälen gleichzeitig und mit gleichem Ausfallverhalten versagen.

(6) Auf diese Analysen darf verzichtet werden, wenn bei Einsatz diversitärer Messeinrichtungen für die Steuerung und Regelung einerseits und den A-Funktions-Einrichtungen andererseits ein systematischer Ausfall dieser Messeinrichtungen nicht unterstellt werden muss.

4 Auslegungsgrundlagen

4.1 Auslegungsanforderungen an A-Funktions-Einrichtungen

4.1.1 Grundsätzliche Anforderungen

(1) Es ist nachzuweisen, dass A-Funktions-Einrichtungen im Zusammenwirken mit aktiven und passiven Sicherheitseinrichtungen so ausgelegt, ausgeführt und betrieben werden, dass nichttolerierbare Auswirkungen der Störfälle und von Einwirkungen von innen und außen verhindert werden.

(2) Dabei sind zusätzlich zum Störfall die unter 4.1.2.1 und 4.1.2.2 beschriebenen versagensauslösenden Ereignisse, die sich entweder als Zufallsausfall oder als systematischer Ausfall auswirken zu unterstellen.
Sollte ein versagensauslösendes Ereignis aus 4.1.2.1 oder 4.1.2.2 einen Störfall auslösen (abhängiger Störfall), so muss kein weiterer Störfall unterstellt werden. Dann muss jedoch ein zusätzliches versagensauslösendes Ereignis entweder als Zufallsausfall oder als systematischer Ausfall unterstellt werden.

(3) Aus diesen versagensauslösenden Ereignissen resultierende Ausfälle sind nach 4.1.3 zu kombinieren, sofern sie nicht durch technische Maßnahmen ausgeschlossen werden können.

Hinweise:

(1) Dieser Nachweis kann für die Gesamtheit aller Komponenten des Sicherheitssystems gemeinsam erbracht werden.

(2) Wenn hinsichtlich systematischer Ausfälle aufgrund potenziell übergreifender Einwirkungen wie z.B. Brand oder Wassereinbruch durch geeignete Maßnahmen sichergestellt ist, dass der Auswirkungsbereich hinreichend begrenzt bleibt (siehe auch 5.1.5), bezieht sich der unterstellte systematische Ausfall auf diesen begrenzten Auswirkungsbereich.

(3) Anforderungen zum Brandschutz sind in KTA 2101.1 geregelt.

4.1.2 Versagensauslösende Ereignisse

4.1.2.1 Versagensauslösende Ereignisse innerhalb der A-Funktions-Einrichtungen

Es sind versagensauslösende Ereignisse innerhalb der A-Funktions-Einrichtungen in Betracht zu ziehen, wie z. B.:

a) Ausfälle durch Kurzschlüsse, Unterbrechungen, Störungen im Programmablauf oder der Datenübertragung, Erdschlüsse, Spannungs- und Frequenzänderungen, Beeinflussung durch leitungs- und feldgebundene elektromagnetische Störgrößen, mechanisches Versagen oder Brände
b) mehrere gleichzeitig oder kurzzeitig aufeinanderfolgende Ausfälle nach a), die eine gemeinsame Ursache (z. B. Fertigungsfehler, Auslegungsfehler, Drift) im System selbst haben, und
c) Fehler bei Bedienung, Prüfung, Wartung und Instandsetzung der A-Funktions-Einrichtungen durch das Personal.

4.1.2.2 Versagensauslösende Ereignisse innerhalb der Reaktoranlage

Es sind versagensauslösende Ereignisse innerhalb der Reaktoranlage im Rahmen des "Einzelfehlerkonzepts" in Betracht zu ziehen.

Hinweis:

Siehe Sicherheitsanforderungen für Kernkraftwerke, Anhang 4: „Grundsätze für die Anwendung des Einzelfehlerkriteriums und für die Instandhaltung“. Beispiele für versagensauslösende Ereignisse innerhalb der Reaktoranlage sind: Elektromagnetische feld- und leitungsgebundene Beeinflussung, Brand, Wassereinbruch, schlagende Rohrleitung, Bruchstücke einer versagenden Komponente, mechanische Strahlwirkung von Medien wie Dampf, Wasser, Gas und Öl.

4.1.2.3 Auslegung gegen versagensauslösende Ereignisse außerhalb der Reaktoranlage

Gegen Ereignisse durch Einwirkungen von außen wie Brand, Netzstörungen, Überflutung, Blitz, Sturm und induzierte Erschütterungen sind ausreichende Vorsorgemaßnahmen gemäß SiAnf Abschnitt 2.4 „Schutzkonzept gegen Einwirkungen von innen und außen sowie gegen Notstandsfälle“ nachzuweisen, so dass durch diese Ereignisse die Funktion der A-Funktions-Einrichtungen nicht unzulässig beeinträchtigt wird.

4.1.3 Ausfallkombinationen

4.1.3.1 Grundannahmen

(1) Folgende Ausfälle sind zu betrachten:

a) Zufallsausfall Z,
b) Systematischer Ausfall S,
c) Folgeausfälle F,
d) Instandhaltungsfall (Inspektion, Wartung, Instandsetzung) I.

(2) Es ist nachzuweisen, dass die Gesamtheit der A-Funktions-Einrichtungen im Zusammenwirken mit aktiven und passiven Sicherheitseinrichtungen zusätzlich zum Störfall

a) einen Zufallsausfall, Z,
b) und einen systematischen Ausfall (soweit er nicht nach (6) ausgeschlossen werden kann) S,
c) und Folgeausfälle F

beherrscht.

Hinweis:

Ein Zufallsausfall oder systematischer Ausfall kann durch die in 4.1.2.1 und 4.1.2.2 genannten versagensauslösenden Ereignisse verursacht werden.

(3) Während des bestimmungsgemäßen Betriebs der Reaktoranlage ist die Ausfallkombination nach Bild 4-1 bezüglich eintretender Störfälle zu beherrschen, wobei während eines Instandhaltungsfalls (I) innerhalb einer Zeitspanne von 100 h das gleichzeitige Auftreten des systematischen Ausfalls (S) und des Zufallsausfalls (Z) nicht unterstellt werden muss. Der Instandsetzungsfall beginnt mit der Erkennung des Ausfalls

(4) Sind Leittechnikeinrichtungen redundanter verfahrenstechnischer Komponenten redundanzweise mit unterschiedlichen Gerätesystemen ausgelegt, muss nicht angenommen werden, dass der Zufallsausfall (Z) und der systematische Ausfall (S) gleichzeitig auftreten, wenn folgende Voraussetzungen erfüllt werden:

a) hoher Selbstüberwachungsgrad für Ausfälle,
b) Einhaltung kurzer Instandsetzungszeiten.

Hinweis:

Absatz (4) gilt z. B. für eine 4x50%-Auslegung verfahrenstechnischer Redundanzen mit paarweise unterschiedlichen Gerätesystemen. Bei Auftreten eines systematischen Ausfalls erfüllen die verbleibenden Redundanzen die verfahrenstechnische Aufgabe.

5) Der Zufallsausfall und der Instandhaltungsfall sind in der Gesamtheit der Komponenten des Sicherheitssystems, die zur Beherrschung eines Störfalls notwendig sind, nur einmal anzunehmen.

(6) Bei der Auslegung von A-Funktions-Einrichtungen sind die Potenziale für und die Auswirkungen von systematischem

Versagen der leittechnischen Einrichtungen auf die Störfallabläufe unter Berücksichtigung der verfahrenstechnischen Vorgaben zu analysieren. Es sind Vorkehrungen gegen systematisches Versagen zur Minderung von dessen Eintrittswahrscheinlichkeit derart zu treffen, dass es zum Nachweis der Störfallbeherrschung nicht mehr unterstellt werden muss.

(7) Kann für leittechnische Einrichtungen eine Nachweisführung nach (6) nach dem Stand von Wissenschaft und Technik nicht erfolgen, sind Vorkehrungen derart zu treffen, dass ein systematisches Versagen von Hardware und Software der A-Funktions-Einrichtungen durch diversitäre oder dissimilare leittechnische Einrichtungen mit gleichen Qualitätsanforderungen beherrscht wird. Diversitätsgrad und Struktur sind dabei derart zu wählen, dass das systematische Versagen mit den damit verbundenen Auswirkungen die Störfallbeherrschung durch die verbleibenden diversitären Einrichtungen nicht unzulässig beeinflusst.

Hinweis:

In festverdrahteten Systemen kann die Eintrittswahrscheinlichkeit systematischer Ausfälle zum Beispiel durch die Auswahl geeigneter Gerätesysteme, Prüfzyklen, Grenzbelastungsprüfungen so weit herabgesetzt werden, dass die systematischen Ausfälle in der Ausfallkombination nach (2) nicht mehr betrachtet zu werden brauchen.

(8) Für rechnerbasierte und programmierbare A-Funktions-Einrichtungen sind fehlervermeidende und fehlerbeherrschende Maßnahmen vorzusehen. Dies beinhaltet insbesondere geeignete Systemeigenschaften und eine geeignete Systemauslegung.

Hinweise:

(1) Fehlervermeidende Maßnahmen für rechnerbasierte A-Funktions-Einrichtungen sind z. B.:

a) Es wird keine absolute Uhrzeit geführt (wirkt auch fehlerbeherrschend).
b) Die rechnerbezogene Bearbeitung der Anwenderfunktionen und die Datenübertragung erfolgt in festen Zeitzyklen (wirkt auch fehlerbeherrschend).
c) Bei der Datenübertragung per Datenbus werden alle Daten zyklisch übertragen, unabhängig davon ob sie sich geändert haben (Datenpolling, wirkt auch fehlerbeherrschend).
d) Alle Rechner und Datenbusse im Auslösepfad haben keine direkten Datenbusverbindungen nach außen. (Sie haben lediglich indirekte Datenbusverbindungen nach außen über einen Schnittstellenrechner, der eine leittechnische Einrichtung der Kategorie A ist.)
e) Alle Rechner im Auslösepfad sind mit einem Rechner (Schnittstellenrechner) in der gleichen leittechnischen Redundanz verbunden, der die Datenverbindung nach außen ermöglicht. Mit „außen“ sind damit Wartungsrechner, Prozessrechneranlage des Kraftwerks und gegebenenfalls weitere funktionsbezogene Rechner gemeint.
f) Die Programmierung von Rechnern im Auslösepfad ist im Betriebsmodus nicht möglich. Das Verlassen des Betriebsmodus wird gemeldet.
g) Der Funktionsumfang der A-Funktions-Einrichtungen wird auf die notwendigen Aufgaben beschränkt.

(2) Fehlerbeherrschende Maßnahmen für rechnerbasierte A-Funktions-Einrichtungen sind z. B.:

a) Die Aufteilung der Leittechnikfunktionen auf eigenständige und voneinander unabhängige Teilsysteme,
b) der Einsatz diversitärer oder dissimilarer leittechnischer Einrichtungen für die Beherrschung von systematischen Fehlern und
c) der Einsatz unabhängiger, diversitärer Leittechnikfunktionen speziell für die Beherrschung von Fehlern in der verfahrenstechnischen Aufgabenstellung.

4.1.3.2 Schutzvollaktion

Die Auslösung der Schutzvollaktion muss bei den Grundannahmen nach 4.1.3.1 sichergestellt sein.

Hinweis:

Beispiele, die diese Forderungen erfüllen zeigen die **Bilder 4-2** bis **4-7**. **Bild 4-2** zeigt den ungestörten Betrieb, die **Bilder 4-3** bis **4-7** verschiedene Ausfallkombinationen. Es wird nur von Ausfällen ausgegangen, die die Sicherheit beeinträchtigen.

Unter Schutzvollaktionen werden nur eindeutig sicherheitsgerichtete Schutzvollaktionen verstanden, z. B. die Reaktorschnellabschaltung.

4.1.3.3 Schutzteilaktionen

4.1.3.3.1 Eindeutig sicherheitsgerichtete Schutzteilaktionen

Die Auslösung der eindeutig sicherheitsgerichteten Schutzteilaktionen muss bei den Grundannahmen nach 4.1.3.1 so sichergestellt sein, dass die aufgrund der angenommenen Ausfallkombinationen verbleibenden Schutzteilaktionen die erforderliche sicherheitstechnische Aufgabe erfüllen.

Hinweis:

Beispiele, die diese Forderungen erfüllen, zeigen die **Bilder 4-8** bis **4-9**. Es wird nur von Ausfällen ausgegangen, welche die Sicherheit beeinträchtigen.

4.1.3.3.2 Nicht eindeutig sicherheitsgerichtete Schutzteilaktionen

Hinweis:

Unter den hier betrachteten Schutzteilaktionen werden solche verstanden, die bei Fehlauslösung andere Schutzaktionen verhindern können.

(1) Die Auslösung der nicht eindeutig sicherheitsgerichteten Schutzteilaktionen muss bei den Grundannahmen nach 4.1.3.1 so sichergestellt sein, dass die aufgrund der angenommenen Ausfallkombinationen verbleibenden Schutzteilaktionen die erforderliche sicherheitstechnische Aufgabe erfüllen.

(2) Bei Fehlauslösung nicht eindeutig sicherheitsgerichteter Schutzteilaktionen durch einen Zufallsausfall, muss auch während einer Instandhaltungsarbeit im Sicherheitssystem sichergestellt sein, dass durch die verbleibenden Schutzaktionen die erforderlichen sicherheitstechnischen Aufgaben des Sicherheitssystems erfüllt werden.

(3) Bezüglich der Fehlauslösungen nicht eindeutig sicherheitsgerichteter Schutzteilaktionen durch systematische Ausfälle sind die Forderungen von 4.1.3.1 (6) anzuwenden.

Hinweis:

Bei der Auslegung dieses Teils der A-Funktions-Einrichtungen ist auch auf auslösegerichtete Ausfälle zu achten, da Fehlauslösungen die Wirksamkeit des Sicherheitssystems in unzulässiger Weise vermindern können.

4.1.3.4 Fehlauslösungen von Schutzaktionen

Fehlauslösungen von Schutzaktionen sind unter Einhaltung der Grundannahmen nach 4.1.3.1 zu verhindern, wenn sie zu einem Schaden führen können, der über die Auswirkungen der zu betrachtenden Störfälle hinausgeht. Auch während des Instandhaltungsfalls im Sicherheitssystem dürfen durch einen Zufallsausfall in A-Funktions-Einrichtungen einschließlich Folgeausfällen keine Störfälle mit Schadensfolge herbeigeführt werden.

4.1.4 Anregung von Schutzaktionen

4.1.4.1 Festlegung der Sicherheitsvariablen

Eine Sicherheitsvariable soll aus nur einer Prozessvariablen gebildet werden (siehe auch 5.1.7.1.1).

4.1.4.2 Automatisierungsgrad

(1) Die A-Funktions-Einrichtungen sollen Schutzaktionen automatisch auslösen. Handmaßnahmen wie Auslösen,

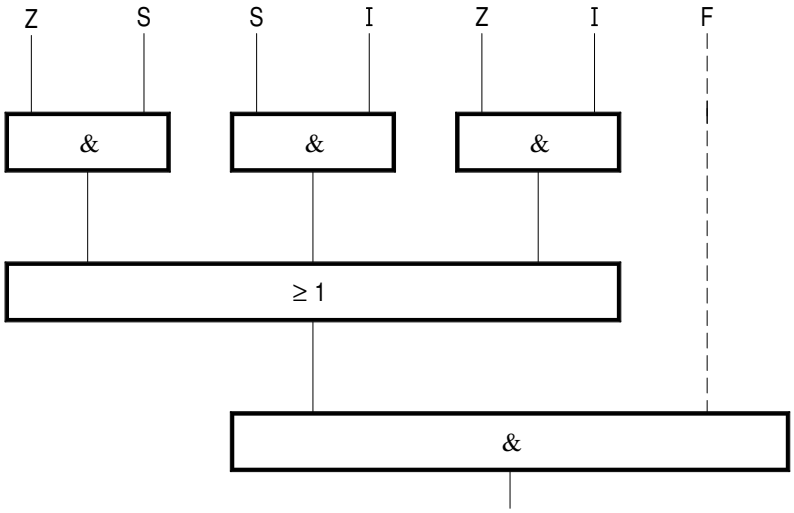

Bild 4-1: Anzuwendende Ausfallkombinationen

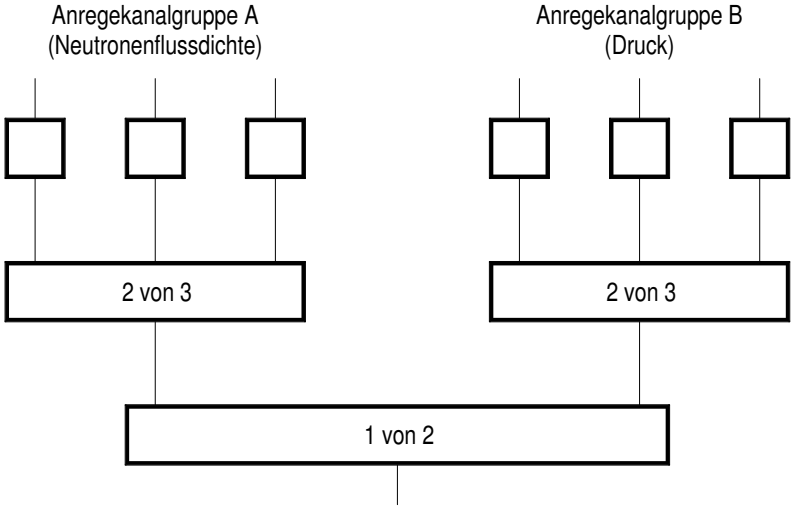

Bild 4-2: Für die Auslösung der Reaktorschnellabschaltung aufgrund von Reaktivitätsstörungen, bei denen zwei aus verschiedenartigen Prozessvariablen, z. B. Neutronenflussdichte und Druck, abgeleitete Auslösekriterien vorhanden sind und Folgefehler im Bereich der Messwerterfassung ausgeschlossen werden können, ist der hier prinzipiell dargestellte Schaltungsaufbau möglich.

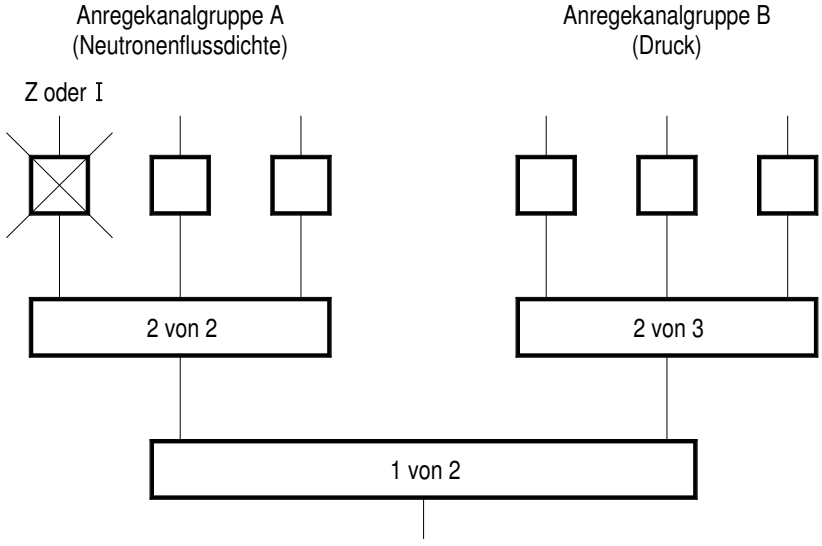

Bild 4-3: Durch Instandsetzung oder Ausfall eines Anregekanals durch einen einzelnen Zufallsausfall ist ein Anregekanal der Anregekanalgruppe A nicht funktionsfähig. Der Störfall wird mindestens durch Anregekanalgruppe A (2 von 2) und Anregekanalgruppe B (2 von 3) erfasst.

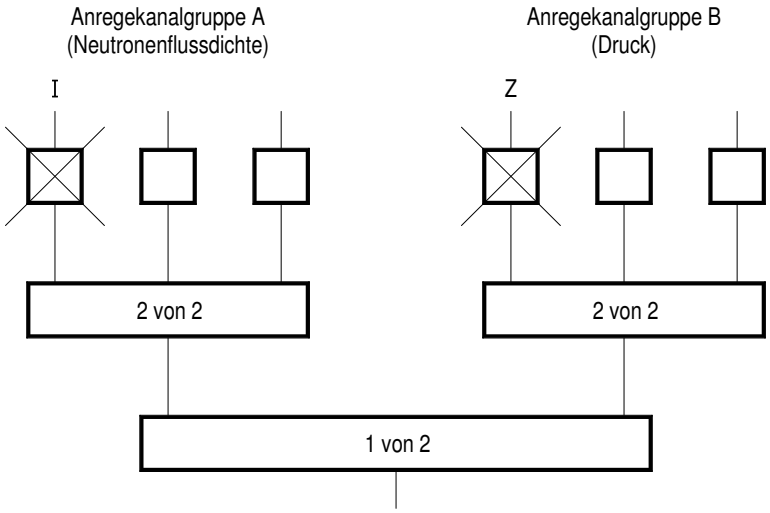

Bild 4-4: Während der Instandsetzung eines Anregekanals in Anregekanalgruppe A tritt ein Zufallsausfall in Anregekanalgruppe B auf. Der Störfall wird durch Anregekanalgruppe A (2 von 2) und Anregekanalgruppe B (2 von 2) erfasst.

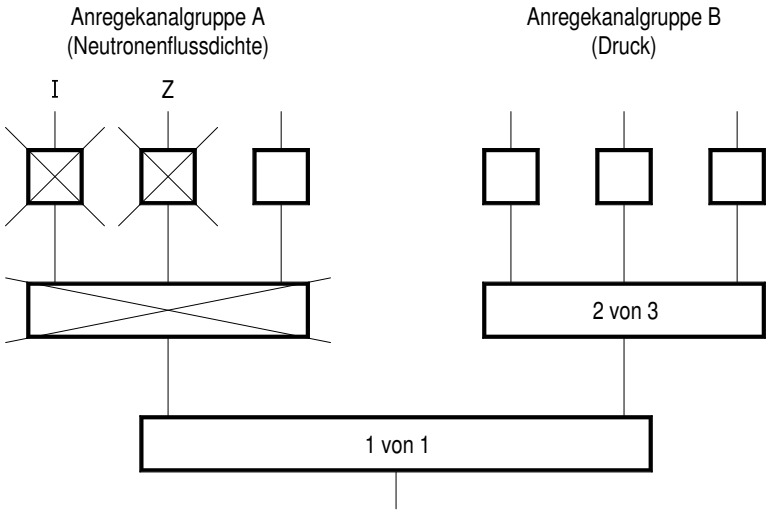

Bild 4-5: Während der Instandsetzung eines Anregekanals in Anregekanalgruppe A tritt ein Zufallsausfall in einem anderen Anregekanal der gleichen Anregekanalgruppe auf. Der Störfall wird durch Anregekanalgruppe B (2 von 3) erfasst.

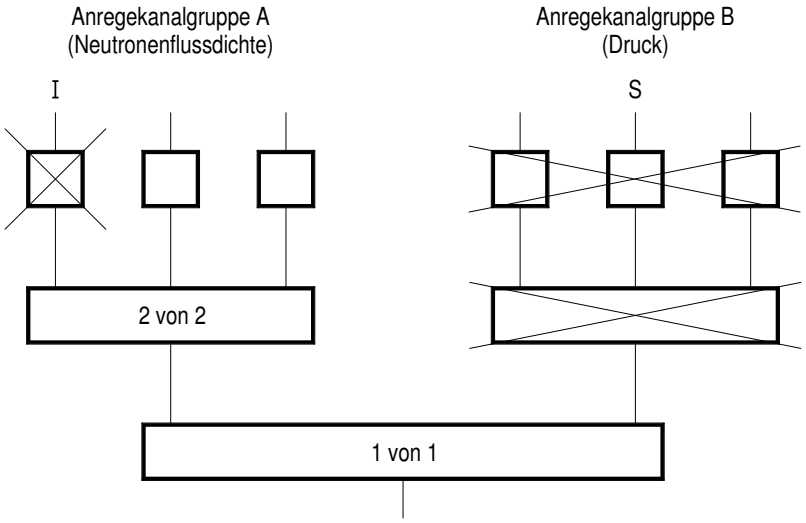

Bild 4-6: Während der Instandsetzung eines Anregekanals in Anregekanalgruppe A tritt ein systematischer Ausfall in Anregekanalgruppe B auf. Der Störfall wird durch Anregekanalgruppe A erfasst.

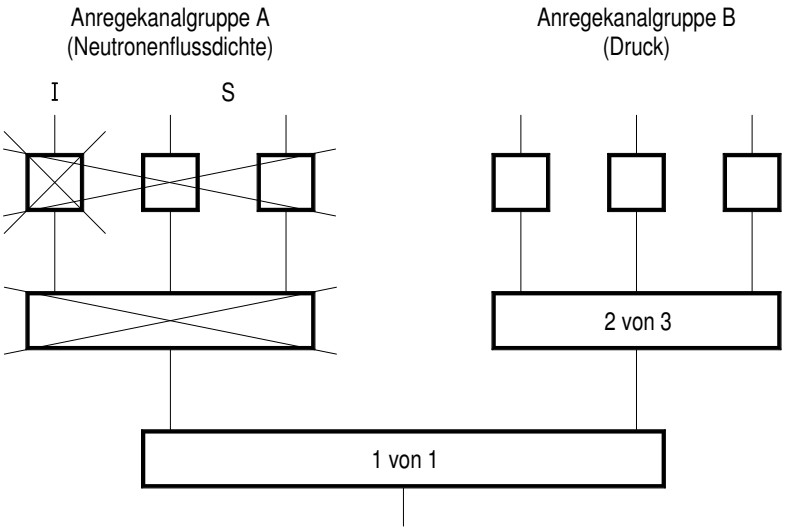

Bild 4-7: Während der Instandsetzung eines Anregekanals in Anregekanalgruppe A tritt ein systematischer Ausfall in der gleichen Anregekanalgruppe auf. Der Störfall wird durch Anregekanalgruppe B erfasst.

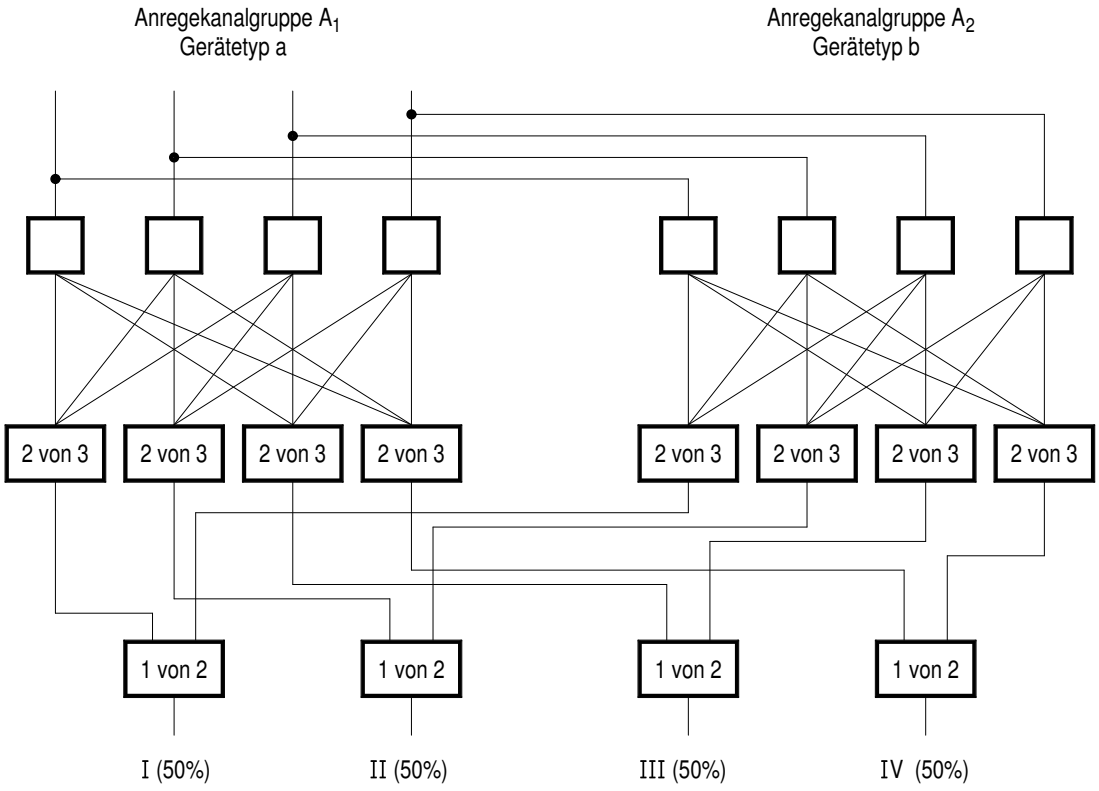

Bild 4-8: Für die Auslösung von 4 zueinander redundanten 50 %-Sicherheitsteileinrichtungen bei einem Störfall, für dessen Erkennung nur eine einzige Sicherheitsvariable vorhanden ist, ist der hier dargestellte prinzipielle Schaltungsaufbau möglich, wenn Folgeausfälle im Bereich der Messwerterfassung (z. B. Bruch einer Wirkdruckleitung) physikalisch möglich und nicht auslösegerichtet zu unterstellen sind. Die Geräte zur Messwerterfassung bis einschließlich Messumformer in den beiden Messkanalgruppen sind diversitär (Gerätetyp a und Gerätetyp b).

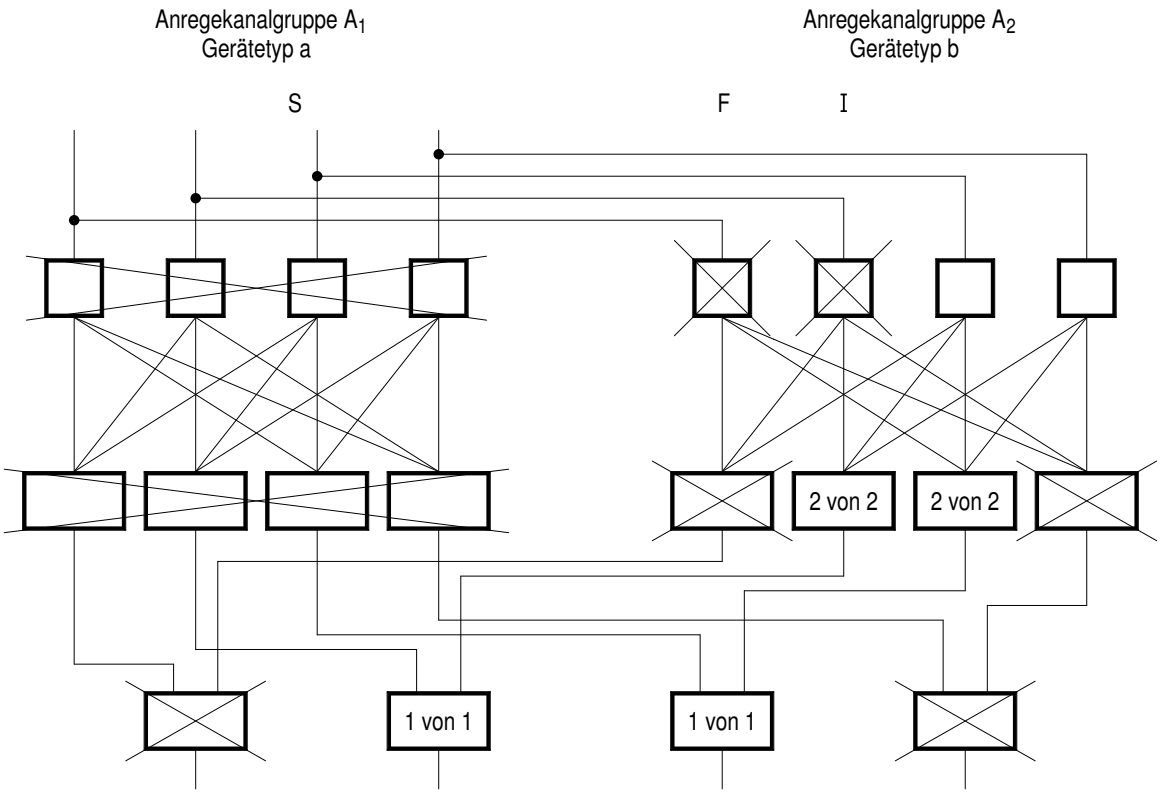

Bild 4-9: Bei ungünstigster Ausfallkombination kann aus dem System nach Bild 4-8 Folgendes entstehen: Während der Instandsetzung eines Anregekanals in Anregekanalgruppe A_1 tritt ein systematischer Geräteausfall im Gerätetyp a auf. Zusätzlich wird ein Anregekanal in der Anregekanalgruppe A_2 aufgrund eines Folgeausfalls funktionsunfähig. Der Störfall wird durch Auslösung von zwei 50%-Systemen ausreichend beherrscht.

Unterbrechen oder Rückstellen von Schutzaktionen sind nur in begründeten Ausnahmefällen vorzusehen. Das Sicherheitssystem ist so auszulegen, dass notwendige von Hand auszulösende Schutzaktionen zur Beherrschung von Störfällen nicht vor Ablauf von 30 Minuten erforderlich werden.

H i n w e i s :

Bei der Auslösung von Schutzaktionen, die zur Beherrschung sehr seltener Ereignisse vorgesehen werden sind begründete Ausnahmen zulässig (z. B. Einwirkungen von außen während des Brennelementwechsels).

(2) Eine Möglichkeit der Auslösung der Reaktorschnellabschaltung von Hand ist vorzusehen. Diese ist unabhängig von rechnerbasierten Einrichtungen auszuführen.

4.1.4.3 Protokollierung

Es sind die Anregesignale der A-Funktions-Einrichtungen und weitere Meldungen aus den aktiven Sicherheitseinrichtungen übersichtlich und in der richtigen zeitlichen Reihenfolge zu dokumentieren. Diese Dokumentation soll in Form einer selbsttätigen Meldungs- und Zeitprotokollierung erfolgen. Das Meldungsprotokoll darf auch andere, einem zugeordneten Störfall nicht betreffende Signale beinhalten, soweit die Übersichtlichkeit nicht beeinträchtigt wird.

4.1.5 Redundanz und Unabhängigkeit

(1) Zur Beherrschung versagensauslösender Ereignisse innerhalb der A-Funktions-Einrichtungen ist ein redundanter Aufbau der A-Funktions-Einrichtungen vorzusehen.

(2) Redundanzgruppen müssen voneinander so unabhängig sein, dass bei Ausfällen innerhalb von Redundanzgruppen durch ein versagensauslösendes Ereignis nach 4.1.2.1 und 4.1.2.2 die verbleibenden Einrichtungen zur Störfallbeherrschung ausreichen.

(3) An Verbindungsstellen zwischen mehreren Redundanzgruppen der A-Funktions-Einrichtungen, wie sie zum Beispiel an Vergleichs-, Wertungs- und Mittelwerteinheiten auftreten, ist die Unabhängigkeit von verschiedenen Redundanzgruppen durch Entkoppelung sicherzustellen. Die Entkoppelungsglieder müssen die Redundanzgruppen gegeneinander rückwirkungsfrei abgrenzen.

(4) Es dürfen nur systemspezifisch geeignete Service- oder Programmiergeräte eingesetzt werden. Sie müssen den Einrichtungen der Kategorie A zugeordnet sein. Es dürfen keine datentechnischen Verbindungen von den Service- oder Programmiergeräten zu anderen rechnerbasierten Systemen bestehen.

(5) Zum Schutz gegen versagensauslösende Ereignisse innerhalb der A-Funktions-Einrichtungen und innerhalb der Reaktoranlage sollen zueinander redundante Komponenten räumlich getrennt angeordnet werden. Räumliche Trennung ist nicht erforderlich, wenn diese Ereignisse die Auslösung von Schutzaktionen nicht verhindern und nur zur Auslösung eindeutig sicherheitsgerichteter Schutzaktionen führen können.

4.1.6 Trennung der A-Funktions-Einrichtungen von anderen Systemen

(1) Komponenten der A-Funktions-Einrichtungen dürfen in begründeten Fällen auch für Aufgaben mit sicherheitstechnisch geringerer Bedeutung eingesetzt werden.

H i n w e i s :

Unter dem Gesichtspunkt der Einfachheit ist es jedoch zweckmäßig, A-Funktions-Einrichtungen möglichst frei von anderen Funktionen zu halten.

(2) Die A-Funktions-Einrichtungen müssen von Einrichtungen mit sicherheitstechnisch geringerer Bedeutung so unabhängig sein, dass bei bestimmungsgemäßem Betrieb und bei versa-

gensauslösenden Ereignissen in Einrichtungen mit sicherheitstechnisch geringerer Bedeutung die Funktion der A-Funktions-Einrichtungen erhalten bleibt.

(3) Verbindungen von A-Funktions-Einrichtungen zu leittechnischen Einrichtungen mit geringerer sicherheitstechnischer Bedeutung sind auf das technisch und betrieblich Notwendige zu minimieren. Werden Signale der A-Funktions-Einrichtungen für die Messwertverarbeitung außerhalb der A-Funktions-Einrichtungen benutzt, zum Beispiel Signale zu Schreibern, Anzeigegeräten, so müssen diese Signale rückwirkungsfrei ausgekoppelt werden.

(4) Bei Verwendung gemeinsamer Messeinrichtungen für Steuerung, Regelung und A-Funktions-Einrichtungen ist der Nachweis zu führen, dass der Ausfall dieser Messeinrichtungen entweder nicht zu Störfällen führt oder dass diese nach 3.4 (1) und (2), 4.1.4.1 und 4.1.4.2 erfasst werden.

(5) Die Ansteuerung von aktiven Sicherheitseinrichtungen durch die A-Funktions-Einrichtungen muss so ausgelegt werden, dass das Signal für die Auslösung der Schutzaktionen Vorrang vor Steuersignalen mit geringerer sicherheitstechnischer Bedeutung hat, soweit dies in Abschnitt 6 nicht anders geregelt ist.

(6) Die A-Funktions-Einrichtungen müssen gegen in Betracht zu ziehende systemfremde Überspannungen ausgelegt oder entkoppelt werden. Es sind die anlagenspezifischen Spannungsebenen und -toleranzen zu berücksichtigen.

4.1.7 Instandhaltung

(1) Wenn bei Instandhaltungsarbeiten an A-Funktions-Einrichtungen der noch wirksame Teil des Sicherheitssystems bei einem zusätzlich unterstellten Zufallsausfall einschließlich Folgeausfällen seine sicherheitstechnische Aufgabe nicht mehr erfüllen kann, ist die Reaktoranlage unverzüglich in einen sicheren Zustand zu überführen.

(2) Das Überführen in einen sicheren Zustand kann z. B. durch unverzügliche Instandsetzung oder Abfahren der Reaktoranlage erfolgen. Einer unverzüglichen Instandsetzung ist dann der Vorzug zu geben, wenn die Instandsetzung schneller abgeschlossen werden kann als das Abfahren.

(3) Die Anforderungen an den Austausch von Hardware- und Softwarekomponenten sind bei der Entwicklung des Gesamtsystems und der Einzelsysteme festzulegen. Hierzu sind Anweisungen zur Durchführung, Prüfung und Dokumentation zu erstellen.

(4) Werden im Rahmen der Instandhaltung bei Betrieb der Reaktoranlage Eingriffe in die A-Funktions-Einrichtungen erforderlich, so sollen sie ohne Eingriff in die Verdrahtung an vorinstallierten und geprüften Eingriffsstellen nach vorgeplanten Anweisungen durchgeführt werden können.

(5) Die Funktionsbereitschaft und die anforderungsgerechte Funktion der A-Funktions-Einrichtungen sind nach abgeschlossener Instandhaltungsmaßnahme durch entsprechende Funktionsprüfungen sicherzustellen.

(6) Für die Instandsetzung müssen vollständige Geräte- und Schaltungsunterlagen vorliegen.

(7) Die Instandhaltungsarbeiten müssen von dem für diese Arbeiten befugten Personal durchgeführt werden.

(8) Zur Instandsetzung dürfen nur typgleiche Ersatzteile eingesetzt werden. Werden neuartige oder geänderte Bausteine eingesetzt, so sind Prüfungen nach 10.1.1.2 und 10.1.1.3 durchzuführen.

(9) Die bei Instandhaltungsarbeiten festgestellten Ausfälle, ihre Ursachen und die Art der Instandsetzung sind zu dokumentieren. Die Betriebserfahrung aus der Instandhaltung der A-Funktions-Einrichtungen muss erfasst, dokumentiert und systematisch ausgewertet werden.

4.1.8 Abstimmung zwischen den A-Funktions-Einrichtungen und den aktiven Sicherheitseinrichtungen

(1) Die A-Funktions-Einrichtungen sind so auszulegen, dass sie die Unverfügbarkeit des Sicherheitssystems nicht bestimmen.

(2) Die A-Funktions-Einrichtungen sind so aufzubauen, dass die in den aktiven Sicherheitseinrichtungen vorgegebene Redundanz gewahrt bleibt. Eine gemeinsame Messwerterfassung zur Ansteuerung redundanter aktiver Sicherheitseinrichtungen ist zulässig, wenn die Forderungen nach 4.1.3 erfüllt werden.

4.1.9 Überwachung auf Funktionsbereitschaft und Prüfbarkeit

4.1.9.1 Überwachung auf Funktionsbereitschaft

(1) Es ist eine Informationsdarstellung vorzusehen, die einen Überblick über den Zustand der Komponenten der A-Funktions-Einrichtungen und der aktiven Sicherheitseinrichtungen einschließlich ihrer Energie- und Hilfsmedienversorgung gibt.

(2) A-Funktions-Einrichtungen sollen selbstüberwachend ausgelegt werden. Für Funktionen und Eigenschaften, die von der Selbstüberwachung nicht erfasst sind, sind Einrichtungen vorzusehen, die eine regelmäßige und überlappende Überprüfung ermöglichen. Diese Prüfungen sollen mit Prüfhilfsmitteln an für diesen Zweck vorgesehenen Schnittstellen leicht durchführbar sein. Prüfeingriffe und Handbetätigungen sind so festzulegen, dass notwendige Sicherheitsfunktionen weder verhindert werden noch die Zuverlässigkeit ihrer Anregung signifikant vermindert wird.

H i n w e i s :

Mittel zur Selbstüberwachung sind z. B. Signalvergleich zwischen redundanten Kanälen, Antivalenzüberwachung, dynamisch arbeitende Systeme, zyklische Speichertests, Überwachung der Datenübertragung.

(3) Erkannte Ausfälle in A-Funktions-Einrichtungen müssen soweit lokalisierbar sein, dass eine Instandsetzung möglich ist.

H i n w e i s :

Mittel zur Lokalisierung sind z. B. optische Meldungen in der Warte, an Schrankreihen, Schränken und Einschüben und Systemfehlermeldungen (siehe Abschnitt 10).

4.1.9.2 Prüfbarkeit der A-Funktions-Einrichtungen

(1) Die A-Funktions-Einrichtungen müssen so ausgelegt sein, dass während des bestimmungsgemäßen Betriebs die zum Nachweis der auslegungsgemäßen Funktion erforderlichen Prüfungen ohne eine unzulässige Minderung der Sicherheit der Anlage durchgeführt werden können. Die Unabhängigkeit von Redundanzgruppen muss bei der Prüfung erhalten bleiben. Eine gleichzeitige Prüfung redundanter Teilsysteme ist zu verhindern, wenn dadurch die Funktionsfähigkeit der A-Funktions-Einrichtungen beeinträchtigt wird. Hierzu sind technische Maßnahmen vorrangig vor administrativen vorzusehen.

(2) Die A-Funktions-Einrichtungen müssen so ausgelegt sein, dass sowohl das Abweichen von den der Auslegung zugrunde gelegten Toleranzwerten der Einzelgeräte und Baugruppen, als auch die einwandfreie Funktion der Schutzuntersysteme und der gesamten A-Funktions-Einrichtungen im Rahmen einer vorbetrieblichen Prüfung und während der Abschaltpause der Anlage überprüft werden können.

H i n w e i s :

Bei der Bewertung der Prüfergebnisse darf die verfahrenstechnisch zulässige Toleranz berücksichtigt werden.

(3) Während des Leistungsbetriebs der Reaktoranlage sollen Prüfungen durchgeführt werden können, die unter Nutzung vorprojektierter Prüfeingriffe und -geräte und ohne Eingriff in die Verdrahtung, die einwandfreie Funktion der Schutzuntersysteme feststellen. Durch die Prüfung der Schutzuntersysteme muss die einwandfreie Funktion der gesamten A-Funktions-Einrichtungen nachgewiesen werden können. Teilprüfungen müssen überlappend durchführbar sein. Der Prüfumfang ist in Abhängigkeit von der Wirksamkeit der Selbstüberwachung festzulegen (vgl. KTA 3506, Abschnitt 3.1 Absatz 2).

Hinweis:

Geeignete Einrichtungen zur Erfüllung dieser Forderung sind z. B. Prüfbuchsen, Testschalter, Anzeigen, die es ermöglichen, simulierte Signale aufzuschalten und den Erfolg der Prüfung festzustellen.

(4) Die A-Funktions-Einrichtungen sollen so ausgelegt und betrieben werden, dass Funktionsprüfungen von dafür vorgesehenen Prüfstellen (z. B. von Prüftafeln oder Servicestationen) durchführbar sind.

Hinweis:

Messumformer und Messwertgeber werden in der Regel dezentral geprüft.

(5) Die Durchführung von Prüfungen an A-Funktions-Einrichtungen soll von zentraler Stelle aus erkennbar sein.

(6) Werden zur Prüfung der Funktionsfähigkeit der A-Funktions-Einrichtungen automatische Prüfeinrichtungen eingesetzt (festverdrahtete oder freiprogrammierbare Prüfeinrichtungen), so gelten die folgenden Bedingungen:

a) Für die Prüfeinrichtung ist die Qualität und Eignung nachzuweisen.
b) Die Prüfeinrichtung ist in einer Konfigurations- und Identifikations- Dokumentation (siehe Abschnitt 11) zu spezifizieren.
c) Die Prüfeinrichtungen sollen die richtige Ankopplung an die zu prüfenden Einrichtungen überprüfen.
d) Die Prüfeinrichtungen sollen nach der Verbindung mit den zu prüfenden Einrichtungen und dem Start des Prüfvorgangs die Prüfung selbsttätig durchführen.
e) Die Qualität automatischer Prüfungen muss mindestens der Qualität vergleichbarer bestehender Handprüfungen entsprechen.

4.1.10 Handeingriffe

Hinweis:

Unter Handeingriffen sind keine Änderungen in der projektierten Hard- und Software zu verstehen.

(1) Werden bei Betrieb der Reaktoranlage Handeingriffe zur Anpassung von A-Funktions-Einrichtungen erforderlich, so müssen sie ohne Eingriff in die Verdrahtung an vorinstallierten und geprüften Eingriffsstellen nach vorgeplanten Anweisungen durchgeführt werden können.

Hinweis:

Beispiele für zulässige Anpassungen sind:

a) bei Freischaltung eines verfahrenstechnischen Stranges die Überführung des zugehörigen Anregekanals in den angeregten Zustand,
b) die Aktivierung von Streckbetriebsparametern und
c) Ersatzwertaufschaltungen.

(2) Fehlern durch Irrtümer und Fahrlässigkeit bei notwendigen Handeingriffen zur Bedienung und Instandhaltung der A-Funktions-Einrichtungen ist vorzubeugen durch

a) vorzugsweise schaltungstechnische Maßnahmen bei der Systemauslegung,
b) Meldeeinrichtungen des Sicherheitssystems,
c) administrative Anweisungen für Bedienung und Instandhaltung

und es sind Maßnahmen zur Begrenzung der Auswirkungen von Fehlern zu berücksichtigen.

Hinweis:

Hierzu geeignete Maßnahmen sind z. B.:

a) redundanter Aufbau der A-Funktions-Einrichtungen,
b) Entkopplung der A-Funktions-Einrichtungen von Einrichtungen mit sicherheitstechnisch geringerer Bedeutung,
c) Vorrang von Signalen der A-Funktions-Einrichtungen vor Prüfsignalen,
d) Verriegelungen zur Verhinderung der gleichzeitigen Prüfung von redundanten Einrichtungen,
e) Einsatz von selbstüberwachenden Systemen,
f) Einbau von Prüfeinrichtungen,
g) Minimierung von nicht mit Prüfeinrichtungen durchzuführenden Vor-Ort-Prüfungen durch die Systemauslegung,
h) eindeutige System- und Komponentenkennzeichnung,
i) Zustandsmeldung von aktiven Komponenten des Sicherheitssystems,
j) Überwachung analoger Messkanäle durch Vergleicher,
k) Meldeeinrichtungen zur Ausfallerkennung und Ausfalllokalisierung,
l) Einsteckü̈berwachung von elektrischen Baugruppen,
m) Sicherung der Betriebsstellung von Komponenten durch Verplombung oder sonstige mechanische Einrichtungen,
n) eindeutige Festlegungen für die Bedienung der A-Funktions-Einrichtungen,
o) Durchführung von Instandhaltungsarbeiten in A-Funktions-Einrichtungen durch fachkundiges Personal nach schriftlichen Anweisungen,
p) Kontrolle der ordnungsgemäßen Durchführung von Instandhaltungsarbeiten und deren Dokumentation und
q) Übersichtliche Anordnung der Komponenten des Sicherheitssystems durch ergonomische Gestaltung.

(3) Handeingriffe in A-Funktions-Einrichtungen durch Unbefugte sind

a) vorzugsweise durch technische Maßnahmen und
b) durch administrative Maßnahmen

zu erschweren.

Hinweis:

Hierzu geeignete Maßnahmen sind z. B.:

a) räumliche Trennung redundanter Komponenten,
b) überwachte Zutrittsbarrieren zu Gebäuden, Räumen und Schränken und
c) administrative Regelung der Berechtigung und Kontrolle des Zutritts zu Komponenten der A-Funktions-Einrichtungen.

(4) Maßnahmen zur Erschwerung von Handeingriffen durch Unbefugte sind so zu gestalten, dass die notwendige Bedienung und Instandhaltung durch befugtes Personal nicht unvertretbar behindert wird.

(5) Bei Leittechnikfunktionen, die im aktuellen Anlagenzustand benötigt werden, ist durch technische und administrative Verfahren sicherzustellen, dass Eingriffe nur redundanzweise, und sequentiell durchgeführt werden können. Die Eingriffe sind - vorzugsweise durch technische Maßnahmen - auf der Warte zu melden und zu protokollieren.

Hinweis:

Messumformer, die ausschließlich vor Ort modifiziert werden, werden üblicherweise verplombt.

4.2 Auslegungsanforderungen an B-Funktions-Einrichtungen

4.2.1 Grundsätzliche Anforderungen

(1) Es ist nachzuweisen, dass B-Funktions-Einrichtungen auch bei den unter 4.2.2 beschriebenen versagensauslösenden Ereignissen die in 2.2 b) angegebenen sicherheitstechnischen Aufgaben im Anforderungsfall erfüllen.

(2) Aus diesen versagensauslösenden Ereignissen resultierende Ausfälle sind nach 4.2.3 zu kombinieren, wenn sie nicht durch technische Maßnahmen ausgeschlossen werden können.

4.2.2 Versagensauslösende Ereignisse

Es sind folgende versagensauslösende Ereignisse in Betracht zu ziehen:

a) anlagenintern (einschließlich innerhalb der B-Funktions-Einrichtungen): z. B. Ausfälle durch Kurzschlüsse, Überflutungen, Unterbrechungen, Störungen im Programmablauf oder der Datenübertragung, Erdschlüsse, Spannungs- und Frequenzänderungen, Beeinflussung durch leitungs- und feldgebundene elektromagnetische Störgrößen, mechanisches Versagen oder Brände,

b) Fehler bei Bedienung, Prüfung, Wartung und Instandsetzung der B-Funktions-Einrichtungen durch das Personal und

c) anlagenextern: z. B. Brand, Netzstörungen, Überflutung, Blitz, Sturm und Erdbeben. Für diese Ereignisse sind Vorsorgemaßnahmen nachzuweisen, so dass durch diese Ereignisse die Sicherheit der Anlage nicht unzulässig beeinträchtigt wird.

4.2.3 Ausfallkombinationen und Grundannahmen für B-Funktions-Einrichtungen

(1) Es ist nachzuweisen, dass B-Funktions-Einrichtungen im Zusammenwirken mit der Gesamtheit ihrer Stelleinrichtungen in ihrem Anforderungsfall

a) einen Zufallsausfall Z

b) und Folgeausfälle F

beherrschen.

Hinweis:

Ein Zufallsausfall kann auch durch eines der in 4.2.2 genannten versagensauslösenden Ereignisse verursacht werden.

(2) Während eines Instandhaltungsfalls (Inspektion, Wartung, Instandsetzung) ist auch der Anforderungsfall zu unterstellen.

(3) Für den lokalen Schutz des Kerns gilt: Ist der leittechnischen Funktion der Kategorie B eine leittechnischen Funktion der Kategorie A überlagert, die den Störfall bei einer höheren noch zulässigen Schadensgrenze beherrscht, braucht für die leittechnischen Funktion der Kategorie B eine mehrfache Erfassung der gleichen Prozessvariablen am selben Ort nicht zu erfolgen.

4.2.4 Fehlauslösungen von B-Funktions-Einrichtungen

Durch Fehlauslösungen von Kategorie B-Funktions-Einrichtungen darf kein Störfall herbeigeführt werden.

4.2.5 Anregung von B-Funktions-Einrichtungen

4.2.5.1 Automatisierungsgrad

Die B-Funktions-Einrichtungen sollen automatisch ausgelöst werden.

4.2.5.2 Protokollierung

Das Ansprechen der B-Funktions-Einrichtungen ist in zeitlicher Reihenfolge zu dokumentieren. Diese Dokumentation soll in Form einer selbsttätigen Meldungs- und Zeitprotokollierung erfolgen.

4.2.6 Redundanz und Unabhängigkeit

(1) Zur Beherrschung versagensauslösender Ereignisse innerhalb der B-Funktions-Einrichtungen ist ein redundanter Aufbau vorzusehen.

(2) Redundante Teilsysteme müssen voneinander so unabhängig sein, dass bei Ausfall von Teilsystemen durch ein versagensauslösendes Ereignis nach 4.2.2 die übrigen Teilsysteme zur Störungsbeherrschung ausreichen.

(3) Es dürfen nur systemspezifisch geeignete Service- oder Programmiergeräte eingesetzt werden. Sie müssen den Einrichtungen der Kategorie B zugeordnet sein. Es dürfen keine datentechnischen Verbindungen von den Service- oder Programmiergeräten zu anderen rechnerbasierten Systemen bestehen.

4.2.7 Trennung der B-Funktions-Einrichtungen von anderen Systemen

(1) Komponenten der B-Funktions-Einrichtungen dürfen für Aufgaben mit geringerer sicherheitstechnischer Bedeutung eingesetzt werden.

(2) Die B-Funktions-Einrichtungen müssen von Einrichtungen mit sicherheitstechnisch geringerer Bedeutung so unabhängig sein, dass bei bestimmungsgemäßem Betrieb und bei versagensauslösenden Ereignissen in Einrichtungen mit sicherheitstechnisch geringerer Bedeutung die Funktion der B-Funktions-Einrichtungen erhalten bleibt.

(3) Verbindungen von B-Funktions-Einrichtungen zu leittechnischen Einrichtungen mit geringerer sicherheitstechnischer Bedeutung sind auf das technisch und betrieblich Notwendige zu minimieren. Werden Signale der B-Funktions-Einrichtungen für Einrichtungen mit sicherheitstechnisch geringerer Bedeutung benutzt, so müssen diese Signale rückwirkungsfrei ausgekoppelt werden.

(4) Die Ansteuerung von B-Funktions-Einrichtungen muss so erfolgen, dass dies mit Vorrang vor Signalen mit geringerer sicherheitstechnischer Bedeutung geschieht.

(5) Die B-Funktions-Einrichtungen müssen gegen in Betracht zu ziehende systemfremde Überspannungen ausgelegt oder entkoppelt werden. Es sind die anlagenspezifischen Spannungsebenen und -toleranzen zu berücksichtigen.

4.2.8 Instandhaltung

(1) Wenn bei Instandhaltungsarbeiten an B-Funktions-Einrichtungen der noch wirksame Teil bei einem zusätzlich unterstellten Zufallsausfall einschließlich Folgeausfällen seine sicherheitstechnische Aufgabe nicht mehr erfüllen kann, so sind anlagen- und funktionsspezifisch Maßnahmen für den weiteren Anlagenbetrieb festzulegen.

Hinweis:

Die Anforderungen an den Austausch von Hardware- und Softwarekomponenten werden bei der Entwicklung des Gesamtsystems und der Einzelsysteme festgelegt. Hierzu werden fallspezifisch Anweisungen zur Durchführung, Prüfung und Dokumentation erstellt.

(2) Bei Instandhaltungsarbeiten innerhalb der B-Funktions-Einrichtungen kann eine Anpassung, z. B. Einstellen von Streckbetriebsparametern, erforderlich sein. Wird diese manuell durchgeführt, so muss sie an fest vorgegebenen Eingriffsstellen erfolgen.

(3) Die Funktionsbereitschaft und die anforderungsgerechte Funktion der B-Funktions-Einrichtungen sind nach abgeschlossener Instandhaltungsmaßnahme durch entsprechende Funktionsprüfungen sicherzustellen.

(4) Für die Instandsetzung müssen vollständige Geräte- und Schaltungsunterlagen vorliegen.

(5) Die Instandhaltungsarbeiten müssen von dem für diese Arbeiten befugten Personal durchgeführt werden.

(6) Zur Instandsetzung dürfen nur typgleiche Ersatzteile eingesetzt werden. Werden neuartige oder geänderte Bausteine eingesetzt, so sind Prüfungen nach 10.1.1.2 und 10.1.1.3 durchzuführen.

(7) Die bei Instandhaltungsarbeiten festgestellten Ausfälle, ihre Ursachen und die Art der Instandsetzung sind zu dokumentieren. Die Betriebserfahrung aus der Instandhaltung der B-Funktions-Einrichtungen muss erfasst, dokumentiert und systematisch ausgewertet werden.

4.2.9 Abstimmung zwischen den B-Funktions-Einrichtungen und zugeordneten verfahrenstechnischen Einrichtungen

(1) Die B-Funktions-Einrichtungen sind so auszulegen, dass sie die Unverfügbarkeit der zugeordneten verfahrenstechnischen Einrichtungen nicht bestimmen.

(2) Die B-Funktions-Einrichtungen sind so aufzubauen, dass der durch die zugeordneten verfahrenstechnischen Einrichtungen vorgegebene Redundanzgrad gewahrt bleibt.

4.2.10 Überwachung auf Funktionsbereitschaft und Prüfbarkeit

4.2.10.1 Überwachung auf Funktionsbereitschaft

(1) Es ist eine Informationsdarstellung vorzusehen, die einen Überblick über die Funktionsbereitschaft der B-Funktions-Einrichtungen einschließlich ihrer Energieversorgung gibt.

(2) Die B-Funktions-Einrichtungen sollen selbstüberwachend ausgelegt werden.

Hinweis:

Mittel zur Selbstüberwachung sind z. B. Signalvergleich zwischen redundanten Kanälen, Antivalenzüberwachung, dynamisch arbeitende Systeme, zyklische Speichertests, Überwachung der Datenübertragung.

(3) Nicht selbstüberwachende Teile der B-Funktions-Einrichtungen müssen Einrichtungen haben, die eine Überprüfung in Abschaltpausen und, soweit aus Zuverlässigkeitsgründen erforderlich, auch während des Normalbetriebs ermöglichen.

(4) Erkannte Ausfälle in B-Funktions-Einrichtungen müssen soweit lokalisierbar sein, dass eine Instandsetzung möglich ist.

Hinweis:

Mittel zur Lokalisierung sind z. B. optische Meldungen in der Warte, an Schrankreihen, Schränken und Einschüben sowie Systemfehlermeldungen.

4.2.10.2 Prüfbarkeit der B-Funktions-Einrichtungen

(1) Die B-Funktions-Einrichtungen müssen so ausgelegt sein, dass während des bestimmungsgemäßen Betriebs Prüfungen ohne eine unzulässige Minderung der Sicherheit der Anlage durchgeführt werden können. Eine gleichzeitige Prüfung redundanter Teilsysteme ist zu verhindern, wenn der Betriebszustand der Anlage eine Funktionsfähigkeit der B-Funktions-Einrichtungen erfordert. Hierzu sind technische Maßnahmen vorrangig vor administrativen vorzusehen.

(2) Die B-Funktions-Einrichtungen müssen so ausgelegt sein, dass sowohl das Abweichen von den der Auslegung zugrunde gelegten Toleranzwerten der Einzelgeräte und Baugruppen, als auch die einwandfreie Funktion der Untersysteme und der gesamten B-Funktions-Einrichtungen während der Abschaltpause der Anlage überprüft werden können.

Hinweis:

Bei der Bewertung der Prüfergebnisse darf die verfahrenstechnisch, zulässige Toleranz berücksichtigt werden.

(3) Während des Leistungsbetriebs der Reaktoranlage sollen Prüfungen durchgeführt werden können, die unter Nutzung vorprojektierter Prüfeingriffe und -geräte und ohne Eingriff in die Verdrahtung, die einwandfreie Funktion der Untersysteme feststellen. Durch die Prüfung der Untersysteme muss die einwandfreie Funktion der gesamten B-Funktions-Einrichtungen nachgewiesen werden können. Teilprüfungen müssen überlappend durchführbar sein. Der Prüfumfang ist in Abhängigkeit von der Wirksamkeit der Selbstüberwachung festzulegen.

Hinweis:

Geeignete Einrichtungen zur Erfüllung dieser Forderung sind z. B. Prüfbuchsen, Testschalter, Anzeigen, die es ermöglichen, simulierte Signale aufzuschalten und den Erfolg der Prüfung festzustellen.

(4) Die B-Funktions-Einrichtungen sollen so ausgelegt und betrieben werden, dass Funktionsprüfungen von dafür vorgesehenen Prüfstellen (z. B. von Prüftafeln oder Servicestationen) durchführbar sind.

(5) Die Durchführung von Prüfungen an B-Funktions-Einrichtungen soll von zentraler Stelle aus erkennbar sein.

(6) Werden zur Prüfung der Funktionsfähigkeit der B-Funktions-Einrichtungen automatische Prüfeinrichtungen eingesetzt (festverdrahtete oder freiprogrammierbare Prüfeinrichtungen), so gelten die folgenden Bedingungen:

a) Für die Prüfeinrichtung ist die Qualität und Eignung nachzuweisen.
b) Die Prüfeinrichtung ist in einer Konfigurations- und Identifikations- Dokumentation (siehe Abschnitt 11) zu spezifizieren.
c) Die Prüfeinrichtungen sollen die richtige Ankopplung an die zu prüfenden Einrichtungen überprüfen.
d) Die Prüfeinrichtungen sollen nach der Verbindung mit den zu prüfenden Einrichtungen und dem Start des Prüfvorgangs die Prüfung selbsttätig durchführen.
e) Die Qualität automatischer Prüfungen muss mindestens der Qualität vergleichbarer Handprüfungen entsprechen.

4.2.11 Handeingriffe

Hinweis:

Unter Handeingriffen sind keine Änderungen in der projektierten Hard- und Software zu verstehen.

(1) Werden bei Betrieb der Reaktoranlage Handeingriffe zur Anpassung von B-Funktions-Einrichtungen erforderlich, so müssen sie ohne Eingriff in die Verdrahtung an vorinstallierten und geprüften Eingriffsstellen durchgeführt werden können.

(2) Fehlern durch Irrtümer und Fahrlässigkeit bei notwendigen Handeingriffen zur Bedienung und Instandhaltung der B-Funktions-Einrichtungen ist vorzubeugen

a) vorzugsweise durch schaltungstechnische Maßnahmen bei der Systemauslegung,
b) durch Meldeeinrichtungen und
c) durch administrative Anweisungen für Bedienung und Instandhaltung.

Hinweis:

Hierzu geeignete Maßnahmen sind z. B.:

a) redundanter Aufbau der B-Funktions-Einrichtungen,
b) Entkopplung der B-Funktions-Einrichtungen von Einrichtungen mit sicherheitstechnisch geringerer Bedeutung,
c) Verriegelungen zur Verhinderung der gleichzeitigen Prüfung von redundanten Einrichtungen,
d) Einsatz von selbstüberwachenden Systemen,
e) Einbau von Prüfeinrichtungen,
f) Minimierung von nicht mit Prüfeinrichtungen durchzuführenden Vor-Ort-Prüfungen durch die Systemauslegung,
g) eindeutige System- und Komponentenkennzeichnung,
h) Zustandsmeldung von aktiven Komponenten,
i) Überwachung analoger Messkanäle durch Vergleicher,

j) Meldeeinrichtungen zur Ausfallerkennung und Ausfalllokalisierung,
k) Einstecküberwachung von elektrischen Baugruppen,
l) Sicherung der Betriebsstellung von Komponenten durch Verplombung oder sonstige mechanische Einrichtungen,
m) eindeutige Festlegungen für die Bedienung der B-Funktions-Einrichtungen,
n) Durchführung von Instandhaltungsarbeiten in B-Funktions-Einrichtungen durch fachkundiges Personal nach schriftlichen Anweisungen,
o) Kontrolle der ordnungsgemäßen Durchführung von Instandhaltungsarbeiten und deren Dokumentation und
p) Übersichtliche Anordnung der Komponenten.

(3) Handeingriffe in B-Funktions-Einrichtungen durch Unbefugte sind zu erschweren

a) vorzugsweise durch technische Maßnahmen,
b) durch administrative Maßnahmen.

Hinweis:

Hierzu geeignete Maßnahmen sind z. B.:

a) räumliche Trennung redundanter Komponenten,
b) überwachte Zutrittsbarrieren zu Gebäuden, Räumen und Schränken und
c) administrative Regelung der Berechtigung und Kontrolle des Zutritts zu Komponenten der B-Funktions-Einrichtung.

(4) Maßnahmen zur Erschwerung von Handeingriffen durch Unbefugte sind so zu gestalten, dass die notwendige Bedienung und Instandhaltung durch befugtes Personal nicht unvertretbar behindert wird.

(5) Bei Leittechnikfunktionen, die im aktuellen Anlagenzustand benötigt werden, ist durch technische und administrative Verfahren sicherzustellen, dass Eingriffe im Leistungsbetrieb der Anlage nur redundanzweise, und sequentiell durchgeführt werden können. Die Eingriffe sind - vorzugsweise durch technische Maßnahmen - auf der Warte zu melden und zu protokollieren.

Hinweis:

Messumformer, die ausschließlich vor Ort modifiziert werden, werden üblicherweise verplombt.

4.3 Änderungen an der Sicherheitsleittechnik

Bei Änderungen an der Sicherheitsleittechnik sind der Umfang und die Auswirkung der Änderungen zu analysieren und die Änderungen in Übereinstimmung mit den Vorgaben dieser Regel durchzuführen. Die geänderte Einrichtung muss die Anforderungen dieser Regel erfüllen. Im Rahmen der Änderungen sind Prüfungen nach Abschnitt 10 und KTA 3506 durchzuführen.

4.4 IT-Sicherheit

Hinweis:

Anforderungen zum Schutz von IT-Systemen gegen Störmaßnahmen oder sonstige Einwirkungen Dritter werden in der „Richtlinie für den Schutz von IT-Systemen in kerntechnischen Anlagen und Einrichtungen der Sicherungskategorien I und II gegen Störmaßnahmen oder sonstige Einwirkungen Dritter (SEWD-Richtlinie IT)" gestellt.

5 Aufbau und Ausführung

5.1 Aufbau und Ausführung von A-Funktions-Einrichtungen

Die sicherheitsrelevanten Eigenschaften von A-Funktions-Einrichtungen werden bestimmt durch:

a) die Gerätequalität (Hardware und ggf. Firmware/Software) (5.1.1)
b) die Qualität der System- und Anwendersoftware (5.1.2) und
c) den funktionalen und konstruktiven Systemaufbau (5.1.3)

5.1.1 Gerätequalität

5.1.1.1 Eignungsnachweis für betriebsbewährte Geräte

(1) Es sollen betriebsbewährte Geräte eingesetzt werden.

(2) Die Betriebsbewährung ist durch statistische Auswertung von Betriebsaufzeichnungen auf der Grundlage der im Datenblatt festgelegten betrieblichen Eigenschaften und der Einsatzbedingungen nachzuweisen.

Hinweis:

Weitere Details werden in der KTA 3507 geregelt.

(3) Ergänzende Prüfungen zur Betriebsbewährung sind nach 10.1.1.1 durchzuführen, wenn die Einsatzbedingungen über die im Datenblatt festgelegten betrieblichen Eigenschaften hinausgehen oder durch die Betriebsbewährung nicht erfasst werden.

(4) Ein Eignungsnachweis allein basierend auf Betriebsbewährung kann für programmierbare und rechnerbasierte Geräte mit dieser Methode nicht erreicht werden. Für diesen Eignungsnachweis sind weitere Nachweise zur Softwarequalität erforderlich.

Hinweis:

Weitere Details werden in der KTA 3503 oder der KTA 3505 geregelt.

5.1.1.2 Eignungsnachweis für neu entwickelte oder modifizierte Geräte

(1) Die Qualität von Fertigung und Design der leittechnischen Baugruppen, Geräte und Systemteile ist nachzuweisen.

(2) Die erforderliche Qualität von Fertigung und Design muss mindestens der Stufe B nach DIN EN 61192-1 genügen.

Hinweis:

(1) Hier kann neben der DIN EN 61192 Stufe B auch die IPC A 610 Klasse 2 angewendet werden.

(2) Eine Überprüfung der einsatzspezifischen Anforderungen kann ergeben, dass die Stufe C notwendig ist.

(3) Bei modifizierten Geräten betrifft die Anforderung nur den Auswirkungsbereich der Änderung.

(3) Für neu entwickelte oder modifizierte Geräte sind Prüfungen nach 10.1.1.2 durchzuführen.

5.1.1.3 Anforderungen an die Auslegung neu entwickelter oder modifizierter Geräte

(1) Das Schaltungskonzept muss einfach, übersichtlich und zweckentsprechend sein.

(2) Es sollen bewährte und zuverlässige Bauteile und Schaltungen vorgesehen werden, Betriebserfahrungen sind zu beachten.

(3) Das Gerät muss so ausgelegt sein, dass eine Prüfung der Gerätefunktion ohne Eingriff in die Verdrahtung möglich ist.

(4) Das Gerät muss für die nach 5.1.4 genannten Umgebungseinflüsse ausgelegt sein.

(5) Die Geräte müssen bezüglich der statischen und dynamischen Eigenschaften den Anforderungen der A-Funktion genügen.

Hinweis:

Dies betrifft z. B. Stabilität, Genauigkeit, Nutz-Störsignalverhältnis, Drift, Hysterese, Zeitverhalten und Reproduzierbarkeit.

5.1.1.4 Zuverlässigkeit und Qualitätsprüfung

(1) Es sind Angaben über die Zuverlässigkeit der Gerätetypen zu machen, zum Beispiel durch statistische Methoden, Ausfalleffektanalysen, Grenzbelastungsprüfungen oder durch Auswertung von Betriebserfahrungen.

(2) Die geforderte Gerätequalität von Fertigungsserien ist im Rahmen der Werksprüfungen an einer repräsentativen Stichprobe unter Betriebs- und Grenzbelastungen zu überprüfen.

(3) Das Qualitätssicherungssystem zur Sicherstellung der Gerätequalität ist nachzuweisen.

Hinweise:

(1) Anforderungen an das Qualitätssicherungssystem sind in KTA 1401 geregelt.

(2) Zusätzliche Anforderungen an Firmware in Geräten sind in 5.1.2 gestellt.

5.1.2 Softwarequalität

5.1.2.1 Grundsätze

(1) Die Software ist in verifizierbaren Schritten in einem Phasenmodell zu entwickeln. Hierbei ist die Anwendersoftware ausgehend von der verfahrenstechnischen Aufgabenstellung zu entwickeln.

(2) Die Funktionen der Anwendersoftware und der Systemsoftware sind in eigenständigen Softwareeinheiten zu realisieren. In der Softwarearchitektur ist die Anwendersoftware von der Systemsoftware zu trennen.

Hinweise:

(1) Unter Software wird sowohl Anwendersoftware als auch Systemsoftware und Firmware verstanden.

(2) Zur Systemsoftware gehören z. B. das Betriebssystem, bei Mehrrechnersystemen die Software zur Kommunikation der Rechner

(3) Die Software ist so auszulegen, dass keine unzulässigen Rückwirkungen von leittechnischen Einrichtungen der sicherheitstechnisch niederwertigeren Kategorie auf die leittechnischen Einrichtungen der sicherheitstechnisch höherwertigeren Kategorie auftreten.

(4) Der anforderungsgerechte Ablauf der Programme ist unabhängig von Art und Umfang der zeitlichen Änderung ihrer Eingangssignale zu gewährleisten.

(5) Die Entwicklung und Qualifizierung der Software hat so zu erfolgen, dass eine durchgängige Nachweisführung der korrekten Arbeitsweise der Software gewährleistet ist.

(6) Die Software soll einfach aufgebaut sein.

(7) Der Funktionsumfang der Software soll auf das für die jeweilige Funktion notwendige Maß begrenzt sein.

(8) Die Programme sind robust und selbstüberwachend auszulegen.

Hinweis:

Robustheit beschreibt die Unempfindlichkeit gegenüber nicht spezifikationsgerechten Bedingungen.

Softwarerobustheit bedeutet, dass undefinierte Zustände verhindert werden. Für jeden Eingangswert muss es zu jedem Zeitpunkt einen wohl definierten Ausgangswert geben.

5.1.2.2 Qualitätssicherung

5.1.2.2.1 Konstruktive Qualitätssicherung

(1) Entwurf und Implementierung der Software sind in den einzelnen Schritten des Phasenmodells mit formalisierten und rechnergestützten Konstruktions- und Prüfmethoden durchzuführen.

(2) Die Software ist aus klar abgegrenzten und mit geringem Funktionsumfang versehenen Einheiten aufzubauen. Diese Softwareeinheiten sind möglichst einfach bei Beschränkung auf unverzichtbare Anweisungen und Schnittstellen zu programmieren und zu einer übersichtlichen Programmstruktur zu integrieren.

5.1.2.2.2 Analytische Qualitätssicherung

(1) Die Ergebnisse der einzelnen Phasen der Softwareentwicklung sind unter Anwendung systematischer Analysen und daraus abgeleiteter Tests an den Vorgaben vollständig zu verifizieren. Dazu sind an definierten Meilensteinen Prüfungen mit rechnergestützten Werkzeugen vorzunehmen.

(2) Nach Installation der Software auf der Zielhardware ist das anforderungsgerechte Verhalten des Hardware- und Softwaresystems zu validieren. Wird die Validierung in mehreren Schritten durchgeführt, so müssen die einzelnen Validierungsschritte insgesamt abdeckend sein.

5.1.2.2.3 Organisation und Administration

(1) Die Organisation und Administration der Softwareentwicklung und der Qualitätssicherung müssen sicherstellen, dass die Software nach vollständigen Entwicklungs-, Prüf-, Änderungs- und Qualitätssicherungsplänen erstellt und eingesetzt wird. Die Unabhängigkeit zwischen Entwicklung und Qualitätssicherung muss durchgehend gewahrt werden. Es muss eine vollständige und aktuelle Entwicklungs-, Qualitätssicherungs- und Benutzerdokumentation vorhanden sein.

(2) Die konsistente Konfiguration der Software ist sicherzustellen (Konfigurationsmanagement).

5.1.2.3 Einsatz von vorgefertigter Software

(1) Der Einsatz vorgefertigter Software, die nicht entsprechend den Anforderungen der Abschnitte 5.1.2.1 und 5.1.2.2 ausgelegt ist, soll auf unverzichtbare Bestandteile beschränkt sein, wobei Softwareänderungen vermieden werden sollen. Diese Teile sind Prüfungen und Tests zu unterziehen, die in Umfang und Tiefe den Nachweisen nach 5.1.2.2.1 und 5.1.2.2.2 gleichwertig sind.

(2) Zur Bewertung der Gleichwertigkeit sollen herangezogen werden:

a) Referenzen über den Hersteller der Software,
b) die Entwicklungs-, Anwender- und Qualitätssicherungsdokumentation der Software,
c) die Ergebnisse unabhängiger Begutachtung (Zertifikate) der Software,
d) die Betriebserfahrung der Software unter Berücksichtigung der Anwendungsprofile und
e) zusätzliche Softwaretests.

5.1.3 Systemeigenschaften und –aufbau

(1) Zur Sicherstellung der Unabhängigkeit der einzelnen redundanten und diversitären Teilsysteme sind Fehlerfortpflanzungsbarrieren in Form von funktionalen, gerätetechnischen und datentechnischen Barrieren zu realisieren.

Hinweis:

Aspekte zur Realisierung von Fehlerfortpflanzungsbarrieren sind in DIN EN 62340 enthalten.

(2) Es ist eine geeignete Verteilung von leittechnischen Funktionen auf unabhängige leittechnische Einrichtungen vorzunehmen, damit ein Fehler in einer leittechnischen Einrichtung sich nicht auf leittechnische Funktionen auswirkt, die aus verfahrenstechnischer Sicht unabhängig von der ausgefallenen Funktion wirken sollen.

(3) Zur Reduzierung der Eintrittswahrscheinlichkeit systematischer Ausfälle sind bei der Systemauslegung geeignete Vorkehrungen zu treffen.

Hinweis:

Dies kann beispielsweise durch folgende Maßnahmen erreicht werden:

a) keine direkte Kommunikation zwischen Verarbeitungseinheiten, deren Unabhängigkeit zu gewährleisten ist,
b) Kommunikationsverbindungen zwischen den redundanten Verarbeitungseinheiten als Punkt zu Punkt-Verbindung und
c) unterschiedliche relative Systemalter in den redundanten Einrichtungen (z. B.: Systemstart zu unterschiedlichen Zeiten).

(4) Zur Beherrschung von systematischen Ausfällen, sofern diese nicht nach 4.1.3.1 (6) ausgeschlossen werden können, sind diversitäre Systemstrukturen zu realisieren.

(5) Bei Einsatz von rechnerbasierten oder programmierbaren Geräten sind im Rahmen einer Fehlermöglichkeits- und Einflussanalyse auf Systemebene (System-FMEA) die Auswirkungen auf die Anlage bei aktiven und passiven Fehlern der Komponenten darzustellen. Ausfälle, die zu nicht sicherheitsgerichteten Maßnahmen und kritischen Anlagenzuständen führen können, sind zu ermitteln und hierfür geeignete Maßnahmen zur Fehlerbeherrschung vorzusehen. Das Verhalten der Ausgangssignale beim Auftreten von Fehlern ist zu spezifizieren.

Hinweis:

Aktive Fehler führen zu fehlerhaften Anregesignalen. Passive Fehler blockieren Anregesignale im Anforderungsfall.

(6) Das leittechnische System soll deterministisches Systemverhalten aufweisen.

Hinweis:

Deterministisches Systemverhalten stellt sicher, dass das resultierende Verhalten von realisierten Systemen in vorhersagbarer Weise allein durch Projektierung bestimmt (determiniert) wird. Entsprechende Eigenschaften einer rechnerbasierten Gerätefamilie als Voraussetzung zur Gewährleistung des deterministischen Verhaltens von realisierten Systemen sind z. B.:

a) strikt zyklische Bearbeitung aller Systemfunktionen,
b) statische Speicherzuordnung für Programme und Daten,
c) keine Interrupts mit Abhängigkeiten vom verfahrenstechnischen Prozess,
d) Invarianz des Bearbeitungszyklus gegenüber beliebigen Trajektorien der Eingangsdaten aus dem verfahrenstechnischen Prozess,
e) Kommunikationsbelastungen, die unabhängig von Transienten des verfahrenstechnischen Prozesses sind,
f) Reaktionszeiten, die unabhängig von verfahrenstechnischen Signal-Trajektorien aus dem Prozess sind und
g) Möglichkeiten zum Berechnen und Messen der Systembelastungen.

(7) Eingriffe in leittechnische Einrichtungen müssen erkennbar sein und sollen auf der Warte gemeldet werden. Die zu ergreifenden Zugriffsschutzmaßnahmen sind im Rahmen einer Analyse zu identifizieren. Es sind wirksame Verriegelungen zur Einschränkung von Eingriffen auf den notwendigen Umfang vorzusehen. Erfolgt der Eingriff über zentrale Geräte, z. B. Servicestationen, sind wirksame Verriegelungen zur Verhinderung des gleichzeitigen Eingriffs auf mehrere Redundanzen vorzusehen.

5.1.4 Umgebungseinflüsse

5.1.4.1 Beanspruchungen bei bestimmungsgemäßem Betrieb

(1) Alle Teile von A-Funktions-Einrichtungen, zum Beispiel Messwertgeber, Messumformer, Verkabelung oder Durchführungen, müssen den am Einbauort oder Aufstellort zu unterstellenden Umgebungs- und Einsatzbedingungen genügen. Insbesondere ist nachzuweisen, dass die Funktionen nicht unzulässig beeinträchtigt werden durch:

a) mechanische Beanspruchungen (z. B. Vibration),
b) Einflüsse des Messmediums,
c) Temperatur, Druck, Feuchtigkeit und Strahlung,
d) chemische Einflüsse und
e) elektromagnetische Einflüsse hinsichtlich Störfestigkeit und Störaussendung für leitungsgeführte und feldgebundene Störgrößen.

Hinweis:

Beispielsweise dürfen bei Widerstandsthermometern Eigenerwärmung durch den Messstrom sowie Erwärmung durch Strahlungsabsorption nicht zu unzulässigen Messfehlern führen. Bei Thermoelementen dürfen z. B. nachfolgend genannte Einflüsse nicht zu unzulässigen Messfehlern führen:

a) Strukturveränderung des Hüllrohres durch Neutronenstrahlung,
b) Veränderung des keramischen Isoliermaterials durch Neutronen- und Gammastrahlung,
c) Strukturveränderung der Thermoelement-Schenkel durch thermische Neutronen und
d) Aufheizung des Thermoelements durch Gamma- und Temperaturstrahlung.

(2) Anregekanäle müssen so ausgeführt werden, dass galvanisch, induktiv oder kapazitiv eingekoppelte Störspannungen die Auslösung der Schutzaktionen nicht unwirksam machen und keine Fehlauslösungen verursachen.

Hinweise:

(1) Geeignete Maßnahmen gegen galvanische Einkopplung von Störspannungen sind z. B.: Einpunkterdung (vom Gehäuse isolierte Messwertgeber oder Messumformer mit galvanischer Trennung), getrennte Stromversorgung.

(2) Geeignete Maßnahmen gegen induktive Einkopplung von Störspannungen sind z. B.: Verdrillen der Leitungen, magnetische Abschirmung durch Verlegen der Messleitungen in Stahlpanzer-Rohren, elektrische Abschirmung durch Verlegung der Messleitungen in leitfähigen Rohren, ausreichender Abstand der Messleitungen von beeinflussenden anderen Leitungen (Starkstromleitungen).

(3) Geeignete Maßnahmen gegen kapazitive Einkopplung von Störspannungen sind z. B.: Elektrische Abschirmung, Verlegung von Messleitungen in leitfähigen Rohren, Verwendung von Koaxial- oder Triaxialkabeln bei kleinen Messströmen.

5.1.4.2 Beanspruchungen bei Leckratenprüfungen des Reaktorsicherheitsbehälters

Die im Sicherheitsbehälter montierten Geräte, Leitungen und Leitungsverbindungen sollen den bei Leckratenprüfungen auftretenden Beanspruchungen gewachsen sein. Ist dies in Ausnahmefällen nicht möglich, sind sie vor den Leckratenprüfungen auszubauen oder vor den Beanspruchungen durch die Leckratenprüfungen zu schützen. Danach sind Prüfungen nach KTA 3506 erforderlich.

5.1.4.3 Beanspruchungen bei Störfällen

(1) Teile der A-Funktions-Einrichtungen, die Störfälle überdauern müssen - weil sie auch nach Eintritt von Störfällen, zum Beispiel zur Nachwärmeabfuhr, gebraucht werden - müssen so ausgelegt und aufgebaut sein, dass die Komponenten (Messwertgeber, Bestandteile des Signal- und Versorgungsweges einschließlich Kabel- und Durchführungen) den auftretenden Bedingungen bei den Störfällen und ihren Auswirkungen widerstehen und die zu messenden Größen kontinuierlich über den gesamten Auslegungsbereich erfasst werden.

Hinweis:

Es dürfen z. B. die bei den Störfällen auftretenden Temperaturen und Drücke, Wasserdampf oder Wasser an elektrischen Durchführungen, Geräten und Verteilerkästen sowie die bei den Störfalltemperaturen an Materialübergängen entstehenden Thermospannungen nicht zu unzulässigen Funktionsbeeinflussungen führen.

(2) Teile der A-Funktions-Einrichtungen, die nur bei Eintritt von Störfällen die erforderlichen Schutzaktionen auslösen müssen und danach funktionsunfähig sein dürfen, müssen nachweislich so ausgelegt sein, dass die Komponenten bis nach Auslösung der erforderlichen Schutzaktion den auftretenden Störfallbedingungen,

zum Beispiel Strahlung, Temperatur, Druck und Feuchtigkeit, gewachsen sind und durch ihren Ausfall die übrigen zur Störfallbeherrschung erforderlichen Komponenten der A-Funktions-Einrichtungen nicht unzulässig beeinflussen.

5.1.5 Räumliche Anordnung, Trennung zueinander redundanter Einrichtungen

5.1.5.1 Gesamtsystem

(1) Zueinander redundante A-Funktions-Einrichtungen sind so anzuordnen und in genügendem Abstand voneinander aufzustellen, dass ein einzelnes versagensauslösendes Ereignis nach 4.1.2.1 und 4.1.2.2 nicht zum Ausfall einer unzulässigen Anzahl redundanter Einrichtungen führen kann.

(2) Ist eine räumliche Trennung nicht möglich, so muss ein ausreichender mechanischer Schutz vorgesehen werden, zum Beispiel Abmauern, Verbunkern. Ein mechanischer Schutz oder die Unterbringung in getrennten Schränken ist nicht erforderlich, wenn eine Beschädigung die Auslösung von Schutzaktionen nicht verhindern und nur zur Fehlauslösung eindeutig sicherheitsgerichteter Schutzaktionen führen kann.

5.1.5.2 Kabel

(1) Kabel zueinander redundanter A-Funktions-Einrichtungen sind nach 5.1.5.1 räumlich getrennt oder gegeneinander geschützt zu verlegen.

(2) Signale zueinander redundanter A-Funktions-Einrichtungen dürfen nicht in einem Kabel, einem örtlichen Kabelverteiler oder einer Kabeldurchführung geführt werden.

(3) Eine ungeschützte Verlegung von Kabeln der A-Funktions-Einrichtungen ist nur zulässig, wenn unbeabsichtigte mechanische Beschädigungen während des bestimmungsgemäßen Betriebs ausgeschlossen sind. In allen anderen Fällen sind die Kabel mechanisch zu schützen, zum Beispiel durch Schutzrohre oder Stahlblechabdeckung.

(4) Kabel der A-Funktions-Einrichtungen sind von den sie gefährdenden Komponenten, zum Beispiel Rohrleitungen, getrennt zu verlegen oder mechanisch zu schützen.

(5) Kabel zur Signalübertragung und Kabel zur Stromversorgung von zueinander redundanten Mess- und Steuereinrichtungen der A-Funktions-Einrichtungen sollen nicht über zentrale Rangierverteiler zu den signalverarbeitenden Baugruppen geführt werden.

5.1.5.3 Wirkdruckleitungen

(1) Für Wirkdruckleitungen gelten die Anforderungen nach 5.1.5.1.

(2) Für redundante Messanordnungen an einem Messort, zum Beispiel bei einem gemeinsamen Drosselgerät, sollen getrennte Entnahmestutzen vorgesehen werden. Gemeinsame Entnahmestutzen sind zugelassen, wenn die Anforderungen nach 4.1.3 erfüllt werden.

(3) Ein unbeabsichtigtes Schließen von Absperrarmaturen in Wirkdruckleitungen ist zu verhindern, zum Beispiel sind Handräder abzuziehen. Automatische Absperrungen sollen nicht eingebaut werden.

(4) Abhängig von der Messanordnung sind Vorrichtungen zum Spülen, Füllen und Entleeren bzw. Entlüften von Wirkdruckleitungen zu berücksichtigen.

5.1.6 Mechanischer Aufbau

5.1.6.1 Anschlüsse und Verbindungen

(1) Schraub- und Steckanschlüsse sind so zu sichern, dass eine Selbstauftrennung nicht möglich ist, oder der aufgetrennte Zustand selbsttätig gemeldet wird.

(2) Zwischen den Anschlüssen verschiedener Einrichtungen der gleichen Redundanzgruppe ist ein so großer Zwischenraum vorzusehen, dass die ungewollte Überbrückung einer Auslösung oder eine Fehlauslösung verhindert wird, oder es sind gleichwertige Maßnahmen zu treffen.

5.1.6.2 Kennzeichnung

(1) A-Funktions-Einrichtungen sind deutlich und eindeutig zu kennzeichnen.

(2) Kabel der A-Funktions-Einrichtungen sind an beiden Enden deutlich und eindeutig zu kennzeichnen.

(3) Bei Bausteinsystemen sind die Plätze und die zugeordneten Bausteine deutlich und eindeutig zu kennzeichnen.

5.1.6.3 Justier- und Einstellvorrichtungen

(1) Für Geräte, die während des Betriebes justiert werden müssen, oder für Parameter von Funktionen, die während des Betriebs angepasst oder betriebsabhängig eingestellt werden müssen, sind vordefinierte Einstellmöglichkeiten vorzusehen.

(2) Alle Einstellvorrichtungen an A-Funktions-Einrichtungen sind so anzuordnen oder abzusichern, dass sie gegen eine ungewollte, unbeabsichtigte und selbsttätige Verstellung geschützt sind.

(3) Eine Zugriffsmöglichkeit von außerhalb des technischen Umfelds der A-Funktions-Einrichtungen (z. B. von den Verwaltungsgebäuden oder von außerhalb der Anlage), durch den Softwarefunktionen oder Daten beeinflusst werden können, darf nicht realisiert werden.

(4) Erfolgt die Einstellung rechnergestützt mit entsprechender Bedieneinrichtung, so gilt zusätzlich:

a) Die Benutzerführung muss einfach und eindeutig sein.

b) Alle aktuellen Einstellwerte, müssen einfach aus dem Zielsystem ausgelesen und übersichtlich protokolliert werden können.

(5) Es ist vorzugsweise durch technische Maßnahmen sicherzustellen, dass Einstellungen in mehreren Redundanzen während des Betriebes der A-Funktions-Einrichtungen nur nacheinander erfolgen können. Bei technischen Maßnahmen muss die Redundanz, für die die Freigabe zur Einstellung vorliegt, eindeutig erkennbar sein und auf der Warte angezeigt und dokumentiert werden.

H i n w e i s :
Die technische Absicherung kann über Schlüsselschalter erfolgen.

5.1.6.4 Zugänglichkeit

(1) Die A-Funktions-Einrichtungen sollen so angeordnet werden, dass sie für Instandhaltungsarbeiten leicht zugänglich sind.

(2) Zur Erleichterung von Instandhaltungsarbeiten sowie zur Verringerung der Strahlenbelastung des Instandhaltungspersonals sollen Systeme mit leicht auswechselbaren Geräten eingesetzt werden.

H i n w e i s :
Hierzu kann z. B. der elektrischen Anschluss von vor Ort befindlichen Geräten über Steckvorrichtungen ausgeführt werden.

5.1.7 Aufbau von Schutzuntersystemen

5.1.7.1 Anregeebene

Für Anregekanäle sollen Geräte eingesetzt werden, bei denen eine kontinuierliche Messsignalerfassung und –verarbeitung möglich ist.

5.1.7.1.1 Analoge Anregekanäle

Die Sicherheitsvariable soll eine stetige Abhängigkeit von den Prozessvariablen aufweisen. Ist eine direkte Messung der Sicherheitsvariablen nicht möglich, z. B. DNB-Verhältnis, oder ist der Einsatz eines direkten Messverfahrens technisch nicht sinnvoll, so dürfen Rechenschaltungen eingesetzt werden, zum Beispiel Durchsatzmessung mit Blende und radizierenden Messumformern.

Hinweis:

Analoge Anregekanäle verarbeiten Messsignale mit einem kontinuierlichen Wertebereich. Die Messsignalerfassung und -verarbeitung kann mit analoger oder digitaler Gerätetechnik erfolgen.

5.1.7.1.2 Grenzsignalgeber und Vergleicher

(1) Es sollen selbst überwachende Grenzsignalgeber eingesetzt werden. Bei elektronisch arbeitenden Grenzsignalgebern soll der Grenzwert (Referenzspannung) überwacht werden.

H i n w e i s :

Eine Selbstüberwachung der Vergleicher wird nicht gefordert.

(2) Die Grenzsignalgeber und Vergleicher sollen mit einstellbarer Schalthysterese und ohne Selbsthaltung ausgeführt werden.

(3) Der Grenzwert muss am Gerät mit einer den Erfordernissen entsprechenden Genauigkeit einstellbar sein (Auflösungsvermögen). Der Grenzwert soll während des Betriebs prüfbar sein, ohne die Grenzwerteinstellung selbst ändern zu müssen.

(4) Der Messbereich des Anregekanals muss so festgelegt werden, dass unter Beachtung der Genauigkeit und Hysterese des Grenzsignalgebers ein ausreichender Abstand von den Messbereichsendwerten eingehalten wird.

(5) Das Ansprechen von Grenzsignalgeber und Vergleicher muss am Gerät und in der Warte angezeigt werden.

(6) Bei rechnerbasierten Geräten kann der Vergleich zueinander redundanter Messsignale rechnerintern erfolgen.

5.1.7.1.3 Wächter

Wächter sollen nur dann zum Einsatz kommen, wenn eine analoge Messung in einer für A-Funktions-Einrichtungen erforderlichen Qualität nicht realisiert werden kann. Die Kontakte sind durch geeignete Kontrollschaltungen (Antivalenzüberwachung, Drahtbruchüberwachung) zu überwachen.

5.1.7.1.4 Endlagenschalter

(1) Endlagenschalter zur Bildung von Anregesignalen sollen nur dann zum Einsatz kommen, wenn eine analoge Messung in einer für A-Funktions-Einrichtungen erforderlichen Qualität nicht realisiert werden kann.

(2) Werden für Anregesignale Endlagenschalter eingesetzt, die nicht zwangsgeführte Kontakte besitzen, sind - soweit kein zweites Anregekriterium vorhanden ist - die Anforderungen nach 4.1.4.2 (2) einzuhalten. Die Kontakte sind durch geeignete Kontrollschaltungen (Antivalenzüberwachung) zu überwachen.

(3) Die Betätigungseinrichtungen redundanter Endlagenschalter, zum Beispiel Spindelwellen, Stößel, Nocken, Schaltlineale, sollen für jeden redundanten Endlagenschalter getrennt aufgebaut sein.

5.1.7.2 Logikebene

(1) Die zueinander parallelen Signalpfade der Logikebene für die Reaktorschnellabschaltung müssen verschiedenen Redundanzgruppen angehören. Am Ausgang sollen sie mindestens zweifach durch logische Wertungen verbunden werden. Das Ausgangssignal jeder dieser logischen Wertungen muss zu einer Auslösung führen.

(2) Für die Auslösung jeder von mehreren parallelen Schutzteilaktionen muss ein eigener Signalpfad vorgesehen werden. Jeder dieser parallelen Signalpfade muss einer anderen Redundanzgruppe angehören.

(3) Werden von Hand auszulösende Schutzaktionen aufgrund der Analyse der Ereignisabläufe nach 3.1 zur Störfallbeherrschung vorgesehen, so sollen die Eingriffsmöglichkeiten nicht in der Steuerebene sondern in der Logikebene der A-Funktions-Einrichtungen realisiert werden.

5.1.7.2.1 Verriegelungen

(1) Bei Vorhandensein von nur einem Anregekriterium zur Erkennung eines Störfalls ist die Schutzüberbrückung dieses Anregekriteriums nach 4.1.4.2 (2) auszulegen.

(2) Bei redundant ausgeführten Anregekanälen müssen die Einrichtungen zur Umschaltung oder Übernahme von Messbereichen redundant ausgeführt werden.

(3) Umschaltungen und Übernahmen von Messbereichen sowie Schutzüberbrückungen müssen automatisch aufgehoben werden, wenn die Freigabebedingungen nicht mehr gegeben sind.

5.1.7.3 Steuerebene

5.1.7.3.1 Einzelantriebssteuerungen

Die Einzelantriebssteuerungen für ein verfahrenstechnisches System müssen redundanzbezogen ohne Vermaschung aufgebaut werden.

H i n w e i s :

Hierbei wird vorausgesetzt, dass die verfahrenstechnischen Systeme redundant aufgebaut sind. Unter System wird hier z. B. ein vierfach redundantes Hochdruck-Einspeisesystem verstanden.

5.1.7.3.2 Vorrangsteuerung

(1) Der Vorrang der Signale von A-Funktions-Einrichtungen vor den Steuersignalen mit geringerer sicherheitstechnischer Bedeutung muss sichergestellt sein. Steuersignale mit geringerer sicherheitstechnischer Bedeutung sind gegenüber Signalen von A-Funktions-Einrichtungen zu entkoppeln. Sie sollen nur in der Steuerebene der A-Funktions-Einrichtungen, die der Logikebene nachgeschaltet ist, verknüpft werden.

(2) Die Vorrangsteuerungen müssen bezogen auf die verfahrenstechnische Redundanz aufgebaut werden. Signalverknüpfungen zwischen verschiedenen verfahrenstechnischen Redundanzen sind nach der Vorrangbildung nicht zulässig.

(3) Die Verknüpfung von Signalen verschiedener sicherheitstechnischer Bedeutung soll in der Steuerebene nach Prioritäten erfolgen.

(4) Koppelglieder, z. B. Koppelrelais, müssen innerhalb der zulässigen Grenzen der Ein- und Ausgangsspannungen sicher funktionieren.

(5) Bei der Umsetzung von Steuersignalen auf andere Spannungen und Frequenzen durch Koppelglieder, z. B. Koppelrelais, müssen die Ein- und Ausgänge der Koppelglieder zuverlässig getrennt werden.

(6) Die Koppelglieder, z. B. Koppelrelais, sind so auszulegen und anzuordnen, dass sie durch Schaltvorgänge in der Schaltanlage keinen unzulässigen mechanischen, thermischen oder elektrischen Beanspruchungen ausgesetzt werden.

5.1.8 Schaltung

Die Zusammenschaltung von A-Funktions-Einrichtungen ist so auszuführen, dass ein eindeutiger Funktionsablauf sichergestellt ist. Bauteileigenschaften, wie Eigenzeiten, Toleranzen, Drift- und Störfallverhalten dürfen den zeitlichen Ablauf von Befehlen nicht unzulässig beeinflussen.

5.2 Aufbau und Ausführung von B-Funktions-Einrichtungen

Die sicherheitsrelevanten Eigenschaften von B-Funktions-Einrichtungen werden bestimmt durch:

a) die Gerätequalität (Hardware und ggf. Firmware/Software) (5.2.1),
b) die Qualität der System- und Anwendersoftware (5.2.2) und
c) den funktionalen und konstruktiven Systemaufbau (5.2.3)

5.2.1 Gerätequalität

5.2.1.1 Eignungsnachweis für betriebsbewährte Geräte

(1) Es sollen betriebsbewährte Geräte eingesetzt werden.

(2) Die Betriebsbewährung ist durch statistische Auswertung von Betriebsaufzeichnungen auf der Grundlage der im Datenblatt festgelegten betrieblichen Eigenschaften und der Einsatzbedingungen nachzuweisen.

(3) Ergänzende Prüfungen zur Betriebsbewährung sind nach 10.1.1.1 durchzuführen, wenn die Einsatzbedingungen über die im Datenblatt festgelegten betrieblichen Eigenschaften hinausgehen oder durch die Betriebsbewährung nicht erfasst werden.

(4) Ein Eignungsnachweis allein basierend auf Betriebsbewährung kann für programmierbare und rechnerbasierte Geräte mit dieser Methode nicht erreicht werden. Für diesen Eignungsnachweis sind weitere Nachweise zur Softwarequalität erforderlich.

H i n w e i s :
Weitere Details werden in KTA 3503 oder KTA 3505 geregelt.

5.2.1.2 Eignungsnachweis für neu entwickelte oder modifizierte Geräte

(1) Die Qualität von Fertigung und Design der leittechnischen Baugruppen, Geräte und Systemteile ist nachzuweisen.

(2) Die erforderliche Qualität von Fertigung und Design muss mindestens der Stufe B nach DIN EN 61192-1 genügen.

H i n w e i s :
a) Hier kann neben der DIN EN 61192 Stufe B auch die IPC A 610 Klasse 2 angewendet werden.
b) Eine Überprüfung der einsatzspezifischen Anforderungen kann ergeben, dass die Stufe C notwendig ist.
c) Bei modifizierten Geräten betrifft die Anforderung nur den Auswirkungsbereich der Änderung.

(3) Für neu entwickelte oder modifizierte Geräte sind Prüfungen nach 10.1.1.2 durchzuführen.

5.2.1.3 Anforderungen an die Auslegung neu entwickelter oder modifizierter Geräte

(1) Es sollen bewährte und zuverlässige Bauteile und Schaltungen vorgesehen werden, Betriebserfahrungen sind zu beachten.

(2) Das Gerät muss so ausgelegt sein, dass eine Prüfung der Gerätefunktion ohne Eingriff in die Verdrahtung möglich ist.

(3) Das Gerät muss für die nach 5.2.4 genannten Umgebungseinflüsse ausgelegt sein.

(4) Die Geräte müssen bezüglich der statischen und dynamischen Eigenschaften den Anforderungen der B-Funktion genügen.

H i n w e i s :
Dies betrifft z. B. Stabilität, Genauigkeit, Nutz-Störsignalverhältnis, Drift, Hysterese, Zeitverhalten und Reproduzierbarkeit.

5.2.1.4 Zuverlässigkeit und Qualitätsprüfung

(1) Es sind Angaben über die Zuverlässigkeit der Gerätetypen zu machen, zum Beispiel durch statistische Methoden, Ausfalleffektanalysen, Grenzbelastungsprüfungen oder durch Auswertung von Betriebserfahrungen.

(2) Die geforderte Gerätequalität von Fertigungsserien ist im Rahmen der Werksprüfungen an einer repräsentativen Stichprobe unter Betriebs- und Grenzbelastungen zu überprüfen.

(3) Das Qualitätssicherungssystem zur Sicherstellung der Gerätequalität ist nachzuweisen.

H i n w e i s :
(1) Anforderungen an das Qualitätssicherungssystems sind in KTA 1401 geregelt.
(2) Zusätzliche Anforderungen an Firmware in Geräten sind in 5.2.2 gestellt.

5.2.2 Softwarequalität

5.2.2.1 Grundsätze

(1) Für die Entwicklung und Qualifizierung der Software der Leittechnik-Funktionen der Kategorie B sind Beschreibungen und rechnergestützte Testverfahren anzuwenden, die den Nachweis der korrekten Arbeitsweise unterstützen.

(2) Die Programme sind robust und selbstüberwachend auszulegen.

H i n w e i s :
(1) Robustheit beschreibt die Unempfindlichkeit gegenüber nicht spezifikationsgerechten Bedingungen.
(2) Softwarerobustheit bedeutet, dass undefinierte Zustände verhindert werden. Für jeden Eingangswert muss es zu jedem Zeitpunkt einen wohl definierten Ausgangswert geben.

5.2.2.2 Qualitätssicherung

5.2.2.2.1 Konstruktive Qualitätssicherung

(1) Die Softwareerstellung muss nach einem Phasenmodell weitgehend mit rechnergestützten Werkzeugen erfolgen.

(2) Die Software ist aus hinsichtlich der Funktion klar abgegrenzten Einheiten aufzubauen. Diese Softwareeinheiten sollen mit Beschränkung auf unverzichtbare Anweisungen und Schnittstellen programmiert und in eine übersichtliche Programmstruktur integriert werden.

5.2.2.2.2 Analytische Qualitätssicherung

(1) Die Ergebnisse der einzelnen Phasen der Softwareentwicklung sind einer dokumentierten Prüfung zu unterziehen. Alle sicherheitsrelevanten Programmteile sind durch eine Kombination von Testverfahren zu prüfen, wobei eine vollständige Funktionstestüberdeckung erreicht werden soll.

(2) Das anforderungsgerechte Verhalten des Hardware- und Softwaresystems ist zu validieren.

5.2.2.2.3 Organisation und Administration

(1) Die Organisation und Administration der Softwareentwicklung und der Qualitätssicherung ist so zu gestalten, dass sichergestellt ist, dass die Software nach vollständigen Entwicklungs-, Prüf-, Änderungs- und Qualitätssicherungsplänen erstellt und eingesetzt wird. Die Unabhängigkeit zwischen Entwicklung und Qualitätssicherung muss durchgehend gewahrt werden. Es ist eine vollständige Entwicklungs-, Qualitätssicherungs- und Benutzerdokumentation zu erstellen.

(2) Die konsistente Konfiguration der Software ist sicherzustellen (Konfigurationsmanagement).

5.2.2.3 Einsatz von vorgefertigter Software

(1) Der Einsatz vorgefertigter Software, die nicht entsprechend den Anforderungen in den Abschnitten 5.2.2.1 und 5.2.2.2 ausgelegt ist, soll auf unverzichtbare Bestandteile beschränkt sein, wobei Softwareänderungen vermieden werden sollen. Diese Teile sind Prüfungen und Tests zu unterziehen, die in Umfang und Tiefe den Nachweisen nach 5.2.2.2.1 und 5.2.2.2.2 gleichwertig sind.

(2) Zur Bewertung der Gleichwertigkeit sollen herangezogen werden:

a) Referenzen über den Hersteller der Software,
b) die Entwicklungs-, Anwender- und Qualitätssicherungsdokumentation der Software,
c) das Ergebnis unabhängiger Begutachtung (Zertifikate) der Software,
d) die Betriebserfahrung der Software unter Berücksichtigung der Anwendungsprofile und
e) zusätzliche Softwaretests.

5.2.3 Systemeigenschaften und -aufbau

(1) Zur Sicherstellung der Unabhängigkeit der einzelnen redundanten Teilsysteme sind Fehlerfortpflanzungsbarrieren in Form von funktionalen, gerätetechnischen und datentechnischen Barrieren zu realisieren.

Hinweis:

Aspekte zur Realisierung von Fehlerfortpflanzungsbarrieren sind in DIN EN 62340 enthalten.

(2) Bei Einsatz von rechnerbasierten oder programmierbaren Geräten sind mittels einer systematischen Methode zur Identifikation von Fehlermöglichkeiten und zur Analyse der Auswirkungen dieser Fehler auf die Anlage bei aktiven und passiven Fehlern darzustellen. Das Verhalten der Ausgangssignale beim Auftreten von Fehlern ist zu spezifizieren.

Hinweis:

Aktive Fehler führen zu fehlerhaften Anregesignalen. Passive Fehler blockieren Anregesignale im Anforderungsfall.

(3) Das leittechnische System soll deterministisches Systemverhalten aufweisen.

Hinweis:

Deterministisches Systemverhalten stellt sicher, dass das resultierende Verhalten von realisierten Systemen in vorhersagbarer Weise allein durch Projektierung bestimmt (determiniert) wird. Wesentliche Eigenschaften einer rechnerbasierten Gerätefamilie als Voraussetzung zur Gewährleistung des deterministischen Verhaltens von realisierten Systemen sind:

a) strikt zyklische Bearbeitung aller Systemfunktionen,
b) statische Speicherzuordnung für Programme und Daten,
c) keine Interrupts mit Abhängigkeiten vom verfahrenstechnischen Prozess,
d) Invarianz des Bearbeitungszyklus gegenüber beliebigen Trajektorien der Eingangsdaten aus dem verfahrenstechnischen Prozess,
e) Kommunikationsbelastungen, die unabhängig von Transienten des verfahrenstechnischen Prozesses sind,
f) Reaktionszeiten, die unabhängig von verfahrenstechnischen Signal-Trajektorien aus dem Prozess sind, und
g) Möglichkeiten zum Berechnen und Messen der Systembelastungen.

(4) Eingriffe in leittechnische Einrichtungen müssen erkennbar sein und sollen auf der Warte gemeldet werden. Die zu ergreifenden Zugriffsschutzmaßnahmen sind im Rahmen einer Analyse zu identifizieren. Es sind wirksame Verriegelungen zur Einschränkung von Eingriffen auf den notwendigen Umfang vorzusehen. Erfolgt der Eingriff über zentrale Geräte, z. B. Servicestationen, sind wirksame Verriegelungen zur Verhinderung des gleichzeitigen Eingriffs auf mehrere Redundanzen vorzusehen.

5.2.4 Umgebungseinflüsse

5.2.4.1 Beanspruchungen bei bestimmungsgemäßem Betrieb

(1) Alle Teile von B-Funktions-Einrichtungen, zum Beispiel Messwertgeber, Messumformer, Verkabelung, Durchführungen, müssen den am Einbauort oder Aufstellort zu unterstellenden Umgebungs- und Einsatzbedingungen genügen. Insbesondere ist nachzuweisen, dass die Funktionen nicht unzulässig beeinträchtigt werden durch:

a) mechanische Beanspruchungen (z. B. Vibration),
b) Einflüsse des Messmediums,
c) Temperatur, Druck, Feuchtigkeit und Strahlung,
d) chemische Einflüsse und
e) elektromagnetische Einflüsse hinsichtlich Störfestigkeit und Störaussendung für leitungsgeführte und feldgebundene Störgrößen.

Hinweis:

Beispielsweise dürfen bei Widerstandsthermometern Eigenerwärmung durch den Messstrom sowie Erwärmung durch Strahlungsabsorption nicht zu unzulässigen Messfehlern führen. Bei Thermoelementen dürfen z. B. nachfolgend genannte Einflüsse nicht zu unzulässigen Messfehlern führen:

a) Strukturveränderung des Hüllrohres durch Neutronenstrahlung,
b) Veränderung des keramischen Isoliermaterials durch Neutronen- und Gammastrahlung,
c) Strukturveränderung der Thermoelement-Schenkel durch thermische Neutronen und
d) Aufheizung des Thermoelements durch Gamma- und Temperaturstrahlung.

(2) Anregekanäle müssen so ausgeführt werden, dass galvanisch, induktiv oder kapazitiv eingekoppelte Störspannungen die Auslösung der Kategorie B Funktion nicht unwirksam machen und keine Fehlauslösungen verursachen.

Hinweise:

(1) Geeignete Maßnahmen gegen galvanische Einkopplung von Störspannungen sind z. B.: Einpunkterdung (vom Gehäuse isolierte Messwertgeber oder Messumformer mit galvanischer Trennung), getrennte Stromversorgung.

(2) Geeignete Maßnahmen gegen induktive Einkopplung von Störspannungen sind z. B.: Verdrillen der Leitungen, magnetische Abschirmung durch Verlegen der Messleitungen in Stahlpanzer-Rohren, elektrische Abschirmung durch Verlegung der Messleitungen in leitfähigen Rohren, ausreichender Abstand der Messleitungen von beeinflussenden anderen Leitungen (Starkstromleitungen).

(3) Geeignete Maßnahmen gegen kapazitive Einkopplung von Störspannungen sind z. B.: Elektrische Abschirmung, Verlegung von Messleitungen in leitfähigen Rohren, Verwendung von Koaxial- oder Triaxialkabeln bei kleinen Messströmen.

5.2.4.2 Beanspruchungen bei Störfällen

Teile der B-Funktions-Einrichtungen, die Störfälle überdauern müssen, weil sie nach Eintritt von Störfällen gebraucht werden,

müssen so ausgelegt und aufgebaut sein, dass die Komponenten (Messwertgeber, Bestandteile des Signal- und Versorgungsweges einschließlich Kabel- und Durchführungen) den auftretenden Bedingungen bei den Störfällen und ihren Auswirkungen widerstehen.

Hinweis:

Es dürfen z. B. die bei den Störfällen auftretenden Temperaturen und Drücke, Wasserdampf oder Wasser an elektrischen Durchführungen, Geräten und Verteilerkästen sowie die bei den Störfalltemperaturen an Materialübergängen entstehenden Thermospannungen nicht zu unzulässigen Funktionsbeeinflussungen führen.

5.2.5 Mechanischer Aufbau

5.2.5.1 Anschlüsse und Verbindungen

Schraub- und Steckanschlüsse sind so zu sichern, dass eine Selbstauftrennung nicht möglich ist, oder der aufgetrennte Zustand selbsttätig gemeldet wird.

5.2.5.2 Kennzeichnung

(1) B-Funktions-Einrichtungen sind deutlich und eindeutig zu kennzeichnen.

(2) Kabel der B-Funktions-Einrichtungen sind an beiden Enden deutlich und eindeutig zu kennzeichnen.

(3) Bei Bausteinsystemen sind die Plätze und die zugeordneten Bausteine deutlich und eindeutig zu kennzeichnen.

5.2.5.3 Justier- und Einstellvorrichtungen

(1) Für Geräte, die während des Betriebes justiert werden müssen, oder für Parameter von Funktionen, die während des Betriebs angepasst oder betriebsabhängig eingestellt werden müssen, sind vordefinierte Einstellmöglichkeiten vorzusehen.

(2) Alle Einstellvorrichtungen an B-Funktions-Einrichtungen sind so anzuordnen oder abzusichern, dass sie gegen eine ungewollte, unbeabsichtigte und selbsttätige Verstellung geschützt sind.

(3) Eine Zugriffsmöglichkeit von außerhalb des technischen Umfelds der B-Funktions-Einrichtungen (z. B. von den Verwaltungsgebäuden oder von außerhalb der Anlage), durch den Softwarefunktionen oder Daten beeinflusst werden können, ist nicht zulässig.

(4) Erfolgt die Einstellung rechnergestützt mit entsprechender Bedieneinrichtung, so gilt zusätzlich:

a) Die Benutzerführung muss eindeutig sein.

b) Die Einstellwerte müssen aus dem Zielsystem ausgelesen und übersichtlich protokolliert werden können.

(5) Es ist vorzugsweise durch technische Maßnahmen sicherzustellen, dass Einstellungen in mehreren Redundanzen während des Betriebes der B-Funktions-Einrichtungen nur nacheinander erfolgen können. Bei technischen Maßnahmen muss die Redundanz, für die die Freigabe zur Einstellung vorliegt, eindeutig erkennbar sein und auf der Warte angezeigt und dokumentiert werden.

Hinweis:

Die technische Absicherung kann über Schlüsselschalter erfolgen.

5.2.5.4 Zugänglichkeit

(1) Die B-Funktions-Einrichtungen sollen so angeordnet werden, dass sie für Instandhaltungsarbeiten leicht zugänglich sind.

(2) Zur Erleichterung von Instandhaltungsarbeiten sowie zur Verringerung der Strahlenbelastung des Instandhaltungspersonals sollen Systeme mit leicht auswechselbaren Geräten eingesetzt werden.

Hinweis:

Z. B. kann der elektrische Anschluss von vor Ort befindlichen Geräten über Steckvorrichtungen vorgesehen werden.

5.2.6 Aufbau von Untersystemen

5.2.6.1 Messwerterfassung und Aufbereitung

(1) Als Eingangswerte der Kategorie B-Funktionen sind vorzugsweise analoge Messwerte zu verwenden. Der Einsatz von Binärsignalgebern ist zulässig, wenn diese durch geeignete Kontrollschaltungen (Antivalenzüberwachung, Drahtbruchüberwachung) überwacht werden.

(2) Die Gültigkeit der Messwerte soll durch Validierungsfunktionen überwacht werden.

(3) Das Ansprechen von Grenzwerten und von Überwachungsfunktionen muss am Gerät und in der Warte angezeigt werden.

(4) Endlagenschalter sollen zwangsläufig schaltende Kontakte besitzen. Sofern dies nicht realisierbar ist, sind die Kontakte durch geeignete Kontrollschaltungen (Antivalenzüberwachung) zu überwachen.

5.2.6.2 Signalverarbeitung

(1) B-Funktions-Einrichtungen sind von leittechnischen Einrichtungen mit geringerer sicherheitstechnischer Bedeutung unabhängig und rückwirkungsfrei zu realisieren. Zueinander redundante B-Funktionen sind in unabhängigen Einrichtungen auszuführen.

(2) Die Gültigkeit der Ergebnisse der Messsignalverarbeitung soll durch Validierungsfunktionen überwacht werden.

5.2.6.3 Vorrang

(1) Der Vorrang der Signale von B-Funktions-Einrichtungen vor den Steuersignalen mit geringerer sicherheitstechnischer Bedeutung muss sichergestellt sein. Steuersignale mit geringerer sicherheitstechnischer Bedeutung sind gegenüber Signalen von B-Funktions-Einrichtungen zu entkoppeln.

(2) Anforderungen an Koppelglieder sind in 5.1.7.3.2 festgelegt.

5.2.7 Schaltung

Die Zusammenschaltung von B-Funktions-Einrichtungen ist so auszuführen, dass ein eindeutiger Funktionsablauf sichergestellt ist. Bauteileigenschaften, wie Eigenzeiten, Toleranzen und Driftverhalten dürfen den zeitlichen Ablauf von Befehlen nicht unzulässig beeinflussen.

6 Aggregateschutz

(1) Im Anforderungsfall von A-Funktions-Einrichtungen sollen die Schutzeinrichtungen der für eine Schutzaktion erforderlichen Aggregate und Hilfseinrichtungen nicht wirksam werden. Dies darf nicht erfolgen, wenn hierdurch Folgeschäden verursacht werden können, die die Sicherheit der Reaktoranlage mehr beeinträchtigen als der Ausfall des Aggregats. Die Unterdrückung des Aggregatschutzes muss durch die A-Funktions-Einrichtungen erfolgen.

(2) Ist in einer Schutzeinrichtung ein Vorrang vor Leittechnik-Funktionen der Kategorie A notwendig (vorrangiger Aggregateschutz), müssen an die Schutzeinrichtungen die Anforderungen an leittechnische Einrichtungen gestellt werden, die Kategorie A Funktionen ausführen.

(3) Die Anforderungen an leittechnische Einrichtungen, die Funktionen der Kategorie A ausführen, müssen an die Schutzeinrichtungen nicht gestellt werden, wenn nachgewiesen wird, dass Fehler der Schutzeinrichtung so unwahrscheinlich sind, dass eine dadurch verursachte Fehlauslösung nicht mehr unterstellt werden muss.

(4) Ein Zufallsausfall in einer Einrichtung des vorrangigen Aggregateschutzes darf keine Schutzaktion mit Folgen nach 4.1.3.4 auslösen oder Schutzvollaktionen verhindern. Diese Einrichtungen des Aggregateschutzes sollen das Aggregat über 2 von 2 oder 2 von 3-Wertungsschaltungen bei Grenzwertüberschreitung abschalten.

(5) Einrichtungen des Aggregateschutzes, deren Signale Vorrang vor Signalen von A-Funktions-Einrichtungen haben, sind dem zu schützenden Aggregat zuzuordnen.

(6) Einrichtungen zur Handüberbrückung am Aggregateschutz sind so auszulegen, dass unbefugte Eingriffe erschwert werden.

7 Lüftungstechnische Anlagen zur Raumkühlung von A-Funktions-Einrichtungen

(1) Durch die räumliche Unterbringung der A-Funktions-Einrichtungen muss sichergestellt werden, dass bei Ausfall der gesamten Lüftung für A-Funktions-Einrichtungen die zulässige Raumtemperatur nicht überschritten wird. Andernfalls sind lüftungstechnische Anlagen vorzusehen, die nach (2) und (3) dieses Abschnitts auszulegen sind.

Hinweis:

Zur Einhaltung der zulässigen Raumtemperatur dürfen zum Beispiel sicherheitstechnisch nicht relevante Einrichtungen abgeschaltet werden.

(2) Die lüftungstechnischen Anlagen für A-Funktions-Einrichtungen sind einschließlich ihrer zugehörigen Kühlkreisläufe redundant auszuführen. Die Kühlung der A-Funktions-Einrichtungen muss auch bei Auftreten eines Zufallsausfalls innerhalb der A-Funktions-Einrichtungen oder eines versagensauslösenden Ereignisses nach 4.1.2.2 aufrechterhalten werden, so dass die Funktionsfähigkeit der A-Funktions-Einrichtungen noch sichergestellt bleibt.

Hinweis:

Der Ausfall einer lüftungstechnischen Anlage stellt ein versagensauslösendes Ereignis nach 4.1.2.2 dar.

(3) A-Funktions-Einrichtungen, die Kühlung benötigen, sind mit notstromversorgten lüftungstechnischen Anlagen auszurüsten.

(4) A-Funktions-Einrichtungen, die in Anlagen- oder Messumformerräumen untergebracht sind, dürfen aufgrund des geringen Wärmeanfalls in Abweichung von (2) und (3) von den allgemeinen lüftungstechnischen Anlagen des Kontrollbereichs mitgekühlt werden, wenn die Anforderung aus (1) erfüllt wird.

8 Elektrische Energieversorgung

(1) A-Funktions-Einrichtungen sowie B-Funktions-Einrichtungen, die im Notstromfall benötigt werden, sind aus einer unterbrechungslosen Notstromversorgung mit Energiespeicherung durch Batterien im Parallelbetrieb mit Gleichrichtergeräten zu versorgen. Für die zugehörige Notstromerzeugungsanlage gelten die Anforderungen der Regel KTA 3701. Für Energieversorgungseinrichtungen innerhalb der A-Funktions-Einrichtungen sind die Anforderungen nach 5.1.1 und 10.1 anzuwenden.

(2) Die Energieversorgung der A-Funktions-Einrichtungen ist redundant so auszuführen, dass eine ausreichende Versorgung der Gesamtheit der A-Funktions-Einrichtungen auch bei Auftreten eines versagensauslösenden Ereignisses nach 4.1.2.1 und 4.1.2.2 und den Grundannahmen nach 4.1.3.1 aufrechterhalten wird.

(3) Die Energieversorgungseinrichtung muss leistungsmäßig so ausgelegt sein, dass auch bei Ausfall einer Teilversorgungseinrichtung der notwendige Leistungsbedarf der Gesamtheit der A-Funktions-Einrichtungen gedeckt werden kann.

(4) Die Auslegung der einspeisenden Erzeugungsanlagen, der Verteilernetze und der leittechnischen Einrichtungen sind so aufeinander abzustimmen, dass die für die leittechnischen Einrichtungen zu Grunde gelegten Beanspruchungen und die statischen und dynamischen Grenzwerte der für die leittechnischen Einrichtungen spezifizierten zulässigen Versorgungsspannungen nicht überschritten werden.

(5) Für die Batterien sind die Anforderungen nach KTA 3703 zu erfüllen.

9 Gefahrenmeldeeinrichtungen

9.1 Allgemeines

(1) Bei der Auslegung von Gefahrenmeldeeinrichtungen ist zu unterscheiden zwischen

a) Gefahrenmeldungen der Klasse S (Sicherheitsgefahrenmeldung),

b) Gefahrenmeldungen der Klasse I und

c) Gefahrenmeldungen der Klasse II.

(2) Es sind für den Einsatzzweck geeignete Komponenten zu verwenden. Zur Beurteilung der Eignung der Geräte sind die sicherheitstechnische Bedeutung ihrer Aufgabenstellung und die zu unterstellenden Einsatzbedingungen heranzuziehen.

9.2 Gefahrenmeldeeinrichtungen der Klasse S

9.2.1 Anwendung

Die Einleitung von Schutzaktionen von Hand ist bei Einhaltung der Forderungen nach 4.1.4.3 zulässig, wenn der Zeitraum zwischen Erkennung des Störfalls und der Einleitung der Schutzaktionen ausreichend ist. Diese aufgrund von Gefahrenmeldungen der Klasse S (Sicherheitsgefahrenmeldungen) einzuleitenden Gegenmaßnahmen müssen den Gefahrenmeldungen der Klasse S eindeutig zugeordnet sein und dem Betriebspersonal in verbindlicher schriftlicher Form, unter Angabe des zulässigen Zeitraums bis zur Einleitung der Schutzaktionen und bis zu den zu erwartenden Rückmeldungen und Anzeigen, vorliegen.

9.2.2 Auslegung

(1) Entsprechend Ihrer sicherheitstechnischen Bedeutung sind die Anforderungen an die Gerätequalität in 5.1.1 oder 5.2.1 festgelegt.

(2) Gefahrenmeldungen der Klasse S müssen durch optische und akustische Mittel den Gefahrenzustand signalisieren.

(3) Gefahrenmeldeeinrichtungen der Klasse S und die optischen und akustischen Gefahrenmeldeanlagen sind so auszuführen, dass auch bei Auftreten eines Zufallsausfalls in der Gefahrenmeldeanlage der Klasse S bei Störfällen die Störfallmeldung erscheint.

(4) Gefahrenmeldeeinrichtungen der Klasse S sind redundant, unabhängig und während des bestimmungsgemäßen Betriebs prüfbar aufzubauen. Zugehörige Signale können aus dem Teil der A-Funktions-Einrichtungen ausgekoppelt werden, der zur automatischen Auslösung von Schutzaktionen dient. Dies muss rückwirkungsfrei erfolgen.

(5) Gefahrenmeldungen der Klasse S müssen sich im Erscheinungsbild von Gefahrenmeldungen der Klasse I und II unterscheiden.

(6) Gefahrenmeldungen der Klasse S sind zu speichern.

(7) Die optischen Gefahrenmeldungen der Klasse S müssen im Rahmen des jeweiligen Wartenkonzepts räumlich zusammengefasst angeordnet werden.

(8) Die optischen Gefahrenmeldungen der Klasse S müssen so ausgeführt sein, dass der Meldezustand dauernd erkennbar ist, zum Beispiel aufgelaufen, quittiert, gelöscht.

(9) Die optischen Gefahrenmeldungen der Klasse S müssen aus einer unterbrechungslosen Notstromversorgung mit Energiespeicherung durch Batterien im Parallelbetrieb mit Gleichrichtergeräten versorgt werden.

(10) Die Erkennbarkeit der Gefahrenmeldungen der Klasse S muss durch Schriftbild, Leuchtkraft und Eindeutigkeit der Bezeichnungen sichergestellt werden.

(11) Optische Gefahrenmeldeeinrichtungen der Klasse S sollen für eine ausreichende Lebensdauer bemessen und müssen jederzeit mittels eingebauter Prüfhilfen prüfbar sein.

9.2.3 Software für Gefahrenmeldeeinrichtungen der Klasse S

Entsprechend Ihrer sicherheitstechnischen Bedeutung sind die Anforderungen an die Software in 5.1.2 oder 5.2.2 festgelegt.

9.3 Gefahrenmeldeeinrichtungen der Klasse I

9.3.1 Anwendung

Die A-Funktions-Einrichtungen und die aktiven Sicherheitseinrichtungen sind mit Gefahrenmeldungen der Klasse I auszustatten, die das Betriebspersonal veranlassen, die Störung zu beseitigen.

H i n w e i s :

Hierzu gehören z. B. bei A-Funktions-Einrichtungen die Sammelmeldung „Grenzwertmelder angesprochen“, bei der Notspeisewasserversorgung die Meldung „Deionatbehälterfüllstand zu tief“ und bei Stellgeräten die Sammelmeldung „Bereitschaftsstellung gestört“.

9.3.2 Auslegung

(1) Gefahrenmeldungen der Klasse I müssen durch optische und akustische Mittel den Gefahrenzustand signalisieren.

(2) Gefahrenmeldungen der Klasse I sollen sich im Erscheinungsbild von Gefahrenmeldungen der Klasse II unterscheiden lassen.

(3) Einzelmeldungen funktionell zusammengehöriger Komponenten dürfen zu Sammelmeldungen zusammengefasst werden, wenn die Herkunft der Einzelmeldungen lokalisiert werden kann. Einzelmeldungen brauchen dann nicht der Klasse I anzugehören.

(4) Die optischen Gefahrenmeldungen der Klasse I, die funktionsmäßig zusammengehören, sollen funktional zusammengefasst im Rahmen des jeweiligen Wartenkonzepts angezeigt werden.

(5) Die optische Gefahrenmeldung der Klasse I muss so ausgeführt sein, dass der Meldezustand dauernd erkennbar ist, zum Beispiel aufgelaufen, quittiert, gelöscht.

(6) Die Gefahrenmeldeeinrichtungen der Klasse I einschließlich der zu einer Sammelmeldung zusammengefassten Einzelmeldungen müssen aus einer unterbrechungslosen Notstromversorgung mit Energiespeicherung durch Batterien im Parallelbetrieb mit Gleichrichtergeräten versorgt werden.

(7) Die Erkennbarkeit der Gefahrenmeldungen der Klasse I muss durch Schriftbild, Leuchtkraft und Eindeutigkeit der Bezeichnungen sichergestellt werden.

(8) Optische Gefahrenmeldeeinrichtungen der Klasse I sollen für eine ausreichende Lebensdauer bemessen und müssen jederzeit mittels eingebauter Prüfhilfen prüfbar sein.

9.3.3 Software für Gefahrenmeldeeinrichtungen der Klasse I

Die Software für Gefahrenmeldeeinrichtungen der Klasse I ist nach anerkannten Methoden der Softwaretechnik zu qualifizieren.

H i n w e i s :

Als anerkannte Methode gilt z. B. die DIN EN 62138, wobei die Kategorie C herangezogen werden kann.

10 Prüfungen

10.1 Prüfungen an A- und B-Funktions-Einrichtungen und an Gefahrenmeldeeinrichtungen der Klasse S

10.1.1 Prüfung der Eignung der Gerätetypen

10.1.1.1 Ergänzende Typprüfungen für betriebsbewährte Geräte

(1) Für betriebsbewährte Einrichtungen sind zum Nachweis bestimmter nach 5.1.1.1 (2) oder nach 5.2.1.1 (2) nicht nachgewiesener Eigenschaften ergänzende Typprüfungen durchzuführen.

(2) Die Erstellung der Unterlagen für den theoretischen Teil der Typprüfungen soll durch den Hersteller erfolgen. Diese Unterlagen sollen der atomrechtlichen Behörde oder einem von ihr nach § 20 AtG zugezogenen Sachverständigen zur Prüfung vorgelegt werden. Das Prüfprogramm für den praktischen Teil der Typprüfungen soll vom Hersteller erstellt und mit der atomrechtlichen Behörde oder einen von ihr nach § 20 AtG zugezogenen Sachverständigen abgestimmt werden. Die Durchführung der praktischen Prüfungen sollte durch einen Werkssachverständigen erfolgen. Sie kann auch durch eine geeignete Prüfstelle erfolgen.

10.1.1.2 Typprüfungen für neu entwickelte oder modifizierte Geräte

(1) Für neu entwickelte oder modifizierte Einrichtungen ist durch eine Typprüfung die Einhaltung der im Datenblatt spezifizierten Eigenschaften nachzuweisen.

(2) Die Erstellung der Unterlagen für den theoretischen Teil der Typprüfungen soll durch den Hersteller erfolgen. Diese Unterlagen sollen der atomrechtlichen Behörde oder einem von ihr nach § 20 AtG zugezogenen Sachverständigen zur Prüfung vorgelegt werden. Das Prüfprogramm für den praktischen Teil der Typprüfungen soll vom Hersteller erstellt und mit der atomrechtlichen Behörde oder einem von ihr nach § 20 AtG zugezogenen Sachverständigen abgestimmt werden. Die Durchführung der praktischen Prüfungen sollte durch einen Werkssachverständigen erfolgen. Sie kann auch durch eine geeignete Prüfstelle erfolgen.

(3) Für Baugruppen der A- und B-Funktions-Einrichtungen ist die Typprüfung nach KTA 3503 durchzuführen. Für Messwertgeber und Messumformer der A- und B-Funktions-Einrichtungen ist die Typprüfung nach KTA 3505 durchzuführen.

10.1.1.3 Eignungsüberprüfung

Die anlagenbezogene Eignung betriebsbewährter Einrichtungen nach 5.1.1.1 (2) oder typgeprüfter Einrichtungen nach 10.1.1.1 oder 10.1.1.2 ist durch den Vergleich der Eigen-

schaften der Geräte mit den Anforderungen nach den Abschnitten 4 und 5 und für Gefahrenmeldeeinrichtungen der Klasse S nach 9.2 nachzuweisen.

Hinweis:

Die Eignungsüberprüfung kann zu dem Ergebnis führen, dass zusätzlich zur Typprüfung nach 10.1.1.1 oder 10.1.1.2 weitere praktische oder theoretische Prüfungen erforderlich sind.

10.1.2 Werksprüfungen

Die ordnungsgemäße Herstellung der leittechnischen Baugruppen, Geräte und Systemteile ist durch eine Werksprüfung nachzuweisen.

Hinweis:

Anforderungen an Werksprüfungen werden in der KTA 3507 behandelt.

10.1.3 Systemprüfungen

Die Systemprüfungen sind nach KTA 3506 durchzuführen.

10.2 Prüfungen an Gefahrenmeldeeinrichtungen der Klasse I

(1) Für die Gefahrenmeldeeinrichtungen der Klasse I sind Werksprüfungen durchzuführen.

Hinweis:

Anforderungen an Werksprüfungen werden in der KTA 3507 behandelt.

(2) Für die Gefahrenmeldeeinrichtungen der Klasse I sind Systemprüfungen nach KTA 3506 durchzuführen.

11 Konfigurations- und Identifikations-Dokumentation

(1) Für ein Leittechniksystem ist eine Konfigurations- und Identifikations-Dokumentation zu erstellen, in der die dazugehörigen Hard- und Softwarekomponenten einschließlich deren Einstellungen sowie die Systemstruktur spezifiziert und identifizierbar sind.

(2) Die Anforderungen an die Konfigurations- und Identifikations-Dokumentation sind in der KTA 3506 festgelegt.

Anhang A

Bestimmungen, auf die in dieser Regel verwiesen wird

(Die Verweise beziehen sich nur auf die in diesem Anhang angegebene Fassung. Darin enthaltene Zitate von Bestimmungen beziehen sich jeweils auf die Fassung, die vorlag, als die verweisende Bestimmung aufgestellt oder ausgegeben wurde.)

AtG		Gesetz über die friedliche Verwendung der Kernenergie und den Schutz gegen ihre Gefahren (Atomgesetz – AtG) in der Fassung der Bekanntmachung vom 15. Juli 1985 (BGBl. I S. 1565), zuletzt geändert durch Artikel 307 der Verordnung vom 31. August 2015 (BGBl. I 2015, Nr. 35, S. 1474)
StrlSchV		Verordnung über den Schutz vor Schäden durch ionisierende Strahlen (Strahlenschutzverordnung – StrlSchV)) vom 20. Juli 2001 (BGBl. I S. 1714; 2002 I S. 1459), zuletzt geändert durch Artikel 5 der Verordnung vom 11. Dezember 2014 (BGBl. I S. 2010)
SiAnf	(2015-03)	Sicherheitsanforderungen an Kernkraftwerke in der Fassung der Bekanntmachung vom 3. März 2015 (BAnz AT 30.03.2015 B2)
Interpretationen	(2015-03)	Interpretationen zu den Sicherheitsanforderungen an Kernkraftwerke vom 22. November 2012, geändert am 3. März 2015 (BAnz AT 30.03.2015 B3)
SEWD Richtlinie IT	(2013-07)	„Richtlinie für den Schutz von IT-Systemen in kerntechnischen Anlagen und Einrichtungen der Sicherungskategorien I und II gegen Störmaßnahmen oder sonstige Einwirkungen Dritter (SEWD-Richtlinie IT)" Gemeinsames Ministerialblatt, Ausgabe Nr. 36/2013 vom 08.07.2013, Bekanntmachung des BMUB
KTA 1401	(2013-11)	Allgemeine Anforderungen an die Qualitätssicherung
KTA 1403	(2010-11)	Alterungsmanagement in Kernkraftwerken
KTA 2101.3	(2015-11)	Brandschutz in Kernkraftwerken; Teil 3: Brandschutz an maschinen- und elektrotechnischen Anlagen
KTA 2201.4	(2012-11)	Auslegung von Kernkraftwerken gegen seismische Einwirkungen; Teil 4: Anlagenteile
KTA 3503	(2015-11)	Typprüfung von elektrischen Baugruppen der Sicherheitsleittechnik
KTA 3504	(2015-11)	Elektrische Antriebe des Sicherheitssystems in Kernkraftwerken
KTA 3505	(2015-11)	Typprüfung von Messwertgebern und Messumformern der Sicherheitsleittechnik
KTA 3506	(2012-11)	Systemprüfung der Sicherheitsleittechnik von Kernkraftwerken
KTA 3507	(2014-11)	Werksprüfungen, Prüfungen nach Instandsetzung und Nachweis der Betriebsbewährung der Baugruppen und Geräte der Sicherheitsleittechnik
KTA 3601	(2005-11)	Lüftungstechnische Anlagen in Kernkraftwerken
KTA 3701	(2014-11)	Übergeordnete Anforderungen an die elektrische Energieversorgung in Kernkraftwerken
KTA 3702	(2014-11)	Notstromerzeugungsanlagen mit Dieselaggregaten in Kernkraftwerken
KTA 3703	(2012-11)	Notstromerzeugungsanlagen mit Batterien und Gleichrichtergeräten in Kernkraftwerken
KTA 3704	(2013-11)	Notstromanlagen mit statischen und rotierenden Umformern in Kernkraftwerken
KTA 3705	(2013-11)	Schaltanlagen, Transformatoren und Verteilungsnetze zur elektrischen Energieversorgung des Sicherheitssystems in Kernkraftwerken
KTA 3706	(2000-06)	Sicherstellung des Erhalts der Kühlmittelverlust-Störfallfestigkeit von Komponenten der Elektro- und Leittechnik in Betrieb befindlicher Kernkraftwerke
KTA 3904	(2007-11)	Warte, Notsteuerstelle und örtliche Leitstände in Kernkraftwerken
DIN EN 61192-1	(2003-11)	Anforderungen an die Ausführungsqualität von Lötbaugruppen - Teil 1: Allgemeines (IEC 61192-1:2003); Deutsche Fassung EN 61192-1:2003
DIN EN 62340 (VDE 0491-10)	(2010-12)	Kernkraftwerke - Leittechnische Systeme mit sicherheitstechnischer Bedeutung - Anforderungen zur Beherrschung von Versagen aufgrund gemeinsamer Ursache (IEC 62340:2007); Deutsche Fassung EN 62340:2010
DIN EN 62138 (VDE 0491-3-3)	(2010-03)	Kernkraftwerke - Leittechnik für Systeme mit sicherheitstechnischer Bedeutung - Softwareaspekte für rechnerbasierte Systeme zur Realisierung von Funktionen der Kategorien B oder C (IEC 62138:2004); Deutsche Fassung EN 62138:2009