

**Reaktorschutzsystem und Überwachungs-
einrichtungen des Sicherheitssystems****DIN**
25 434

Reactor protection system and monitoring equipment of the safety system

Ersatz für Ausgabe 10.77

Diese Norm ist wortgleich mit KTA 3501, Ausgabe Juni 1985. Die KTA-Regel wurde im Auftrag des Kerntechnischen Ausschusses vom Normenausschuß Kerntechnik im DIN vorbereitet.

Inhalt

	Seite		Seite
Grundlagen	2	5 Aufbau von Reaktorschutzsystemen	16
1 Anwendungsbereich	2	5.1 Gerätequalität	16
2 Begriffe	2	5.2 Umgebungseinflüsse	16
3 Ermittlung der Aufgabenstellung für das Reaktorschutzsystem	5	5.3 Räumliche Anordnung, Trennung zueinander redundanter Einrichtungen	17
3.1 Grundsätzliche Anforderungen	5	5.4 Mechanischer Aufbau	17
3.2 Ereignisabläufe und ihre Auswirkungen	5	5.5 Aufbau von Schutzuntersystemen	18
3.3 Ausgangszustand der Anlage	6	5.6 Schaltung	19
3.4 Erfassung der Störfälle	6	6 Aggregatschutz	19
4 Auslegungsgrundlagen für das Reaktorschutzsystem	6	7 Zustandsbegrenzungen	19
4.1 Grundsätzliche Anforderungen	6	8 Lüftungstechnische Anlagen zur Kühlung des Reaktorschutzsystems	19
4.2 Versagensauslösende Ereignisse	6	9 Elektrische Energieversorgung	20
4.3 Auslegung gegen versagensauslösende Ereignisse außerhalb der Reaktoranlage	6	10 Gefahrenmeldeeinrichtungen	20
4.4 Ausfallkombinationen	6	10.1 Allgemeines	20
4.5 Anregung von Schutzaktionen	13	10.2 Gefahrenmeldeeinrichtungen der Klasse S	20
4.6 Redundanz und Unabhängigkeit	13	10.3 Gefahrenmeldeeinrichtungen der Klasse I	21
4.7 Trennung des Reaktorschutzsystems von anderen Systemen	13	11 Prüfungen	21
4.8 Betrieb des Reaktorschutzsystems bei Instandhaltungsarbeiten	14	11.1 Prüfungen am Reaktorschutzsystem und an Gefahrenmeldungen der Klasse S	21
4.9 Abstimmung zwischen dem Reaktorschutz- system und den aktiven Sicherheitsein- richtungen	14	11.2 Prüfungen an Gefahrenmeldeeinrichtungen der Klasse I	21
4.10 Überwachung auf Funktionsbereitschaft und Prüfbarkeit	14	12 Zusammenstellung der im atomrechtlichen Genehmigungs- und Aufsichtsverfahren für das Reaktorschutzsystem zur Prüfung erforderlichen Informationen	22
4.11 Schutzbegrenzungen	15	Anhang A: Bestimmungen, auf die in dieser Norm verwiesen wird (Verwiesene Bestimmungen gelten nur in der in diesem Anhang angegebenen Fassung).	22
4.12 Funktionsgruppensteuerungen des Reaktorschutzsystems	15	Stichwortverzeichnis	23
4.13 Ermittlung der Grenzwerte zur Auslösung von Schutzaktionen	15		
4.14 Handeingriffe	15		

Fortsetzung Seite 2 bis 24

Normenausschuß Kerntechnik (NKe) im DIN Deutsches Institut für Normung e.V.
Deutsche Elektrotechnische Kommission im DIN und VDE (DKE)

Grundlagen

(1) KTA-Regeln, die zum Teil auch als DIN-Normen herausgegeben werden, 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 getroffen ist (Atomgesetz § 7 (2) 3), um insbesondere die im Atomgesetz und der Strahlenschutzverordnung festgelegten Schutzziele zu erreichen.

(2) Basierend auf den Abschnitten 2.1 „Qualitätsgewährleistung“, 2.2 „Prüfbarkeit“, 5.1 „Überwachungs- und Meldeeinrichtungen“ und 6.1 „Reaktorschutzsystem“ der „Sicherheitskriterien für Kernkraftwerke“ des Bundesministers des Innern wird in dieser Norm festgelegt, welche Anforderungen an das Reaktorschutzsystem und an die Überwachungseinrichtungen des Sicherheitssystems zu stellen sind.

(3) Die vorliegende Norm wird durch die Regeln KTA 3503 „Typprüfung von elektrischen Baugruppen des Reaktorschutzsystems“, KTA 3504 (= DIN 44 834 (z. Z. Entwurf)) „Elektrische Antriebe des Sicherheitssystems in Kernkraftwerken“, KTA 3505 (= DIN 44 835) „Typprüfung von Meßwertgebern und Meßumformern des Reaktorschutzsystems“, KTA 3506 (= DIN 44 836) „Systemprüfung der leittechnischen Einrichtungen des Sicherheitssystems“ und KTA 3507 (= DIN 44 837 (z. Z. Entwurf)) „Werksprüfungen an leittechnischen Baugruppen, Geräten und Systemteilen des Sicherheitssystems“ ergänzt.

(4) Zusätzlich zu Abschnitt 9 wird die elektrische Energieversorgung des Sicherheitssystems in den Normen KTA 3701 bis KTA 3705 (= DIN 25 417 Teil 1 bis DIN 25 469) geregelt.

(5) Zusätzlich zu Abschnitt 8 sind die Anforderungen an Lüftungstechnische Anlagen zur Kühlung des Reaktorschutzsystems im Regelvorhaben KTA 3601 (= DIN 25 414) „Lüftungstechnische Anlagen in Kernkraftwerken“ enthalten.

(6) Die Anforderungen an den „Nachweis der Beständigkeit von elektrischen Einrichtungen unter Störfallbedingungen“ werden im Regelvorhaben KTA 3706 behandelt. Die Ergebnisse dieses Regelvorhabens stehen im Zusammenhang mit den Regeln KTA 3503 und KTA 3505 (= DIN 44 835) (siehe Absatz (3)).

(7) Weiter gilt zur Erfüllung der Anforderungen an die Qualitätssicherung übergeordnet die Regel KTA 1401.

(8) In dieser Norm wird die Einhaltung der konventionellen Vorschriften und Normen (z. B. Unfallverhütungsvorschriften, DIN-Normen und VDE-Bestimmungen) vorausgesetzt, wenn nicht kernkraftwerksspezifisch bedingt, andere Anforderungen gestellt werden.

1 Anwendungsbereich

(1) Diese Norm ist auf das Reaktorschutzsystem und die Überwachungseinrichtungen des Sicherheitssystems von ortsfesten Kernkraftwerken anzuwenden.

(2) Diese Norm regelt Aufbau, Ausführung, Gerätequalität, Einbau und Prüfung des Reaktorschutzsystems und dessen Komponenten. Sie enthält eine Zusammenstellung von Auslegungskriterien, Anforderungen an die Qualität und Qualitätssicherung und Anforderungen an die Funktionsweise des Reaktorschutzsystems.

(3) In dieser Norm werden Grundanforderungen an die Protokolliereinrichtungen, Gefahrenmeldeeinrichtungen der Klasse I, Zustandsbegrenzungen, Sicherheitsgefahrenmeldungen und Aggregatschutzeinrichtungen, deren Signale Vorrang vor den Signalen des Reaktorschutzsystems haben, gestellt. Spezielle Auslegungsanforderungen an diese Einrichtungen sind nicht Bestandteil dieser Norm.

(4) Nicht zum Anwendungsbereich dieser Norm gehören
a) der nur im bestimmungsgemäßen Betrieb benötigte Teil der Steuerungen, die Betriebsverriegelungen, die Betriebsbegrenzungen und die Gefahrenmeldeeinrichtungen der Klasse II,

b) die Einrichtung des Aggregatschutzes, deren Signale keinen Vorrang vor Signalen des Reaktorschutzsystems haben,

Hinweis: Anforderungen an diese Einrichtungen werden in den Regelvorhaben KTA 3504 (= DIN 44 834 (z. Z. Entwurf)) und KTA 3705 (= DIN 25 469) behandelt.

c) die elektrischen Antriebe, die Leistungskabel und die Schaltanlagenabzweige einschließlich der Steuerstromkreise.

Hinweis: Anforderungen an diese Einrichtungen werden in den Regelvorhaben KTA 3701 bis KTA 3705 gestellt.

2 Begriffe

(1) Aggregatschutz

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

(2) Anregeebe

Die Anregeebe ist der Teil des Reaktorschutzsystems, in dem alle Anregekanalgruppen zusammengefaßt sind.

(3) 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 Grenzsinalgeber-Ausgang.

(4) Anregekanalgruppe

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

(5) Anregekriterium

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

(6) Anregesignal

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

(7) Ansprechverzögerung

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

(8) Antivalenzüberwachung

Die Antivalenzüberwachung ist eine Einrichtung, die binäre Signale auf Eindeutigkeit (z. B. Unterbrechung oder Kurzschluß) überwacht.

(9) Ausfall

Der Ausfall ist das Versagen einer Komponente derart, daß sie eine oder mehrere Auslegungsanforderungen nicht mehr erfüllen kann.

(10) Ausfall, systematischer

Der systematische Ausfall ist das Versagen von Komponenten aufgrund der gleichen Ursache.

Hinweis: Er kann z. B. durch falsche Auslegung, Fehler in einer Fertigungsreihe, falsche Betriebsweise, Wassereintrich, Brand in der Anlage hervorgerufen werden.

(11) Auslösesignal

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

(12) Bestimmungsgemäßer Betrieb

- a) Betriebsvorgänge, für die die Anlage bei funktionsfähigem Zustand der Systeme (ungestörter Zustand) bestimmt und geeignet ist (Normalbetrieb);
- b) Betriebsvorgänge, die bei Fehlfunktion von Anlage-teilen oder Systemen (gestörter Zustand) ablaufen, soweit hierbei einer Fortführung des Betriebs sicherheitstechnische Gründe nicht entgegenstehen (anomaler Betrieb);
- c) Instandhaltungsvorgänge (Inspektion, Wartung, Instandsetzung).

(13) Betriebsbegrenzung

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

(14) Betriebssystem

Das Betriebssystem umfaßt alle Einrichtungen, Kreisläufe und Hilfsanlagen, die nur für den bestimmungsgemäßen Betrieb notwendig sind.

(15) Betriebsverriegelung

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

(16) Einzelantriebssteuerung

Die Einzelantriebssteuerung ist die einem einzelnen Antrieb zugeordnete Steuereinrichtung.

Hinweis: In dieser Norm werden die Anforderungen an Einzelantriebssteuerungen des Reaktorschutzes behandelt (einschließlich Koppelrelais). Die Anforderungen an die anschließenden Steuerstromkreise werden im Regelvorhaben KTA 3705 behandelt.

(17) Fehlauflösung

Die Fehlauflösung ist die Auflösung eines Signals, die aufgrund des Anlagenzustands nicht gerechtfertigt war.

(18) Folgeausfall

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

(19) 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: In dieser Norm werden nur Anforderungen an Funktionsgruppensteuerungen des Reaktorschutzes gestellt.

(20) 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.

(21) Gefahrenmeldung der Klasse I

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

(22) Gefahrenmeldung der Klasse II

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

(23) Gerätediversität

Die Gerätediversität ist die Verwendung redundanter Geräte unterschiedlicher Bauart oder Wirkungsweise.

(24) 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.

(25) Grenzsinal

Das Grenzsinal ist das Ausgangssignal eines Grenzsinalgebers.

(26) Grenzsinalgeber

Der Grenzsinalgeber ist ein Gerät, das den Wert einer Sicherheitsvariablen mit einem festen oder variablen Grenzwert vergleicht. Wird der Grenzwert überschritten, ändert sich das Ausgangssignal sprunghaft.

(27) Grenzwert des Grenzsinalgebers

Der Grenzwert des Grenzsinalgebers ist der in einem Grenzsinalgeber eingestellte Wert.

(28) Instandhaltung

Die Instandhaltung ist die Gesamtheit der Maßnahmen zur Bewahrung und Wiederherstellung des Sollzustandes sowie zur Feststellung und Beurteilung des Istzustandes. Die Instandhaltung gliedert sich in Instandsetzung, Wartung und Inspektion.

(29) Logikebene

Die Logikebene ist der Teil des Reaktorschutzesystems, in dem die Verknüpfung der Anreagesignale und die Wertung der Anreagekriterien vorgenommen werden.

(30) Logische Verknüpfung

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

Hinweis: Logische Verknüpfungen sind z. B. UND, ODER.

(31) 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.

(32) Prozeßvariable

Die Prozeßvariable ist eine unmittelbar im Prozeß meßbare chemische oder physikalische Größe.

(33) Reaktorschutzsystem

Das Reaktorschutzsystem ist der Teil des Sicherheitssystems, welcher die für die Sicherheit der Reaktoranlage und Umgebung wesentlichen Prozeßvariablen zur Vermeidung von unzulässigen Beanspruchungen und zur Erfassung von Störfällen überwacht, verarbeitet und Schutzaktionen auslöst, um den Zustand der Reaktoranlage in sicheren Grenzen zu halten.

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.

Das Reaktorschutzsystem umfaßt als Teil des Sicherheitssystems einer Reaktoranlage alle Geräte und Einrichtungen der Meßwerterfassung, der Signalaufbereitung, der Logikebene und den den Einzelantrieben zugeordneten Teilen der Steuerung zur Auslösung von Schutzaktionen sowie die Funktionsgruppensteuerungen.

(34) 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.

(35) Redundanz

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

Hinweis: In dieser Norm wird die Forderung nach Redundanz als erfüllt angesehen, wenn gleichartige technische Mittel eingesetzt werden.

(36) Redundanzgruppe

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

(37) Rückwirkungsfreiheit

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

Hinweis: Störungen können zum Beispiel Kurzschluß, Überspannung, Erdschluß, Unterbrechung sein.

(38) Schutzaktion

Die Schutzaktion ist die Betätigung oder der Betrieb von aktiven Sicherheitseinrichtungen, die zur Beeinflussung von Störfallabläufen und zur Minderung von Schadensauswirkungen erforderlich sind.

(39) Schutzaktion, eindeutig sicherheitsgerichtete

Die eindeutig sicherheitsgerichtete Schutzaktion ist eine Schutzaktion, die bei Fehlauslösung keine andere Schutzaktion verhindern kann.

Hinweis: Eine Reaktorschnellabschaltung ist in diesem Sinne eine eindeutig sicherheitsgerichtete Schutzaktion.

(40) Schutzaktion, nicht eindeutig sicherheitsgerichtete

Die nicht eindeutig sicherheitsgerichtete Schutzaktion ist eine Schutzaktion, die bei Fehlauslösung andere Schutzaktionen verhindern kann.

(41) Schutzbegrenzung

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

(42) Schutzteilaktion

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

(43) Schutzteilsystem

Das Schutzteilsystem ist der Teil des Reaktorschutzsystems, der zur Auslösung einer Schutzteilaktion benötigt wird.

Hinweis: Ein Schutzteilsystem ist z. B. der Teil des Reaktorschutzsystems, der zum Einschalten einer von mehreren zueinander redundanten Pumpen benötigt wird.

(44) Schutzüberbrückung

Die Schutzüberbrückung ist die Maßnahme, durch die eine Funktion des Reaktorschutzsystems in Abhängigkeit vom Betriebszustand geändert wird.

Hinweis: Die Schutzüberbrückungen werden in der Logikebene oder in der Steuerebene vorgenommen.

Beispiele für Schutzüberbrückungen sind: Steuerstabsausfahrverbote bei Nichtvorhandensein einer Mindestanzeige der Neutronenflußdichte im Anfahrbereich oder in den eingestellten Meßbereichen des linearen Mehrbereichskanals, Überbrückungen von Anregekriterien.

(45) Schutzuntersystem

Das Schutzuntersystem ist ein Teil des Reaktorschutzsystems, der aufgrund seiner Wirkungsweise eine Einheit bildet.

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

(46) 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.

(47) Selbstüberwachung

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

(48) Sicherheitsabstand

Der Sicherheitsabstand ist die Differenz zwischen dem am Grenzsignalgeber eingestellten Grenzwert und dem

bei der Störfallanalyse festgelegten Gefährdungsgrenzwert.

(49) 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.

(50) 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.

(51) Sicherheitsteileinrichtung

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

(52) 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.

(53) Steuerebene

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

(54) Störfall

Ein Störfall ist ein Ereignisablauf, bei dessen Eintreten der Betrieb der Anlage oder die Tätigkeit aus sicherheitstechnischen Gründen nicht fortgeführt werden kann und für den die Anlage ausgelegt ist oder für den bei der Tätigkeit vorsorglich Schutzvorkehrungen vorgesehen sind.

Hinweis: Für Anlagen nach § 7 Atomgesetz ist unter „Störfall“ ein Ereignisablauf zu verstehen, bei dessen Eintreten der Betrieb der Anlage aus sicherheitstechnischen Gründen nicht fortgeführt werden kann und für den die Anlage ausgelegt ist.

(55) Störung

Die Störung ist das Fehlverhalten eines Bauelements, einer Komponente oder eines Systems.

(56) Vergleich

Der Vergleich ist eine Einrichtung, die die Meßwerte zweier Sicherheits- oder Prozeßvariablen miteinander vergleicht und bei vorgegebener Abweichung ein Binärsignal ausgibt.

(57) Vorrangsteuerung

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

(58) Wächter

Der Wächter ist eine binäre Meßeinrichtung, die aus einer Prozeßvariablen ohne Zwischenschaltung eines Grenzsinalgebers eine binäre Information ausgibt.

Hinweis: Ein Beispiel für einen Wächter ist ein Druckwächter.

(59) Werkssachverständiger

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

(60) Zufallsausfall

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

(61) Zustandsbegrenzungen

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

Hinweis: Hierunter fällt z. B. die Begrenzung der Reaktorleistung auf einen Wert, der als Ausgangszustand für die Analyse des Kühlmittelverluststörfalls zugrundegelegt wurde.

3 Ermittlung der Aufgabenstellung für das Reaktorschutzsystem

3.1 Grundsätzliche Anforderungen

Zur Ermittlung der Aufgaben, die das Reaktorschutzsystem zu erfüllen hat, ist eine Analyse der in Abschnitt 3.2 genannten Ereignisabläufe der Anlage vorzunehmen. Die Analyse der Ereignisabläufe ist unter Anwendung rechnerischer Verfahren, experimenteller Methoden oder von Plausibilitätsbetrachtungen durchzuführen. Die für die Analyse getroffenen Annahmen müssen begründet werden. Das Ergebnis der Analyse muß alle für die Auslegung des Reaktorschutzsystems notwendigen Aussagen liefern. Bei dieser Analyse sind auch die Auswirkungen der Fehlauflösungen nach Abschnitt 4.4.4 zu beachten.

Hinweis: Durch technische Maßnahmen außerhalb des Reaktorschutzsystems kann die Eintrittswahrscheinlichkeit bestimmter Ereignisabläufe so weit herabgesetzt werden, daß sie zur Auslegung des Reaktorschutzsystems und der aktiven Sicherheitseinrichtungen nicht herangezogen werden müssen.

3.2 Ereignisabläufe und ihre Auswirkungen

(1) Es sind Ereignisabläufe folgender Art in Betracht zu ziehen:

- a) Ereignisabläufe mit Freisetzung unzulässiger Wärmeenergie im Reaktor,
- b) Ereignisabläufe mit Beeinträchtigung der Wärmeabfuhr aus dem Reaktor,
- c) Ereignisabläufe mit Aktivitätsfreisetzung.

Hinweis: Die unter a) bis c) aufgeführten Ereignisabläufe können zum Teil durch Einwirkungen von außen hervorgerufen werden.

Dabei ist insbesondere das Vorwort zu den „Störfall-Leitlinien“ zu beachten.

(2) Dabei sind die nachfolgend genannten Freisetzungen in ihrer Auswirkung nicht tolerierbar, wenn diese Freisetzungen über festgelegte Werte hinausgehen oder wenn

sie mittelbar Ereignisabläufe mit gleichen Folgen auslösen können:

- a) Freisetzung von radioaktiven Stoffen oder Wärmeenergie aus den Brennelementen in das Kühlmittel,
- b) Freisetzung von radioaktiven Stoffen oder Wärmeenergie aus dem Kernkühlmitteleinschluß in das Reaktorgebäude,
- c) Freisetzung von radioaktiven Stoffen aus dem Reaktorgebäude in die Umgebung,
- d) Freisetzung toxischer, brennbarer oder explosibler Stoffe.

(3) Neben den Ereignisabläufen der genannten Art 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. Diese Ausgangszustände ergeben sich aus quasistationären Betriebszuständen zuzüglich möglicher Abweichungen der Meßwerte der Prozeßvariablen vom Sollwert überlagert durch eine quasistationäre Abweichung der Prozeßvariablen infolge eines einzelnen Zufallsausfalls innerhalb der Gesamtheit des Meß-, Steuer- oder Regelsystems, die Einfluß auf die entsprechenden Betriebsgrößen haben.

3.4 Erfassung der Störfälle

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

(2) Für jeden vom Reaktorschutzsystem zu beherrschenden Störfall sollen mindestens zwei physikalisch unterschiedliche Anregekriterien herangezogen werden (siehe Abschnitt 4.5.2, Absatz (1)). Für jedes Anregekriterium ist eine eigene Analyse der Ereignisabläufe nach Abschnitt 3.1 durchzuführen.

(3) Der Ablauf der Schutzaktionen ist unter Berücksichtigung der Ansprechverzögerung und der Genauigkeit der Anregekanäle für das erste und zweite Anregekriterium zu analysieren und die Auswirkung auf den Ablauf der Störfälle ist aufzuzeigen.

(4) Bei Verwendung gemeinsamer Prozeßvariablen für Steuerung, Regelung und Reaktorschutz sind Analysen für Störungen in der Meßwerterfassung unter Berücksichtigung der Absätze (1) und (2), Abschnitt 3.4, durchzuführen.

Hinweis: Bei diesen Analysen wird betrachtet, daß als Folge eines systematischen Ausfalls alle gleichartigen Geräte eines Fabrikats in den Signalkanälen gleichzeitig und gleichsinnig versagen.

Auf diese Analysen darf verzichtet werden, wenn bei Einsatz diversitärer Meßeinrichtungen für die Steuerung und Regelung einerseits und das Reaktorschutzsystem andererseits ein systematischer Ausfall dieser Meßeinrichtungen nicht unterstellt werden muß.

4 Auslegungsgrundlagen für das Reaktorschutzsystem

4.1 Grundsätzliche Anforderungen

(1) Es ist nachzuweisen, daß das Reaktorschutzsystem im Zusammenwirken mit aktiven und passiven Sicherheitseinrichtungen so ausgelegt, ausgeführt und betrieben wird, daß nichttolerierbare Auswirkungen der Störfälle verhindert werden. Dabei sind die unter Abschnitt 4.2 beschriebenen versagenauslösenden Ereignisse gleichzeitig mit dem Störfall, jedoch unabhängig vom Störfall zu unterstellen.

(2) Aus diesen versagenauslösenden Ereignissen resultierende Ausfälle sind nach Abschnitt 4.4 zu kombinieren, wenn sie nicht durch technische Maßnahmen ausgeschlossen werden können.

Hinweis: Es ist zulässig, diesen Nachweis für die Gesamtheit aller Komponenten des Sicherheitssystems gemeinsam zu erbringen.

4.2 Versagenauslösende Ereignisse

4.2.1 Versagenauslösende Ereignisse innerhalb des Reaktorschutzsystems

Es sind versagenauslösende Ereignisse innerhalb des Reaktorschutzsystems in Betracht zu ziehen, wie zum Beispiel

- a) Ausfälle durch Kurzschlüsse, Unterbrechungen, Erdschlüsse, Spannungs- und Frequenzänderungen, mechanisches Versagen oder Brände,
- b) mehrere gleichzeitig oder kurzzeitig aufeinander folgende Ausfälle nach a), die eine gemeinsame Ursache (z. B. Fertigungsfehler, Auslegungsfehler, Drift) im System selbst haben,
- c) Fehler bei Bedienung und Wartung des Reaktorschutzsystems durch das Personal.

4.2.2 Versagenauslösende Ereignisse innerhalb der Reaktoranlage

Es sind versagenauslösende Ereignisse innerhalb der Reaktoranlage im Rahmen des „Einzelfehlerkonzept“ in Betracht zu ziehen.

Hinweis: Siehe „Interpretationen zu den Sicherheitskriterien für Kernkraftwerke, Einzelfehlerkonzept“.

Beispiele für versagenauslösende Ereignisse innerhalb der Reaktoranlage sind: Brand, Wassereinbruch, schlagende Rohrleitung, Bruchstücke einer versagenden Komponente, mechanische Strahlwirkung von Medien wie Dampf, Wasser, Flüssigmetall, Gas und Öl.

4.3 Auslegung gegen versagenauslösende Ereignisse außerhalb der Reaktoranlage

Gegen Ereignisse wie Überflutung, Blitz, Sturm und Erdbeben sind ausreichende Vorsorgemaßnahmen als getroffen nachzuweisen, so daß durch diese Ereignisse die Funktion des Reaktorschutzsystems nicht unzulässig beeinträchtigt wird.

4.4 Ausfallkombinationen

4.4.1 Grundannahmen

(1) Folgende Ausfälle sind zu betrachten:

- a) Zufallsausfall

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

(2) Es ist nachzuweisen, daß das Reaktorschutzsystem im Zusammenwirken mit aktiven und passiven Sicherheitseinrichtungen zusätzlich zum Störfall

- a) einen Zufallsausfall Z,
- b) und einen systematischen Ausfall (soweit er nicht nach Absatz (5) ausgeschlossen werden kann) S,
- c) und Folgeausfälle F beherrscht.

(3) Während des bestimmungsgemäßen Betriebs der Reaktoranlage ist die Ausfallkombination nach Bild 4-1 bezüglich eintretender Störfälle zu beherrschen, wobei im Instandhaltungsfall (I) nicht angenommen werden muß, daß während einer Zeitspanne von 100 h der systematische Ausfall (S) und der Zufallsausfall (Z) gleichzeitig auftreten. Der Instandsetzungsfall beginnt mit der Erkennung des Ausfalls.

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

(5) Die Auswirkungen systematischer Ausfälle im Reaktorschutzsystem sind zu analysieren. Abhängig vom Ergebnis der Analysen sind zusätzliche Maßnahmen zur Minderung der Eintrittswahrscheinlichkeit systematischer Ausfälle oder der Auswirkungen zu treffen.

Hinweis: Die Eintrittswahrscheinlichkeit systematischer Ausfälle kann zum Beispiel durch die Auswahl geeigneter Gerätesysteme, Prüfzyklen, Grenzbelastungsprüfungen so weit herabgesetzt werden, daß die systematischen Ausfälle in der Ausfallkombination nach Abschnitt 4.4.1, Absatz (2), nicht mehr betrachtet zu werden brauchen. Die Minderung der Auswirkungen kann zusätzliche Maßnahmen außerhalb des Reaktorschutzsystems erfordern.

4.4.2 Schutzvollaktion

Die Auslösung der Schutzvollaktion muß bei den Grundannahmen nach Abschnitt 4.4.1 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.

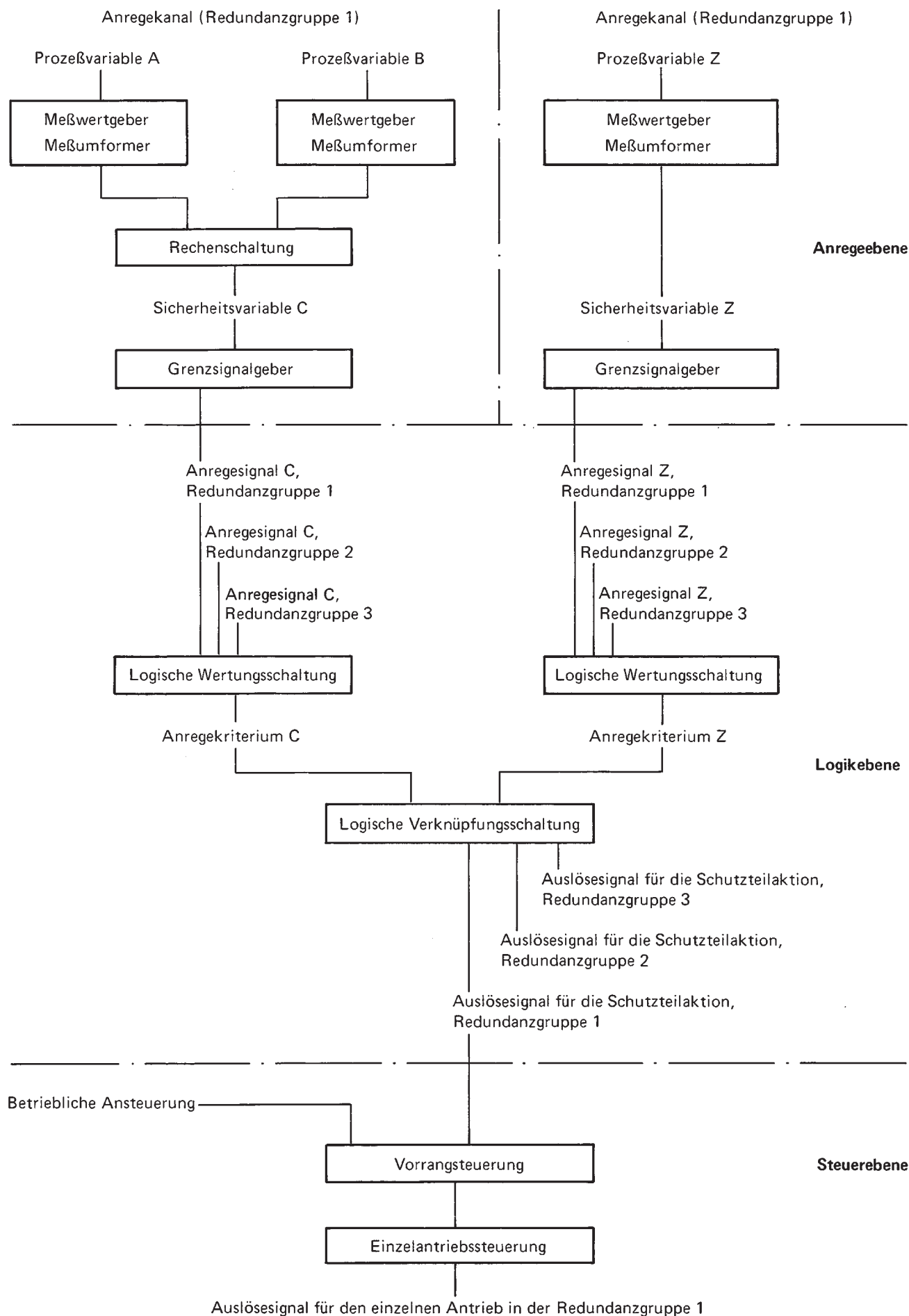


Bild 2-1. Beispielhafte Zuordnung von Begriffen zum funktionellen Aufbau des Reaktorschutzsystems