KTA KERNTECHNISCHER AUSSCHUSS

Bericht zum Regelvorhaben KTA 1407: Methoden zur Ermittlung von zulässigen Instandhaltungszeiten in Kernkraftwerken

(KTA-Dok.-Nr. 1407/87/1)

KTA-GS-55

Juni 1989

Bearbeiter: G. Pommerehne
Dr. G. Roos

GESCHÄFTSSTELLE DES KERNTECHNISCHEN AUSSCHUSSES (KTA)

beim BUNDESAMT FÜR STRAHLENSCHUTZ

Postfach 10 01 49
38201 Salzgitter

Telefon: 03018/333-1621
Telefax: 03018/333-1625
Email: ahihn@bfs.de

Bericht zum Regelvorhaben KTA 1407: Methoden zur Ermittlung von zulässigen Instandhaltungszeiten in Kernkraftwerken

Inhalt

Vorbemerkung

Im Auftrag des Kerntechnischen Ausschusses wurde unter der Federführung des Technischen Überwachungsvereins Stuttgart e.V. der Entwurf der Regel KTA 1407 "Methoden der Ermittlung von zulässigen Instandhaltungszeiten in Kernkraftwerken" von einem Arbeitsgremium vorbereitet. Im Laufe der Arbeiten am Regelentwurf kam der für dieses Regelvorhaben zuständige KTA-Unterausschuss Sicherheitstechnische Grundsatzfragen (SUA) zu der Auffassung, dass von einer Weiterverfolgung und Aufstellung als Regel Abstand genommen werden sollte. Der erarbeitete Sachstand sollte dokumentiert werden. Der Kerntechnische Ausschuss machte sich diese Auffassung zu eigen und beschloss am 20.09.1988 die Einstellung dieses Regelvorhabens. Die bisherigen Arbeitsergebnisse sollten in einem Sachstandsbericht dokumentiert werden. Dieser Bericht ist vom Arbeitsgremium KTA 1407 erarbeitet worden und er wird hie mit auftragsgemäß vorgelegt.

Köln, den 30. Juni 1989

KTA-Dok.-Nr. 1407/87/1

1 Einleitung

1.1 Auftrag des KTA

(1) Im Auftrag des KTA hatte das Arbeitsgremium KTA 1407 unter der Federführung des TÜV Stuttgart einen Vorbericht zum Thema "Ermittlung der zulässigen Reparaturzeiten für Sicherheitssysteme" angefertigt. Der Vorbericht ist vom Unterausschuss SICHERHEITS-TECHNISCHE GRUNDSATZFRAGEN (SUA) ausführlich am 9. März, 20. April und 12. Mai 1982 beraten worden. Die dabei gegebenen Anregungen wurden in die dem KTA im Juni 1982 vorgelegte Fassung des Vorberichts (Mai 1982) eingearbeitet.

(2) Folgende Punkte ergaben die Beratungen. Eine künftige Regel KTA 1407 soll dazu dienen, die in den Betriebshandbüchern bisher niedergelegten Instandsetzungszeiten in künftigen Fällen zu vereinheitlichen. Sehr deutlich wurde darauf hingewiesen, dass in der künftigen Regel nicht bestimmte Zahlenwerte für zulässige Instandhaltungszeiten der betroffenen Systeme angegeben werden sollen, sondern Methoden zu ihrer Ermittlung. Hierbei wurde der Begriff Methoden in einem weiten Sinn und nicht nur bezogen auf mathematische Verfahren verstanden. Diese Vorstellungen fanden später auch ihren Niederschlag im vom KTA geänderten Titel des Regelvorhabens "Methoden zur Ermittlung von zulässigen Instandhaltungszeiten in Kernkraftwerken".

(3) Im Vorbericht zu KTA 1407 (Mai 1982) ist das geplante Vorgehen bei der Regelerstellung zusammengefasst. Wichtige Punkte sind:

"Diese Regel hat die in den Interpretationen der Sicherheitskriterien geforderte Festlegung von zulässigen Instandhaltungszeiten für sicherheitstechnisch wichtige Systeme und Maßnahmen bei Überschreiten fieser Zeiten zum Inhalt. Die Beschränkung dieser Zeiten dient im Verein mit anderen Maßnahmen dem Ziel, eine au reichende Zuverlässigkeit dieser Systeme sicherzustellen. Dabei werden folgende übergeordnete Gesichtspunkte berücksichtigt:

- Ist während der Instandhaltung das Einzelfehlerkonzept noch erfüllt, gelten Zeiten, die so festgelegt werden, dass sie bei entsprechender Instandhaltungsplanung z. B. Ersatzteilhaltung und Schichteinteilung in der Regel eingehalten werden können, dass andererseits die durch die Instandhaltung bedingte Nichtverfügbarkeit tolerierbar ist.
- Die Maßnahmen bei Überschreiten der zulässigen Instandhaltungszeiten dürfen nicht zu einer Anforderung des ausgefallenen Systems führen.
- Auch innerhalb der festgelegten Zeiten müssen die Instandhaltungsarbeiten mit angemessenem Aufwand so schnell wie möglich durchgeführt werden."

(4) Der KTA hat auf seiner 30. Sitzung am 22.6.1982 den Vorbericht als geeignet für die Vorbereitung eines Regelentwurfs angesehen und beschlossen, den TÜV Stuttgart zu beauftragen, federführend einen Regelentwurf KTA 1407 vorzubereiten und ein Jahr nach Aufnahme der I Arbeiten dem zuständigen Unterausschuss Bericht zu (erstatten. Als zuständig wurde vom KTA der Unterausschuss SICHERHEITSTECHNISCHE GRUNDSATZFRAGEN eingesetzt, der in Zusammenarbeit mit den Unterausschüssen BETRIEB, WÄRMEABFUHR UND SYSTEMTECHNIK, STARKSTROM sowie INSTRUMENTIERUNG UND REAKTORSCHUTZ den Regelentwurfsvorschlag KTA 1407 prüfen und eine Beschlussvorlage für den KTA erarbeiten soll (KTA-Beschluss-Nr. 30/4.2/1 und 2).

(5) Der Unterausschuss SICHERHEITSTECHNISCHE GRUNDSATZFRAGEN kam auf seiner Sitzung am 8.10.1985 zum Ergebnis, dass von einer Weiterverfolgung und Aufstellung als Regel

Abstand genommen werden sollte. Der erarbeitete Sachstand sollte dokumentiert werden. Die Sachstandsdokumentation ist Gegenstand dieses Berichts.

1.2 Grundlagen für die Festlegung von zulässigen Instandhaltungszeiten

(1) Die Zielsetzung für eine Festlegung von zulässigen Instandhaltungszeiten ist im Zitat aus dem Vorbericht, das in Abschnitt 1.1 Absatz 3 wiedergegeben ist, ausgedrückt. Die dort erwähnten Sicherheitskriterien für Kernkraftwerke enthalten Grundsätze für sicherheitstechnische Anforderungen, die der Auslegung von Kernkraftwerken zugrunde gelegt werden.

(2) In den Sicherheitskriterien für Kernkraftwerke wird gefordert, dass für Nachwärmeabfuhr nach Kühlmittelverlusten (Kriterium 4.3), Reaktorschutzsystem (Kriterium 6.1) und Notstromversorgung (Kriterium 7.1) zuverlässige Systeme zur Verfügung stehen müssen, für die auch während Instandhaltungsvorgängen das Einzelfehlerkonzept noch erfüllt sein muss.

(3) In den Interpretationen zu den Sicherheitskriterien für Kernkraftwerke; Einzelfehlerkonzept (GMBl. Nr. 13, 1984, Seite 208 bis 210) wird das Einzelfehlerkonzept noch genauer präzisiert. In diesem Zusammenhang sind folgende Präzisierungen für die Kriterien 4.2, 4.3, 6.1 und 7.1 sowie für die Sicherheitseinrichtungen zur Reaktorabschaltung und zur Nachwärmeabfuhr bei nicht verfügbarer Hauptwärmesenke und aktiven Einrichtungen des Sicherheitseinschlusses von Bedeutung:

a) Instandhaltungsvorgänge an Sicherheitseinrichtungen, während derer das betroffene Systemteil nicht funktionsbereit ist, sind ohne besondere, seine Funktion ersetzende oder seine Funktionsbereitschaft überflüssig machende Maßnahmen (z. B. Abschaltung, Leistungsminderung, Rückgriff auf andere Systeme) nur zulässig, wenn für die Dauer der Instandhaltungsvorgänge das Einzelfehlerkonzept erfüllt ist.

b) Das gilt nicht für Inspektionen, wenn die Funktionsbereitschaft des betroffenen Systemteils im Anforderungsfall rechtzeitig wieder hergestellt werden kann.

c) Während kurzzeitiger Wartungs- oder Instandsetzungsvorgänge braucht das zusätzliche Auftreten eines Einzelfehlers an Systemteilen ebenfalls nicht unterstellt zu werden, wenn wegen der Kürze der Wartungs- oder Instandsetzungsdauer die Zuverlässigkeit der betrachteten Sicherheitseinrichtung nicht wesentlich herabgesetzt wird.

Die ohne besondere Maßnahmen zulässigen Wartungs- und Instandsetzungszeiten (Zeit ab Schadenserkennung bis Abschluss der Instandsetzung) sowie festzulegende Inspektionskonzepte sind unter Verwendung der für die genannten Sicherheitseinrichtungen durchgeführten Zuverlässigkeitsanalysen (so weit erforderlich) und von Betriebserfahrungen so festzulegen, dass die Zuverlässigkeiten dieser Sicherheitseinrichtungen durch die Instandhaltungsvorgänge nicht unter die zur Störfallbeherrschung erforderlichen Zuverlässigkeiten herabgesetzt werden.

Bei anlageninternen Ereignissen mit sehr geringer Eintrittswahrscheinlichkeit, bei äußeren Einwirkungen mit sehr geringer Eintrittswahrscheinlichkeit und bei Ereignisketten mit sehr geringer Eintrittswahrscheinlichkeit, die keine Auslegungsstörfälle im Sinne des § 28 Abs. 3 StrlSchV sind, ist das gleichzeitige Auftreten eines Einzelfehlers nicht zu unterstellen; auch ein gleichzeitiger Instandsetzungsfall wird nicht postuliert.

(4) Der vorliegende Bericht hat die in den Interpretationen der Sicherheitskriterien geforderte Festlegung von zulässigen Instandhaltungszeiten für sicherheitstechnisch wichtige Systeme und Maßnahmen bei Überschreiten dieser Zeiten zum Inhalt. Die Festlegung dieser Zeiten dient im Verein mit anderen Maßnahmen dem Ziel, eine ausreichende Zuverlässigkeit dieser Systeme sicherzustellen. Dabei werden die übergeordneten Gesichtspunkte aus Abschnitt 1.1 Absatz 3 berücksichtigt.

(5) Bei der Bewertung der Instandsetzungen wird davon ausgegangen, dass Instandsetzungen im wesentlichen nach Ausfälle erforderlich sind und aufgrund der hohen Zuverlässigkeit der

Redundanten selten sind. Außerdem wird davon ausgegangen, dass die tatsächlichen Instandsetzungszeiten im Mittel deutlich kürzer sind als die zulässigen Zeiten. Andererseits werden Wartungsarbeiten regelmäßig und relativ häufig durchgeführt und sie sind planbar. Sie sind daher getrennt von den Instandsetzungen zu behandeln.

2 Begriffe

(1) Instandhaltung

Instandhaltung ist die Gesamtheit der Maßnahmen zu Bewahrung und Wiederherstellung des Sollzustands sowie zur Feststellung und Beurteilung des Istzustands. Die Instandhaltung gliedert sich in Instandsetzung, Wartung und Inspektion. (aus: KTA 140 (2/80))

Hinweis:

Instandsetzung: Maßnahmen zur Wiederherstellung des Sollzustandes.

Wartung: Maßnahmen zur Bewahrung des Sollzustandes.

Inspektion: Maßnahmen zur Feststellung und Beurteilung des Istzustandes.

(2) Instandhaltungszeit

Instandhaltungszeit ist die Zeitdauer vom Erkennen der Nichtverfügbarkeit eines betroffenen Systembestandteils bis zur Wiederherstellung seiner Funktionsfähigkeit. Bei Wartung und Inspektion ist Instandhaltungszeit die Gesamtdauer der Nichtverfügbarkeit.

(3) Instandhaltungszeit, zulässige

Zulässige Instandhaltungszeit ist die Zeitdauer, während der das betroffene Systembestandteil instandhaltungsbedingt nicht verfügbar sein darf, ohne dass Zusatzmaßnahmen ergriffen werden müssen.

(4) Ereignisklasse

Ereignisklasse ist eine Gruppe von auslösende Ereignissen mit vergleichbar hoher Eintrittshäufigkeit.

(5) Ereignisklassennummer

Ereignisklassennummer (E_e) ist ein Maß für die erwartete Häufigkeit eines auslösenden Ereignisses (e).

(6) Redundante

Redundante ist ein Systembestandteil (z. B. Komponente, Teilsystem, Strang), der gleichwertig mit anderen Systembestandteilen die gleichen Funktionen erfüllen und der bei Bedarf einen dieser anderen Systembestandteile voll ersetzen oder durch diesen ersetzt werden kann.

(aus: KTA 3301 (11/84))

Hinweis:

In diesem Bericht wird der Begriff Redundante in folgenden Punkten enger gefasst:

a) Redundante fasst alle Komponenten zusammen, die zur Erfüllung von Systemfunktionen bei einem Ereignisablauf angefordert werden.

b) Es hängt vom jeweils betrachteten Ereignisablauf ab, welche Komponenten zu einer Redundanten gehören und welche Systembestandteile zueinander gleichwertig sind.

c) Zur Redundanten gehören auch die zu Erfüllung ihrer Funktion erforderlichen Hilfs- und Nebensysteme.

Folgende Beispiele erläutern den Sachverhalt:

Beispiel 1: Kleines Leck im Primärkreis

Bei den neueren DWR-Anlagen besteht das Not- und Nachkühlsystem aus jeweils vier Redundanten. Dabei gehören die logisch in Reihe geschalteten Komponenten eines Teilsystems des Nebenkühlwassersystems, Zwischenkühlwassersystems und der Niederdruckeinspeisung mit ihren Hilfs- und Nebensystemen zu einer Redundanten der Niederdruckeinspeisung, da der Ausfall einer Komponente zum Nichtwirksamwerden der anderen Komponenten dieser Redundanten führt.

Die Hochdruckeinspeisung gehört nicht zur selben Redundanten wie die Niederdruckeinspeisung, da sie eine andere Systemfunktion erfüllt. Die logisch in Reihe geschalteten Komponenten eines Teilsystems der Hochdruckeinspeisung, des Zwischenkühlwassersystems und des Nebenkühlwassersystems (einschließlich Hilfs- und Nebensysteme) bilden zusammen eine Redundante der Hochdruckeinspeisung

Die funktionell in Reihe geschalteten Komponenten eines Teilsystems des Notspeisesystems bilden zusammen mit dem dazugehörigen Notspeisediesel und den Hilfs- und Nebensystemen eine Redundante der sekundärseitige Dampferzeugerbespeisung.

Die logisch in Reihe geschalteten Komponenten eines Teilsystems des An- und Abfahrsystems bilden beim Kleinen Leck ebenfalls eine Redundante der sekundärseitigen Dampferzeugerbespeisung, weil sie beim Störfall kleines Leck zu einer Redundanten des Notspeisesystems gleichwertig sind, so dass es 6 Redundanten der sekundärseitigen Dampferzeugerbespeisung gibt. Ein Ausfall des Deionatsystems ist dem Ausfall beider Redundanten des An- und Abfahrsystems gleichzusetzen.

Beispiel 2: Notstromfall

Da im Notstromfall die Notstromdiesel zur Energieversorgung des An- und Abfahrsystems benötigt werden, bilden im Notstromfall die logisch in Reihe geschalteten Komponenten eines Teilsystems des An- und Abfahrsystems zusammen mit dem zugehörigen Notstromdiesel eine Redundante der sekundärseitigen Dampferzeugerbespeisung.

Bei den neueren DWR.-Anlagen gibt es 6 Redundanten der Dampferzeugerbespeisung.

Beispiel 3: Bruch von Rohrleitungen im Speisewassersystem

Bei konservativer Betrachtungsweise muss davon ausgegangen werden, das bei einem Bruch von Rohrleitungen im Speisewassersystem sowohl die Hauptspeisewasserversorgung als auch das An- und Abfahrsystem ausfallen. Für diesen Störfall ist das An- und Abfahrsystem daher nicht gleichwertig zum Notspeisesystem. Es gibt nur 4 Redundanten der Dampferzeugerbespeisung.

(7) Redundanzgrad

Der Redundanzgrad (k_e) eines Systems ergibt sich aus der Anzahl der bei einer Anforderung durch ein auslösendes Ereignis (e) verfügbaren Redundanten vermindert um die Anzahl der zur Erfüllung der angeforderten Systemfunktion erforderlichen Redundanten.

3 Systeme, für die zulässige Instandhaltungszeiten festzulegen sind

(1) Instandhaltungszeiten sind für alle Sicherheitseinrichtungen zu begrenzen, die bei Anlagenstörfällen (Kühlmittelverluststörfälle, Transienten oder Einwirkungen von außen) die Abschaltung und Kühlung des Reaktorkernes sowie die Rückhaltung der Aktivität in der Anlage gewährleisten müssen, d. h. für Einrichtungen, bei denen das Einzelfehlerkonzept Anwendung findet.

(2) Die Anwendung des Einzelfehlerkonzepts erfolgt auf

- Reaktorschutz,
- Reaktorabschaltung,
- Nachwärmeabfuhr im bestimmungsgemäßen Be rieb und nach Kühlmittelverlusten,
- Nachwärmeabfuhr bei nicht verfügbarer Hautwärmesenke,
- Notstromversorgung,
- Wärmeabfuhr aus dem Sicherheitseinschluss,
- aktive Einrichtungen des Sicherheitseinschlusses.

Das kerntechnische Regelwerk enthält für einzelne Sicherheitseinrichtungen bereits Festlegungen, so werden

Reaktorschutzsystem und Überwachung von Sicherheitseinrichtungen in KTA 3501 "Reaktorschutzsystem und Überwachungseinrichtungen des Sicherheitssystems",

Netzanschlüsse und Eigenbedarfsversorgung in KTA 3701 "Übergeordnete Anforderungen an die elektrische Energieversorgung des Sicherheitssystems in Kernkraftwerken",

Störfallinstrumentierung in KTA 3502 "Störfallinstrumentierung",

Beckenkühlsysteme in KTA 3303 "Wärmeabfuhrsysteme für wassergekühlte Leichtwasser-reaktoren" und

Druckentlastungsarmaturen in KTA 3302 "Anforderungen an primärseitige und sekundärseitige Druckentlastungsarmaturen für ortsfeste Kernkraftwerke mit Leichtwasserreaktoren" geregelt.

(4) Auch Systeme, die nicht dem Einzelfehlerkonzept unterworfen sind, aber als zusätzliche Redundanten bei der Bestimmung des Redundanzgrads gemäß Abschnitt 5.2 berücksichtigt werden sind in diese Regelung einzubeziehen.

(5) Systeme, die zur Beherrschung von Anlagenstörfällen nach Tabelle 5-3 nicht zwingend erforderlich sind, wie Prozessrechnersysteme, Kommunikationseinrichtungen, Feuermelde- und -löschsysteme, werden in diesem Bericht nicht behandelt. Ebenfalls nicht behandelt werden Systeme, die der Erfüllung des radiologische Minimierungsgebotes dienen.

4 Probabilistische Methoden zur Ermittlung von zulässigen Instandhaltungszeiten

4.1 Allgemeines

(1) Nach dem Einzelfehlerkonzept (s. Abschnitt 1.2, Absatz 3) sind die Instandhaltungszeiten der Sicherheitseinrichtungen so festzulegen, dass die Zuverlässigkeiten dieser Sicherheitseinrichtungen durch die Instandhaltungsvorgänge nicht unter die zur Störfallbeherrschung erforderlichen Zuverlässigkeiten herabgesetzt werden. Will man den Einfluss von zulässigen Instandhaltungszeiten - wie sie in den Betriebshandbüchern der Kernkraftwerke festgeschrieben sind - auf die Nichtverfügbarkeit U eines Systems ermitteln, erfordert dies im allgemeinen eine detaillierte Zuverlässigkeitsanalyse für die zu betrachtenden Systeme. Erforderlich ist hierfür die Darstellung des System-Ausfallverhaltens, z. B. in Form eines Fehlerbaumes. Ein vereinfachtes Beispiel für ein 3-strängiges System ist in Bild 1 dargestellt. Als Fehlerbaum-Eingangsdaten müssen für die einzelnen Komponenten

- Ausfallraten, -wahrscheinlichkeiten,
- Instandsetzungszeiten,
- Testintervalle,
- Betriebsart (Standby oder Dauerbetrieb) und
- Wartungszeiten

bekannt sein, um die Nichtverfügbarkeit U des Systems bestimmen zu können. Bei den Instandsetzungszeiten für die einzelnen Komponenten handelt es sich um Erfahrungswerte aus Kernkraftwerken, die im allgemeinen unter 40 Stunden liegen. Diese Zeiten werden in einer Zuverlässigkeitsanalyse entsprechend berücksichtigt. In den bisher in den Genehmigungsverfahren durchgeführten Zuverlässigkeitsanalysen wurde jedoch der Einfluss der Wartungszeiten größtenteils nicht berücksichtigt, d. h. es wurde davon ausgegangen, dass während des Leistungsbetriebes der Kernkraftwerke keine Wartungsarbeiten, die zur Nichtverfügbarkeit einer Redundanten führen, durchgeführt werden.

(2) Treten nun während des Leistungsbetriebes aufgrund eines größeren Schadens an einer sicherheitstechnisch wichtigen Komponente oder aus Lieferschwierigkeiten für Ersatzteile Instandsetzungszeiten auf, die erheblich länger sind als die in den Zuverlässigkeitsanalysen berücksichtigten Werte, verschlechtert sich die Zuverlässigkeit des Sicherheitssystems unter die ausgewiesenen Werte. Den gleichen Effekt bewirken längere, während des Leistungsbetriebes durchzuführende Wartungsarbeiten an einzelnen Redundanten.

4.2 Einfluss von Instandhaltungszeiten auf die Nichtverfügbarkeit von Sicherheitssystemen

(1) Die mittlere Nichtverfügbarkeit U eines Systems läst sich unter Vorgabe der Nichtverfügbarkeitszeiten l_k und des Betrachtungszeitraumes T in anschaulicher Form aus folgender Beziehung errechnen.

$$U = \frac{\sum I_k}{T} = \frac{\text{Summe der Nichtverfügbarkeitszeiten (einschließlich Instandsetzung und Wartung)}}{\text{Betrachtungszeitraum}} \qquad (4\text{-}1)$$

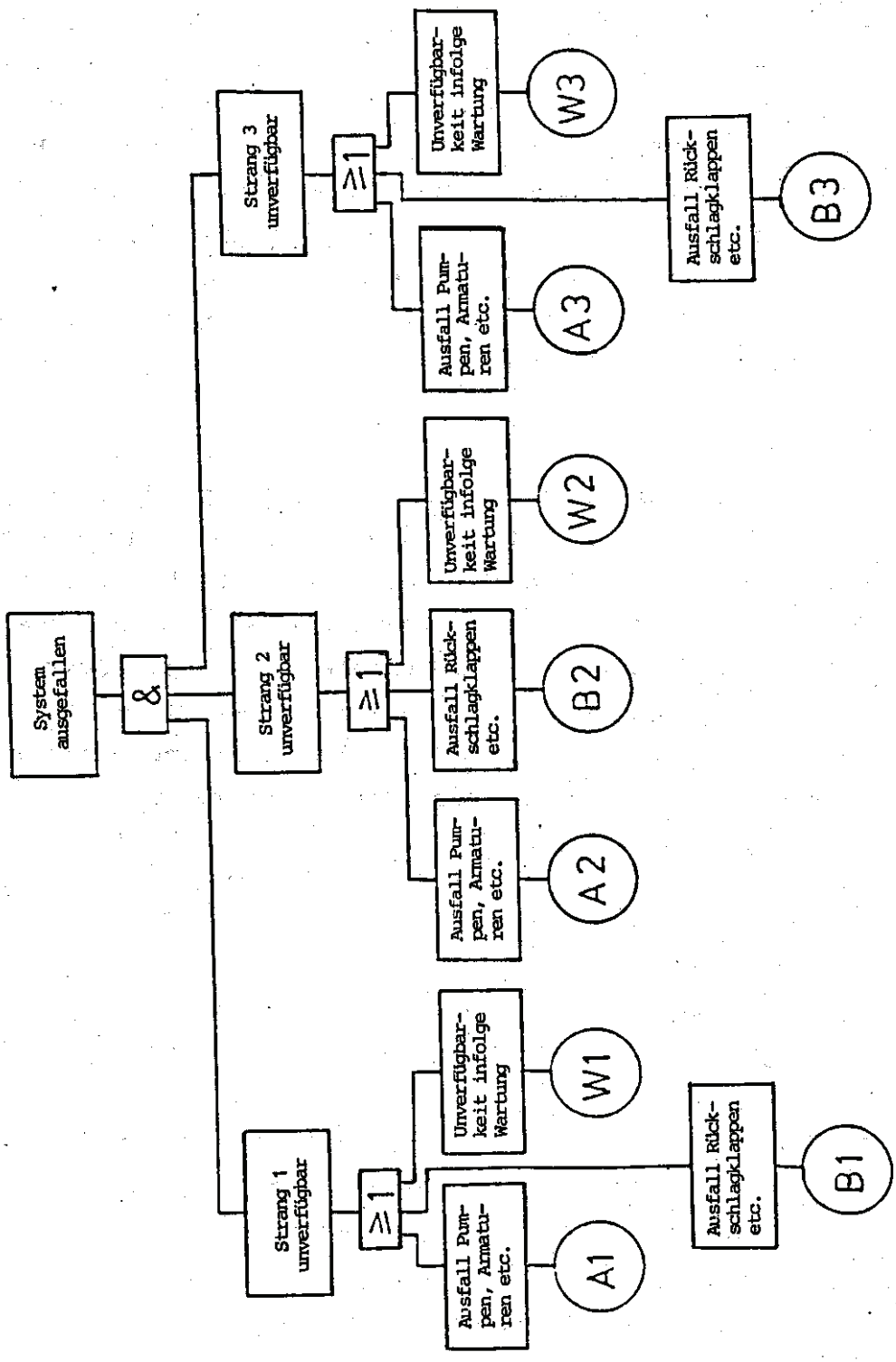

Bild 1: **Vereinfachter Fehlerbaum für ein 1v3-System**

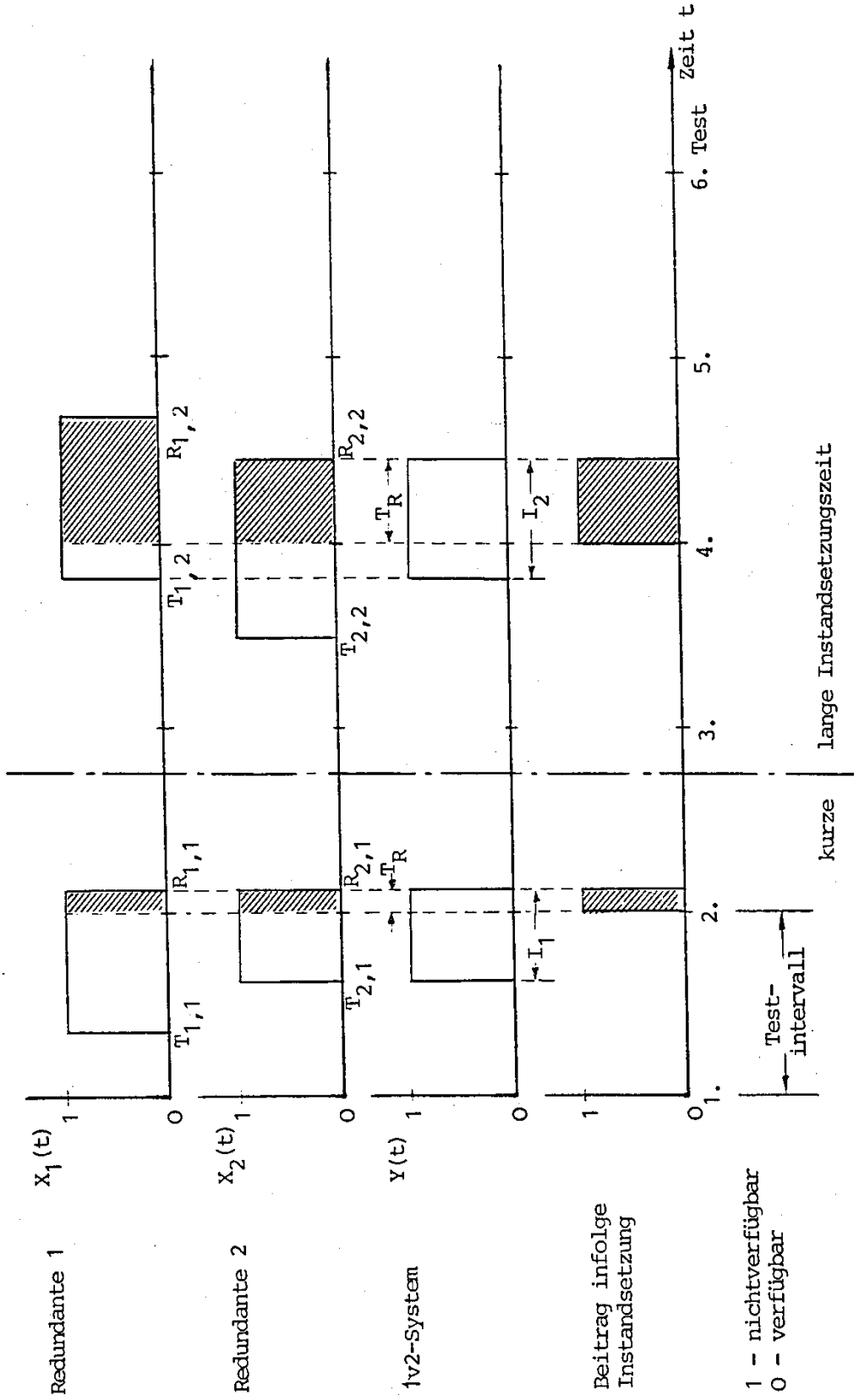

Bild 2: **Nichtverfügbarkeit eines 1v2-Systems bei gleichzeitigen Feststellen der Nichtverfügbarkeiten der beiden Redundanten; Einfluss kurzer und langer Instandsetzungszeiten**

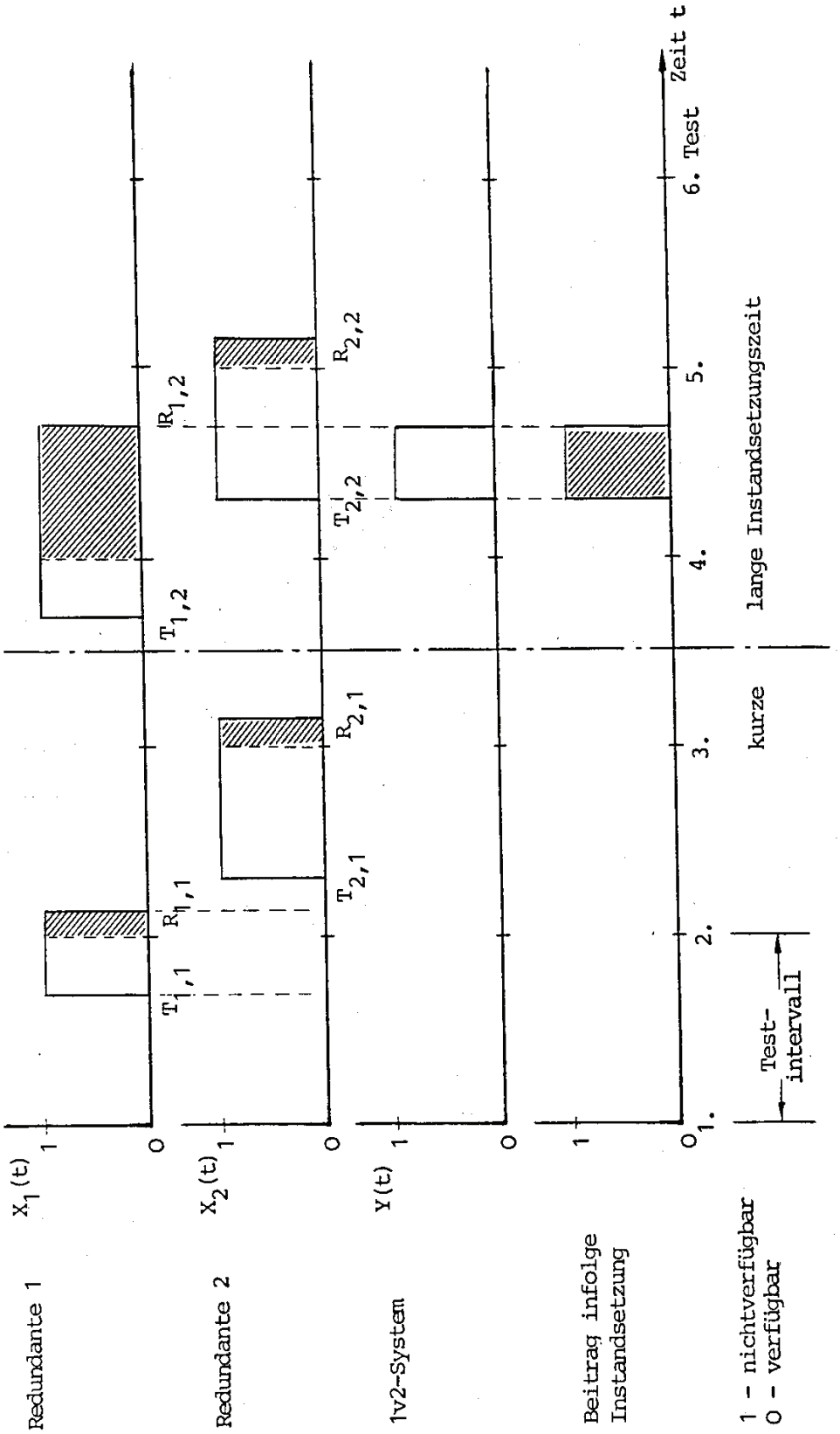

Bild 3: **Nichtverfügbarkeit eines 1v2-Systems bei versetztem Feststellen der Nichtverfügbarkeiten der beiden Redundanten; Einfluss kurzer und langer Instandsetzungszeiten**

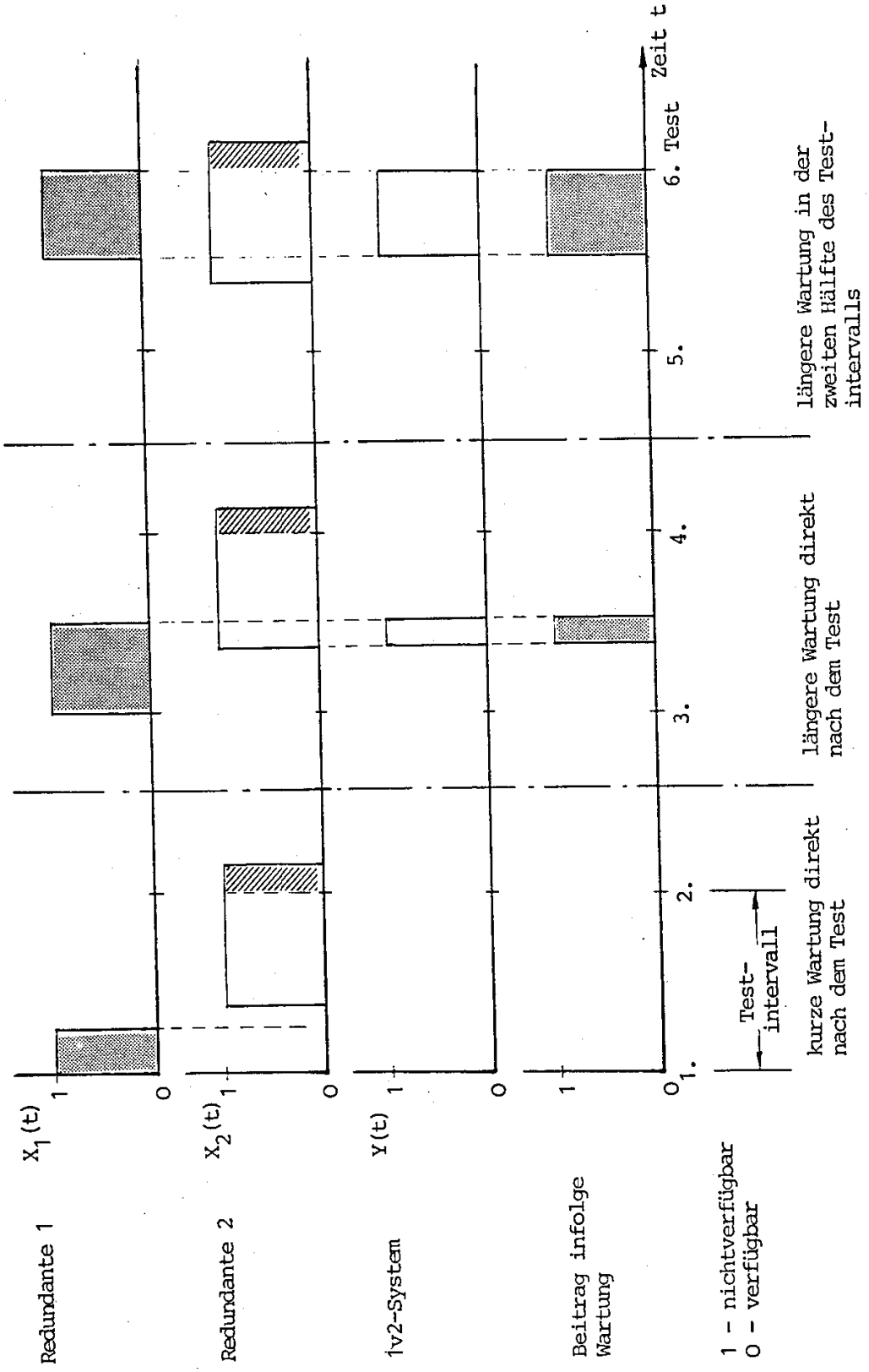

Bild 4: **Nichtverfügbarkeit eines 1v2-Systems bei kurzer oder längerer Wartungszeit sowie längerer Wartungszeit in der zweiten Hälfte eines Testintervalls und bei Nichtverfügbarkeit der anderen Redundanten**

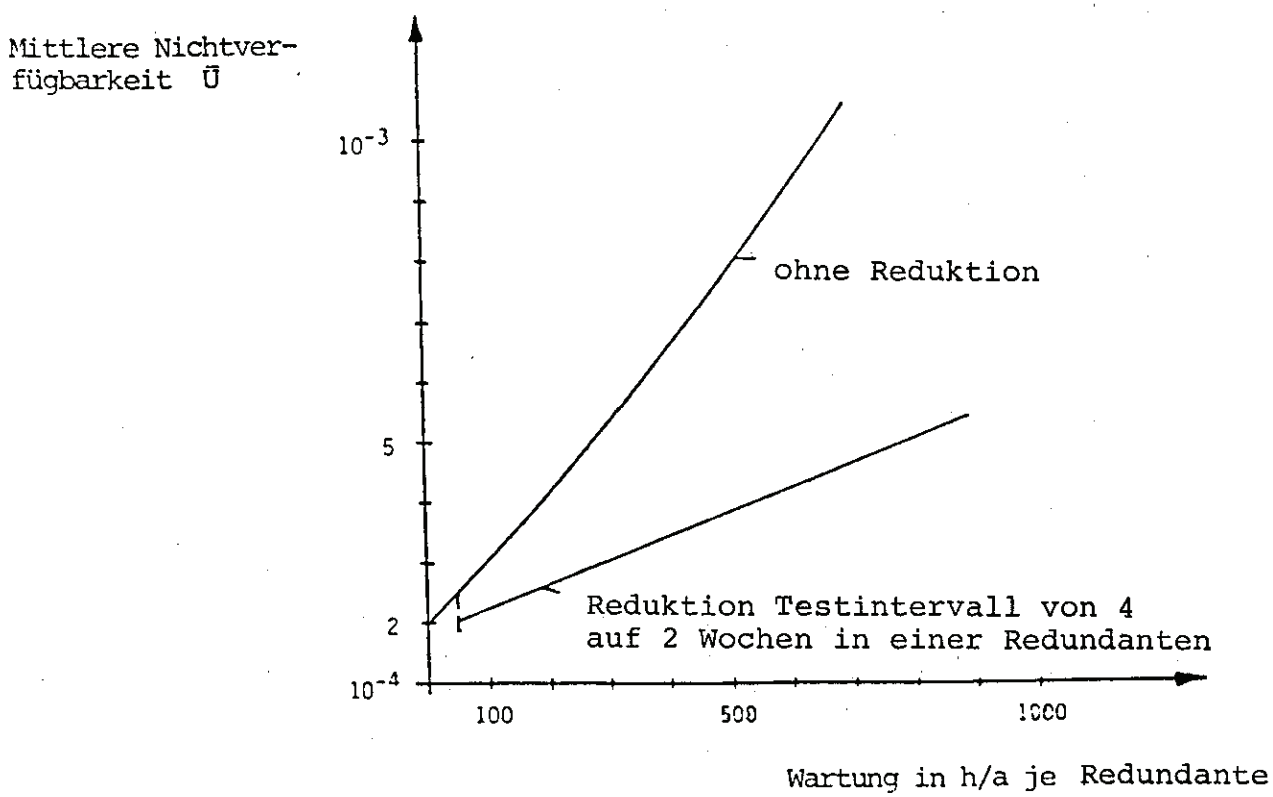

Bild 5: **Einfluss von Wartungsarbeiten auf die Nichtverfügbarkeit eines 1v3-Systems**

(2) Der Einfluss von Instandsetzungszeiten und Wartungszeiten auf die Nichtverfügbarkeit U lässt sich qualitativ am anschaulichsten anhand der logischen Diagramme in den nachfolgenden Bildern 2 bis 5 erläutern. Dargestellt werden die Zustände der Stränge bzw. Komponenten X_1 (t) und X_2 (t) in Abhängigkeit von der Zeit und ein daraus gebildetes 1v2-System Y (t), wobei nur hinsichtlich intakt und ausgefallen unterschieden wird. Sind die logischen Größen (X_1 (t), X_2 (t), Y (t)) gleich 0, so bedeutet dies, die Komponente oder das System ist intakt, sind diese Größen gleich 1, so bedeutet das, sie sind ausgefallen.

(3) Bild 2 enthält als Beispiel das Ausfallverhalten eines 1v2Standby-Systems einmal mit kurzer und einmal mit langer Instandsetzungszeit. Hierbei fällt die Redundante 1 z. B. zu einem bestimmten Zeitpunkt $T_{1,1}$ aus (X_1 (t) = 1). Da es sich in diesem Beispiel um ein Standby-System handelt, wird der Fehler erst beim nächsten Funktionstest bemerkt und die Instandsetzung entsprechend eingeleitet. Für die Redundante 2 gilt entsprechendes, wobei der Strangausfall (X_2 (t) = 1) etwas später eintritt. Für das Beispiel sind gleichzeitige Tests der Redundanten angenommen. Die Nichtverfügbarkeitszeit des Systems I_k ergibt sich als der Bitraum, in dem beide Systemstränge ausgefallen sind. In Bild 2 ist für diesen Fall auch der Beitrag der Instandsetzung zur Systemausfallzeit dargestellt. Da die Testintervalle (ca. 720 h), in denen as System unbemerkt ausfallen kann, im Vergleich zu den Instandsetzungszeiten (40 h) relativ lang sind, ergibt sich ein geringer Beitrag infolge der notwendigen Instandsetzung. Wie in Bild 2 auf der rechten Seite dargestellt, ändert sich die Nichtverfügbarkeit des Systems und der Beitrag infolge Instandsetzung, wenn sich. die Instandsetzungszeiten erheblich verlängern.

(4) In Bild 3 ist ein weiterer Einfluss von langen Instandsetzungszeiten auf die Nichtverfügbarkeit dargestellt. Bei dem auf der linken Seite des Bildes 3 dargestellten Ausfallverhalten ergibt sich kein Systemausfall, da die Wiederinbetriebnahme, der Redundante 1 zum Zeitpunkt $R_{1,1}$ aufgrund der kurzen Instandsetzungszeit bereits vor dem Ausfall der Redundante 2 zum Zeitpunkt $T_{2,1}$ erfolgte. Wenn die Redundante zum Zeitpunkt $T_{1,2}$ ausfällt und eine lange Instandsetzung bis zum Zeitpunkt $R_{1,2}$ notwendig ist und wenn die Redundante 2 vor der Wiederinbetriebnahme der Redundante 1

ausfällt, so ergibt sich ein Systemausfall. Längere Instandsetzungszeiten beeinflussen somit auch die Anzahl der Systemausfälle.

(5) Der Einfluss der Wartung auf die Nichtverfügbarkeit des Systems ist in Bild 4 dargestellt. Bei einer kurzen Wartungszeit ergibt sich bei diesem Beispiel kein Systemausfall, da die Wartung vor Ausfall der Redundante 2 abgeschlossen ist. Wird die Wartung über einen längeren Zeitraum durchgeführt, ergibt sich ein Systemausfall, wobei die Nichtverfügbarkeitszeit allein durch die Wartung bestimmt wird. Ein wesentlich längerer Systemausfall ergibt sich, wenn die Wartung z. B. in der zweiten Hälfte eines Testintervalles durchgeführt wird.

(6) Aufgrund der höheren Wahrscheinlichkeit für den Ausfall der Redundante 2 am Ende des Testintervalles ergibt sich eine höhere Wahrscheinlichkeit für einen Systemausfall bzw. eine längere Systemnichtverfügbarkeitszeit. Wartungszeiten an einer Redundanten direkt nach einem Funktionstest an einer anderen Redundanten sind somit, hinsichtlich ihrer Auswirkungen auf die Zuverlässigkeit des Systems günstiger zu bewerten als Wartungsarbeiten am Ende eines Testintervalles.

(7) Um den tatsächlichen Einfluss der Wartung auf die Zuverlässigkeit von Sicherheitssystemen in Kernkraftwerken beurteilen zu können, wurde eine Beispielrechnung für ein 1v3-System einer Siedewasserreaktoranlage, Bild 1, durchgeführt, wobei der Wartungsbeitrag variiert wurde. Die Ergebnisse sind aus Bild ersichtlich. Die Nichtverfügbarkeit des Systems ohne Wartung beträgt $2 \cdot 10^{-4}$, wobei die meisten Komponenten monatlich (A_1 bis A_3) und einige jährlich (B_1 bis B_3) geprüft werden. Lässt man pro Redundante und Jahr 500 Stunden Wartung zu, vergrößert sich die Nichtverfügbarkeit auf $7{,}9 \cdot 10^{-4}$. Verringert man bei längeren Wartungsarbeiten die Testintervalle von 4 auf 2 Wochen, so sinkt die Nichtverfügbarkeit auf die Hälfte. Hieraus ist ersichtlich, dass längere Wartungszeiten zugelassen werden können, wenn für diesen Zeitraum geeignete Ersatzmaßnahmen wie z. B. eine Verkürzung von Testintervallen vorgenommen werden, worauf im Folgenden noch eingegangen wird.

(8) Zusammenfassend ist festzustellen, dass längere Instandsetzungszeiten sowie Wartungsarbeiten die

- Anzahl von Systemausfällen und
- Systemausfallzeiten (Nichtverfügbarkeiten)

beeinflussen.. Bei Einschränkung der Zeiten und geeigneten Gegenmaßnahmen kann der Einfluss auf die Nichtverfügbarkeit gering gehalten werden.

4.3 Probabilistische Methoden

4.3.1 Mathematische Grundlagen

(1) Als Bewertungsgröße für die Zuverlässigkeit eines Systems wird bei der hier interessierenden Problemstellung die Nichtverfügbarkeit herangezogen. Die Nichtverfügbarkeit U ist die Wahrscheinlichkeit dafür, dass ein System oder eine Komponente z einem Zeitpunkt T nicht funktionsfähig ist. Der zeitliche Mittelwert dieser Größe wird mittlere Nichtverfügbarkeit $\bar{U}$ bezeichnet.

$$\overline{U} = \frac{1}{T}\int_0^T U\,(T)\,dt \qquad (4\text{-}2)$$

Als weitere Bewertungsgröße existiert noch die maximale Nichtverfügbarkeit U_{max}. Diese Größe ist der Maximalwert von U (t) im Betrachtungszeitraum T.

(2) Eine wichtige Größe, die zur Berechnung der Nichtverfügbarkeit eines Systems benötigt wird, ist die Nichtverfügbarkeit der Systemkomponenten, aus denen das Gesamtsystem aufgebaut ist. In den meisten Zuverlässigkeitsanalysen wird davon ausgegangen, dass die Ausfallrate λ einer Komponente zeitlich konstant ist. Dann ergibt sich bei $\lambda \cdot t << 1$, dass die Nichtverfügbarkeit einer Komponente linear von der Zeit t seit der letzten Prüfung abhängt.

$$u(t) = \lambda \cdot t \quad \text{bei } \lambda \cdot t \ll 1 \tag{4-3}$$

Bei Berücksichtigung eines zeitunabhängigen Beitrag q ergibt sich

$$u(t) = q + \lambda \cdot t \quad \text{bei } \lambda \cdot t \ll 1 \tag{4-4}$$

Bezüglich der Herleitungen dieser Beziehungen sowie detaillierterer Modelle sei auf die weiterführende Literatur verwiesen /1, 2, 3/. Bei Zugrundelegung eines Testintervalles t ergeben sich mittlere und maximale Nichtverfügbarkeit einer Komponente zu

$$\bar{u} = \lambda \cdot \tau / 2 \tag{4-5}$$

$$u_{max} = \lambda \cdot \tau \tag{4-6}$$

(3) Zur Ermittlung der Systemnichtverfügbarkeiten lassen sich bei einfachen,. strangweise aufgebauten Systemen Beziehungen aus /1/ und /4/ heranziehen. Bei komplexen, vermaschten Systemen ist der Einsatz von Rechenprogrammen notwendig /2, 5, 6, 7/.

4.3.2 Referenzwertmethode

(1) Die Referenzwertmethode beinhaltet die Forderung, dass die Nichtverfügbarkeit eines Systems, bei dem während es Reaktorleistungsbetriebs Instandsetzungen an einzelnen Komponenten erlaubt sind, zu keinem Zeitpunkt - also auch nicht währen einer kurzzeitigen Instandsetzung - einen bestimmten Referenzwert $U_{R,\,max}$ überschreiten darf. Dieser Referenzwert liegt um den Faktor f über dem Wert der maximalen Systemnichtverfügbarkeit $U_{max'}$ die sich ohne Instandsetzung ergibt. Die zulässige Instandsetzungszeit T_R ergibt sich damit aus der Gleichung

$$U_{R,max}(T_R) = f \cdot U_{max} \tag{4-7}$$

f ist hierbei ein frei wählbarer Faktor. Im Beschluss 66 der TÜV-Leitstelle vom 30.3.1977 (Der Leitstellenbeschluss ist inzwischen durch die Interpretationen zu den Sicherheitskriterien abgelöst worden. Die Referenzwertmethode wurde dabei jedoch nicht übernommen) sowie im Bericht GRS-A-152 /8/ wird z.B. ein Faktor 5 vorgeschlagen.

$U_{R,max}$ (T_R) ist damit die maximale Nichtverfügbarkeit des intakten Teiles des Gesamtsystems am Ende der zulässigen Instandsetzungszeit T_R des ausgefallenen Teilsystems.

(2) In einem sehr stark vereinfachten Beispiel werden die Rechenschritte der Referenzwertmethode dargestellt (in /8/ wird die Methode detailliert dargestellt).

Beispiel:

Betrachtet wird ein 2-von-4-System, gleichzeitige Prüfung aller Redundanten, Zeitabhängigkeit der Nichtverfügbarkeit einer Redundanten λt (d. h. kein zeitunabhängiger Anteil der Nichtverfügbarkeit und $\lambda t << 1$) .

Dann gilt für die Nichtverfügbarkeit U (t) des 2-von-4-Systems $U(t) = 4(\lambda t)^3$, wobei t = Zeit seit der letzten Funktionsprüfung ist. Bei einem Prüfintervall t beträgt die maximale Nichtverfügbarkeit $U_{max} = 4(\lambda\tau)^3$.

Wird eine Redundante als ausgefallen erkannt, so ist das Restsystem ein 2-von-3-System mit einer Nichtverfügbarkeit $U_R(t) = 3(\lambda t)^2$.

Mit dem Erhöhungsfaktor f = 5 erhält man:

$$U_{R,max}(T_R) = 3(\lambda T_R)^2 = 5 \cdot 4(\lambda\tau)^3 = 5 \cdot U_{max}$$

$$\text{bzw. } T_R = \tau\sqrt{\frac{20 \cdot \lambda \cdot \tau}{3}}$$

Mit τ = 720 h erhält man für ein 2-von-4-System:

λ	U_{max}	$U_{R,max}$	T_R (mit Prüfung)
$5 \cdot 10^{-5}\ h^{-1}$	$1{,}9 \cdot 10^{-4}$	$9{,}3 \cdot 10^{-4}$	350 h
$1 \cdot 10^{-4}\ h^{-1}$	$1{,}5 \cdot 10^{-3}$	$7{,}5 \cdot 10^{-3}$	500 h
$2 \cdot 10^{-4}\ h^{-1}$	$1{,}2 \cdot 10^{-2}$	$6{,}9 \cdot 10^{-2}$	710 h

(3) Die wichtigsten Nachteile der Methode sind:

a) Da die Nichtverfügbarkeit von den gewählten Systemgrenzen abhängig ist, hängt auch die zulässige Instandhaltungszeit eines Systems von diesen Systemgrenzen ab.

b) Je geringer die Nichtverfügbarkeit eines Systems ist, desto kleiner wird die zulässige Instandhaltungszeit

c) Die zulässige Instandhaltungszeit hängt stark vom Zuverlässigkeitsmodell für die einzelnen Komponenten ab, d. h. vom zeitunabhängigen Anteil der Nichtverfügbarkeiten.

d) Die Methode berücksichtigt nicht die Häufigkeit von Instandsetzungen.

4.3.3 Relative Risikomethode

(1) Bei der relativen Risikomethode wird die zulässige Instandhaltungszeit aus der Bedingung bestimmt, dass die mittlere Nichtverfügbarkeit des Systems unter Einbeziehung der Instandhaltungsvorgänge einen vorgegebenen Referenzwert nicht überschreite darf, der sich an der mittleren Nichtverfügbarkeit ohne Einbeziehung der Instandhaltung orientiert. Dabei wird wie folgt vorgegangen. Zunächst wird die mittlere Nichtverfügbarkeit der Sicherheitseinrichtungen für einen bestimmten Anforderungsfall unter der ahme berechnet, dass nur vernachlässigbar kurze Instandsetzungszeit n benötigt werden ($T_R << \tau$). In einem zweiten Schritt wird dann die Unverfügbarkeit mit der Annahme berechnet, dass der Reaktor während einer längeren Instandsetzungszeit weiterbetrieben wird. Wegen der dann geringeren Redundanz ist die Nichtverfügbarkeit des Sicherheitssystems während der Instandsetzung höher.

(2) In einem vereinfachten Beispiel werden die Rechenschritte der relativen Risikomethode dargestellt (in /3/ wird die Methode detailliert dargestellt).

Beispiel:

Betrachtet wird ein 2-von-4-System, gleichzeitige Prüfung aller Redundanten, Zeitabhängigkeit der Nichtverfügbarkeit λt der Redundanten.

Dann gilt für die Nichtverfügbarkeit U(t) das 2-von-4-Systems $U(t) = 4(\lambda\ z)^3$, wobei t die Zeit seit der letzen Funktionsprüfung ist.

Bei einem Prüfintervall τ beträgt die mittlere Nichtverfügbarkeit

$$\overline{U} = \frac{1}{\tau}\int_0^{\tau} U(t)dt = (\lambda\tau)^3 \qquad \text{bei } \lambda \cdot t \langle\langle 1$$

Wird eine Redundante als ausgefallen erkannt, so ist das Restsystem ein 2-von-3-System mit einer Nichtverfügbarkeit $U_R(t) = 3(\lambda\ \tau)^2$.

Werden die anderen Redundanten zu den Zeitpunkten geprüft, zu denen sie auch ohne Ausfall geprüft würden, so erhält man für die mittlere Nichtverfügbarkeit während der Instandsetzung

$$\overline{U_R} = \frac{1}{\tau}\int_0^{\tau} U_R(t)dt = (\lambda\tau)^2$$

Der zulässige Anteil x von Instandhaltungszeiten (über alle Redundanten summiert) bezogen auf einen beliebigen Betrachtungszeitraum ergibt sich dann aus:

$$x \cdot \overline{U_R} + (1-x) \cdot \overline{U} = f\overline{U}$$

$$x \cdot (\lambda\tau)^2 + (1-x) \cdot (\lambda\tau)^3 = f \cdot (\lambda\tau)^3$$

$$x = \frac{(f-1) \cdot \lambda\tau}{1-\lambda\tau} \approx (f-1) \cdot \lambda\tau$$

Setzt man f = 2 und nimmt man an, das die Zahl der Instandsetzungen gleich der Zahl der Ausfälle bei Funktionsprüfungen ist, so erhält man eine zulässige Instandsetzungszeit von $T_R = \tau = 720$ h, unabhängig von der Ausfallrate.

(3) Nachteile dieser Methode sind:

a) Sie führt zu, einer Beschränkung der Gesamtinstandsetzungszeit oder zu einer Beschränkung der mittlere Instandsetzungszeit je Systemausfall. Die Ableitung einer maximal zulässigen Instandsetzungszeit für einen Instandsetzungsvorgang ist unmittelbar nicht möglich. Durch lange Instandsetzungszeiten in der Vergangenheit werden die zukünftig erlaubten Instandsetzungszeiten stark herabgesetzt, im Extremfall bis auf null Stunden.

b) In eingeschränkter Weise gelten auch die Nachteile der Referenzwertmethode nach Abschnitt 4.3.2 Punkte a bis c.

4.3.4 Modifizierte Risikomethode

(1) Um den Nachteil der relativen Risikomethode zu vermeiden, dass die Gesamtinstandsetzungszeit beschränkt wird und nicht die Instandsetzungszeit pro Ausfall, wurde die Risikomethode vom Arbeitsgremium wie folgt modifiziert:

Es wird ein Betrachtungszeitraum T (z. B. 1 Jahr) (eingeführt und angenommen, dass in einem solchen Betrachtungszeitraum eine längere Instandsetzung im Mittel nur einmal auftritt.

Die zulässige Instandhaltungszeit wird dann so festgelegt, dass der Beitrag zur Nichtverfügbarkeit nicht größer ist als der Beitrag des restlichen Betrachtungszeitraumes (d. h. Erhöhungsfaktor f 2).

Es gilt dann

$$U_R \cdot T_R/T < \bar{U} \qquad (4\text{-}8)$$

T_R = zulässige Instandhaltungszeit

T = Betrachtungszeitraum (z. B. 1 Jahr)

U_R = mittlere Nichtverfügbarkeit während der Instandhaltungszeit T_R

$\bar{U}$ = mittlere Nichtverfügbarkeit während der Betrachtungszeit T ohne Berücksichtigung von Instandhaltungszeiten, Referenzwert.

(2) Dabei gelten folgende Bedingungen

a) Für die Ausfallraten und Ausfallwahrscheinlichkeiten sind anerkannte Literaturwerte zu verwenden.

b) Die Teststrategie (z. B. versetztes Testen oder vorgezogene Prüfungen) ist zu berücksichtigen. Hierbei ist jedoch ein konstanter Anteil de Ausfallwahrscheinlichkeit der Komponenten bei Anforderung anzusetzen. Bei nicht gesicherter Datendifferenzierung wird empfohlen, diesen konstanten Anteil auf 1/5 der maximalen Nichtverfügbarkeit der Komponenten für den Fall einer 4-wöchentliche Prüfung festzulegen.

c) Probabilistische Daten für Common-mode-Ausfälle sind zu berücksichtigen.

4.3.5 Absolute Risikomethode

(1) Der Grundgedanke der absoluten Risikomethode ist, dass die Häufigkeit eines unerwünschten Anlagenzustandes während der Instandhaltung (d. h. das Produkt aus Anforderungshäufigkeit des Systems und Nichtverfügbarkeit des Restsystems währen der Instandhaltung) einen vorzugebenden Grenzwert nicht überschreiten darf. Damit geht im Gegensatz zu den vorgenannten Methoden die Eintrittshäufigkeit von Störfällen in die Festlegung der zulässige Instandhaltungszeiten ein.

(2) Diese Methode erfordert die Festlegung einer zulässigen absoluten Risikogrenze. Außerdem wirken sich die Unsicherheiten bei den statistischen Daten sehr stark auf die errechneten Instandhaltungszeiten aus, insbesondere wenn vorgezogene Prüfungen der anderen Redundanten betrachtet werden.

(3) Alternativ zur Festlegung einer absolute Risikogrenze können die Eintrittshäufigkeiten der Störfälle in Verbindung mit den Nichtverfügbarkeiten der Systeme auch zu einem Vergleich des Risikos mit und ohne Berücksichtigung der Instandhaltungszeiten herangezogen werden. Dieser Gedanke wird in der Ereignisklassenmethode qualitativ umgesetzt (s. Kapitel 5).

4.3.6 Risiko-Minimum-Ansatz

(1) Der Grundgedanke des Risko-Minimum-Ansatzes ist, dass Maßnahmen, die bei Überschreiten der zulässigen Instandhaltungszeiten ergriffen werden müssen, auch ein gewisses Risiko beinhalten, da sie zu einer erhöhten Anforderungswahrscheinlichkeit des Sicherheitssystems, insbesondere auch des ausgefallenen Systems führen können. Die zulässigen Instandhaltungszeiten sollten so festgelegt werden, dass bei längeren Instandhaltungszeiten die Risikoerhöhung durch Weiterbetrieb im Ausgangszustand größer ist als die Risikoerhöhung durch die Zustandsänderung. Falls man erwartet, dass die zulässigen Instandhaltungszeiten überschritten werden, müssen die Maßnahmen sofort ergriffen werden.

(2) Dieser Risiko-Minimum-Ansatz ist geeignet zur Ableitung qualitativer Aspekte, wie z. B. der Festlegung von Maßnahmen, die bei Nichteinhalten der Instandhaltungszeiten ergriffen werden müssen. Sie ist jedoch gegenwärtig auch aufgrund fehlender Daten nicht für die Berechnung zulässiger Instandhaltungszeiten belastbar. Falls nämlich z. B. das ausgefallene System nicht selbst zur Zustandsänderung benötigt wird, kann die Risikoänderung durch die Zustandsänderung sehr klein sein und ist dann nur sehr ungenau berechenbar.

5 Ereignisklassenmethode

5.1 Randbedingungen für die Entwicklung der Methode

Ausgehend von den in Kap. 1 zusammengestellten Grundsätzen wurde eine risikobezogene qualitative Methode zur Festlegung zulässiger Instandhaltungszeiten entwickelt, die

- sich an der zur Störfallbeherrschung erforderlichen Zuverlässigkeit der betroffenen Systeme orientiert, wobei die kumulierte Eintrittshäufigkeit unzulässiger Kernzustände als Maßstab dient,
- auf den einzelnen Instandhaltungsfall und nicht auf einen Betriebszeitraum bezogene Zeiten festlegt,
- auf Betriebserfahrungen und auf der bisherige Genehmigungspraxis aufbaut,
- im Falle besonders unwahrscheinlicher Abläufe längere zulässige Zeiten liefert,
- durch eine möglichst geringe Zahl direkt ablesbarer Parameter leicht zu handhaben ist (keine quantitative Zuverlässigkeitsanalyse erfordert),
- durch Angabe von Unter- und Obergrenzen die nötige Flexibilität lässt, um im Einzelfall besondere sicherheitstechnische Gegebenheiten, Maßnahmen oder Nachweise berücksichtigen zu können.

5.2 Methodischer Ansatz

(1) Die zulässige Instandhaltungszeit einer Redundanten eines Systems wird ermittelt unter Berücksichtigung

- der Eintrittshäufigkeit einer Anforderung des Systems,
- der mittleren Nichtverfügbarkeit dieses Systems.

Dabei sind nur solche Ereignisabläufe zu betrachten, bei denen die deterministisch festgelegten Auslegungsbedingungen nicht eingehalten werden. Von Ereignisabläufen, die beherrscht werden, brauchen keine Beschränkungen der Instandhaltungszeiten abgeleitet zu werden.

Die zulässige Instandhaltungszeit einer Redundanten wird somit von der Änderung der Eintrittshäufigkeiten der zu betrachtenden Ereignisabläufe (Absolutwert) durch Instandhaltung abhängig gemacht.

(2) Zur Charakterisierung von Eintrittshäufigkeiten und Nichtverfügbarkeiten werden zwei diskrete Parameter herangezogen.

Erster Parameter: Ereignisklasse E_e

Die Ereignisklasse charakterisiert die Häufigkeit, mit der Ereignisse, die die Sicherheitseinrichtungen anfordern, auftreten können. Ein handhabbares Raster mit ausreichender Differenzierung stellt in Anlehnung an ein Konzept des KTA, Bericht KTA-GS-47 /9/, eine Einteilung in 5 Klassen dar:

Ereignis-klasse	Kennzeichnung
1	Normalbetrieb und Instandhaltung
2	Ereignisabläufe, die nicht der vorstehenden Ereignisklasse angehören und deren angenommene Häufigkeit so groß ist, dass mit ihrem Eintreten während der Betriebszeit einer Anlage gerechnet werden muss
3	Ereignisabläufe, deren angenommene Häufigkeit so gering ist, dass ihr Eintreten innerhalb der Lebensdauer einer Anlage nicht erwartet wird, jedoch innerhalb der Lebensdauer anderer Anlagen für eine dieser Anlagen nicht ausgeschlossen werden kann
4	Ereignisabläufe, deren angenommene Häufigkeit so gering ist, dass ihr Eintreten bei keiner Anlage erwartet wird, die jedoch zur sicherheitstechnischen Auslegung der Anlage als Grenzfälle herangezogen werden
5	Ereignisabläufe, deren angenommene Häufigkeit so gering ist, dass ihr Eintreten bei keiner Anlage erwartet wird, und gegen die wegen ihrer geringen Eintrittshäufigkeit nicht gemäß §28 Abl. 3 StrlSchV ausgelegt werden muss, gegen deren Folgen die Anlagenkonstruktionen risikomindernde Eigenschaften haben muss

Tabelle 5-1: Festlegung von Ereignisklassen in Abhängigkeit von Eintrittshäufigkeiten von Ereignisabläufen

Die Eintrittshäufigkeit von Ereignissen in den Ereignisklassen E und E + 1 unterscheiden sich typischerweise um ein bis zwei Größenordnungen.

In den Tabellen 5-2 und 5-3 sind die gleichen auslösenden Ereignisse diesen Ereignisklassen zugeordnet, wobei die auslösenden Ereignisse in Tabelle 5-3 sachlich geordnet sind. Für die Auswahl von auslösenden Ereignissen aus der Zahl der mögliche ist maßgebend, dass sie für den vorliegenden Zweck, Ermittlung von zulässigen Instandhaltungszeiten, abdeckend sind. Die Tabellen 5-2 und 5-3 gelten nur für Leichtwasserreaktoren. Demgemäß ist die Ereignisklassenmethode zur Festlegung von Instandhaltungszeiten nur auf Kernkraftwerke mit Leichtwasserreaktor anwendbar. Eine Übertragung der Methode auf andere Reaktortypen ist zwar prinzipiell möglich, setzt aber die Zuordnung von auslösenden Ereignisse zu Ereignisklassen gemäß ihrer Eintrittshäufigkeit und ihrer Auswirkungen voraus. In Tabelle S-2 werden die auslösenden Ereignisse ur Veranschaulichung nach Ereignisklassen sortiert, dabei wird ein Bezug zu den Störfall-Leitlinien hergestellt. Die Aufstellung zeigt, dass zwei auslösende Ereignisse mit einbezogen sind, die den Betriebsstörungen zuzurechnen sind, deren Nichtbeherrschung jedoch einen Ereignisablauf mit unerwünschten Auswirkungen einleiten kann. Zwei weitere auslösende Ereignisse sind aufgeführt, die nicht zu den Störfällen gehören, gegen die aber nach den Störfall-Leitlinien auch in KTARegeln Maßnahmen vorgesehen werden müssen, die der Risikominderung dienen. Auslösende Ereignisse sind in diesem Abschnitt explizit aufgeführt, weil die Störfall-Leitlinien nur für Druckwasserreaktoren gelten, das Konzept aber auch Siedewasserreaktoren und im Prinzip auch andere Kernkraftwerkstypen mit einschließt. Es wird darauf hingewiesen, dass aus Ereignissen, die der Ereignisklasse 1 (Normalbetrieb) zugeordnet werden, keine Beschränkungen von Instandhaltungszeiten abgeleitet werden.

Ereignis-klasse	Auslösende Ereignisse	Störfall nach Störfall-Leitlinien Tabellen I u. II
1	-	-
2	Notstromfall, kurzzeitig (< 30 min) …	-
	Ausfall der betrieblichen Speisepumpen …	-
	Fehlerhafte Änderung der Reaktivität und Leistungs-verteilung …	II.1
	Ausfall der Hauptwärmesenke…	1.3.1
3	Bruch von Anschlussleitungen im Frischdampfsystem und absperrbare Anrisse der Frischdampfleitung…..	-
	Notstromfall, langzeitig (> 30 min)	II.2
	Bruch von Rohrleitungen im Speisewasserleitungssystem, der das betriebsübliche Abschalten und Abfahren ausschließt…..	-
	Kleines Leck im Primärkühlkreislauf	I.1.2
	Heizrohrabriss …..	I.2
	Abriss einer Anschlussleitung des Primärsystems …..	I.4.1/2
4	Frischdampfleck zwischen Sicherheitsbehälter und Absperrarmatur …..	II.4
	2F-Bruch der Frischdampfleitung …..	II.1.2
	Großes Leck im Primärkreislauf …..	II.1.1
	Sicherheitserdbeben …..	I.7
5	Flugzeugabsturz …..	-
	Explosionsdruckwellen …..	-

Tabelle 5-2: Zuordnung von auslösenden Ereignissen zu Ereignisklassen

Nr.	Auslösende Ereignisse	Ereignisklasse E_e für den abdeckenden Ereignisablauf
1.	Leckagen und Brüche im Frischdampfsystem	
1.1	Bruch von Anschlussleitungen im FD-System und absperrbare Anrisse der FD-Leitung	3
1.2	FD-Leck zwischen Sicherheitsbehälter und Absperrarmatur	4
1.3	2F-Bruch der Frischdampfleitung	4
2.	Notstromfall	
	kurzfristig (≤ 30 min)	2
	langfristig (> 30 min)	3
3.	Ausfall Speisewasserversorgung	
3.1	Ausfall der betrieblichen Speisepumpen	2
3.2	Bruch von Rohrleitungen im Speisewasserleitungssystem, der das betriebsübliche Abschalten und Abfahren ausschließt (DWR)	3
4.	Fehlerhafte Änderung der Reaktivität und der Leistungsverteilung	2
5.	Leckagen von Primärkühlmittel	
5.1	Kleines Leck	3
5.2	Großes Leck	4
5.3	Heizrohrabriss	3
5.4	Abriss einer Anschlussleitung des Primärsystems (z. B. des Volumenregelsystems)	3
6.	Ausfall der Hauptwärmesenke	2
7.	Einwirkungen von außen	
7.1	Sicherheitserdbeben	4
7.2	Flugzeugabsturz, Explosionen	5

Tabelle 5-3: Ereignisklassen für zu beherrschende Ereignisabläufe als Folge von auslösenden Ereignissen für DWR und SWR

Zweiter Parameter: Redundanzgrad k_e

Der zweite Parameter basiert auf der Überlegung, da um so kürzere Instandhaltungszeiten eingehalten werden müssen, je weniger der vorhandenen Redundanten noch verfügbar sind. Im Sinne einer konsistenten Zuverlässigkeitsbetrachtung, wie sie in den durchgeführten Zuverlässigkeitsanalysen angestellt wurde, müssen in eine solche Wertung auch die Redundanten einbezogen werden, die nach deterministischer Betrachtungsweise für Instandhaltungsarbeiten ständig zur Verfügung stehen, da jeder Ausfall von Redundanten zu einer Erhöhung der Wahrscheinlichkeit des Ausfalls des Sicherheitssystems führt. Eine Beschränkung der zulässigen Instandhaltungszeiten ergibt sich für seltene auslösende Ereignisse (Ereignisklasse 5) daraus nicht, wie später dargestellt werden wird, wohl aber bei häufigeren auslösenden Ereignissen (Ereignisklasse 2).

Der Redundanzgrad charakterisiert die Nichtverfügbarkeit insofern, als sich die mittleren Nichtverfügbarkeiten der betrachteten Systeme, deren Redundanzgrad um 1 differieren, analog zu den Ereignisklassen typischerweise um ein bis zwei Größenordnungen unterscheiden.

0	Zur Erfüllung der angeforderten Funktion sind nur die gerade dafür erforderlichen Redundanten verfügbar (d.h. das Auftreten eines Einzelfehlers wird nicht beherrscht)
1	Zur Erfüllung der angeforderten Funktion ist eine Redundante mehr als erforderlich verfügbar (d.h. das Auftreten eines Einzelfehlers wird beherrscht)
2	Zur Erfüllung der angeforderten Funktion sind zwei Redundanten mehr als erforderlich verfügbar

Tabelle 5-4: Redundanzgrad k_e während des Instandhaltungsvorgangs

(3) Mit Ereignisklasse und Redundanzgrad stehen zwei Parameter zur Verfügung, die leicht zu handhaben sind. Die Summe beider Zahlenwerte charakterisiert die Häufigkeit für das Nichteinhalten deterministisch vorgegebener Auslegungsgrenzen. Kleinere Werte dieser Summe kennzeichnen eine größere Häufigkeit. Dem mit Hilfe der beiden Kriterien gebildeten Zahlenwert der Summe wird jeweils ein Zeitbereich zugeordnet. Der unterste Wert dieses Bereichs ist dann die ohne weitere Nachweise zulässige Instandhaltungszeit. Größere Werte können im Einzelfall im Genehmigungsverfahren festgelegt werden, z. B. unter Anwendung der probabilistischen Verfahren von Kap. 4.

5.3 Überlegungen zur Festlegung von Zeitbereichen

Für die Festlegung zulässiger Zeiten gelten folgende Überlegungen:

a) 24 Stunden:

Gemäß Einzelfehlerkonzept Ziffer 7 Absatz 3 braucht das zusätzliche Auftreten eines Einzelfehlers n Systemteilen während kurzzeitiger Wartungs- und Instandsetzungsvorgänge nicht unterstellt zu werden, wenn wegen der Kürze der Wartungs- und Instandsetzungsdauer die Zuverlässigkeit der betrachteten Sicherheitseinrichtungen nicht wesentlich herabgesetzt wird. Da Maßnahmen wie Abfahren mehrere Stunden dauern und mit dem Risiko einer Anforderung des ausgefallene Systems verbunden sein können, ist das Arbeitsgremium der Sicht, daß.24 Stunden ausreichend kurz sind. In der Deutschen Risikostudie werden mittlere Instandsetzungszeiten für verschiedene Komponenten angegeben (vgl. Fachband 3, Seite 66 . Diese lagen in den meisten Fällen unter 24 Stunden. Nur für wenige Komponenten lagen die längsten benötigten Instandsetzungszeiten über 24 Stunden. Diese Zeit entspricht auch weitgehend der gegenwärtigen Genehmigungspraxis (KKU 2h, GKN1 l0h, KKG l0h, KKP2 24h, KWG 24h).

b) 14 Tage:

In Betriebshandbüchern (KKG und GKN1) sind zulässige Instandsetzungszeiten von 7 (nach Tests) und 10 Tagen festgeschrieben. Diesen Festlegungen lagen Zuverlässigkeitsanalysen zugrunde. Die Betriebserfahrungen haben gezeigt, dass diese Zeiten eingehalten werden können. Bei den neueren Anlagen Grohnde und Philippsburg sind 14 Tage festgelegt worden. Diese Zeit entspricht dem Fall $E_e + k_e = 4$. Sie gilt (ebenfalls für relativ häufige auslösende Ereignisse mit $E_e = 2$ und $k_e = 1$, bei denen also' auch während der Instandsetzu9ig der Einzelfehler noch beherrscht wird. Die Zeit von 14 Tagen gilt z. B. für den Ausfall einer Nachkühlkette.

c) 2 Monate:

Diese Zeit gilt für $E_e + k_e = 5$. Damit wird seltenen Anforderungsfällen bzw. hohen Redundanzgraden Rechnung getragen. Die Zulässigkeit so langer Instandhaltungszeiten ist bei bisherigen Anlagen, ausgenommen KKP und KWG, noch nicht vorgesehen worden.

d) Brennelementwechsel:

Für noch seltenere Anforderungsfälle bzw. noch höhere Redundanzgrade wird die Möglichkeit geboten, Maßnahmen zur Instandsetzung die bei Leistungsbetrieb nicht durchführbar sind, bis zum nächsten Brennelementwechsel zu verschieben.

Die gewählten zulässigen Instandhaltungszeiten sind dem neuen Genehmigungsstand angepasst und im allgemeinen länger als sie bei Altanlagen genehmigt worden sind. ,

5.4 Festlegung der zulässigen Instandhaltungszeiten

(1) Zur Ermittlung zulässiger Instandhaltungszeiten für ein bestimmtes System sind alle auslösenden Ereignisse gemäß Tabelle 5-3 zu betrachten, die zu einer Anforderung des Systems führen. Andere auslösende Ereignisse, die zu Anforderungen von Einrichtungen des Sicherheitssystems führen und die mit den Ereignissen in Tabelle 5-3 nicht abgedeckt sind, sind entsprechend zu klassifizieren, zum Beispiel Absicherung gegen Überspeisungstransienten, Kombinationen von auslösenden Ereignissen. Für jedes dieser auslösenden Ereignisse ist die Summe aus der zugehörigen Ereignisklassennummer E_e und dem Redundanzgrad k_e des betrachteten Systems während es Instandhaltungsvorgangs zu bilden: sie charakterisiert die Eintrittshäufigkeit für unzulässige Kernzustände oder unzulässige Aktivitätsfreisetzungen, wobei ein kleiner Wert von $E_e + k_e$ einer hohen Eintrittshäufigkeit entspricht.

(2) Mit dem minimalen Wert der Summen aus E_e und k_e liefert Tabelle 5-5 den Zeitbereich für die zulässige Instandhaltungszeit I.

k_e / E_e	-1	0	1	2
2	-	24 h	14 d	14 d-2 m
3	-	24 h	14 d-2 m	2 m-BE
4	-	14 d-2 m	2m-BE	BE
5	14 d-2 m	BE	BE	-
BE = bis zum nächsten Brennelementwechsel				

Tabelle 5-5: Bereiche für zulässige Instandhaltungszeiten I in Abhängigkeit von Ereignisklassen er E_e und Redundanzgrad k_e während der Instandhaltung.

Die Tabelle ist wie folgt anzuwenden:

- Beträgt der minimale Wert von $E_e + k_e = 4$, so wird eine zulässige Instandhaltungszeit I im Bereich 14 Tage ≤ I ≤ 2 Monate festgelegt
- Beträgt der minimale Wert von $E_e + k_e = 5$, so wird eine zulässige Instandhaltungszeit im Bereich Monate ≤ I ≤ Brennelementwechsel festgelegt.
- Beträgt der minimale Wert von $E_e + k_e \geq 6$, so wird die zulässige Instandhaltungszeit nicht beschränkt .
- Für die Systeme, für die im Einzelfehlerkonzept die Beherrschung des Einzelfehlers gefordert wird und für die während der Instandhaltung der Einzelfehler nicht mehr beherrscht wird, ist die zulässige Instandhaltungszeit auf 24 Stunden zu begrenzen.
- Für den Fall, dass $E_e = 2$ und $k_e = 1$ ist wird die zulässige Instandhaltungszeit auf 14 Tage festgelegt

Ohne weitere Nachweise gilt als zulässige Instandhaltungszeit die Untergrenze aus Tabelle 5-5.

(3) Im Einzelfall dürfen aufgrund von Nachweisen für zulässige Instandhaltungszeiten Werte zwischen den Untergrenzen und Obergrenzen der nach Absatz 2 festgelegten Bereiche genommen werden.

5.5 Anwendungsbeispiele

5.5.1 Druckwasserreaktor - Konvoi

a) <u>HD-, ND- Einspeisung und Nachkühlketten</u>

HD-, ND-Einspeisung und Nachkühlketten sind angefordert durch folgende auslösende Ereignisse:

5.1 Kleines Leck - Ereignisklasse 3

5.2 Großes Leck - Ereignisklasse 4

Da in beiden Fällen die gleiche Zahl von Redundanten (2 von 4) zur Störfallbeherrschung benötigt wird, wird die zulässige Instandhaltungszeit vom Störfall der niedrigeren Ereignisklasse, dem "Kleinen Leck", bestimmt ($E_e = 3$).

Ist eine Redundante ausgefallen, so steht noch eine Redundante mehr zur Verfügung als zur Störfallbeherrschung erforderlich ist, d.h. $k_e = 1$. Damit ergibt sich $E_e + k_e = 4$ und eine zulässige Instandhaltungszeit von 14 d bis 2 m. Dieser Zeitbereich deckt die gegenwärtige Genehmigungspraxis ab. Sind zwei Redundanten ausgefallen (aber kein Common-Mode), so beträgt die zulässige Instandsetzungszeit 24 Stunden.

b) <u>Notspeisesystem</u>

Das Notspeisesystem wird angefordert durch die Störfälle

2 Notstromfall - Ereignisklasse 2

3.1 Ausfall der betrieblichen Speisepumpen - Ereignisklasse 2

3.2 Bruch von Rohrleitungen im Speisewasserleitungssystem - Ereignisklasse 3

5.1 Kleines Leck - Ereignisklasse 3

7.1 Sicherheitserdbeben - Ereignisklasse 4

7.2 Flugzeugabsturz - Ereignisklasse 5

Bei den Störfällen 2, 3.1 und 5.1 darf das An- und Abfahrsystem als eine Redundante des Notspeisesystems berücksichtigt werden. Bei den Störfällen 2, 3.1 und 3.2 konnte nachgewiesen werden, dass eine Redundante zur Störfallbeherrschung ausreicht. Damit erhält man bei Ausfall einer Redundanten des Notspeisesystems abhängig vom Störfall folgende Redundanzgrade. Mit der Ereignisklassennummer wird die Summe aus beiden Größen gebildet:

2	$k_e = 3$, $E_e = 2$	$E_e + k_e = 5$
3.1	$k_e = 3$, $E_e = 2$	$E_e + k_e = 5$
3.2	$k_e = 2$, $E_e = 3$	$E_e + k_e = 5$
5.1	$k_e = 2$, $E_e = 3$	$E_e + k_e = 5$
7.1	$k_e = 1$, $E_e = 4$	$E_e + k_e = 5$
7. 2	$k_e = 1$, $E_e = 5$	$E_e + k_e = 6$

Der maßgebliche minimale Wert von $E_e + k_e$ beträgt 5. Damit liefert Tabelle 5-5 für den Ausfall einer Redundanten eine zulässige Instandhaltungszeit von 2 m bis BE. Für die bereits in Betrieb befindlichen Anlagen wurde eine zulässige Instandhaltungszeit von meist 7 bis 14 Tagen festgelegt. Dieses Beispiel zeigt, dass die vorgeschlagenen Kriterien aufgrund der Flexibilität bei der Berücksichtigung von Betriebssysteme und realistischen Wirksamkeits-bedingungen zu einer deutlichen Verlängerung der zulässigen Instandhaltungszeiten führen können.

5.5.2 Siedewasserreaktor - KKK

Nachkühlketten

Die Nachkühlketten werden angefordert durch die auslösenden Ereignisse:

2 Notstromfall - Ereignisklasse 2

5.1 Kleines Leck - Ereignisklasse 3

6 Ausfall Hauptwärmesenke – Ereignisklasse 2

7.1 Sicherheitserdbeben - Ereignisklasse 4 (Standortspezifisch evtl. 5)

7.2 Flugzeugabsturz - Ereignisklasse 5

Bei den Störfällen 2 und 6 konnte nachgewiesen werden, dass eine Redundante zur Störfallbeherrschung ausreicht. Bei den Störfällen 7.1 und 7.2 muss berücksichtigt werden, dass nur 2 Redundanten gegen diese Ereignisse ausgelegt sind, von denen eines zur Störfallbeherr-schung ausreicht. Damit erhält man bei Ausfall einer Redundanten der Nachkühlketten die aufgeführten Redundanzgrade. Mit der Ereignisklassennummer wird die Summe aus beiden Größen gebildet:

2	$k_e = 2$, $E_e = 2$	$E_e + k_e = 4$
5.1	ke = 1, Ee =3	Ee + ke = 4
6	ke = 2, Ee =2	Ee + ke = 4
7 .1	ke = 0, Ee =4	Ee + ke = 4
7.2	$k_e = 0$, $E_e = 5$	$E_e + k_e = 5$

Der minimale Wert von $E_e + k_e$ beträgt 4. Damit ergibt sich bei Ausfall einer Redundanten eine zulässige Instandhaltungszeit von 14 d bis 2 m. Die genehmigte Zeit beträgt 150 h, d. h. weniger als 7 Tage.

5.5.3 Zusammenfassende Bewertung

a) Die beiden Parameter Ereignisklasse und Redundanzgrad erlauben mit geringem Aufwand die Festlegung von zulässigen Instandhaltungszeiten.

b) Die ermittelten Zeiten sind in den meisten Fäll n vergleichbar zu oder etwas länger als die entsprechenden Zeiten bei bereits genehmigten Anlagen.

c) In Einzelfällen, in denen sehr viele Redundanten vorhanden sind oder Systeme nur mit sehr geringer Wahrscheinlichkeit angefordert werden, ergibt sich eine deutlich Verlängerung der zulässigen Instandhaltungszeit.

5.6 Diskussion und Schlussfolgerung

(1) Mit den vorgeschlagenen Kriterien zur Festlegung zulässiger Instandhaltungszeiten hat das AG mit seiner überwiegenden Mehrheit der Ereignisklassenmethode in Anlehnung an das Ereignisklassenkonzept /9/ den Vorrang gegen die als bisherigen Stan d der Technik anzusehenden Methoden, die vorzugebende Referenzwerte verwenden, gegeben.

(2) Es sei nochmals auf die Unterschiedlichkeit beider Ansätze hingewiesen. Bei Methoden, die vorzugebende Referenzwerte verwenden, wird nur die Nichtverfügbarkeit eines Systems mit und ohne Berücksichtigung der Instandhaltungszeiten verglichen. Bei der Ereignisklassenmethode wird als zusätzlicher Parameter die Eintrittshäufigkeit der auslösenden Ereignisse berücksichtigt. Das führt zu gegenläufigen Abhängigkeiten vom Redundanzgrad bei beiden Methoden und im Einzelfall auch zu inkompatiblen Ergebnissen.

(3) Die Zugrundelegung von Ereignisklassen setzt bei der Anwendung des Konzepts auf Nicht-LWR voraus, dass ein allgemeiner Konsens über die Klassifizierung auslösender Ereignisse herbeigeführt wird. Durch die alleinige Erfassung des Redundanzgrads als Maß für die Nichtverfügbarkeit werden Kombinatorikfaktoren, Unterschiede in den Nichtverfügbarkeiten der Redundanten und Common-Mode Einflüsse vernachlässigt, Effekte deren Variationsbreite durchaus den anzusetzenden Redundanzgrad k_e um 1-2 verändern können. Auch werde das Konzept nicht so weit ausgearbeitet, um in konsistenter Weise vermaschte Strukturen berücksichtigen zu können. In diese Fällen ist eine detaillierte probabilistische Analyse, die die Gesichtspunkte der Ereignisklassenmethode berücksichtigt, durchzuführen. Vor diesem Hintergrund muss deutlich darauf hingewiesen werden, dass die in Abschnitt 5.5 angegebenen Mindestwerte von $E_e + k_e$ nicht als Risikoschätzungen für die jeweiligen Anlagen interpretiert werden dürfen.

(4) Trotz aller durch die Komplexität der Beurteilungsgrundlagen bedingten Nachteile der Ereignisklassenmethode zur Festlegung zulässiger Zeiten ist das Arbeitsgremium der Ansicht, ein in der Praxis anwendbares und zur Vereinheitlichung beitragendes Konzept vorgelegt zu haben, das den Umfang der auf der Ebene der Fachleute derzeit konsensfähigen Festlegungen widerspiegelt.

6 Ergänzende Gesichtspunkte bei der Durchführung von Instandhaltungsmaßnahmen

(1) Die zulässige Instandhaltungszeit gilt für die Instandsetzung nach der Entdeckung eines Ausfalles. Dabei gilt jedoch einschränkend:

a) Die mittlere Instandsetzungszeit sollte wesentlich kürzer sein als die zulässige Instand-haltungszeit I.

b) Falls bei einem Ausfall eines Systemteils nach Feststellung der Ausfallursache ein Hinweis auf einen Aus all infolge gleicher Ursache (Common-mode-Ausfall) vorliegt, so ist dies in den gleichartigen Systemteilen der anderen Redundanten zu überprüfen. c) Instandsetzungs-maßnahmen nach Ausfällen, die zur Nichtverfügbarkeit einer oder mehrerer Redundanten eines der in Abschnitt 3 aufgeführten Systeme führen, sind unverzüglich zu beginnen.

(2) Wartungs- und Inspektionsarbeiten die eine Nichtverfügbarkeit einer Redundanten zur Folge haben, dürfen auch während des Leistungsbetriebes des Reaktors durchgeführt werden, wenn folgende Bedingungen erfüllt sind:

a) Abgesehen von kurzzeitigen Funktionsprüfungen, die mit einer Nichtverfügbarkeit der Redundanten verbunden sind, dürfen während der Wartung und Inspektion an einer Redundanten keine anderen Redundanten als nichtverfügbar bekannt sein.

b) Für Wartungsarbeiten während des Leistungsbetriebs dürfen je Redundante und Jahr 7 Tage vorgesehen werden.

c) Wartungsarbeiten, die länger als 24 Stunden dauern, dürfen nur begonnen werden, wenn die letzte Prüfung einer anderen Redundanten nicht länger als 14 Tage zurückliegt, andernfalls sind vorgezogene Prüfungen durchzuführen (wenn das Testintervall vier Wochen oder weniger beträgt).

(3) Instandhaltungsarbeiten sind auch innerhalb der zulässigen Instandhaltungszeiten so schnell wie mit angemessenem ‚Aufwand möglich durchzuführen.

7 Maßnahmen bei Nichteinhaltung von zulässigen Instandhaltungszeiten

7.1 Übergeordnete Gesichtspunkte

(1) Grundsätzlich sind Maßnahmen zu treffen, wenn (erkennbar wird, dass zulässige Instandhaltungszeiten nicht eingehalten werden können

(2) Gibt es keine Maßnahmen, die die Bedingungen von Absatz 3 erfüllen, so muss durch Instandhaltungsplanung und Ersatzteilhaltung sichergestellt sein, dass die nach Kapitel 5 festgelegten zulässigen Instandhaltungszeiten eingehalten werden können.

(3) Diese Maßnahmen müssen folgenden Bedingungen genügen:

a) Die Maßnahmen müssen entweder die Funktionsbereitschaft des betroffenen Systems überflüssig machen, sie ersetzen oder dazu führen, dass zur Beherrschung des Ereignisablaufs weniger Redundanten des betroffenen Systems ausreichen als auslegungsgemäß vorgesehen worden sind.

b) Die Maßnahmen sollen nicht zu einer Anforderung des betroffenen Systems führen.

7.2 Auszuwählende Maßnahmen

Die auszuwählenden Maßnahmen richten sich nach Anforderungszustand, Art und Aufgabenstellung des Systems, z. B.:

a) Abfahren der Anlage in den Zustand heiß unterkritisch oder kalt drucklos,

b) Leistungsreduzierung auf Teillast, wenn dadurch der ursprüngliche Redundanzgrad des Systems wieder hergestellt wird,

c) Einsatz von normalerweise nicht zur Beherrschung von Ereignisabläufen verwendeten Aggregaten, die die Aufgaben der ausgefallenen Redundanten übernehmen können, z B. mobile Aggregate,

d) Schaltmaßnahmen, durch die die Funktion der ausgefallenen Komponente ersetzt wird, z. B. Anregung eine ausgefallenen Kanals im Reaktorschutzsystem bei eindeutig sicherheitsgerichteten Signalen oder Verfahren einer Armatur in die sichere Stellung,

e) Besetzung von örtlichen Leitständen, Teil oder Notsteuerstellen bei Ausfall von Anzeigen oder Auslöskriterien, wenn dadurch das ausgefallene System überflüssig wird.

8 Behandlung von Instandhaltungszeitbeschränkungen im deutschen Genehmigungsverfahren

8.1 Rückblick

(1) Als das Sicherheitssystem von Kernkraftwerken ab etwa 1970 derart ausgelegt wurde, dass Einzelfehler und Instandhaltungsfall beim Störfall beherrscht werden, sah man den vierten Strang von viersträngigen Sicherheitssystemen zunächst als reinen "Reparaturstrang" an.

(2) Das Sicherheitssystem wurde aber nicht ur deterministisch, sondern auch probabilistisch bewertet. Mit Hilfe der Referenzwertmethode (siehe Kap. 4.3.2) wurden auch für Ausfälle einer Redundanten zulässige Instandhaltungszeiten ermittelt

(3) Zur Vereinheitlichung der Vorgehensweise wurde 1977/78 eine Untersuchung durchgeführt, in der für die Anlagen Neckarwestheim, Biblis A/B, Unterweser sowie Brunsbüttel, Philippsburg, Isar die Beschränkungen zusammengestellt und bewertet wurden /8/. In einer anschließenden Arbeit wurde versucht, durch Einfuhr ng einer "Risikomethode" die Mängel der damals üblichen Referenzwertmethode zu beheben. Die in /3/.dokumentierten Vorschläge dient n als Grundlage für die Festlegung der zulässigen Instandhaltungszeiten des KKW Grafenrheinfeld - und damit auch der Folgeanlage . Gleichzeitig stellten sie den Ausgangspunkt für die Arbeiten am Regelvorhaben KTA 1407 dar.

8.2 Umfang der zu betrachtenden Systeme

(1) Der Umfang der zu betrachtenden Systeme orientierte sich bei den Druckwasserreaktoren ab KKW Grafenrheinfeld an /3/ sowie an den jeweiligen Gutachtensbedingungen.

(2) Dieser Umfang ist zum Beispiel aus der Anlage 2 zu ersehen, die einen Auszug aus den Sicherheitstechnischen Bedingungen einer Anlage wiedergibt. Das Beispiel umfallt alle Teile d s Sicherheitssystems. Weiterhin sind Systeme oder Systemteile erfasst, die zur Versorgung von Sicherheitseinrichtungen nötig sind. Dies gilt insbesondere für die Energieversorgung. Über den genannten Bereich hinausgehend wurden auch anlagenspezifische Sonderegelungen für Ausfall/-Teilausfall von Prozessrechneranlagen, Kerninstrumentierung und Begrenzungen sowie für die Sicherheitseinrichtungen gegen Drucküberschreitung mit dem Gutachter vereinbar .

(3) In einer anderen Anlage ist der Umfang wesentlich erweitert worden.

8.3 Behandlung von Instandsetzung, Wartung und Inspektion

In der Sicherheitsspezifikation der Betriebshandbücher für neuere Kernkraftwerke wurde überwiegend nur die Instandsetzung geregelt. Wartungen und Inspektionen wurden dabei im allgemeinen im Rahmen der Regelungen zur Instandsetzung durchgeführt. Bei einer Anlage darf während des Leistungsbetriebs grundsätzlich keine Wartungsarbeit mit Nichtverfügbarkeit von einer oder mehr Redundanten des Sicherheitssystems durchgeführt werden. Bei einer anderen Anlage flossen die Vorschläge aus der laufenden Arbeit am Regelvorhaben KTA 1407 in die Festlegungen ein (siehe Anlage 3).

8.4 Festlegung von zulässigen Instandsetzungszeiten

(1) Generell wurde zunächst überprüft, ob durch das kerntechnische Regelwerk oder durch Gutachtensbedingungen Instandsetzungszeiten bereits festgelegt sind. Dabei wurden insbesondere KTA 3301 "Nachwärmeabfuhrsysteme von Kernkraftwerken", KTA 3501 "Reaktorschutzsystem und Überwachungseinrichtungen des Sicherheitssystems", KTA 3701 "Übergeordnete Anforderungen an die elektrische Energieversorgung des Sicherheitssystems in Kernkraftwerken" berücksichtigt.

(2) Die Ermittlung der zulässigen Instandsetzungszeiten erfolgt dann nach dem Redundanzgrad des ungestörten Sicherheitssystems - evtl. unter Einbeziehung von Betriebssystem n - in Bezug auf die zu beherrschenden Störfälle. Bestimmend ist er Störfall, für denn das Sicherheitssystem den geringsten Redundanzgrad aufweist (Probabilistische Aspekte wie Ereignisklasse des Störfalles bleiben außer acht), allerdings wurden Störfälle, die gemäß den Interpretationen zum Einzelfehlerkonzept unter Ereignisse oder Ereignisketten mit sehr geringer Eintrittswahrscheinlichkeit einzustufen sind, im allgemeinen nicht oder in abgestufter Weise berücksichtigt.

(3) Bei einigen Anlagen wurde wie folgt verfahren:

a) (n+1)-Systeme

Ein (n+1)-System ist ein System, das - zusätzlich zu den für die Beherrschung von Störfällen benötigten Redundanten - eine weitere Redundante besitzt.

Bei erkanntem Ausfall einer Redundante beträgt die zulässige Instandsetzungszeit 24 h. Bei Ausfall von mehr als einer Redundanten ist die Anlage unverzüglich in einen sicheren Zustand zu überführen.

Hiervon abweichende spezielle Regelungen wurde separat aufgeführt und sind zu beachten.

b) (n+2)-Systeme

Wird der Ausfall einer Redundanten festgestellt, so ist die Instandsetzung unverzüglich einzuleiten und die erwartete Instandhaltungsdauer abzuschätzen.

Bei erkanntem Ausfall einer Redundante beträgt die zulässige Instandsetzungszeit 14 Tage. Wenn sich absehen lässt, dass die Dauer der Instandsetzung 14 Tage überschreite wird, ist nach Punkt a) zu verfahren.

Der Ausfall zweier Redundanten wird wie der Ausfall einer Redundanten eines (n+1)-Systems behandelt. Bei Ausfall von mehr als zwei Redundanten ist die Anlage unverzüglich in einen sicheren Zustand zu überführen.

c) (n+3)-Systeme

Die Instandsetzung ist bis zum nächsten Wiederanfahren zu beenden.

8.5 Maßnahmen bei Überschreitung der zulässigen Instandhaltungszeit

(1) Bei Überschreitung von kurzen Instandsetzungszeiten (I < 24 h) gilt generell: Die Anlage ist in den sicheren Zustand zu überführen und die Aufsichtsbehörde zu verständigen.

(2) Diese Bestimmungen gelten für einige Anlagen auch bei längeren Instandsetzungszeiten, bei anderen wird nur verlangt, dass rechtzeitig vor Überschreiten der zulässigen Instandhaltungszeit das weitere Vergehen mit der Aufsichtsbehörde abzustimmen ist.

(3) Der sichere Zustand wird für Druckwasserreaktoren im allgemeinen wie folgt definiert:

a) Bei Ausfällen im Bereich der Nachkühlkette:

- Primärkreisdruck $p_e \approx 31$ bar,
- Primärkreistemperatur 120 °C,
- Wärmeabfuhr über die Sekundärseite.

b) Bei sonstigen Ausfällen, insbesondere im Bereich der sekundärseitigen Wärmeabfuhr:

- Primärkreisdruck $p_e \approx 31$ bar,
- Primärkreistemperatur < 100 °C,
- Wärmeabfuhr über die Nachkühlkette.

Anlage 1
zu Regelvorhaben KTA 1407
von R 542/Dre/R 351/Mü/ka vom 26.08.1986

Vereinfachter Vergleich der Regelungen bei neueren KWU-DWR

	KKU	GKN1	KKG/BAG	KKP 2	KWG	KBR
1 Ausfall (n+3)-Systeme	-	-	BE 1)	BE 1)	BE 1)	2 mon. 2)
1 Ausfall (n+2)-Systeme	2 mon.	10 d	7 d	14 d	14 d	14 d
1 Ausfall (n+1)-Systeme	2 h	0	10 h	24 h	24 h	24 h
2 Ausfälle (n+2)-Systeme	2 h	0	10 h	24 h	24 h	24 h

1) BE = bis zum nächsten Wiederanfahren

2) Sofern keine speziellen Regelungen getroffen wurden

Anlage 2.1
zu Regelvorhaben KTA 1407
von R 542/Dre/R 351/Mü/ka vom 26.08.1486

Sicherheitstechnische Bedingungen bei eingeschränkter Verfügbarkeit von Systemen und Komponenten, Geltungsbereich

Sicherheitsspezifikation

System/Funktion

1. Systeme zur Abschaltung
   Schnellabschaltsystem
   Zusatzboriersystem

2. Systeme zur Nachwärmeabfuhr im Betrieb und bei Störfällen
   Nachkühlkette (TH, TF, VE)
   Allgemeine Verfahrensweise
   Sonderregelung in Verbindung mit der Beckenkühlung
   Notspeisesystem inkl. Notspeisenotstromdiesel
   Bespeisung DE
   Sekundärkreisabschluss
   Sekundärseitige Abblaseeinrichtung

3. Aktivitätseinschluss
   Ringraumabsaugung
   Gebäudeabschluss

4. Sicherheitseinrichtungen gegen Drucküberschreitung
   Druckabsicherung des Reaktorkühl- und Druckhaltesystems
   Druckhalter-Sicherheitsventile
   Druckabsicherung der Frischdampfleitungen
   Frischdampfseitige Druckabsicherungsfunktion.

Anlage 2.2
zu Regelvorhaben KTA 1407
von R 542/Dre/R 351/Mü/ka vom 26.08.1986

Sicherheitstechnische Bedingungen bei eingeschränkter Verfügbarkeit von Systemen und Komponenten, Geltungsbereich	Sicherheitsspezifikation

System/Funktion

5. Energieversorgung

Notstromerzeugungsaggregate einschl. Hilfssysteme und äußerer Kühlkreis VJ sowie Drehstromschaltanlagen und Transformatoren des Notstromsystems

Notspeisenotstromaggregate einschl. Hilfssysteme und äußerer Kühlkreis RS sowie Drehstromschaltanlagen des Notspeisenotstromsystems

Gleichstromanlagen

220 V-Gleichrichter

220 V-Verteilungsanlagen

220 V-Batterie

24 V-Gleichrichter

24 V-Verteilungsanlagen

24 V-Batterie

Umformeranlagen, Wechselrichter

6. Leittechnik

Reaktorschutzsystem einschl. Reaktorschutzinstrumentierung

Prozessrechneranlage

Begrenzungen

Störfallinstrumentierung

Kerninstrumentierung

Anlage 3
zu Regelvorhaben KTA 1407
von R 542/Dre/R 351/Mü/ka vom 26.08.1986

Sicherheitstechnische Bedingungen bei eingeschränkter Verfügbarkeit von Systemen und Komponenten, Geltungsbereich

Sicherheitsspezifikation

Allgemeine Verfahrensweise bei Wartung und Inspektion

Allgemeines

Wartungs- und Inspektionsarbeiten sowie wiederkehrende Prüfungen, die eine Nichtverfügbarkeit einer Redundanten oder einer anderen sicherheitstechnisch wichtigen Einrichtung im Anforderungsfall zur Folge haben, dürfen grundsätzlich auch während des Leistungsbetriebes des Reaktors durchgeführt werden.

Alle Wartungs- und Inspektionsarbeiten sind auch innerhalb der zulässigen Instandhaltungszeiten so schnell wie mit angemessenem Aufwand möglich durchzuführen.

Die aufgrund von Wartung und Inspektion entstandenen Nichtverfügbarkeiten der aufgeführten Systeme und Funktionen sind in einem Verfügbarkeitsbuch zu registrieren und zu bilanzieren.

Die jeweils maßgebliche Verfahrensweise wird den einzelnen Systemen ggf. Systemfunktionen zugeordnet.

(n+1)-System

Eine Wartung an einer Redundante eines (n+1)-Systems ist ohne eine - seine Funktion ersetzende oder überflüssig machende - Maßnahme nicht zulässig.

(n+2)-Systeme

Für Wartungsarbeiten dürfen je Redundante und Jahr 7 Tage vorgesehen werden, wenn folgende Bedingungen erfüllt sind:

- Abgesehen von kurzzeitigen Funktionsprüfungen dürfe während der Wartung. und Inspektion an einer Redundanten keine anderen Redundanten als nichtverfügbar bekannt sein.
- Wartungsarbeiten, die länger als 24 Stunden dauern, dürfen nur begonnen werden, wenn die letzte Prüfung der anderen Redundanten nicht länger als 14 Tage zurückliegt. Andernfalls sind diese vorgezogen zu prüfen.

(n+3)-Systeme

Wartungsarbeiten an einer Redundante dürfen durchgeführt werden, wenn bei Beginn keine anderen Redundanten als nicht verfügbar bekannt sind.

9 Schlussbemerkung

(1) Die Festlegung von zulässigen Instandhaltungszeiten für Einrichtungen des Sicherheitssystems wird in den Sicherheitskriterien für Kernkraftwerke gefordert. Die Forderung dient ein Ziel, sicherzustellen, dass die Zuverlässigkeiten dieser Sicherheitseinrichtungen durch Instandhaltungsvorgänge nicht unter die zur Störfallbeherrschung erforderlichen Zuverlässigkeiten herabgesetzt werden.

(2) Zulässige Instandhaltungszeiten wurden individuell für jede Anlage festgelegt und im Betriebshandbuch festgeschrieben. Das war und ist auch dann der Fall, wenn durch anlagentechnische Veränderungen Einrichtungen des Sicherheitssystems betroffen sind. Bei der Festlegung dieser Zeiten hat man sich auf Zuverlässigkeitsanalysen abgestützt; ein einheitliches methodisches Vorgehen ist jedoch nicht erkennbar.

(3) Probabilistische Methoden sind für die Festlegung von zulässigen Instandhaltungszeiten grundsätzlich geeignet haben aber Spezifische Nachteile. Als eine leicht zu handhabende pragmatische Methode wurde vom Arbeitsgremium die Ereignisklassenmethode entwickelt. Bei ihr werden zwei Parameter verwendet. Der erste Parameter, die Ereignisklasse, charakterisiert die Häufigkeit von Ereignissen, die die Einrichtungen des Sicherheitssystems anfordert . Der zweite Parameter, der Redundanzgrad, charakterisiert die Wahrscheinlichkeit, mit der das Sicherheitssystem bei einer Anforderung ausfällt. Der Summe beider Parameter wird deterministisch ein Intervall für die zulässige Instandhaltungszeit zugeordnet.

(4) Auch die Ereignisklassenmethode hat einige Schwächen. Eine besteht z. B. darin, dass die Klassifizierung von Ereignisabläufen und mithin die Ereignisklassen nicht als verbindlich Regel, sondern lediglich als Konzept vorliegen. Für andere Reaktortypen als dem Leichtwasserreaktor liegen Ereignisklassen noch nicht einmal im Konzept vor. Insofern ist der Anwendungsbereich des Verfahrens gegenwärtig auf Leichtwasserreaktoren beschränkt, und er schließt beispielsweise Hochtemperaturreaktoren aus. Schließ ich werden Bedenken vorgebracht, dass die Summe aus Ereignisklassenummer und Redundanzgrad zu einem unzulässig vereinfachten Vergleich von Sicherheitsniveaus verschiedener Anlagen missbraucht werden könnte.

10 Literatur

/1/ E DIN 25 424 Teil 2 (Veröffentlichung in Vorbereitung) Fehlerbaumanalyse; Handrechenverfahren zur Auswertung eines Fehlerbaumes

/2/ L. Kamarinopoulus:
Anwendung von Monte-Carlo-Verfahren zur Ermittlung von Zuverlässigkeitsmerkmalen technischer Systeme, ILR-Bericht 14, TU Berlin 1976

/3/ TÜV-Stuttgart:
Vorschlag zur Festlegung von zulässigen Reparaturzeiten, Auftragsbericht Nr. 81413/SR 121-A1.7, Juni 1980

/4/ Dressler, E., H. Spindler:
Die Nichtverfügbarkeit von Bereitschaftssystemen in Abhängigkeit von Teststrategie und Reparaturzeit, MRR 144, März 1975

/5/ L. Kamarinopoulus:
Direkte und gewichtete Simulationsmethoden zur Zuverlässigkeitsuntersuchung technischer Systeme, Dissertation D83, TU-Berlin 1972, Fachbereich Verkehrswesen

/6/ Schlösser, L.:
STREUSL - Ein Rechenprogramm zur Ermittlung der Streuung in Zuverlässigkeitskenngrößen aufgrund der Streuungen der Eingabedaten, Programmbeschreibung, GRS-19, Juli 1980

/7/ Dressler, E.:
Theoretische Grundlagen zum Programmsystem SAFTL und CRESS zur Berechnung der Zuverlässigkeit von Systemen, MRR 164, September 1976.

/8/ Albertz V.; K. Boesebeck, E. Schimetschka:
Ausführungsvorschläge zur Festlegung zulässiger Reparaturzeiten für Sicherheitssysteme GRS-A-152, 05/78

/9/ Statusbericht zum Konzept: Klassifizierung von Ereignisabläufen für die Auslegung von Kernkraftwerken, Juni 1985 (KTA-GS-47)