Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH

Institut für Sicherheitstechnologie (ISTec) GmbH

- Textmodul -

„Sicherheitsanforderungen für Kernkraftwerke:

Anforderungen an die Leittechnik und Störfallinstrumentierung“

ENTWURF

Revision C

SR 2602

Ergebnisse Team 5

Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH

Institut für Sicherheitstechnologie (ISTec) GmbH

- Textmodul -

„Sicherheitsanforderungen
für Kernkraftwerke:
Anforderungen an die Leittechnik
und Störfallinstrumentierung“

Revision C ENTWURF

Dieser Bericht ist im Auftrag des BMU im Rahmen des Vorhabens SR 2602 erstellt worden. Die Arbeiten des Vorhabens SR 2602 werden in Teams durchgeführt. Der vorliegende Bericht gibt die gemeinsamen Arbeitsergebnisse des Teams 5 „Digitale Leittechnik“ wieder.

Die Mitglieder des Teams 5 sind:

E. Piljugin, Teamleiter, GRS
W. Frey, GRS
R. Grinzinger, GRS
H. Heinsohn, GRS
Dr. A. Lindner**, ISTec

** außer 3.2 (11) und 3.2 (12)

August 2008

Auftrags-Nr.: 813000

Anmerkung:

Der Bericht gibt die Auffassung und Meinung des Auftragnehmers bzw. der Unterauftragnehmer wieder und muss nicht mit der Meinung des Auftraggebers übereinstimmen.

Vorwort

Im Vorhaben SR 2475 wurden zu den im kerntechnischen Regelwerk nicht verankerten oder erheblich überarbeitungsbedürftigen Sicherheitsaspekten modulartig Sicherheitsanforderungen nach Stand von Wissenschaft und Technik als Regeltextmodule im Detaillierungsgrad der „BMI-Sicherheitskriterien“ und „RSK-Leitlinien“ zusammengestellt. Den Sicherheitsanforderungen sind insgesamt 11 Module zugeordnet. Die Sicherheitsanforderungen wurden in einem transparenten Prozess umfassend kommentiert. Alle dazu eingegangenen Kommentare sind in die Bearbeitung eingeflossen und, soweit erforderlich, bei der Erstellung der Revision B der Module berücksichtigt worden. Die Revision B der Module ist seit September 2006 im Internet (http://regelwerk.grs.de) veröffentlicht.

Alle seit September 2006 zur Rev. B der Regeltextmodule eingegangenen Kommentare einschließlich der Hinweise aus den Beratungen des Fachausschuss Reaktorsicherheit (FARS) wurden bei der Erstellung der Rev. C ausgewertet.

Die Rev. C der Regeltextmodule umfasst insgesamt 12 Module. Gegenüber Rev. B wurde Modul 5 neu strukturiert. Die Anforderungen an die Leittechnik sowie an die Störfallinstrumentierung sind, wie bisher, Modul 5 zugeordnet. Die Anforderungen an die Elektrische Energieversorgung sind nun in einem neuen Modul 12 integriert.

Zu folgenden Sicherheitsaspekten wurden Regeltextmodule erstellt:

- Modul 1: „Sicherheitsanforderungen für Kernkraftwerke: Grundlegende Sicherheitsanforderungen“
- Modul 2: „Sicherheitsanforderungen für Kernkraftwerke: Anforderungen an die Auslegung und den Betrieb des Reaktorkerns“
- Modul 3 „Sicherheitsanforderungen für Kernkraftwerke: Bei Druck- und Siedewasserreaktoren zu berücksichtigende Ereignisse“
- Modul 4 „Sicherheitsanforderungen für Kernkraftwerke: Anforderungen an die Ausführung der Druckführenden Umschließung, der drucktragenden Wandung der Äußeren Systeme sowie des Sicherheitseinschlusses“

- Modul 5 „Sicherheitsanforderungen für Kernkraftwerke: Anforderungen an die Leittechnik und Störfallinstrumentierung“
- Modul 6 „Sicherheitsanforderungen für Kernkraftwerke: Anforderungen an die Nachweisführungen und Dokumentation“
- Modul 7 „Sicherheitsanforderungen für Kernkraftwerke: Anforderungen an den anlageninternen Notfallschutz“
- Modul 8 „Sicherheitsanforderungen für Kernkraftwerke: Anforderungen an das Sicherheitsmanagement“
- Modul 9 „Sicherheitsanforderungen für Kernkraftwerke: Anforderungen an den Strahlenschutz“
- Modul 10 „Sicherheitsanforderungen für Kernkraftwerke: Anforderungen an die Auslegung und den sicheren Betrieb von baulichen Anlagenteilen, Systemen und Komponenten“
- Modul 11 „Sicherheitsanforderungen für Kernkraftwerke: Anforderungen an die Handhabung und Lagerung der Brennelemente“
- Modul 12 „Sicherheitsanforderungen für Kernkraftwerke: Anforderungen an die Elektrische Energieversorgung“

Zusätzlich wurden die in den Modulen verwendeten Begriffe in einer Definitionsliste zusammengestellt. Die vorliegende Unterlage des Regeltextmoduls in der Fassung Rev. C enthält dementsprechend in synoptischer Darstellung die Ergebnisse der Auswertung aller bisher zum Modul 5 „Sicherheitsanforderungen für Kernkraftwerke: Anforderungen an die Leittechnik und Störfallinstrumentierung“ übermittelten Kommentare und Hinweise. Zur besseren Lesbarkeit ist Rev. C von Modul 5 in einen Fließtext umgesetzt worden. Rev. C von Modul 5 ist im Internet unter http://regelwerk.grs.de verfügbar.

Das Zusammenwirken aller Regeltextmodule und der weiteren kerntechnischen Regelungen ist in einem Wegweiser dargestellt.

Gliederung

1 Geltungsbereich

Die nachfolgenden Anforderungen gelten für leittechnische Einrichtungen, die auf den Sicherheitsebenen 1 bis 4 Leittechnik-Funktionen mit sicherheitstechnischer Bedeutung ausführen.

Die Anforderungen werden durch Einrichtungen realisiert, bei denen Hard- und Software Leittechnik-Funktionen ausführen.

2 Kategorisierung

Entsprechend ihrer sicherheitstechnischen Bedeutung sind die Leittechnik-Funktionen in unterschiedliche Kategorien eingeordnet, für die abgestufte Anforderungen gelten:

Kategorie A
Die Leittechnik-Funktionen der Kategorie A umfassen alle Funktionen, die erforderlich sind, um Ereignisse der Sicherheitsebene 3 zu beherrschen.

Kategorie B
Die Leittechnik-Funktionen der Kategorie B umfassen alle Funktionen, die erforderlich sind, um Ereignisse der Sicherheitsebene 2 zu beherrschen sowie das Eintreten von Ereignissen der Sicherheitsebene 3 zu vermeiden.

Kategorie C
Die Leittechnik-Funktionen der Kategorie C umfassen alle übrigen Funktionen mit sicherheitstechnischer Bedeutung.

Nicht kategorisiert sind Leittechnik-Funktionen, die keine unmittelbare sicherheitstechnische Bedeutung haben.

Hinweis Für leittechnische Einrichtungen, die nicht kategorisierte Leittechnik-Funktionen ausführen, werden im Folgenden keine Anforderungen gestellt.

3 Auslegung

3.1 Leittechnische Einrichtungen für Leittechnik-Funktionen der Kategorien A bis C

3.1 (1) Leittechnische Einrichtungen, die für die Ausführung von Leittechnik-Funktionen unterschiedlicher Kategorien vorgesehen sind, sind nach den Anforderungen der Kategorie mit der höchsten sicherheitstechnischen Bedeutung geplant, ausgelegt und werden nach den Anforderungen dieser Kategorien betrieben.

3.1 (2) Eine auf ihre Eignung überprüfte oder für den Einsatzfall und für die unterstellten Einsatzbedingungen betriebsbewährte und möglichst wartungsfreie Hardware ist eingesetzt.
Eine auf ihre Eignung überprüfte Software ist eingesetzt.

3.1 (3) Leitungen und Kabel einschließlich Lichtwellenleiter sind nach Redundanten getrennt und, soweit erforderlich, gegen Einwirkungen von innen und außen geschützt verlegt.

3.1 (4) Die leittechnischen Einrichtungen sind so ausgelegt, montiert, abgeschirmt und geschützt, dass eine unzulässige Beeinflussung der Signale durch anlageninterne sowie durch äußere Störquellen vermieden wird.

3.1 (5) Es sind Maßnahmen und Einrichtungen vorhanden, die es ermöglichen, die Funktionsfähigkeit der leittechnischen Einrichtungen und ihr Zusammenwirken mit den aktiven und passiven Komponenten des Sicherheitssystems zu überprüfen und den Zustand dieser sicherheitstechnischen Einrichtungen zu überwachen.

3.1 (6) Meldungen von aktiven Komponenten, welche den Funktionsablauf der leittechnischen Einrichtungen mitbestimmen, werden vorzugsweise aus der Prozessvariablen abgeleitet oder unmittelbar am verfahrenstechnischen Stellglied abgegriffen.

3.1 (7) Leittechnische Einrichtungen, die Leittechnik-Funktionen der Kategorien A und B ausführen, sind so ausgelegt und werden so betrieben, dass ihre Funktionsfähigkeit unabhängig von Art und Umfang der zeitlichen Änderung ihrer Eingangssignale gewährleistet wird.

Die Meldeanlagen sind so ausgelegt, dass ein Meldeschwall ohne Verlust sicherheitsrelevanter Informationen verarbeitet wird.

3.1 (8) Die leittechnischen Einrichtungen sind so ausgelegt, dass notwendige Anpassungen an regelmäßig wiederkehrende Zustände des Normalbetriebs (z.B. Streckbetrieb) einfach und zuverlässig durchführbar sind.

3.1 (9) Die leittechnischen Einrichtungen sind so ausgelegt, dass die in den aktiven verfahrenstechnischen Einrichtungen vorhandene Unabhängigkeit und Fehlertoleranz durch sie nicht beeinträchtigt werden.

3.1 (10) Die Störfallfestigkeit der leittechnischen Einrichtungen ist, soweit erforderlich, nachgewiesen.

3.1 (11) Zur Absicherung gegen Bedienungsfehler werden technische Vorkehrungen vorzugsweise vor organisatorischen Maßnahmen angewandt.

3.1 (12) Die leittechnischen Einrichtungen sind so ausgelegt, dass die für die Beherrschung von Ereignissen und für die Durchführung von Maßnahmen des anlageninternen Notfallschutzes erforderlichen Eingriffsmöglichkeiten vorhanden sind. Die Eingriffsmöglichkeiten sind so ausgelegt, dass sie die Funktionsfähigkeit der leittechnischen Einrichtungen bei der Beherrschung der Ereignisse der Sicherheitsebenen 2 und 3 nicht unzulässig beeinträchtigen. Die Eingriffsmöglichkeiten sind gegen Fehlbedienung gesichert.

3.2 Leittechnische Einrichtungen für Leittechnik-Funktionen der Kategorie A

3.2 (1) Bei der Auslegung der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, sind versagensauslösende Ereignisse innerhalb und außerhalb des Sicherheitssystems berücksichtigt.

3.2 (2) Veränderungen an Bereitschaftsstellungen von Einrichtungen des Sicherheitssystems werden nur dann vorgenommen, wenn entsprechende Freigabebedingungen erfüllt sind und wenn diese Veränderungen automatisch oder durch technische Vorkehrungen bzw. organisatorische Maßnahmen wieder aufgehoben werden, wenn die Freigabebedingungen nicht mehr erfüllt sind. In dem sicherheitstechnisch geforderten Zustand sind diese Einrichtungen gegen unzulässige Eingriffe geschützt.

3.2 (3) Sind bei Einrichtungen des Sicherheitssystems eindeutige Bereitschaftsstellungen von Stellgliedern bei Normalbetrieb vorgeschrieben, so wird das Verlassen dieser Bereitschaftsstellung signalisiert.

3.2 (4) Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, sind zur Sicherstellung ihrer Funktionsfähigkeit zuverlässig ausgelegt. Sie sind so ausgelegt, dass auch bei Instandhaltungsmaßnahmen an diesen Einrichtungen das Sicherheitssystem seine Aufgabe mit ausreichender Zuverlässigkeit erfüllt (siehe auch „Sicherheitsanforderungen für Kernkraftwerke: Anforderungen an die Auslegung und den sicheren Betrieb von baulichen Anlagenteilen, Systemen und Komponenten“ (Modul 10) Abschnitt 1.1).

a) Die leittechnischen Einrichtungen des Sicherheitssystems, die Leittechnikfunktionen der Kategorie A ausführen, sind redundant ausgelegt. Sie sind räumlich getrennt oder durch sicherheitstechnisch gleichwertige Vorkehrungen geschützt und unabhängig ausgeführt.

b) Ein Ausfall in den leittechnischen Einrichtungen des Sicherheitssystems hat höchstens Auswirkungen auf die Funktion der betroffenen Redundante des Sicherheitssystems.

c) Die leittechnischen Einrichtungen, die für die Funktionsfähigkeit des Sicherheitssystems nach Eintritt von Ereignissen der Sicherheitsebene 3 erforderlich sind, sind so ausgelegt, dass sie den jeweils ungünstigsten Umgebungs- und Störfallbedingungen standhalten, die im zugehörigen Aufstellungs- und Installationsbereich auftreten können.

3.2 (5) Die leittechnischen Einrichtungen sind so ausgelegt, dass fehlerhaftes Ansteuern des Sicherheitssystems unter Berücksichtigung der Ziffer 3.2 (11) verhindert wird, wenn dies zu auslegungsüberschreitenden Anlagenzuständen führen kann.

3.2 (6) Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, sind so ausgelegt, dass Schutzaktionen grundsätzlich automatisch ausgeführt werden.

Nur wenn sichergestellt ist, dass vom Zeitpunkt des Erkennens eines Ereignisses der Sicherheitsebene 3 bis zur Auslösung der zur Beherrschung notwendigen Schutzaktion ausreichend Zeit für die Entscheidungsfindung und für die Durchführung der Schutzaktion durch das Personal zur Verfügung steht, dürfen notwendige Schutzaktionen auch von Hand ausgelöst werden.

Der Richtwert für die Zeitspanne, ab der Handmaßnahmen zulässig sind, beträgt 30 Minuten.

3.2 (7) Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, sind grundsätzlich selbstüberwachend ausgelegt. Die Funktionen und Eigenschaften, die von der Selbstüberwachung nicht erfasst sind, werden einer regelmäßigen und lückenlosen Überprüfung unterzogen. Die Prüfzyklen sind auf Grundlage von Zuverlässigkeitsbetrachtungen festgelegt. Diese Prüfungen sollen mittels eingebauter Prüfhilfen an dafür vorgesehenen Schnittstellen leicht durchführbar sein.

Prüfeingriffe und Handbetätigungen sind so festgelegt, dass notwendige Sicherheitsfunktionen weder verhindert werden noch die Zuverlässigkeit ihrer Anregung signifikant vermindert wird.

Hinweis Siehe auch die Anforderungen zur Sicherstellung der Funktionsbereitschaft von Sicherheitseinrichtungen gemäß „Sicherheitsanforderungen für Kernkraftwerke: Anforderungen an die Auslegung und den sicheren Betrieb von baulichen Anlagenteilen, Systemen und Komponenten“ (Modul 10) Abschnitt 1.4.

3.2 (8) Die Selbstüberwachung ist so ausgelegt, dass sie die Funktion der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, nicht beeinträchtigt. Die regelmäßigen Überprüfungen nach Ziffer 3.2 (7) sind so geplant und werden so durchgeführt, dass eine gleichzeitige Prüfung redundanter leittechnischer Einrichtungen nicht stattfindet.

3.2 (9) Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, werden grundsätzlich nur für Aufgaben innerhalb des Sicherheitssystems benutzt. Sofern Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, auch für Aufgaben auf den Sicherheitsebenen 1 oder 2 eingesetzt werden, sind die zugehörigen leittechnischen Einrichtungen so ausgelegt, dass die geforderte Zuverlässigkeit der Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, nicht beeinträchtigt wird.

3.2 (10) Leittechnische Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, sind so aufgebaut, dass die erforderlichen Nachweise zur Qualifizierung der leittechnischen Einrichtungen des Sicherheitssystems zuverlässig möglich sind.

3.2 (11) Bei der Auslegung der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, sind Vorkehrungen gegen systematische Ausfälle der festverdrahteten leittechnischen Einrichtungen derart getroffen, dass ein systematischer Ausfall ausgeschlossen werden kann.

Bei der Auslegung der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, sind Vorkehrungen gegen systematische Ausfälle der software-basierten leittechnischen Einrichtungen einschließlich systematisches Software-Versagen derart getroffen, dass ein systematischer Ausfall beherrscht wird.

Beim Einsatz software-basierter Leittechnik werden grundsätzlich dissimilare leittechnische Einrichtungen verwendet. Es bestehen keine Anforderungen hinsichtlich des Einsatzes dissimilarer Einrichtungen, wenn für die jeweils auszuführende Leittechnikfunktion:

- ein aktiver systematischer Ausfall sicherheitsgerichtet ist und

- bei einem passiven systematischen Ausfall der Störfall durch andere Leittechnikfunktionen der Kategorie A, die durch zu der ausgefallenen Einrichtung dissimilare leittechnische Einrichtungen ausgeführt werden, beherrscht wird.

Für Schutzaktionen, die nicht für jeden Anlagenzustand sicherheitsgerichtet sind, ist in Abhängigkeit von den Auswirkungen von passiven oder aktiven systematischen Ausfällen in den leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, eine zweifache oder dreifache dissimilare Ausführung der software-basierten Leittechnik eingesetzt. Eine zweifache dissimilare Ausführung ist eingesetzt,

- wenn mit den noch verfügbaren Sicherheitseinrichtungen unter Berücksichtigung von Ziffer 3.2(6) der Störfall beherrscht wird oder
- wenn jede der beiden dissimilaren leittechnischen Einrichtungen für sich alleine die erforderliche Schutzaktion auslöst.

Trifft eine der beiden genannten Voraussetzungen für den Einsatz einer zweifach dissimilaren Ausführung nicht zu, ist eine dreifach dissimilar ausgeführte software-basierte Leittechnik eingesetzt.

3.2 (12) Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, sind grundsätzlich so ausgelegt, dass sie ihre Aufgaben im Anforderungsfall unter Berücksichtigung folgender Annahmen erfüllen:

a) ein Zufallsausfall durch einen Einzelfehler,

b) und ein systematischer Ausfall (systematischer Ausfall der Hardware oder systematisches Softwareversagen), gilt nicht für festverdrahtete Leittechnik (siehe Ziffer 3.2 (11)),

c) und Folgeausfälle

d) und ein Instandhaltungsfall vorliegt.

Während eines Instandhaltungsfalls wird innerhalb einer Zeitspanne von 100 h das gleichzeitige Auftreten des systematischen Ausfalls und des Zufallsausfalls nicht unterstellt.

Bei software-basierten leittechnischen Einrichtungen mit einem ausreichend hohen Selbstüberwachungsgrad und nachgewiesenen Instandhaltungszeiten kleiner als 10 h wird gleichzeitig mit dem systematischen Ausfall das Auftreten eines Zufallsausfalls oder des Instandhaltungsfalls nicht unterstellt.

Zum Ausfall durch Einzelfehler und Unverfügbarkeit durch Instandhaltung sind weitere Anforderungen in den „Sicherheitsanforderungen für Kernkraftwerke: Anforderungen an die Auslegung und den sicheren Betrieb von baulichen Anlagenteilen, Systemen und Komponenten“ Modul 10, Abschnitt 1, festgelegt.

3.2 (13) Schutzeinrichtungen an Aggregaten und Hilfseinrichtungen sind so ausgelegt, dass bei Anforderung eines Aggregats durch die leittechnischen Einrichtungen des Sicherheitssystems die Schutzeinrichtungen grundsätzlich nicht wirksam werden, es sei denn, die dadurch möglichen Folgeschäden beeinträchtigen die Sicherheit der Anlage mehr als der Ausfall des Aggregats.

Die Schutzeinrichtungen sind grundsätzlich so ausgelegt, dass der Vorrang der Leittechnik-Funktionen der Kategorie A vor den Schutzeinrichtungen sichergestellt ist.

Ist in einer Schutzeinrichtung ein Vorrang vor Leittechnik-Funktionen der Kategorie A notwendig, werden an die Schutzeinrichtungen die Anforderungen der Kategorie A gestellt.

Die Anforderungen der Kategorie A an die Schutzeinrichtungen werden nicht gestellt, wenn nachgewiesen wird, dass Fehler der Schutzeinrichtung so unwahrscheinlich sind, dass eine dadurch verursachte Fehlauslösung ausgeschlossen werden kann.

3.2 (14) Die leittechnischen Einrichtungen sind so ausgelegt, dass sie die Unverfügbarkeit des Sicherheitssystems nicht bestimmen.

3.2 (15) In den Betriebsphasen, in denen die Verfügbarkeit der Reaktorschnellabschaltung erforderlich ist, ist jederzeit eine Reaktorschnellabschaltung von Hand möglich, auch beim unterstellten systematischen Ausfall softwarebasierter Leittechnik einschließlich Softwareversagen (siehe Ziffer 3.2 (11)).

3.2 (16) In Betriebsphasen, in denen Teile von Leittechnik-Funktionen der Kategorie A planungsgemäß nicht verfügbar sind, ist die zuverlässige und wirksame Störfallbeherrschung für die in diesen Betriebsphasen zu unterstellenden Ereignisse unter diesen Bedingungen gewährleistet.

3.2 (17) Die leittechnischen Einrichtungen, die Leittechnikfunktionen der Kategorie A ausführen, sind so ausgelegt, dass auch beim Eintreten des zu unterstellenden Einzelfehlers in diesen Einrichtungen keine Aktionen ausgelöst werden, die die Anlage in einen Störfall überführen können.

3.2 (18) Die Anregekriterien für Leittechnik-Funktionen der Kategorie A und die dadurch ausgelösten Schutzaktionen und Maßnahmen werden in der Warte übersichtlich angezeigt.

3.2 (19) Die durch die Leittechnik-Funktionen der Kategorie A ausgelösten Schutzaktionen und Maßnahmen werden zusammen mit ihren Auswirkungen auf den Prozess so in der Warte und in der Notsteuerstelle dargestellt, dass eine Überprüfung des Anlagenzustandes durch das Betriebspersonal zuverlässig und rechtzeitig möglich ist.

3.3 Leittechnische Einrichtungen für Leittechnik-Funktionen der Kategorie B

Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie B ausführen, sind so ausgelegt, dass sie ihre Aufgaben auch dann erfüllen, wenn im Anforderungsfall zusätzlich ein Zufallsausfall und daraus resultierende Folgeausfälle eintreten.

Eine leittechnische Einrichtung, die durch eine fehlerhafte Ansteuerung einen Störfall auslösen kann, ist durch eine von der als fehlerhaft angenommenen leittechnischen Einrichtung unabhängige leittechnische

Einrichtung überlagert. Die Leittechnik-Funktion dieser unabhängigen leittechnischen Einrichtung ist nach Kategorie B eingestuft.

3.4 Leittechnische Einrichtungen für Leittechnik-Funktionen auf der Sicherheitsebene 4

Die leittechnischen Einrichtungen, die für vorgeplante Maßnahmen auf den Sicherheitsebenen 4a, 4b und 4c, Leittechnik-Funktionen ausführen sollen, sind so ausgelegt, dass sie unter den für die jeweilige Aufgabe zu unterstellenden Umgebungsbedingungen ihre Aufgaben mit der für diese Sicherheitsebenen jeweils ausreichender Zuverlässigkeit erfüllen. Für Maßnahmen des anlageninternen Notfallschutzes können alle leittechnischen Einrichtungen eingesetzt werden, die dazu geeignet sind.

4 Anforderungsspezifikation für leittechnische Einrichtungen für Leittechnik-Funktionen der Kategorien A bis C

4 (1) Sämtliche Anforderungen an Leittechnik-Funktionen der Kategorien A bis C sind in einer Anforderungsspezifikation in übersichtlicher Darstellung dokumentiert.

4 (2) Die Aufgaben der Leittechnik-Funktionen, die auf den Sicherheitsebenen 2, 3 und 4a eingesetzt werden, sind auf Basis einer Analyse der Ereignisabläufe ermittelt, die die in den Sicherheitsebenen 2, 3 und 4a unterstellten Ereignisse umfasst.

Für Maßnahmen des anlageninternen Notfallschutzes sind Betrachtungen zur Nutzung der verfügbaren leittechnischen Einrichtungen angestellt.

4 (3) Die Anforderungsspezifikation für die Leittechnik-Funktionen der Kategorien A und B ist so gestaltet, dass die verfahrenstechnische Aufgabenstellung in klar abgegrenzte Teilaufgaben gegliedert ist. Diese Teilaufgaben sind in Leittechnik-Funktionen dargestellt.

Die Teilaufgaben der softwarebasierten leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, sind so ausgelegt, dass diese einen geringen Funktionsumfang haben.

Die Gesamtheit aller Leittechnik-Funktionen ist übersichtlich strukturiert dokumentiert.

4 (4) Für die Leittechnik-Funktionen sind die Aufgaben, die Zuordnung zu Kategorien nach Abschnitt 2, die Anregekriterien, die Eingangssignale, die Signalverarbeitung, die Ansteuerungen der Stellglieder, die Meldungen / Anzeigen, die Datenspeicherung und die Schnittstellen zu anderen Leittechnik-Funktionen angegeben.

4 (5) Es ist nachgewiesen, dass die Schutzziele mit den Leittechnik-Funktionen entsprechend der Anforderungsspezifikation bei allen zu unterstellenden Ereignissen und Ereignisabläufen sichergestellt sind.

4 (6) Die sicherheitstechnisch relevanten Funktionen der Prozessführungs- und der Informationseinrichtungen sind in der Anforderungsspezifikation festgelegt.

5 Erfassung von Prozessvariablen

5 (1) Für die unterstellten Ereignisse der Sicherheitsebenen 2 bis 4a sowie für die vorgeplanten Maßnahmen des anlageninternen Notfallschutzes (Notfallmaßnahmen) werden die erforderlichen Prozessvariablen erfasst.

5 (2) Für jedes von den leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, zu beherrschende Ereignis der Sicherheitsebene 3 werden grundsätzlich mindestens zwei unterschiedliche Anregekriterien herangezogen, die aus physikalisch unterschiedlichen Prozessvariablen gebildet werden. Wenn dies technisch nicht realisierbar ist, sind andere Maßnahmen und Einrichtungen zum Erreichen hoher Zuverlässigkeit vorgesehen.

6 Redundanz und Unabhängigkeit

6 (1) Die leittechnischen Einrichtungen sind so aufgebaut, dass die in den aktiven Einrichtungen des Sicherheitssystems vorgegebene Redundanz gewahrt bleibt.

6 (2) Redundante leittechnische Einrichtungen sind voneinander so unabhängig ausgelegt, dass ein anlageninternes versagensauslösendes Ereignis nicht zum Ausfall mehrerer Redundanten führt. Wenn einzelne Redundanten leittechnischer Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, durch Einwirkungen von außen ausfallen, reichen die übrigen Redundanten zur Beherrschung dieses Ereignisses aus.

6 (3) Zum Schutz gegen redundanzübergreifende versagensauslösende Ereignisse innerhalb der leittechnischen Einrichtungen und innerhalb der Anlage sind Redundanten grundsätzlich räumlich getrennt angeordnet.

6 (4) Verbindungen der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A und B ausführen, zu nicht kategorisierten oder Datenverarbeitungs- oder Datenübertragungseinrichtungen der Kategorie C sind auf ein Minimum begrenzt und nachweislich rückwirkungsfrei gestaltet.

6 (5) Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorien A bis C ausführen, sind von einander so unabhängig ausgelegt, dass bei versagensauslösenden Ereignissen in den Einrichtungen sicherheitstechnisch niederwertigeren Kategorien die Funktionen der sicherheitstechnisch höherwertigeren Kategorie erhalten bleiben.

6 (6) Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorien A bis C ausführen, sind so ausgelegt, dass die Ausgangssignale von Einrichtungen einer sicherheitstechnisch höherwertigeren Kategorie Priorität vor den Ausgangssignalen von Einrichtungen einer sicherheitstechnisch niederwertigeren Kategorie haben.

7 Qualifizierung

7.1 Qualifizierung der Hard- und Software der leittechnischen Einrichtungen für Leittechnik-Funktionen der Kategorien A bis C

7.1 (1) In allen Phasen der Entwicklung, Herstellung, Inbetriebnahme und des Betriebs der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorien A bis C ausführen, werden administrative, konstruktive und analytische Maßnahmen einschließlich praktischer Prüfungen im Rahmen der Qualitätssicherung, durchgeführt und dokumentiert.

7.1 (2) Die Prüfung der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorien A bis C ausführen, erfolgt im Fertigungs- und Montageprozess mit der Integration der Systemteile. Die einzelnen Systemteile sind hinsichtlich Systemspezifikation und Ausführung darauf zu prüfen, ob die an sie gestellten leittechnischen Anforderungen erfüllt werden.

7.1 (3) Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorien A bis C ausführen, sind unter möglichst realistischen Anlagen- und Einsatzbedingungen umfassend daraufhin getestet, alle zu unterstellenden Ereignisabläufe zu beherrschen.

7.1 (4) Nach Abschluss der Montage in der Anlage oder nach Änderungen an den leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A bis C ausführen, wird eine Inbetriebsetzungsprüfung durchgeführt.

7.1 (5) Die Informationssysteme sind gemäß ihrer sicherheitstechnischen Bedeutung qualifiziert.

7.2 Qualifizierung der Hardware

7.2 (1) Für leittechnische Einrichtungen, die Leittechnik-Funktionen der Kategorie A und B ausführen, ist zuverlässige, typgeprüfte oder für die unterstellten

Einsatzbedingungen betriebsbewährte sowie möglichst wartungsfreie Hardware eingesetzt.

7.2 (2) Für leittechnische Einrichtungen, die Leittechnik-Funktionen der Kategorie C ausführen, ist zuverlässige und für die unterstellten Einsatzbedingungen geeignete Hardware eingesetzt.

7.2 (3) Die anlagenbezogene Eignung ist durch den Vergleich der Eigenschaften der Hardware mit den für den Einsatzfall spezifizierten Anforderungen nachgewiesen.

7.3 Qualifizierung der Software

7.3.1 Software für Leittechnik-Funktionen der Kategorien A bis C

7.3.1 (1) Die Software ist in verifizierbaren Schritten nach einem Phasenmodell entwickelt.

7.3.1 (2) Die Softwarearchitektur ist so gestaltet, dass die Funktionen der Anwendersoftware und der Systemsoftware in eigenständigen Softwareeinheiten realisiert sind und die Anwendersoftware von der Systemsoftware getrennt ist.

Hinweis Zur Systemsoftware gehört z.B. das Betriebssystem und bei Mehrrechnersystemen die Software zur Kommunikation der Rechner.

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

7.3.1 (4) Die Software ist so gestaltet, dass deren anforderungsgerechter Ablauf unabhängig von Art und Umfang der zeitlichen Änderung ihrer Eingangssignale gewährleistet ist.

7.3.2 Software für Leittechnik-Funktionen der Kategorie A

7.3.2.1 Grundsätze

7.3.2.1 (1) Die Entwicklung und Qualifizierung der Software für Leittechnik-Funktionen der Kategorie A erfolgen so, dass eine durchgängige Nachweisführung der korrekten Arbeitsweise der Software gewährleistet ist. Entwurf und Implementierung sind mit formalisierten und rechnergestützten Konstruktions- und Prüfmethoden entsprechend dem Stand von Wissenschaft und Technik durchgeführt.

7.3.2.1 (2) Die Software für Leittechnik-Funktionen der Kategorie A ist grundsätzlich einfach aufgebaut.

7.3.2.1 (3) Der Funktionsumfang der Software für Leittechnik-Funktionen der Kategorie A ist grundsätzlich auf das für die jeweilige Funktion notwendige Maß begrenzt.

7.3.2.1 (4) Die Software ist robust und selbstüberwachend ausgelegt.

7.3.2.2 Qualitätssicherung

7.3.2.2 (1) Die Software ist nach einem Phasenmodell durchgängig mit rechnergestützten Werkzeugen erstellt.

7.3.2.2 (2) Die Software ist aus klar abgegrenzten und mit geringem Funktionsumfang versehenen Einheiten aufgebaut. Diese Softwareeinheiten sind möglichst einfach bei Beschränkung auf unverzichtbare Anweisungen und Schnittstellen programmiert und in eine übersichtliche Programmstruktur integriert.

7.3.2.2 (3) Die Ergebnisse der einzelnen Phasen der Softwareentwicklung sind unter Anwendung formaler Analysemethoden und zusätzlicher Tests an den Vorgaben vollständig verifiziert. Dazu werden an definierten Meilensteinen Prüfungen vorgenommen.

7.3.2.2 (4) Nach Installation der Software auf den Rechnern wird das anforderungsgerechte Verhalten des Hardware- und Softwaresystems validiert. Wird die

Validierung in mehreren Schritten durchgeführt, so erfolgen die einzelnen Validierungsschritte überlappend.

7.3.2.2 (5) Die Organisation und Administration der Softwareentwicklung und der Qualitätssicherung ist so gestaltet, dass sichergestellt ist, dass die Software nach vollständigen Entwicklungs-, Prüf-, Wartungs- und Qualitätssicherungsplänen erstellt und eingesetzt wird. Die Unabhängigkeit zwischen Konstruktion und Qualitätssicherung wird durchgehend gewahrt. Es ist eine vollständige Entwicklungs-, Qualitätssicherungs- und Benutzerdokumentation vorhanden.

7.3.2.2 (6) Es werden Verfahren und Methoden angewandt, die die konsistenten Konfigurationen der Software sicherstellen (Konfigurationsmanagement).

7.3.2.3 Einsatz von vorgefertigter Software

7.3.2.3 (1) Der Einsatz vorgefertigter Software, sofern nicht entsprechend den Anforderungen 7.3.2.1 und 7.3.2.2 ausgelegt, ist auf unverzichtbare Bestandteile beschränkt, wobei Softwareänderungen vermieden werden. Diese Teile sind Prüfungen und Tests unterzogen, die in Umfang und Tiefe den Nachweisen nach den Abschnitten 7.3.2.1 und 7.3.2.2 gleichwertig sind.

7.3.2.3 (2) Zur Bewertung der Gleichwertigkeit werden herangezogen:

- Referenzen über den Hersteller der Software,
- die Entwicklungsdokumentation, Anwenderdokumentation und QS-Dokumentation der Software,
- die Ergebnisse unabhängiger Begutachtung (Zertifikate) der Software,
- die Betriebserfahrung der Software unter Berücksichtigung der Anwendungsprofile,
- zusätzliche Softwaretests.

7.3.3 Software für Leittechnik-Funktionen der Kategorie B

7.3.3.1 Grundsätze

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

7.3.3.1 (2) Die Software ist robust und selbstüberwachend ausgelegt.

7.3.3.2 Qualitätssicherung

7.3.3.2 (1) Die Softwareerstellung erfolgt nach einem methodisch abgestimmten Phasenmodell weitgehend mit rechnergestützten Werkzeugen.

7.3.3.2 (2) Die Software ist aus hinsichtlich der Funktion klar abgegrenzten Einheiten aufgebaut. Diese Softwareeinheiten sind auf unverzichtbare Anweisungen und Schnittstellen beschränkt und in eine übersichtliche Programmstruktur integriert.

7.3.3.2 (3) Die Ergebnisse der einzelnen Phasen der Softwareentwicklung sind einer dokumentierten Prüfung unterzogen. Es ist eine Kombination von Testverfahren angewandt, so dass für alle sicherheitsrelevanten Programmteile eine vollständige Funktionstestüberdeckung erreicht wird.

7.3.3.2 (4) Das anforderungsgerechte Verhalten des Hardware- und Softwaresystems ist validiert.

7.3.3.2 (5) Die Organisation und Administration der Softwareentwicklung und der Qualitätssicherung ist so gestaltet, dass sichergestellt ist, dass die Software nach vollständigen Entwicklungs-, Prüf-, Wartungs- und Qualitätssicherungsplänen erstellt und eingesetzt wird. Die Unabhängigkeit zwischen Konstruktion und Qualitätssicherung wird durchgehend gewahrt. Es ist eine vollständige Entwicklungs-, Qualitätssicherungs- und Benutzerdokumentation vorhanden.

7.3.3.2 (6) Die konsistente Konfiguration der Programme ist sichergestellt.

7.3.3.3 Einsatz von vorgefertigter Software

7.3.3.3 (1) Bei vorgefertigter Software wird eine Beschränkung auf unverzichtbare Bestandteile vorgenommen, wobei Softwareänderungen vermieden werden. Diese Teile werden Prüfungen und Tests unterzogen, die in Umfang und Tiefe den Nachweisen nach den Abschnitten 7.3.3.1 und 7.3.3.2 gleichwertig sind.

7.3.3.3 (2) Zur Bewertung der Gleichwertigkeit werden herangezogen:

- Referenzen über den Hersteller der Software,
- die Entwicklungsdokumentation, Anwenderdokumentation und QS-Dokumentation der Software,
- die Ergebnisse unabhängiger Begutachtung (Zertifikate) der Software,
- die Betriebserfahrung der Software unter Berücksichtigung der Anwendungsprofile,
- zusätzliche Softwaretests.

7.3.4 Software für Leittechnik-Funktionen der Kategorie C

7.3.4.1 Grundsatz

Die Software für Leittechnik-Funktionen der Kategorie C ist nach anerkannten Methoden der Softwaretechnik qualifiziert.

7.3.4.2 Qualitätssicherung

7.3.4.2 (1) Bei der Softwareerstellung sind die Entwicklungsschritte einzeln ausgewiesen.

Nach Möglichkeit werden bei wesentlichen Entwicklungsschritten Software-Werkzeuge genutzt.

7.3.4.2 (2) Das Erreichen der Phasenziele ist durch Prüfungen nachgewiesen und dokumentiert.

7.3.4.2 (3) Das anforderungsgerechte Verhalten des Hardware- und Softwaresystems ist in seinen sicherheitsrelevanten Funktionen validiert.

7.3.4.2 (4) Die Software ist nach einem Qualitätssicherungsplan gemäß den anerkannten Regeln der Technik erstellt. Es ist eine vollständige Entwicklungs-, Qualitätssicherungs- und Benutzerdokumentation vorhanden.

7.3.4.3 Einsatz von vorgefertigter Software

Für eingesetzte vorgefertigte Software ist die Betriebserfahrung dokumentiert oder die Software ist zertifiziert.

Die zu Beurteilung der Einsetzbarkeit erforderlichen Eigenschaften sind dokumentiert.

8 Robustheit

8 (1) Die elektrischen, elektromagnetischen, thermischen, mechanischen und strahlungs- sowie feuchtigkeitsbedingten Einwirkungen sind für leittechnische Einrichtungen so festgelegt, dass die unterstellten Betriebs- und Störfallbedingungen zuverlässig abgedeckt werden.

8 (2) Bedienung und Instandhaltung sind so gestaltet, dass die Funktionssicherheit der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A bis C ausführen, nicht unzulässig beeinträchtigt wird.

8 (3) Die leittechnischen Einrichtungen, die für die Durchführung der im Rahmen des anlageninternen Notfallschutzes vorgesehenen Maßnahmen erforderlich sind, sind so beschaffen, dass sie durch die Folgen der zu Grunde gelegten Ereignisabläufe oder Anlagenzustände ihre erforderliche Funktionsfähigkeit nicht verlieren.

8 (4) Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A bis C ausführen, sind so auslegt, dass hinreichende Reserven gegenüber Alterungseffekten vorhanden sind.

8 (5) Der zulässige Spannungsbereich für die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A bis C ausführen, ist unempfindlich gegenüber Über- und Unterschreitungen des spezifizierten Spannungsbereichs der elektrischen Energieversorgung.

8 (6) Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A und B ausführen, sind fehlertolerant aufgebaut. Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A und B ausführen, sind so ausgelegt, dass das Ausfallverhalten grundsätzlich definiert und möglichst sicherheitsgerichtet ist.

8 (7) Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorien A bis C ausführen, sind grundsätzlich so ausgelegt, dass während des Leistungsbetriebs keine Wartungsarbeiten erforderlich sind.

9 Instandhaltung und Änderungen

9 (1) Die Funktionsfähigkeit der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A bis C ausführen, ist während der Betriebsdauer der Anlage durch Prüfungen nachgewiesen. Diese Prüfungen erfassen alle funktionswichtigen Einrichtungen.

9 (2) Art und Umfang der Prüfungen und die Zeitabstände zwischen den Prüfungen sind festgelegt. Diese Festlegungen werden in regelmäßigen Abständen u. a. anhand der Betriebserfahrungen überprüft.

9 (3) Die Ergebnisse der Prüfungen werden dokumentiert.

9 (4) Die leittechnischen Einrichtungen sind grundsätzlich so ausgelegt, dass durch Prüfungen verursachte Veränderungen nach den Prüfungen rückgesetzt werden. Prüfungen werden automatisch oder manuell durchgeführt. Die Prüfungen sind so geplant und durchgeführt, dass die Anforderungen

aus den „Sicherheitsanforderungen für Kernkraftwerke: Anforderungen an die Auslegung und den sicheren Betrieb von baulichen Anlagenteilen, Systemen und Komponenten“ (Modul 10) Abschnitt 1.2 eingehalten werden.

9 (5) Prüfungen an leittechnischen Einrichtungen sollen von zentralen Stellen durch verantwortliches Betriebspersonal überwacht werden.

9 (6) Instandhaltungsarbeiten sind so gestaltet, dass sie ohne unzulässige Minderung der Sicherheit der Anlage durchführbar sind und Auswirkungen zu unterstellender Fehlhandlungen auf eine Redundante beschränkt bleiben.

9 (7) Bei Änderungen in den leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A bis C ausführen, werden mindestens die gleichen Qualitätsstandards angewendet wie bei Herstellung der leittechnischen Einrichtungen.

9 (8) Bei Änderungen in den leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A bis C ausführen, ist sichergestellt, dass die geänderten Teile ihre Funktion erfüllen und mit den unveränderten Teilen anforderungsgemäß zusammenwirken.

9 (9) Änderungen der Software der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A bis C ausführen, werden unter Einhaltung der Qualitätsanforderungen nach Abschnitt 7.3 vorgenommen. Änderungen der Software und dazu erforderliche Eingriffe in die leittechnischen Einrichtungen erfolgen so, dass die Anforderungen aus den „Sicherheitsanforderungen für Kernkraftwerke: Anforderungen an die Auslegung und den sicheren Betrieb von baulichen Anlagenteilen, Systemen und Komponenten“ (Modul 10) Abschnitt 1.2 eingehalten werden. Alle Eingriffe in die Software sind dokumentiert.

9 (10) Änderungen von Parametrierdaten und Software der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A bis C ausführen, werden so behandelt, dass sie rekonstruierbar sind. Dazu werden regelmäßig sowie bei Änderungen der Software Sicherungskopien angefertigt. Software- und Parametrierdatenbestände sind archiviert.

10 Anforderungen an die Zugriffskontrolle

10 (1) Eingriffe in die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A und B ausführen, werden auf der Warte angezeigt. In Fällen, in denen dies technisch nicht möglich ist, wird das Wartenpersonal vor dem geplanten Eingriff über die Eingriffe informiert.

10 (2) Die unberechtigten Zugriffe in die leittechnischen Einrichtungen einschließlich der Software sind vorzugsweise durch technische Vorkehrungen soweit wie möglich erschwert oder verhindert. Eine Absicherung durch organisatorische Maßnahmen ist auf solche Bereiche beschränkt, die durch technische Vorkehrungen nicht sinnvoll abgesichert werden können.
Die Wirksamkeit und Zuverlässigkeit der vorgesehenen Maßnahmen und technischen Vorkehrungen entspricht der sicherheitstechnischen Bedeutung der leittechnischen Einrichtungen.

11 Dokumentation

11 (1) Die anlagenspezifische Konfiguration der Hard- und Software leittechnischer Einrichtungen, die Leittechnik-Funktionen der Kategorie A bis C ausführen, wird während ihres gesamten Lebenszyklus hinsichtlich des aktuellen Zustands und durchgeführter Änderungen dokumentiert.

11 (2) Die Instandhaltungsvorgänge und Eingriffe in die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A bis C ausführen, sind dokumentiert.

11 (3) Die Betriebserfahrung aus der Instandhaltung der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A bis C ausführen, wird erfasst, dokumentiert und systematisch ausgewertet.

12 Elektrische Energieversorgung der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorien A bis C ausführen

12 (1) Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A bis C ausführen, werden von unterbrechungslosen Notstromanlagen mit Energiespeicherung versorgt. Die Kapazität des Energiespeichers ist unter der Annahme, dass der Leistungsbedarf einer Redundante nur aus dem redundanzzugehörigen Energiespeicher gedeckt wird, so bemessen, dass die Versorgung mindestens 2 h aufrechterhalten wird, ohne dass die zulässige Mindestspannung unterschritten wird. Die leittechnischen Einrichtungen und deren Energieversorgung sind so ausgelegt, dass nach vollständigem Spannungsausfall oder Unterschreiten der Mindestspannung die leittechnischen Einrichtungen nach Spannungswiederkehr funktionsfähig sind.

Hinweis Siehe auch „Sicherheitsanforderungen für Kernkraftwerke: Anforderungen an die Elektrische Energieversorgung“ (Modul 12).

12 (2) Bei der Auslegung der elektrischen Energieversorgung der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A bis C ausführen, sind die gleichen Ausfallkombinationen zu Grunde gelegt wie bei der Auslegung der zu versorgenden leittechnischen Einrichtungen (vgl. für Kategorie A: Ziffer 3.2 (12) und vgl. für Kategorie B: Abschnitt 3.3).

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

12 (4) Ausfälle der elektrischen Energieversorgung für die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A bis C ausführen, werden durch Überwachungseinrichtungen erfasst und gemeldet.

13 Störfallinstrumentierung

13.1 Geltungsbereich Störfallinstrumentierung

Die Störfallinstrumentierung hat die Aufgabe, vor, während und nach

- einem Störfall oder
- einem Ereignis, das zu einer erhöhten Freisetzung von radioaktiven Stoffen in die Kernkraftwerksumgebung führen kann,

einen Überblick über den Anlagenzustand zu ermöglichen und alle den Anlagenzustand beschreibenden wesentlichen Daten sowie die wichtigsten Wetterdaten anzuzeigen und zeitgerecht zu dokumentieren.

13.2 Übergeordnete Anforderungen an die Störfallinstrumentierung

13.2 (1) Die Störfallinstrumentierung ist in eine Störfallanzeige und eine Störfallaufzeichnung unterteilt.

13.2 (2) Die Komponenten der Störfallinstrumentierung sind, soweit erforderlich, störfallfest ausgelegt.

13.2 (3) Die Einrichtungen der Störfallinstrumentierung sind an eine unterbrechungslose Notstromversorgung des Notstromsystems angeschlossen. Für Einrichtungen der Störfallinstrumentierung, bei denen aufgrund ihrer Aufgabenstellung eine kurzzeitige Nichtverfügbarkeit zulässig ist, muss die Stromversorgung nicht unterbrechungslos erfolgen.

13.2 (4) Das Auslegungskonzept und die sicherheitstechnisch wichtigen Einzelheiten der Störfallinstrumentierung sind prüffähig dokumentiert.

13.3 Auslegung der Störfallinstrumentierung

13.3.1 Störfallanzeige

13.3.1 (1) Die Störfallanzeige ist so ausgelegt, dass Daten, die vor, während und nach Eintreten eines Ereignisses der Sicherheitsebenen 3 oder 4a für die Beurteilung der Anlagensicherheit, der Wirksamkeit des Sicherheitssystems und für die Entscheidung über Maßnahmen des anlageninternen Notfallschutzes erforderlich sind, zuverlässig und ausreichend genau angezeigt werden.

Bei Auslegung der Störfallanzeige ist berücksichtigt, dass die Daten, die vor, während und nach Eintreten eines Ereignisablaufs bzw. Anlagenzustands, welche zu einer erhöhten Freisetzung radioaktiver Stoffe in die Kernkraftwerksumgebung führen können (Sicherheitsebenen 4b oder 4c), für die Entscheidung über Maßnahmen des anlageninternen Notfallschutzes erforderlich sind, unter den anzunehmenden Umgebungsbedingungen mit der erforderlichen Genauigkeit angezeigt werden.

13.3.1 (2) Die Störfallanzeige ist in eine Störfallübersichts-, Weitbereichs- und Störfalldetailanzeige unterteilt.

13.3.1 (3) Die Störfallübersichtsanzeige ist so ausgelegt, dass die vor, während und nach Eintritt eines Ereignisses der Sicherheitsebene 3 oder 4a zur Beurteilung des Anlagenzustands und der radiologischen Auswirkungen auf die Umgebung wesentlichen Messgrößen erfasst werden.

13.3.1 (4) Es ist eine Weitbereichsanzeige für die Messgrößen vorgesehen, die die repräsentativen Ereignisabläufe und daraus abgeleiteten Anlagenzustände der Sicherheitsebenen 4b und 4c charakterisieren (siehe „Sicherheitsanforderungen für Kernkraftwerke: Anforderungen an den anlageninternen Notfallschutz“ (Modul 7, Ziffer 3.3 (2)).

13.3.1 (5) Die Störfalldetailanzeige ist so ausgelegt, dass die Funktion der Sicherheitseinrichtungen einschließlich der zu ihrer Funktion notwendigen Hilfseinrichtungen überwacht wird. Hierzu dürfen leittechnische Einrichtungen aller Kategorien verwendet werden.

13.3.1 (6) Es werden eignungsgeprüfte oder für den Einsatzfall und für die unterstellten Einsatzbedingungen bewährte und möglichst wartungsfreie Geräte verwendet.

13.3.1 (7) Die Einrichtungen zur Erfassung, Verarbeitung und Dokumentation der Messgrößen sind technisch so einfach wie möglich aufgebaut.

13.3.1 (8) Die Messgrößen der Störfallübersichts- und Weitbereichsanzeige werden grundsätzlich in der Warte des Kernkraftwerks und in der Notsteuerstelle angezeigt.

13.3.1 (9) Die Funktion der Störfallübersichts- und Weitbereichsanzeige wird durch Ereignisse der Sicherheitsebenen 3 und 4a und ihre Folgen nicht beeinträchtigt.

13.3.1 (10) Eine redundante Messwerterfassung und Messwertverarbeitung für eine Messgröße der Störfallübersichtsanzeige und der Weitbereichsanzeige ist nicht erforderlich, wenn:

- der Informationsgehalt dieser Messgröße auch durch Messwerte anderer Messgrößen der Störfallanzeige oder durch Messgrößen einer gleichwertigen Instrumentierung vermittelt werden kann,
- der Ausfall von Messwerten einer Messgröße im Bedarfsfall für eine bestimmte Zeitdauer akzeptiert und innerhalb dieser Zeit unter den dann herrschenden Bedingungen der Ausfall behoben oder eine Ersatzlösung realisiert werden kann.

13.3.1 (11) Die Einrichtungen der Störfallanzeige im Bereich, der nicht gegen Einwirkungen von außen geschützt ist, sind rückwirkungsfrei von den Einrichtungen des geschützten Bereichs entkoppelt.

13.3.1 (12) Die Einrichtungen der Störfallanzeige sind nach ergonomischen Gesichtspunkten so gestaltet, dass die Voraussetzungen für ein sicherheitstechnisch optimales Verhalten des Betriebspersonals gewährleistet sind.

13.3.1 (13) Die Störfallanzeige ist so ausgelegt, dass eine lückenlose Überprüfung möglich ist und die Prüfungen einfach durchführbar sind.

13.3.1 (14) Die Funktionsfähigkeit der Störfallübersichts- und Weitbereichsanzeige wird während der Betriebsdauer der Anlage durch Prüfungen nachgewiesen. Diese Prüfungen erfassen alle funktionswichtigen Komponenten.

13.3.1 (15) Art und Umfang der Prüfungen und die Zeitabstände zwischen den Prüfungen sind festgelegt.

13.3.1 (16) Die Ergebnisse der Prüfungen sind dokumentiert.

13.3.2 Störfallaufzeichnung

13.3.2 (1) Die Störfallaufzeichnung ist so ausgelegt, dass die Messgrößen, die vor, während und nach Eintreten

- eines Ereignis der Sicherheitsebenen 3 oder 4a oder
- eines Ereignisses, das zu einer erhöhten Freisetzung radioaktiver Stoffe in die Kernkraftwerksumgebung führen kann (Sicherheitsebenen 4b oder 4c),

übersichtlich und in der richtigen zeitlichen Folge dokumentiert werden.

13.3.2 (2) Die Störfallaufzeichnung ist so ausgelegt, dass für jede erfasste Messgröße der Störfallinstrumentierung der Zeitbezug aus den zugehörigen Dokumentationsunterlagen so genau bestimmt werden kann, dass eine zeitliche Zuordnung zu Daten aus anderen Informationsquellen möglich ist.

13.3.2 (3) Die Dokumentationseinrichtungen sind so ausgelegt, dass das Zeitverhalten der Messgrößen mit erforderlicher Genauigkeit erfasst wird.

13.3.2 (4) Die Störfallaufzeichnung ist grundsätzlich jederzeit in Betrieb. Eine eingeschränkte Funktionsfähigkeit (z. B. bei erforderlichen Instandsetzungsarbeiten) ist zulässig, wenn im Bedarfsfall die erforderliche Information durch den funktionsfähigen Teil der Störfallinstrumentierung gewährleistet ist. Die vollständige Funktionsfähigkeit der Störfallaufzeichnung wird so schnell wie möglich wiederhergestellt.

13.3.2 (5) Es ist festgelegt, welche Einrichtungen der Störfallaufzeichnung in den Betriebsphasen B-F der Anlage in Betrieb sind.

13.3.2 (6) Für die Aufzeichnung und Speicherung der Störfallablaufdaten werden zur Vorsorge gegen einen systematischen Ausfall mindestens zwei Datenspeicher eingesetzt. Der Ausfall eines Datenspeichers wird angezeigt.

13.3.2 (7) Die Störfallaufzeichnungen werden gesichert aufbewahrt. Es ist sichergestellt, dass diese Daten weder verändert noch gelöscht werden.

13.3.2 (8) Die nach Eintritt eines Ereignisses der Sicherheitsebene 3 auftretenden Umgebungsbedingungen führen nicht dazu, dass die zur Störfallbeurteilung erforderlichen Informationen nicht zur Verfügung stehen.

13.3.2 (9) Die Dokumentationseinrichtungen sind übersichtlich angeordnet sowie deutlich und eindeutig gekennzeichnet.

13.3.2 (10) Die Messgrößen der Störfallübersichts- und Weitbereichsanzeige werden grundsätzlich in der Warte des Kernkraftwerks und in der Notsteuerstelle aufgezeichnet.

Bearbeitung der zu Rev. B von Modul 5 vorliegenden Einträge in der Kommentardatenbank

Anmerkung:
In der folgenden Tabelle sind die Kommentare zu Teil 1 und Teil 2-Kap. 2 jetzt aktuell Modul 5 zugeordnet und die Kommentare zu Teil 2-Kap. 1 Modul 12 zugeordnet.

Nr. in DB	Kapitel in Modul	Kommentar	Änderung	Begründung	Vorschlag Textänderung
	Übergreifend				
1315	Übergreifend	**Kommentar:** Das Modul-Team hat sich mit den Kommentaren zur Revision A auseinandergesetzt und Vorschläge übernommen. Im Vergleich zur Revision A ist in Revision B des Moduls der Detaillierungsgrad nun einheitlicher. Das Modul wirkt in sich "stimmiger" und "runder". In der Ad-hoc-Arbeitsgruppe „Regelwerk“ des Fachausschusses Reaktorsicherheit wurden die Inhalte des Moduls 5 in vier Sitzungen beraten. Die Vorschläge und Anmerkungen des UM BW sind in das Arbeitsergebnis eingeflossen. Offen sind noch viele Kommentare von grundsätzlichem Charakter, die in der Ad-hoc Arbeitsgruppe in einer Tabelle aufgelistet wurden. Diese können erst nach Vorliegen des übergeordneten Moduls 1 bearbeitet werden. Des Weiteren müssen nach der Bearbeitung weiterer Module die Verknüpfungen zu diesen Modulen geprüft werden. Nach Vorliegen der RSK- Stellungnahme zu Modul 5 ist vor einem abschließenden Vorschlag der Ad-hoc-Arbeitsgruppe .Regelwerk" eine erneute Bewertung der von der RSK eingebrachten Vorschläge erforderlich.	**NEIN**	Im Kommentar werden keine fachspezifischen Aspekte für Modul 5 angesprochen.	
1230	Übergreifend	**Kommentar:** Die redaktionelle Aufbereitung ist sehr unübersichtlich, weil das Modul in zwei Teile geteilt ist, und im Teil 2 jedes Kapitel nicht nur mit der Zählung der Unterpunkte sondern auch mit der Seitenzählung (!) bei 1 beginnt.	**Teilweise**	Im Teil 2 wiederholen sich die Abschnitte 1-3 in den Kapiteln 1 „Elektrische Energieversorgung“ und 2 „Störfallinstrumentierung“. Die Unterpunkte der Zählung sind allerdings nicht abhängig von der Seitenzahl, sondern in Übereinstimmung mit der Gliederung des Moduls. T5 hat bei der Überprüfung des Kommentars erkannt, dass die Abschnitte 5 (3) nach Abschnitt 4 und 5(4) nach Abschnitt 7 aus inhaltlichen Gründen verschoben werden müssen. Diese Änderungen werden an den entsprechenden Textstellen dokumentiert. Es wird vorgeschlagen, die Anforderungen an die leittechnischen Einrichtungen (Teil 1) und an die Störfallinstrumentierung (Teil 2, Kapitel 2) in Modul 5 zusammen zu führen. Die Anforderungen an die elektrische Energieversorgung aus dem Modul 5 (Teil 2, Kapitel 1) sollen dann ausgegliedert und in einem eigenen Modul 12 konzentriert werden.	

Nr. in DB	Kapitel in Modul	Kommentar	Änderung	Begründung	Vorschlag Textänderung
1231	Übergreifend	**Kommentar:** Eine weitere wichtige Fragestellung betrifft den Detaillierungsgrad des Regelwerks und hier insbesondere die Zuweisung zu den Kategorien: verordnungswürdig, „Modulbereich“, KTA- Fachregel -Bereich. Hierzu hat der KTA-UA PG wertvolle Vorarbeiten geleistet. Aus hiesiger Sicht ist nicht erkennbar, ob diese Aufgabenstellung in den Modulen Berücksichtigung gefunden hat. Daher wird es für erforderlich gehalten, die Vorschläge des UA-PG zu jedem einzelnen Kapitel zu erörtern und über den Vorschlag in der Ad- hoc- AG zu entscheiden (Forderung 3).	**NEIN**	Die Kommentare von Arbeitsgruppen des KTA-UA PG betreffen im Wesentlichen die Rev. A des M5. Die angesprochenen Aspekte wurden weitgehend in der Rev. B berücksichtigt oder beantwortet.	
1232	Übergreifend	**Kommentar:** Hinsichtlich der Ausgewogenheit wurde ein Vorschlag durch eine vom KTA-UA-PG eingesetzte ad hoc-Gruppe erarbeitet. Diese Arbeitsergebnisse sind bisher nicht eingeflossen.	**NEIN**	Siehe Antwort zum Kommentar Nr.1231.	
1233	Übergreifend	**Kommentar:** Der Derzeitige Detaillierungsgrad ist inhomogen und wird nur selten der zugedachten übergeordneten Position der formulierten Regeln gerecht. Es gibt starke Überlappungen mit KTA und anderen bestehenden Regeln. Abschließend machen wir darauf aufmerksam, dass der Detaillierungsgrad in diesem Modul weitgehend dem von KTA-Regeln entspricht. Deshalb ist es sinnvoll, übergeordnete Anforderungen in der vorgesehenen Verordnung zu regeln und Detailanforderungen -wie sie z. Zt. im Modul 5 vorgesehen sind - in KTA-Regeln aufzunehmen. Damit erübrigt sich die Erstellung eines „Moduls 5". In weiten Bereichen Abschrift der KTA 3502, die Punkte 1 und 2 sind als übergeordnete Anforderungen ausreichend.	**NEIN**	Der in Modul 5 enthaltene Detaillierungsgrad entspricht unserem Verständnis nach nicht dem von KTA Regeln, es sei denn, es handelt sich dort um übergeordnete Anforderungen, in Orientierung auch an den RSK LL. „Überlappungen“ zu KTA Regeln sind nicht nur üblich, sondern teilweise auch Ziel führend, jedenfalls jedoch zulässig, wenn keine Widersprüche zwischen den Texten bestehen. Aussagen darüber, welche Anforderungen ggf. in einer vorgesehenen Verordnung enthalten sein sollen, werden nicht in Modul 5 getroffen.	
1243	Übergreifend	**Kommentar:** Im Teil Leittechnik sind die Anforderungen dahingehend unterschieden worden, dass diese nur für die sicherheitstechnischen, kategorisierten Funktionen gelten und damit nicht für die betrieblichen Einrichtungen. Im Teil Elektrische Energieversorgung ist diese Eindeutigkeit nicht durchgängig gegeben. Hier sollte eine weitere Differenzierung sowie eine Abgrenzung zur Sicherheitsebene erfolgen.	**NEIN**	Der Kommentar ist insofern nicht nachvollziehbar, als in Modul 5 Teil 2 Kapitel 1 alle sicherheitsrelevanten Aspekte der elektrischen Energieversorgung mit Bezug zu den Sicherheitsebenen behandelt werden. Eine hinsichtlich der Sicherheitsebenen eigene Begrifflichkeit, wie in der Leittechnik, wäre für die Einrichtungen zur elektrischen Energieversorgung nicht sinnvoll.	
1685	Übergreifend	**Kommentar:** Die Anforderungen an die Leittechnik sind über mehrere Module gestreut. Es finden sich beispielsweise Aussagen bzgl. der zu unterstellenden Fehlerpostulate in den Modulen 1,5 und 10. So wird für die Sicherheitsebene 2 beispielsweise in Modul 1 (3.2 (2)) eine n+0, in Modul 5 (3.3) eine n+1 und in Modul 10 (1.1.1.2 (1)) eine n+2 Auslegung gefordert. **Vorschlag:** Anforderungen an die Leittechnik sind nicht doppelt und alle in Modul 5 zu formulieren. Ist es unvermeidlich, Anforderungen an die Leittechnik auch in anderen Modulen zu formulieren, dann sind in Modul 5 Querverweise auf diese Anforderungen aufzunehmen.	**NEIN**	Die Anforderungen an die Leittechnik wurden u. E. im M5 vollständig formuliert. Die Schnittstellen zwischen M5 und M1 wurden überprüft und sind konsistent. Die Querverweise wurden im M5-Text (z. B. im Abschnitt 3.2 wird auf M10 verwiesen) ausgewiesen.	
11	Definitionsliste	**Kommentar:** Müssen die Begriffe „Softwareversagen“ und „Versagen (Software)“ beide definiert werden?	**JA**	In der Definitionsliste und im Modultext sollte einheitlich der Begriff „Softwareversagen“ angewendet werden. Der Begriff „Versagen (Soft-	

Nr. in DB	Kapitel in Modul	Kommentar	Ände-rung	Begründung	Vorschlag Textänderung
				ware)“ entfällt. Der Modultext wird im Folgenden hinsichtlich der Anwendung der Begriffe „Versagen“ und Softwareversagen überprüft und falls erforderlich korrigiert. Ergänzung der Definitionsliste um folgende Definition: Softwareversagen: Nichterfüllung von Funktionen der Software aufgrund eines vorhandenen Softwarefehlers und einer zufälligen, noch nicht aufgetretenen Kombination oder Abfolge von Eingangsdaten.	
1686	Übergreifend	**Kommentar:** Die derzeitige Definition der Begriffe Ausfall und Versagen erlaubt keine Unterscheidung, ob sich ein Fehler spontan funktional auswirkt oder nicht. Diese Unterscheidung ist jedoch sicherheitstechnisch von zentraler Bedeutung. Auch die Definition zu „Fehler“ ist aus Sicht der Leittechnik zu überdenken, z. B. bei unvollständiger oder fehlerhafter Anforderungsspezifikation, Herstellungsfehler. AG5-M5 wird einen Änderungsvorschlag erarbeiten. **Vorschlag:** Die Begriffsdefinitionen sollten derart präzisiert werden, dass klar unterschieden werden kann, ob sich ein Fehler spontan funktional auswirkt oder nicht.	**Teilweise**	Siehe Antwort zum Kommentar Nr. 11.	
	Modul 5 Teil 1				
1688	1 Teil 1	**Kommentar:** In Modul 5 finden sich nahezu keine Anforderung an die Festlegung der leittechnischen Funktionen (nur in 4 (2) aber ohne Anforderungen an Inhalte, Struktur, Verständlichkeit, Vollständigkeit, Korrektheit etc.). Bezüglich des zentralen Stellenwertes, der der Festlegung dieser Funktionen in Modul 1 eingeräumt wird, erscheint das unzureichend und sollte ergänzt werden. Im Rahmen dieser Ergänzungen solle auch die Forderung 3.1 (6), 3.2 (1) und 8.6 aus Modul 1, die sich derzeit in Modul 5 nicht wieder finden, berücksichtigt werden. **Vorschlag:** Anforderungen an leittechnische Funktionen: 1. Die leittechnischen Funktionen sind derart festzulegen, dass die Schutzziele (die in Modul 1 definiert werden) in allen Betriebszuständen der Anlage und bei allen zu unterstellenden Ereignissen sichergestellt werden. 2. Es ist sicherzustellen, dass die verfahrenstechnischen Aufgabenstellungen vollständig durch leittechnische Funktionen in jeder Sicherheitsebene abgebildet sind. 3. Die leittechnischen Funktionen sind einfach strukturiert und vollständig spezifiziert. 4. Die Spezifikation der leittechnischen Funktionen umfasst mindestens	**NEIN**	Die Funktionen werden durch die Analysen festgelegt und in M5 werden die Anforderungen an die Umsetzung der leittechnischen Funktionen gestellt. Dieser Aspekt wird im Abschnitt 2 durch Kategorisierung der LT-Funktionen berücksichtigt. Alle Forderungen des Vorschlags sind sinngemäß entsprechend des Detaillierungsgrads in M5, Teil 1 enthalten.	

Nr. in DB	Kapitel in Modul	Kommentar	Änderung	Begründung	Vorschlag Textänderung
		• Die funktionalen Merkmale (Art und Weise, wie Messsignale von Sicherheitsvariablen zu Auslösesignale für Sicherheitssysteme verarbeitet werden) • Die Leistungsmerkmale (Antwortzeit, Genauigkeit usw.) sowie • Die Sicherheitsmerkmale (Sicherheitskategorie, relevante Störfälle, Unabhängigkeitanforderungen).			
66	2 Teil 1	**Kommentar:** Inkonsistenz zwischen Modul 1 und Modul 5. In der Leittechnik sollen Funktionen kategorisiert werden. In Modul 1 sollen Komponenten klassifiziert werden. **Vorschlag:** Getrennte Geltungsbereiche festlegen: In Modul 1: Klassifizierung von Komponenten In Modul 5. Kategorisierung von Funktionen	**NEIN**	Der Geltungsbereich ist im Modul 5 festgelegt. Die Kategorisierung der LT-Funktionen und die Anwendung dieser Kategorisierung sind u. E. konsistent. Im M5 sind die Anforderungen an die leittechnischen Einrichtungen, die kategorisierte LT-Funktionen ausführen, festgelegt. Es besteht dadurch u. E. keine Inkonsistenz zwischen der Kategorisierung von LT-Funktionen in M5 und Klassifizierung von Komponenten (Einrichtungen) im M1.	
1689	2 Teil 1	**Kommentar:** Inkonsistenz zwischen Modul 1 und Modul 5. Ein Angleich an Modul 1 wurde vorgenommen **Vorschlag:** Die Leittechnik-Funktionen der Kategorie A umfassen alle Funktionen, deren Versagen zu einer nicht beherrschbaren Verletzung von Barrieren führt sowie die Funktionen, die erforderlich sind um Ereignisse der Sicherheitsebene 3 zu beherrschen Kategorie B Die Leittechnik Funktionen der Kategorie B umfassen die Funktionen, die erforderlich sind zur wirksamen und zuverlässigen Störfallvermeidung, sowie zur Beherrschung von Ereignissen der Sicherheitsebene 2. Kategorie C Die Leittechnik Funktionen der Kategorie C umfassen alle übrigen Funktionen mit sicherheitstechnischer Bedeutung.	**NEIN**	Der Vorschlag wird zurückgewiesen. Die Anforderungen an die Einhaltung von Barrieren werden in M1 behandelt. Hierbei werden die unterschiedlichen Funktionen in Abhängigkeit von den Sicherheitsebenen festgelegt. Im Modul 5 werden abgestufte Anforderungen an die Leittechnik-Funktionen in Abhängigkeit von Ereignissen der SE festgelegt.	
67	3.1 (2) Teil 1	**Modultext:** Eine auf ihre Eignung geprüfte oder für den Einsatzfall und für die unterstellten Einsatzbedingungen betriebsbewährte und möglichst wartungsfreie Hardware ist eingesetzt. Eine auf ihre Eignung geprüfte Software ist eingesetzt. **Kommentar:** Betriebsbewährung auch für Software der Kategorie B und C zulässig. Definition zu Software erstellen. Definition zu Eignungsprüfung; Eignungsüberprüfung und Typprüfung erstellen. Eignungsprüfung gemäß KTA enthält Eignungsüberprüfung und Typprüfung **Vorschlag:** ....Eine auf ihre Eignung überprüfte Software ist eingesetzt.	**JA**	Text in M5 wird unter Berücksichtigung des Kommentars präzisiert. T5 empfiehlt die Definitionsliste um den Begriff „Anwendungsprofil“ zu erweitern: Anwendungsprofil der Software: Die Art und Weise der Benutzung der Software, einschließlich der zeitlichen Anforderungen, der zu verarbeitenden Daten, der verwendeten Parameter und der anfallenden Bedienereingriffe.	Eine auf ihre Eignung ~~ge~~überprüfte oder für den Einsatzfall und für die unterstellten Einsatzbedingungen betriebsbewährte und möglichst wartungsfreie Hardware ist eingesetzt. Eine auf ihre Eignung geprüfte Software ist eingesetzt.
68	3.1 (3)	**Modultext:**	**JA**	Um Missverständnisse hinsichtlich der Anwen-	Leitungen und Kabel einschließlich Lichtwellen-

Nr. in DB	Kapitel in Modul	Kommentar	Änderung	Begründung	Vorschlag Textänderung
	Teil 1	Leitungen und Kabel einschließlich Lichtwellenleiter sind nach Strängen getrennt und, soweit erforderlich, gegen Einwirkungen von innen und außen geschützt verlegt. **Kommentar:** Definition: "Strang" ergänzen		dung des Begriffs „Strang“ zu vermeiden, wird im M5-Text der Begriff „Strang“ durch den Begriff „Redundante“ ersetzt. Die Definition „Redundante“ aus KTA 3301 soll in die Definitionsliste aufgenommen werden: Redundante: Bestandteil eines Systems (z.B. Komponente, Teilsystem, Strang), der gleichwertig mit anderen Systembestandteilen die gleichen Funktionen erfüllt und der bei Bedarf einen dieser anderen Systembestandteile voll ersetzt oder durch diesen ersetzt werden kann.	leiter sind nach ~~Strängen~~ Redundanten getrennt und, soweit erforderlich, gegen Einwirkungen von innen und außen geschützt verlegt.
507	3.1 (9) Teil 1	**Modultext:** Die leittechnischen Einrichtungen sind so ausgelegt, dass die in der Verfahrenstechnik vorhandene Unabhängigkeit und Fehlertoleranz durch sie nicht beeinträchtigt ist... **Kommentar:** Der Begriff Fehlertoleranz in der Verfahrenstechnik ist unverständlich	**JA**	Team 5 stimmt der Aussage zu, dass der Begriff Fehlertoleranz vorrangig im Zusammenhang mit Leittechnik (Hard- und Software) angewendet wird. Der VDE- Fachausschuss 6.3 definiert Fehlertoleranz als ein zentrales Mittel zur Erreichung von Verlässlichkeit. Verlässlichkeit als Oberbegriff schließt Aspekte wie Zuverlässigkeit, Verfügbarkeit, Sicherheit, Diagnostizierbarkeit, Datenintegrität und Zugriffschutz ein. In Anlehnung an RSK-LL DWR, 7.3.5 Redundanz und Unabhängigkeit: *(1) „Die Sicherheitsleittechnik ist so aufzubauen, dass die in den aktiven Sicherheitseinrichtungen vorgegebene Redundanz gewahrt bleibt.“* erfolgt nebenstehender Änderungsvorschlag.	Die leittechnischen Einrichtungen sind so ausgelegt, dass die in den aktiven verfahrenstechnischen Einrichtungen ~~der Verfahrenstechnik~~ vorhandene Unabhängigkeit und Fehlertoleranz durch sie nicht beeinträchtigt werden.
69 1690	3.1 (11) Teil 1	**Modultext:** Zur Absicherung gegen Bedienungsfehler sind technische Vorkehrungen vorrangig vor organisatorischen Maßnahmen vorgesehen. **Kommentar:** In Leitlinien: statt vorrangig "vorzugsweise" **Vorschlag:** ...Vorkehrungen vorzugsweise vor organisatorischen Maßnahmen.....	**JA**	Red. Änderung wird umgesetzt.	Zur Absicherung gegen Bedienungsfehler sind technische Vorkehrungen ~~vorrangig~~ vorzugsweise vor organisatorischen Maßnahmen ~~vorgesehen~~ angewandt.
70	3.1 (12) Teil 1	**Modultext:** Die leittechnischen Einrichtungen sind so ausgelegt, dass die für die Beherrschung von Ereignissen und für die Durchführung von Maßnahmen des anlageninternen Notfallschutzes erforderlichen Eingriffsmöglichkeiten vorhanden sind. Die Eingriffsmöglich-keiten sind so ausgelegt, dass sie die Funktionsfähigkeit der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorien A und B ausführen, nicht beeinträchtigen. Die Eingriffsmöglichkeiten sind gegen Fehlbedienung gesichert. **Kommentar:** Präzisierung erforderlich (durch Indikativ kommt es zu Missverständnissen) z.B. "....automatische Maßnahmen des anlageninternen Notfallschutzes erforderlichen Eingriffsmöglichkeiten vorhanden sind.....Ansonsten Widerspruch zu Modul 1 3.2 (6) **Vorschlag:**	**JA**	Vorgeschlagene Präzisierung wird berücksichtigt.	Die leittechnischen Einrichtungen sind so ausgelegt, dass die für die Beherrschung von Ereignissen und für die Durchführung von Maßnahmen des anlageninternen Notfallschutzes erforderlichen Eingriffsmöglichkeiten vorhanden sind. Die Eingriffsmöglichkeiten sind so ausgelegt, dass sie die Funktionsfähigkeit der leittechnischen Einrichtungen ~~die Leittechnik-Funktionen der Kategorien A und B ausführen~~, bei der Beherrschung der Ereignisse der Sicherheitsebenen 2 und 3 nicht unzulässig beeinträchtigen. Die Eingriffsmöglichkeiten sind gegen Fehlbedienung gesichert.

Nr. in DB	Kapitel in Modul	Kommentar	Änderung	Begründung	Vorschlag Textänderung
		Einfügung z.B.: ....Funktionen der Kategorie A und B ausführen, nicht zulässig beieinträchtigen			
1687	3.1 (12) Teil 1	**Kommentar:** Grundsätzlich sind die Anforderungen aus Modul 1 und 5 zueinander konsistent mit folgenden Einschränkungen: Die Anforderung 3.2 (6) in Modul 1 und die Anforderung 3.1 (12) in Modul 5 sind widersprüchlich.	**JA**	Siehe unter Kommentar Nr.70.	
1691	3.1 (12) Teil 1	**Kommentar:** Präzisierung erforderlich (durch Indikativ kommt es zu Missverständnissen). Zur Durchführung von Notfallmaßnahmen wird es auch notwendig sein, ggf. Sicherheitsfunktionen der Kategorie A oder B unwirksam zu machen. **Vorschlag:** Die leittechnischen Einrichtungen sind so ausgelegt, dass die für die Beherrschung von Ereignissen und für die Durchführung von Maßnahmen des anlageninternen Notfallschutzes erforderlichen Eingriffsmöglichkeiten vorhanden sind. **Die Wirksamkeit der anlageninternen Notfallmaßnahmen ist auch bei beliebigem Versagen der Sicherheitsleittechnik sichergestellt. Die Eingriffsmöglichkeiten sind dezentral angeordnet, gegen Fehlbedienung gesichert und soweit erforderlich automatisiert.**	**NEIN**	Dem Vorschlag wird nicht gefolgt. Die Wirksamkeit der anlageninternen Notfallmaßnahmen kann bei dem unterstellten beliebigen Versagen der Sicherheitsleittechnik nicht allein durch Eingriffsmöglichkeiten sichergestellt werden.	
1692	3.1.(13) Teil 1	**Kommentar:** Die in dem Abschnitt über Fehlfunktionen angesprochenen Ereignisse sind in Modul 3 aufgeführt. (siehe Info-1_AG5_Modul5-4) **Vorschlag:** Können Fehler in leittechnischen Einrichtungen einer Sicherheitsebene zu Ereignissen (siehe Modul 3) führen, die nur durch Einrichtungen der nächsten Sicherheitsebene beherrscht werden, dann ist durch die Auslegung sicherzustellen, dass der Beitrag der Leittechnik zu diesen Ereignissen nicht relevant ist.	**NEIN**	Im Kommentar wird vorgeschlagen, einen neuen Abschnitt 3.1(13) in M5 einzufügen. Diesem Vorschlag wird nicht entsprochen, da diese Aspekte in M5 bereits in den Abschnitten 3.2 (5) und 3.3 (neuer Textvorschlag zu Rev. C) berücksichtigt werden. Siehe Vorschlag zu Kommentar Nr. 512.	
1234	3.2 (2) Teil 1	**Modultext:** Veränderungen an Bereitschaftsstellungen von Einrichtungen des Sicherheitssystems werden nur dann vorgenommen, wenn entsprechende Freigabebedingungen erfüllt sind und wenn diese Veränderungen automatisch oder durch technische Vorkehrungen bzw. organisatorische Maßnahmen wieder aufgehoben werden, wenn die Freigabebedingungen nicht mehr erfüllt sind. In dem sicherheitstechnisch geforderten Zustand sind die Einrichtungen gegen Eingriffe gesichert. **Kommentar:** Das sind allg. Anforderungen an das Sicherheitssystem bzw. die Betriebsführung des Kraftwerkes, nicht an die leittechnischen Einrichtungen. Das muss an anderer Stelle aufgeführt werden.	**Teilweise**	Der Kommentar ist insofern zutreffend, als eine generelle Anforderung an anderer Stelle (Modul 10) besteht, in Modul 5 sollte dies jedoch nicht gestrichen werden, da hier insbesondere auf spezifisch leittechnische Aspekte eingegangen wird (z. B. Prüffreigabe, automatische Rücksetzung der Prüffreigabe im Anforderungsfall etc.). Redaktionelle Präzisierung.	Veränderungen an Bereitschaftsstellungen von Einrichtungen des Sicherheitssystems werden nur dann vorgenommen, wenn entsprechende Freigabebedingungen erfüllt sind und wenn diese Veränderungen automatisch oder durch technische Vorkehrungen bzw. organisatorische Maßnahmen wieder aufgehoben werden, wenn die Freigabebedingungen nicht mehr erfüllt sind. In dem sicherheitstechnisch geforderten Zustand sind diese Einrichtungen gegen unzulässige Eingriffe geschützt. ~~ichert.~~
1235	3.2 (3) Teil 1	**Modultext:** Sind bei Einrichtungen des Sicherheitssystems eindeutige Bereitschaftsstellungen von Stellgliedern bei Normalbetrieb vorgeschrieben, so wird das Verlassen dieser Bereitschaftsstellung signalisiert. Handarmaturen sind in Bereitschaftsstellung möglichst eingriffsicher blockiert. **Kommentar:** Regelungen für Handarmaturen gehören nicht hier hin.	**JA**	Der Kommentar ist zutreffend. Der 2. Satz der Ziffer 3.2 (3) von Modul 5 ist an anderer Stelle (Modul 10, Abschnitt 1.4) aufgeführt und kann in Modul 5 gestrichen werden.	Sind bei Einrichtungen des Sicherheitssystems eindeutige Bereitschaftsstellungen von Stellgliedern bei Normalbetrieb vorgeschrieben, so wird das Verlassen dieser Bereitschaftsstellung signalisiert. ~~Handarmaturen sind in Bereitschaftsstellung möglichst eingriffsicher blockiert.~~
71	3.2 (4)	**Modultext:**	**JA**	Vorschlag akzeptiert – „elektrisch“ wird an der	Die leittechnischen Einrichtungen, die Leittech-

Nr. in DB	Kapitel in Modul	Kommentar	Änderung	Begründung	Vorschlag Textänderung
	Teil 1	a) Die leittechnischen Einrichtungen des Sicherheitssystems, die Leittechnikfunktionen der Kategorie A ausführen, sind redundant ausgelegt. Sie sind räumlich getrennt oder durch sicherheitstechnisch gleichwertige Vorkehrungen geschützt und elektrisch unabhängig ausgeführt. b) Ein Ausfall in den leittechnischen Einrichtungen des Sicherheitssystems hat höchstens Auswirkungen auf die Funktion des betroffenen Stranges des Sicherheitssystems. **Kommentar:** Unnötige Einschränkung. Die Forderung nach Unabhängigkeit soll allgemein gefordert werden. Vermeidung von datentechnischer Kopplung **Vorschlag:** Entfallen: elektrisch		Stelle gestrichen, da klarstellender Hinweis. Anpassung der Begrifflichkeit „Strang“ gemäß Antwort auf Kommentar Nr. 68.	nik-Funktionen der Kategorie A ausführen, sind zur Sicherstellung ihrer Funktionsfähigkeit zuverlässig ausgelegt. Sie sind so ausgelegt, dass auch bei Instandhaltungsmaßnahmen an diesen Einrichtungen das Sicherheitssystem seine Aufgabe mit ausreichender Zuverlässigkeit erfüllt (siehe auch „Sicherheitsanforderungen für Kernkraftwerke: Anforderungen an die Auslegung und den sicheren Betrieb von baulichen Anlagenteilen, Systemen und Komponenten“ (Modul 10) Abschnitt 1.1). a) Die leittechnischen Einrichtungen des Sicherheitssystems, die Leittechnikfunktionen der Kategorie A ausführen, sind redundant ausgelegt. Sie sind räumlich getrennt oder durch sicherheitstechnisch gleichwertige Vorkehrungen geschützt und ~~elektrisch~~ unabhängig ausgeführt. b) Ein Ausfall in den leittechnischen Einrichtungen des Sicherheitssystems hat höchstens Auswirkungen auf die Funktion ~~des betroffenen Stranges~~ der betroffenen Redundante des Sicherheitssystems. c) Die leittechnischen Einrichtungen, die für die Funktionsfähigkeit des Sicherheitssystems nach Eintritt von Ereignissen der Sicherheitsebene 3 erforderlich sind, sind so ausgelegt, dass sie den jeweils ungünstigsten Umgebungs- und Störfallbedingungen standhalten, die im zugehörigen Aufstellungs- und Installationsbereich auftreten können.
1693	3.2 (4) Teil 1	**Kommentar:** Unnötige Einschränkung. Die Forderung nach Unabhängigkeit soll allgemein gefordert werden. Z.B die Vermeidung von datentechnischer Kopplung. **Vorschlag:** Die leittechnischen Einrichtungen des Sicherheitssystems, die Leittechnikfunktionen der Kategorie A ausführen, sind redundant ausgelegt. Sie sind räumlich getrennt oder durch sicherheitstechnisch gleichwertige Vorkehrungen geschützt und ~~**elektrisch**~~ unabhängig ausgeführt.	**JA**	Vorschlag akzeptiert – „elektrisch“ wird an der Stelle gestrichen, da klarstellender Hinweis. Siehe vorausgehende Zeile.	
72	3.2 (5) Teil 1	**Modultext:** Die leittechnischen Einrichtungen sind so ausgelegt, dass fehlerhaftes Ansteuern des Sicherheitssystems unter Berücksichtigung der Ausfallkombinationen nach dem Einzelfehlerkonzept verhindert wird, wenn dadurch Ereignisse der Sicherheitsebene 4 ausgelöst werden können. Hinweis Anforderungen	**NEIN**	Nach Ansicht von T5 stimmt der Begriff „Ereignisse der SE4“ mit dem Begriff aus der RSK-LL „Störfälle mit nicht tolerablen Auswirkungen" überein. Demzufolge entspricht der Text im Modul 5 weitgehend der RSK-LL Anforderung	

Nr. in DB	Kapitel in Modul	Kommentar	Änderung	Begründung	Vorschlag Textänderung
		zur Beherrschung von Einzelfehlern sind in „Sicherheitsanforderungen für Kernkraftwerke: Anforderungen an die Auslegung und den sicheren Betrieb von baulichen Anlagenteilen, Systemen und Komponenten“ (Modul 10) Abschnitt 1.1 festgelegt. **Kommentar:** Hinsichtlich der Auswirkung von Fehlanregungen sind die Funktionen in immer sicherheitsgerichtet oder nicht immer sicherheitsgerichtet zu unterscheiden. Immer sicherheitsgerichtete Funktionen z.B. RESA können durch Fehlauslösungen nie eine Verschlechterung des Sicherheitsniveaus zu Folge haben. Eine nicht immer sicherheitsgerichtete Funktion kann dagegen das Potential haben durch Fehlauslösung selbst einen Störfall zu indizieren, der durch eine andere Funktion beherrscht werden muss, um nicht tolerable Auswirkungen zu verhindern. Für diese ist gemäß RSK-LL 7.3.2 (9), was als Quelle für die Anforderung angegeben ist, durch eine entsprechende Auslegung Fehlanregungen zu verhindern **Vorschlag:** Es sollte geprüft werden, ob Sicherheitsebene 4 oder Sicherheitsebene 3 gemeint ist. **Änderung:** .... unter Berücksichtigung des Einzelfehlerkonzepts verhindert wird, wenn.....		und es sind keine Änderungen im Text erforderlich (s. RSK-LL-Text 7.3.2(9): *Fehlerhaftes Ansteuern des Sicherheitssystems ist unter Berücksichtigung der Ausfallkombinationen nach 7.3.2 (6) zu verhindern, wenn dadurch Störfälle mit nichttolerablen Auswirkungen auftreten können.*	
508	3.2 (5) Teil 1	**Kommentar:** Die Formulierung sollte so gewählt werden, dass fehlerhaftes Ansteuern des Sicherheitssystems unter Berücksichtigung der zu unterstellenden Ausfallkombinationen nicht zu unzulässigen Anlagenzuständen führt.	**JA**	Der Einwand ist berechtigt. M5-Text wird dementsprechend mit dem Hinweis auf Einzelfehlerkonzept präzisiert, wobei „unzulässige Anlagenzustände“ durch „auslegungsüberschreitende Anlagenzustände“ ersetzt werden.	Die leittechnischen Einrichtungen sind so ausgelegt, dass fehlerhaftes Ansteuern des Sicherheitssystems unter Berücksichtigung ~~der Ausfallkombinationen nach dem Einzelfehlerkonzept des Einzelfehlerkonzepts~~der Ziffer 3.2 (11) verhindert wird, wenn ~~dadurch Ereignisse der Sicherheitsebene 4 ausgelöst werden können~~ dies zu auslegungsüberschreitenden Anlagenzuständen führen kann.
1694	3.2 (5) Teil 1	**Kommentar:** Hinsichtlich der Auswirkung von Fehlanregungen sind die Funktionen in immer sicherheitsgerichtet und nicht immer sicherheitsgerichtet zu unterscheiden. Immer sicherheitsgerichtete Funktionen z. B. RESA können durch Fehlauslösungen nie eine Verschlechterung des Sicherheitsniveaus zu Folge haben. Eine nicht immer sicherheitsgerichtete Funktion kann dagegen das Potential haben durch Fehlauslösungen selbst einen Störfall zu indizieren, der durch eine andere Funktion beherrscht werden muss, um nicht tolerable Auswirkungen zu verhindern. Für diese ist gemäß RSK-LL 7.3.2 (9), was als Quelle für die Anforderung angegeben ist, durch eine entsprechende Auslegung Fehlanregungen zu verhindern. **Vorschlag:** Die leittechnischen Einrichtungen sind so ausgelegt, dass fehlerhaftes Ansteuern des Sicherheitssystems unter **Berücksichtigung ~~der Ausfallkombinationen nach dem~~ des Einzelfehlerkonzepts** verhindert wird, wenn dadurch Ereignisse der Sicherheitsebene 4 ausgelöst werden können.	**JA**	Siehe vorausgehende Zeile.	
73	3.2 (6) Teil 1	**Modultext:** Die leittechnischen Einrichtungen, die Leittechnik- Funktionen der Kategorie A ausführen, sind so ausgelegt, dass Schutzaktionen grundsätzlich automatisch	**Teilweise**	Der Modultext ist eine Auslegungsanforderung für LT- Funktion Kat. A (Reaktorschutzanregung), so dass die RS-Aktion automatisch erfol-	Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, sind so ausgelegt, dass Schutzaktionen grundsätzlich

Nr. in DB	Kapitel in Modul	Kommentar	Ände-rung	Begründung	Vorschlag Textänderung
		ausgeführt werden. Nur wenn sichergestellt wird, dass vom Zeitpunkt des Erkennens eines Ereignisses der Sicherheitsebene 3 bis zur Auslösung der zur Beherrschung notwendigen Schutzaktion eine ausreichend große Zeitspanne für die Entscheidungsfindung und für die Durchführung der Schutzaktion durch das Personal zur Verfügung steht, dürfen notwendige Schutzaktionen auch von Hand ausgelöst werden. Der Richtwert für die Zeitspanne, ab der Handmaßnahmen zulässig sind, beträgt 30 Minuten. **Kommentar:** Irreführend, Text aus Modul 5 Teil 2 zitieren 2 (14) **Vorschlag:** Die Inbetriebnahme und Zuschaltung der Notstromerzeugungsanlagen erfolgen im Anforderungsfall automatisch, so dass innerhalb von 30 min. keine Handmaßnahme erforderlich ist. Eine manuelle Inbetriebnahme und Zuschaltung der Notstromerzeugungsanlagen ist jederzeit möglich.		gen soll. Die Möglichkeit für eine manuelle Zuschaltung der Notstromerzeugungsanlage (NS-Dieselgenerator) wird aus der Sicht des T5 dadurch nicht eingeschränkt. Der 30-Minuten-Richtwert gilt zudem nicht nur für den Notstromfall sondern für das ganze Sicherheitssystem. Textvorschlag wird abgelehnt. Die Zeit für die Entscheidungsfindung ist immer erforderlich und kann im wirklichen Anforderungsfall auch unterhalb des Richtwertes liegen. Nebenstehende Präzisierung des Textes wird vorgeschlagen.	automatisch ausgeführt werden. Nur wenn sichergestellt wird, dass vom Zeitpunkt des Erkennens eines Ereignisses der Sicherheitsebene 3 bis zur Auslösung der zur Beherrschung notwendigen Schutzaktion ausreichend ~~große Zeitspanne~~ Zeit für die Entscheidungsfindung und für die Durchführung der Schutzaktion durch das Personal zur Verfügung steht, dürfen notwendige Schutzaktionen auch von Hand ausgelöst werden. Der Richtwert für die Zeitspanne, ab der Handmaßnahmen zulässig sind, beträgt 30 Minuten.
509	3.2 (6) Teil 1	**Kommentar:** Die Einführung des Begriffs „Zeitspanne“ ist nicht Ziel führend, da vielmehr die Aufgabe an das Betriebspersonal darin besteht, sich einen eindeutigen Überblick zur Entscheidungsfindung zu verschaffen, bevor Maßnahmen ergriffen werden. Die Größe der Zeitspanne ist zudem unbestimmt.	**JA**	Siehe vorausgehende Zeile.	
1695	3.2 (6) Teil 1	**Kommentar:** Irreführend, Text aus Modul 5 Teil 2 zitieren 2(14) **Vorschlag:** Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, sind so ausgelegt, dass innerhalb von 30 min nach Erkennen des Ereignisses keine Handmaßnahme erforderlich ist. Handmaßnahmen sind jederzeit zulässig. ~~Die Inbetriebnahme und Zuschaltung der Notstromerzeugungsanlagen erfolgen im Anforderungsfall automatisch, so dass innerhalb von 30 min keine Handmaßnahme erforderlich ist. Eine manuelle Inbetriebnahme und Zuschaltung der Notstromerzeugungsanlagen ist jederzeit möglich.~~	**NEIN**	Dieser Vorschlag wird zurückgewiesen, da der Inhalt dieses Vorschlags im Wesentlichen den Anforderungen des Abschnitts 3.2(6) im Teil 1 an die leittechnischen Einrichtungen mit den Leittechnik-Funktionen der Kategorie A entspricht. Im Abschnitt 2(14), Teil 2 des M5 dagegen werden die Anforderungen nur an die Notstromerzeugungsanlagen gestellt.	
74	3.2 (7) Teil 1	**Modultext:** .....Diese Prüfungen sollen mittels eingebauter Prüfhilfen leicht durchführbar sein. Prüfeingriffe und Handbefehle sind so festgelegt, dass notwendige Sicherheitsfunktionen weder verhindert werden noch die Zuverlässigkeit ihrer Anregung signifikant vermindert wird. **Kommentar:** Unnötige Einschränkung Stattdessen Handbetätigung **Vorschlag:** "Diese Prüfungen sollen mittels Prüfhilfen leicht...." "..... Prüfeingriffe und Handbetätigungen sind so festgelegt, dass notwendige Sicherheitsfunktionen"	**JA**	Kommentar wird sinngemäß berücksichtigt. Wichtig ist nicht nur leichte Durchführbarkeit, sondern auch, dass die Prüfhilfen an den vorgesehenen Schnittstellen eingesetzt werden. Andere Arten oder Möglichkeit der Prüfungen sollen eingeschränkt werden.	Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, sind grundsätzlich selbstüberwachend ausgelegt. Die Funktionen und Eigenschaften, die von der Selbstüberwachung nicht erfasst sind, werden einer regelmäßigen und lückenlosen Überprüfung unterzogen. Die Prüfzyklen sind auf Grundlage von Zuverlässigkeitsbetrachtungen festgelegt. Diese Prüfungen sollen mittels eingebauter Prüfhilfen an dafür vorgesehenen Schnittstellen leicht durchführbar sein. Prüfeingriffe und Handbe~~fehle~~tätigungen sind so festgelegt, dass notwendige Sicherheitsfunktionen weder verhindert werden noch die Zuverlässigkeit ihrer Anregung signifikant vermindert wird. Hinweis Siehe auch die Anforderungen zur

Nr. in DB	Kapitel in Modul	Kommentar	Ände-rung	Begründung	Vorschlag Textänderung
					Sicherstellung der Funktionsbereitschaft von Sicherheitseinrichtungen gemäß „Sicherheits-anforderungen für Kernkraftwerke: Anforderun-gen an die Auslegung und den sicheren Betrieb von baulichen Anlagenteilen, Systemen und Komponenten“ (Modul 10) Abschnitt 1.4.
1696	3.2 (7) Teil 1	**Kommentar:** Unnötige Einschränkung. Präzisierung erforderlich Stattdessen Handbetätigungen **Vorschlag:** Diese Prüfungen sollen mittels ~~**eingebauter**~~ Prüfhilfen ***ohne Eingriff in die Anlage*** leicht durchführbar sein … Prüfeingriffe und **Handbetätigungen** sind so festgelegt, dass notwendige Sicherheitsfunktionen weder verhindert werden noch die Zuverlässigkeit ihrer Anregung signifikant vermindert wird.	**JA**	Kommentar wird sinngemäß berücksichtigt. Siehe vorausgehende Zeile.	
75	3.2 (10) Teil 1	**Modultext:** Es ist das Ziel, den Aufbau der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, so einfach zu gestalten, dass die erforderlichen Nachweise zur Qualifizierung der leittechnischen Einrichtungen des Sicherheitssystems zuverlässig möglich sind. **Kommentar:** Welches Ziel? Irreführend durch Indikativ **Vorschlag:** ...leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, sind einfach aufgebaut	**JA**	Die entscheidende Anforderung der Ziffer ist nicht die Einfachheit des Aufbaus, sondern die zuverlässige Nachweisführung. Insofern kann unbestimmte Formulierung „Es ist das Ziel ... „ entfallen. Stattdessen Textänderung wie ange-geben.	~~Es ist das Ziel, den Aufbau der l~~Leittechnische~~n~~ Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, sind ~~so einfach zu ge-stalten~~ aufgebaut, dass die erforderlichen Nach-weise zur Qualifizierung der leittechnischen Einrichtungen des Sicherheitssystems zuverläs-sig möglich sind.
1697	3.2 (10) Teil 1	**Kommentar:** Welches Ziel? Irreführend durch Indikativ. Ansonsten Änderung: **Vorschlag:** …leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen**, sind einfach aufgebaut**	**JA**	Siehe vorausgehende Zeile.	
510	3.2 (11) Teil 1	**Modultext:** Bei der Auslegung der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, sind Vorkehrungen gegen systemati-sche Ausfälle der Hardware und Versagen der Software derart getroffen, dass ein systematischer Ausfall so unwahrscheinlich ist, dass er ausgeschlossen werden kann. **Kommentar:** Die Auslegung nach dem Stand von W&T erfolgte bisher entsprechend RSK-LL derart, dass Vorsorge gegen systematische Fehler zu treffen ist. Die hier gewählte Forderung geht über den bisherigen Stand von W&T hinaus und sollte auch im Hinblick auf KTA 3501 (4.4.1(5) überprüft werden.	**Teil-weise**	Hinsichtlich des Aspekts der Behandlung von systematischen Fehlern in den leittechnischen Einrichtungen mit LEFU Kat. A. besteht Dissens im Team. Die zum nebenstehenden Vorschlag abweichende Meinung ist in Anhang 1 darges-tellt. Die Begründung für den nebenstehenden Vorschlag lautet: Der Wechsel von der festverdrahteten zur rech-nerbasierten Technik stellt einen sicherheits-technisch bedeutsamen Struktur- und Technolo-giewandel für die Sicherheitsleittechnik dar. Mit der Einführung der rechnerbasierten Leittechnik ist eine starke Konzentration der Leittechnikfunk-tionen (LEFU) auf nur wenige Baugruppen ver-bunden. Weiter besitzt die Gerätetechnik der rechnerbasierten Leittechnik gegenüber der festverdrahteten eine höhere Funktionalität und	Bei der Auslegung der leittechnischen Einrich-tungen, die Leittechnik-Funktionen der Kategorie A ausführen, sind Vorkehrungen gegen systema-tische Ausfälle ~~der Hardware und Versagen der Software derart getroffen,~~ der festverdrahteten leittechnischen Einrichtungen derart getroffen, dass ein systematischer Ausfall ~~so unwahr-scheinlich ist, dass er~~ ausgeschlossen werden kann. Bei der Auslegung der leittechnischen Einrich-tungen, die Leittechnik-Funktionen der Kategorie A ausführen, sind Vorkehrungen gegen systema-tische Ausfälle der software-basierten leittechni-schen Einrichtungen einschließlich systemati-sches Software-Versagen derart getroffen, dass ein systematischer Ausfall beherrscht wird.

Nr. in DB	Kapitel in Modul	Kommentar	Ände-rung	Begründung	Vorschlag Textänderung
				Varianz. Beides hat in der Praxis eine Zunahme der Komplexität der Leittechniksysteme und ein diffizileres Verhalten im Fehlerfall zur Folge. Für ein redundantes homogenes Leittechniksystem ist der deterministische Nachweis zur Beherrschung eines GVA nicht möglich. Für probabilistische Nachweise stehen zurzeit ebenfalls keine Methoden zur Verfügung. Daher basiert der Textvorschlag auf lösungsneutralen Auslegungsgrundsätzen, die auf einer deterministischen Sicherheitsphilosophie beruhen. Die bisher bei der festverdrahteten Sicherheitsleittechnik geführten Nachweise einer ausreichenden Vorsorge gegen einen GVA auf der Basis von fehlervermeidenden Maßnahmen (QS-Maßnahmen) sind für rechnerbasierte Leittechniksysteme nicht mehr ausreichend (höherer Komplexität, Verwendung von vorgefertigten Hard- und Software Komponenten). Auch ist ein Betriebsbewährungsnachweis wegen des schnellen Innovationswandels und der hohen Komplexität der rechnerbasierten Technik nur noch eingeschränkt zielführend. Deshalb ist zur Beherrschung eines GVA bei Leittechniksystemen die LEFU der Kategorie A ausführen eine fehlerbeherrschende Systemauslegung unter Berücksichtigung von Hardware- und Software-GVA erforderlich. Hierzu sind strukturelle und gerätetechnische Maßnahmen in einer dissimilaren Gerätetechnik erforderlich. Auch international stellt dieser Ansatz in der Kerntechnik, aber auch in anderen sicherheitskritischen Anwendungen (Flugzeugtechnik, Bahntechnik) den vorherrschenden Lösungsansatz zur Beherrschung von GVA dar. Neue Definitionsvorschläge: Dissimilare leittechnische Einrichtungen: Leittechnische Einrichtungen bestehen aus unterschiedlicher Hardware und Software (falls Software eingesetzt wird), gekennzeichnet durch den Einsatz unterschiedlicher Entwicklungswerkzeuge, Entwicklungsteams, Fertigungsprozesse, Tests und Instandhaltungsstrategien. Hinweis: Die festverdrahteten leittechnischen Einrichtun-	Beim Einsatz software-basierter Leittechnik werden grundsätzlich dissimilare leittechnische Einrichtungen verwendet. Es bestehen keine Anforderungen hinsichtlich des Einsatzes dissimilarer Einrichtungen, wenn für die jeweils auszuführende Leittechnikfunktion: - ein aktiver systematischer Ausfall sicherheitsgerichtet ist und - bei einem passiven systematischen Ausfall der Störfall durch andere Leittechnikfunktionen der Kategorie A, die durch zu der ausgefallenen Einrichtung dissimilare leittechnische Einrichtungen ausgeführt werden, beherrscht wird. Für Schutzaktionen, die nicht für jeden Anlagenzustand sicherheitsgerichtet sind, ist in Abhängigkeit von den Auswirkungen von passiven oder aktiven systematischen Ausfällen in den leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, eine zweifache oder dreifache dissimilare Ausführung der software-basierten Leittechnik eingesetzt. Eine zweifache dissimilare Ausführung ist eingesetzt, - wenn mit den noch verfügbaren Sicherheitseinrichtungen unter Berücksichtigung von Ziffer 3.2 (6) der Störfall beherrscht wird oder - wenn jede der beiden dissimilaren leittechnischen Einrichtungen für sich alleine die erforderliche Schutzaktion auslöst. Trifft eine der beiden genannten Voraussetzungen für den Einsatz einer zweifach dissimilaren Ausführung nicht zu, ist eine dreifach dissimilar ausgeführte software-basierte Leittechnik eingesetzt.

Nr. in DB	Kapitel in Modul	Kommentar	Ände-rung	Begründung	Vorschlag Textänderung
				gen, die ohne Einsatz der Software die Leittechnik-Funktionen ausführen, sind grundsätzlich dissimilar zu software-basierten leittechnischen Einrichtungen. Die leittechnischen Einrichtungen, die der manuellen Auslösung der Sicherheitsfunktionen dienen, sind dissimilar zu den automatischen leittechnischen Einrichtungen, wenn sie nicht von dem unterstellten systematischen Ausfall betroffen sind. Ausfall einer Einrichtung, die Leittechnikfunktionen ausführt, aktiver: Fehlfunktion einer leittechnischen Einrichtung, die eine Leittechnik-Funktion spontan ausführt, ohne dass die für die Ausführung festgelegten Kriterien erfüllt sind. Ausfall einer Einrichtung die Leittechnikfunktionen ausführt, passiver: Fehlfunktion einer leittechnischen Einrichtung, die eine Leittechnik-Funktion im Anforderungsfall nicht ausführt, obwohl die für die Ausführung festgelegten Kriterien erfüllt sind.	
1698	3.2 (11) Teil 1	**Kommentar:** Vorschlag: Bei der Auslegung der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, sind Auslegungsfehler nicht grundsätzlich auszuschließen. 3.2(11a) Mögliche Auswirkungen von zu unterstellenden Auslegungsfehlern[1] sind unter Berücksichtigung der systemimmanenten Versagensmechanismen zu analysieren. 3.2 (11b) Ergibt die Analyse, dass ein nicht gerichtetes Versagen der leittechnischen Einrichtungen mit systematischem Charakter zu unterstellen ist, dann ist die Auslegung zu ändern.	**NEIN**	Dem Vorschlag wird nicht gefolgt, siehe vorausgehende Zeile.	
76	3.2 (12) Teil 1	**Modultext:** Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, sind so ausgelegt, dass sie ihre Aufgaben auch dann erfüllen, wenn im Anforderungsfall ein Zufallsausfall (gemäß Einzelfehlerkonzept) und ein systematischer Ausfall (systematischer Ausfall der Hardware oder Versagen der Software) und daraus resultierende Folgeausfälle eintreten. Während eines Instandhaltungsfalls wird im Anforderungsfall innerhalb einer Zeitspanne von 100 h das gleichzeitige Auftreten des systematischen Ausfalls	**Teilweise**	Die Anforderung wurde auf der Basis der RSK-LL (Kap. 7.3.2(6)) erstellt und stellt u. E. den Stand von W&T dar. In Ziffer 3.2 (11) wird der Instandhaltungsfall nicht explizit geregelt. Der Text wurde unter Berücksichtigung des neuen Textvorschlages zu 3.2 (11) angepasst.	Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, sind grundsätzlich so ausgelegt, dass sie ihre Aufgaben im Anforderungsfall unter Berücksichtigung folgender Annahmen erfüllen: a) ein Zufallsausfall durch einen Einzelfehler, b) und ein systematischer Ausfall (systematischer Ausfall der Hardware oder systemati-

[1] Weiterführende Präzisierung der analytisch konstruierbaren Auslegungsfehler notwendig (entsprechende Liste wird ggf. in KTA-Regel aufgeführt)

Nr. in DB	Kapitel in Modul	Kommentar	Änderung	Begründung	Vorschlag Textänderung
		und des Zufallsausfalls nicht unterstellt. **Kommentar:** Widerspruch zu 3.2 (11) **Vorschlag:** Folgender Satz sollte dahingehend überprüft werden, ob er wegen Nichtrelevanz nicht entfallen kann: Während eines Instandhaltungsfalls wird im Anforderungsfall innerhalb einer Zeitspanne von 100 h das gleichzeitige Auftreten des systematischen Ausfalls und des Zufallsausfalls nicht unterstellt **Änderung:** Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, sind so ausgelegt, dass sie ihre Aufgaben auch dann erfüllen, wenn im Anforderungsfall ein Zufallsausfall (gemäß Einzelfehlerkonzept) und daraus resultierende Folgeausfälle und ein systematischer Ausfall (systematischer Ausfall der Hardware oder Versagen der Software) sofern er nicht nach 3.2. (11) ausgeschlossen werden kann, eintreten.			sches Softwareversagen), gilt nicht für festverdrahtete Leittechnik (siehe Ziffer 3.2 (11)), c) und Folgeausfälle ~~b)~~d) und ein Instandhaltungsfall vorliegt. ~~auch dann erfüllen, wenn im Anforderungsfall ein Zufallsausfall (gemäß Einzelfehlerkonzept) und ein systematischer Ausfall (systematischer Ausfall der Hardware und systematisches Softwa-revVersagen der Software), sofern er nicht nach Ziffer 3.2 (11) ausgeschlossen werden kann,und daraus resultierende Folgeausfälle eintreten.~~ Während eines Instandhaltungsfalls wird im Anforderungsfall innerhalb einer Zeitspanne von 100 h das gleichzeitige Auftreten des systematischen Ausfalls und des Zufallsausfalls nicht unterstellt. Bei software-basierten leittechnischen Einrichtungen mit einem ausreichend hohen Selbstüberwachungsgrad und nachgewiesenen Instandhaltungszeiten kleiner als 10 h wird gleichzeitig mit dem systematischen Ausfall das Auftreten eines Zufallsausfalls oder des Instandhaltungsfalls nicht unterstellt. Zum Ausfall durch Einzelfehler und Unverfügbarkeit durch Instandhaltung sind weitere Anforderungen in den „Sicherheitsanforderungen für Kernkraftwerke: Anforderungen an die Auslegung und den sicheren Betrieb von baulichen Anlagenteilen, Systemen und Komponenten“ Modul 10, Abschnitt 1, festgelegt.
1699	3.2 (12) Teil 1	**Kommentar:** Definition Versagen/Ausfall Die derzeitige Definition der Begriffe Ausfall und Versagen erlaubt keine Unterscheidung, ob sich ein Fehler spontan funktional auswirkt oder nicht. Diese Unterscheidung ist jedoch sicherheitstechnisch von zentraler Bedeutung. Die Präzisierung ist für Sonderfälle in der Leittechnik notwendig, die Definitionen gelten jedoch allgemein. Versagen: Abweichung der ausgeführten Funktion im Anforderungsfall von der geforderten Funktion. Ausfall: Verlust einer oder mehrerer Auslegungsanforderungen derart, dass die geforderte Funktionsfähigkeit nicht mehr gegeben ist **Vorschlag:** Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, sind so ausgelegt, dass sie ihre Aufgaben auch dann erfüllen, wenn im Anforderungsfall ein Zufallsausfall (gemäß Einzelfehlerkonzept) und	**Teilweise**	In neuer Version des M5 werden die Definitionen hinsichtlich „Versagen“ und „Ausfall“ überarbeitet, siehe unter Kommentar - Nr. 10. Der Textvorschlag kann nicht übernommen werden, da Vorschlag zu Ziffer 3.2(11a) nicht aufgenommen wurde.	

Nr. in DB	Kapitel in Modul	Kommentar	Änderung	Begründung	Vorschlag Textänderung
		daraus resultierende Folgeausfälle und ein **systematisches Versagen mit den unter 3.2 (11a) analysierten Auswirkungen eintreten.** Während eines Instandhaltungsfalls wird im Anforderungsfall innerhalb einer Zeitspanne von 100 h das gleichzeitige Auftreten des systematischen **Versagens** nicht unterstellt.			
77	3.2 (13) Teil 1	**Modultext:** Einrichtungen des Aggregateschutzes sind so ausgelegt, dass bei Anforderung eines Aggregats durch die leittechnischen Einrichtungen des Sicherheitssystems der Aggregateschutz grundsätzlich nicht wirksam wird, es sei denn, die dadurch möglichen Folgeschäden beeinträchtigen die Sicherheit der Anlage mehr als der Ausfall des Aggregats. Der Aggregateschutz ist so ausgelegt, dass der Vorrang der Leittechnik-Funktionen der Kategorie A vor dem Aggregateschutz sichergestellt ist. Ist im Aggregateschutz ein Vorrang vor Leittechnik-Funktionen der Kategorie A notwendig, werden an den Aggregateschutz die Anforderungen der Kategorie A gestellt. Die Anforderungen der Kategorie A an die Einrichtungen des Aggregateschutzes werden nicht gestellt, wenn nachgewiesen wird, dass Fehler im Aggregateschutz so unwahrscheinlich sind, dass eine dadurch verursachte Fehlauslösung ausgeschlossen werden kann. **Kommentar:** Abschnitt zu detailliert. Detaillierung sollte entsprechender KTA Regel vorbehalten sein. Auch Widerspruch zwischen Satz 2 und 3 (indikativ) Hier sollten nur allgemeine Anforderungen gestellt werden.	**Teilweise**	Die Anforderung wurde unter Berücksichtigung der Erkenntnisse aus dem Ereignis im KKW Forsmark überarbeitet. Die Anforderung ist allgemein formuliert und entspricht der Detaillierungstiefe des Moduls 5. Ein Widerspruch zwischen dem 2. und 3. Absatz besteht insofern nicht, als der 3. Absatz den Ausnahmefall zum 2. Absatz regelt. Daher hier Ergänzung eines „grundsätzlich“.	Schutzeinrichtungen an Aggregaten und Hilfseinrichtungen ~~Einrichtungen des Aggregateschutzes~~ sind so ausgelegt, dass bei Anforderung eines Aggregats durch die leittechnischen Einrichtungen des Sicherheitssystems die Schutzeinrichtungen ~~der Aggregateschutz~~ grundsätzlich nicht wirksam ~~wird~~werden, es sei denn, die dadurch möglichen Folgeschäden beeinträchtigen die Sicherheit der Anlage mehr als der Ausfall des Aggregats. Die Schutzeinrichtungen sind grundsätzlich ~~Der Aggregateschutz ist~~ so ausgelegt, dass der Vorrang der Leittechnik-Funktionen der Kategorie A vor den Schutzeinrichtungen ~~dem Aggregateschutz~~ sichergestellt ist. Ist in einer Schutzeinrichtung ~~Ist im Aggregateschutz~~ ein Vorrang vor Leittechnik-Funktionen der Kategorie A notwendig, werden an die Schutzeinrichtungen ~~den Aggregateschutz~~ die Anforderungen der Kategorie A gestellt. Die Anforderungen der Kategorie A an die Einrichtungen der Schutzeinrichtungen ~~des Aggregateschutzes~~ werden nicht gestellt, wenn nachgewiesen wird, dass Fehler der Schutzeinrichtung ~~im Aggregateschutz~~ so unwahrscheinlich sind, dass eine dadurch verursachte Fehlauslösung ausgeschlossen werden kann.
1701	3.2 (13) Teil 1	**Kommentar:** Abschnitt zu detailliert. Detaillierung sollte entsprechender KTA-Regel vorbehalten sein. Auch Widerspruch zwischen Satz 2 und 3 (indikativ). Hier sollten nur allgemeine Anforderungen gestellt werden. Es liegt KTA 3504 vor Definition für Aggregatesschutz erforderlich	**NEIN**	Die Detaillierung in diesem Abschnitt ist u. E. erforderlich. Definition des „Aggregateschutzes“ aufgrund neuer Formulierung zu Ziffer 3.2 (13) nicht mehr erforderlich. Siehe Vorschlag zum Kommentar Nr.77.	
	3.2 (15) Teil 1			Folgeanpassung	In den Betriebsphasen, in denen die Verfügbarkeit der Reaktorschnellabschaltung erforderlich ist, ist jederzeit eine Reaktorschnellabschaltung von Hand möglich, auch beim unterstelltem systematischen Ausfall software-basierter Leittechnik einschließlich Softwareversagen (siehe 3.2 (11)).

Nr. in DB	Kapitel in Modul	Kommentar	Änderung	Begründung	Vorschlag Textänderung
78	3.2 (16) Teil 1	**Modultext:** In Betriebsphasen außerhalb der Betriebsphasen A und B, in denen Teile von Leittechnik-Funktionen der Kategorie A planungsgemäß nicht verfügbar sind, ist die zuverlässige und wirksame Störfallbeherrschung für die in diesen Phasen zu unterstellenden Ereignisse unter diesen Bedingungen gewährleistet. **Kommentar:** Unglückliche Formulierung wegen gleicher Buchstaben **Vorschlag:** Entfallen 2. Satz	**JA**	Die Bezüge hinsichtlich Betriebsphasen und Kategorien sind u. E. deutlich im Text dargestellt. Weitere Verdeutlichung durch red. Änderung.	In Betriebsphasen ~~außerhalb der Betriebsphasen A und B,~~ in denen Teile von Leittechnik-Funktionen der Kategorie A planungsgemäß nicht verfügbar sind, ist die zuverlässige und wirksame Störfallbeherrschung für die in diesen Betriebsp~~P~~hasen zu unterstellenden Ereignisse unter diesen Bedingungen gewährleistet.
1251	3.2 (16) Teil 1	**Änderungsvorschlag:** In Betriebsphasen ~~außerhalb der Betriebsphasen A und B~~, in denen Teile von Leittechnik- Funktionen der Kategorie A planungsgemäß nicht verfügbar sind, ist die zuverlässige und wirksame Störfallbeherrschung für die in diesen Phasen zu unterstellenden Ereignisse unter diesen Bedingungen gewährleistet.	**JA**	Siehe vorausgehende Zeile.	
1703	3.2 (16) Teil 1	**Kommentar:** Unglückliche Formulierung wegen gleicher Buchstaben	**JA**	Siehe vorausgehende Zeile.	
511	3.2 (17) Teil 1	**Modultext:** Die leittechnischen Einrichtungen, die Leittechnikfunktionen der Kategorie A ausführen, sind so ausgelegt, dass auch beim Eintreten von Fehlern in diesen Einrichtungen keine Aktionen ausgelöst werden, die die Anlage in einen Störfall überführen können. **Kommentar:** Die leittechnischen Einrichtungen, die Leittechnikfunktionen der Kategorie A ausführen, sind so ausgelegt, dass auch beim Eintreten der unterstellten Fehler in diesen Einrichtungen keine Aktionen ausgelöst werden, die die Anlage in einen Störfall überführen können	**JA**	Präzisierung möglich und sinnvoll (Quelle KTA 3501).	Die leittechnischen Einrichtungen, die Leittechnikfunktionen der Kategorie A ausführen, sind so ausgelegt, dass auch beim ~~Auf~~Eintreten der zu unterstellenden~~von~~ Einzel~~F~~fehlern~~n~~ in diesen Einrichtungen keine Aktionen ausgelöst werden, die die Anlage in einen Störfall überführen können.
512	3.3 Teil 1	**Modultext:** Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie B ausführen, sind so ausgelegt, dass sie ihre Aufgaben auch dann erfüllen, wenn im Anforderungsfall zusätzlich ein Zufallsausfall und daraus resultierende Folgeausfälle eintreten. Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie B ausführen und deren Wirksamkeit für die Störfallbeherrschung erforderlich ist, sind nach den Anforderungen der Kategorie A ausgelegt und werden dementsprechend geprüft. **Kommentar:** Der Text ist missverständlich. **Vorschlag:** Leittechnikfunktionen der Kategorie B, deren Fehlauslösung zu einem Störfall führen können, sind Leittechnikfunktionen der Kategorie A zu überlagern.	**JA**	T5 stimmt dem Kommentar zu, dass der 2. Satz zu Missverständnissen führen kann und inhaltlich auch entbehrlich ist. Wir schlagen vor, den 2. Satz zu streichen und durch einen neuen Textvorschlag zu ersetzen. Siehe Änderungsvorschlag.	Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie B ausführen, sind so ausgelegt, dass sie ihre Aufgaben auch dann erfüllen, wenn im Anforderungsfall zusätzlich ein Zufallsausfall und daraus resultierende Folgeausfälle eintreten. ~~Die~~ Eine leittechnische~~n~~ Einrichtung~~en~~, die durch eine fehlerhafte Ansteuerung einen Störfall auslösen kann, ist durch eine von der als fehlerhaft angenommenen leittechnischen Einrichtung unabhängige leittechnische Einrichtung überlagert. Die Leittechnik-Funktionen dieser unabhängigen leittechnischen Einrichtung ist nach ~~der~~ Kategorie B ~~ausführen und deren Wirksamkeit für die Störfallbeherrschung erforderlich ist, sind nach den Anforderungen der Kategorie A ausgelegt und werden dementsprechend geprüft~~ eingestuft.
716	3.3 Teil 1	**Bemerkung:** Inkonsistent zu M10/1.1.1.2 und M6/3.2.3(2)	**JA**	Durch Änderung (siehe vorausgehende Zeile) u. E. erledigt.	

Nr. in DB	Kapitel in Modul	Kommentar	Ände-rung	Begründung	Vorschlag Textänderung
		Nicht konsistent mit M5-1/2			
79	3.3 2. Satz Teil 1	**Kommentar:** Funktionen die für die Wirksamkeit der Störfallbeherrschung erforderlich sind, sind gemäß Kap. 2 in Kategorie A zu klassifizieren. Der Absatz ist damit in dieser geänderten Fassung in sich widersprüchlich und enthält nicht mehr den in der bisherigen Fassung behandelten Gesichtspunkt der Auswirkungen von Fehlanregung von Funktionen der Kategorie B. Der Satz sollte entweder entfallen, da auch an anderer Stelle geregelt, z.B. 3.1.1 (1) oder die ursprüngliche Fassung aus Rev. A übernommen werden.	**JA**	Durch Änderung (siehe vorausgehende Zeile) u. E. erledigt.	
1705	3.3 2. Satz Teil 1	**Kommentar:** Nach Ansicht der Arbeitsgruppe sollten Schutzbegrenzungen, die für die Störfallbeherrschung erforderlich sind, nach den Anforderungen der Kategorie A ausgelegt werden, wobei ein systematischer Ausfall nicht zu unterstellen ist (Schutzqualität und n+2-Auslegung). Wird umformuliert **Vorschlag:** Wird eine Funktion, die im Störfallablauf notwendige Maßnahmen zur Störfallbeherrschung auslöst, in leittechnischen Einrichtungen der Sicherheitsebene 2 implementiert, dann ist diese Funktion höherwertig (N+2) aufzubauen.	**NEIN**	Die Funktionen, die zur Störfallbeherrschung notwendig sind, werden durch Verfahrenstechnik festgelegt und der Kategorie A zugeordnet. Die Einrichtungen sind entsprechend der Anforderungen an die leittechnischen Einrichtungen mit LEFU Kategorie A auszulegen. Der Vorschlag wird nicht übernommen, weil dieser Satz aufgrund der Kommentierung (siehe Kommentar Nr 512) bereits u. E. unmissverständlich umformuliert wurde.	
1236	3.4 Teil 1	**Modultext:** Die leittechnischen Einrichtungen, die Leittechnik- Funktionen der Sicherheitsebenen 4a, 4b und 4c ausführen sollen, sind so ausgelegt, dass sie unter den für die jeweilige Aufgabe zu unterstellenden Umgebungsbedingungen ihre Aufgaben mit ausreichender Zuverlässigkeit erfüllen. Für Maßnahmen des anlageninternen Notfallschutzes können alle leittechnischen Einrichtungen eingesetzt werden, die dazu geeignet sind. **Kommentar:** Hier werden die Ereignisse der Sicherheitsebene 4 in Richtung der Auslegungsstörfälle verschoben. Die Umgebungsbedingungen sind nicht bekannt, der Zustand der Anlage auch nicht. Leittechnik-Funktionen für die Sicherheitsebenen 4b und 4c gibt es nicht.	**JA**	Für die Maßnahmen, die im Rahmen des anlageninternen Notfallschutzes (Sicherheitsebene 4b und 4c) vorgeplant sind und die auf die Funktionsfähigkeit leittechnischer Einrichtungen angewiesen sind, sollte die Funktionsfähigkeit dieser Einrichtungen unter den zu erwartenden Umgebungsbedingungen gegeben sein. Dabei wird keine Zuverlässigkeit wie bei der Störfallbeherrschung gefordert. Diesbezüglich konkretisierende Änderung am Text.	Die leittechnischen Einrichtungen, die für vorgeplante Maßnahmen auf den ~~Leittechnik-Funktionen der~~ Sicherheitsebenen 4a, 4b und 4c Leittechnik-Funktionen ausführen sollen, sind so ausgelegt, dass sie unter den für die jeweilige Aufgabe zu unterstellenden Umgebungsbedingungen ihre Aufgaben mit der für diese Sicherheitsebenen jeweils ausreichende~~r~~n ~~-~~Zuverlässigkeit erfüllen. Für Maßnahmen des anlageninternen Notfallschutzes können alle leittechnischen Einrichtungen eingesetzt werden, die dazu geeignet sind.
	4 (6) neu		**JA**	Folgewirkung aus Kommentar Nr.1230: T5 hat bei der Überprüfung des Kommentars erkannt, dass die Ziffer 5 (3) nach Abschnitt 4 aus inhaltlichen Gründen verschoben werden sollten. Red. Änderung hinsichtlich Anforderungsspezifikation wurde aufgenommen.	4 (6) Die sicherheitstechnisch relevanten Funktionen der Prozessführungs- und der Informationseinrichtungen sind in der Anforderungsspezifikation festgelegt.
1249	5 (1) Teil 1	**Modultext:** Für die unterstellten Ereignisse der Sicherheitsebenen 2 bis 4a sowie für die vorgeplanten Maßnahmen des anlageninternen Notfallschutzes werden die erforderlichen Prozessvariablen erfasst. **Kommentar:** Für die Sicherheitsebenen 4b und 4c sind keine Prozesse definiert sondern Ziele. Ereignisse der Sicherheitsebene 4 b und speziell c sind bestenfalls als angenommene Zustände bekannt, keinesfalls als Prozesse.	**NEIN**	Gemäß der KTA Begriffesammlung (KTA-GS-47 6/85) ist die Prozessvariable „eine unmittelbar im Prozess messbare chemische oder physikalische Größe.“ Auch Zustände der Sicherheitsebene 4 werden durch physikalische bzw. chemische Prozesse bestimmt. Angesprochen sind hier die vorgeplanten Maßnahmen des anlageninternen Notfallschutzes. Die Wirksamkeit dieser Maßnahmen wird auf der Grundlage definierter Zustände bestimmt. Diese Zustände sind u. a. auch durch Prozessvariable charakterisiert.	Für die unterstellten Ereignisse der Sicherheitsebenen 2 bis 4a sowie für die vorgeplanten Maßnahmen des anlageninternen Notfallschutzes (Notfallmaßnahmen) werden die erforderlichen Prozessvariablen erfasst.

Nr. in DB	Kapitel in Modul	Kommentar	Ände-rung	Begründung	Vorschlag Textänderung
				Daher sollte der Text von Modul 5 unverändert bleiben, bis auf die redaktionelle Ergänzung.	
80	5 (2) Teil 1	**Modultext:** Für jedes von den leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, zu beherrschende Ereignis der Sicherheitsebene 3 werden mindestens zwei unterschiedliche Anregekriterien herangezogen, die aus physikalisch unterschiedlichen Prozessvariablen gebildet werden. Wenn dies technisch nicht realisierbar ist, sind andere Maßnahmen und Einrichtungen zum Erreichen hoher Zuverlässigkeit vorgesehen. **Kommentar:** 1. und 2. Satz widersprechen sich in der vorliegenden Fassung. Im 1. Satz ist daher noch "grundsätzlich" einzufügen, um die Möglichkeit von Ausnahmen gemäß dem 2. Satz darzustellen.	**JA**	Red. Änderung wird übernommen.	Für jedes von den leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, zu beherrschende Ereignis der Sicherheitsebene 3 werden grundsätzlich mindestens zwei unterschiedliche Anregekriterien herangezogen, die aus physikalisch unterschiedlichen Prozessvariablen gebildet werden. Wenn dies technisch nicht realisierbar ist, sind andere Maßnahmen und Einrichtungen zum Erreichen hoher Zuverlässigkeit vorgesehen.
1707	5 (2) Teil 1	**Kommentar:** 1. und 2. Satz widersprechen sich in der vorliegenden Fassung. Im 1. Satz ist daher noch „grundsätzlich“ einzufügen, um die Möglichkeit von Ausnahmen gemäß dem 2. Satz darzustellen **Vorschlag:** Für jedes von den leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, zu beherrschende Ereignis der Sicherheitsebene 3 werden **grundsätzlich** mindestens zwei unterschiedliche Anregekriterien...	**JA**	Red. Änderung wird übernommen. siehe. Antwort auf Kommentar Nr.80.	
	5 (3)	**Modultext:** Die sicherheitstechnisch relevanten Ziele der Prozessführungs- und der Informationseinrichtungen sind in ihrer Spezifikation festgelegt.	**JA**	Folgewirkung aus Kommentar Nr. 1230: T5 hat bei der Überprüfung des Kommentars erkannt, dass die Ziffer 5 (3) nach Abschnitt 4 (Ziffer 4 (6) aus inhaltlichen Gründen verschoben werden sollten.	~~5 (3)~~ ~~Die sicherheitstechnisch relevanten Ziele der Prozessführungs- und der Informationseinrichtungen sind in ihrer Spezifikation festgelegt.~~
	5 (4)	**Modultext:** Die Informationssysteme sind gemäß ihrer sicherheitstechnischen Bedeutung qualifiziert.	**JA**	Folgewirkung aus Kommentar Nr.1230: T5 hat bei der Überprüfung des Kommentars erkannt, dass die Ziffer 5 (4) nach Abschnitt 7 (Ziffer 7.1 (5)) aus inhaltlichen Gründen verschoben werden sollten.	~~5 (4)~~ ~~Die Informationssysteme sind gemäß ihrer sicherheitstechnischen Bedeutung qualifiziert.~~
1237	6 Teil 1	**Kommentar:** Hierzu sind bereits Regelungen in 3.2(4) getroffen.	**NEIN**	In diesem Abschnitt wird die Anforderung aus 3.2 (4) konkretisiert. Die Formulierung von Modul 5 Rev. B sollte beibehalten werden.	
	6 (2)		**JA**	Anpassung der Begrifflichkeit „Strang“ gemäß Antwort auf Kommentar Nr. 68.	~~Die redundanten Stränge~~ Redundante ~~der~~leittechnische~~n~~ Einrichtungen sind voneinander so unabhängig ausgelegt, dass ein anlageninternes versagensauslösendes Ereignis nicht zum Ausfall mehrerer ~~redundanter Stränge~~ Redundanten führt. ~~des Sicherheitssystems führt. Bei Ausfall~~ Wenn einzelne~~r~~ Redundanten leittechnischer Einrichtungen,~~Stränge leittechnischer Einrichtungen~~, die Leittechnik-Funktionen der Kategorie A ausführen, durch Einwirkungen von außen ausfallen, reichen die übrigen ~~Stränge~~ Redundanten zur Beherrschung dieses Ereignisses aus.

Nr. in DB	Kapitel in Modul	Kommentar	Änderung	Begründung	Vorschlag Textänderung
	6 (3)		**JA**	Anpassung der Begrifflichkeit „Strang“ gemäß Antwort auf Kommentar Nr. 68.	Zum Schutz gegen redundanzübergreifende versagensauslösende Ereignisse innerhalb der leittechnischen Einrichtungen und innerhalb der Anlage sind ~~zueinander redundante Stränge~~ Redundanten grundsätzlich räumlich getrennt angeordnet.
1238	7.1 (3) Teil 1	**Kommentar:** Welche Tests sind gemeint und wie, realistisch sollte ein KMV' sein?	**NEIN**	Diese Formulierung entspricht der Anforderung in der RSK-LL 7.3.6.1 (4) „Die Sicherheitsleittechnik ist unter möglichst realistischen Anlagen- und Einsatzbedingungen umfassend daraufhin zu testen, ob alle zu unterstellenden Ereignisabläufe beherrscht werden.“ Diese Formulierung ist sachgerecht und lässt ausreichend Spielraum für sinnvolle technische Lösungen. Die Prüfbedingungen für LEFU A, B und C können unterschiedlich sein. Die Formulierung von Modul 5 Rev. B soll beibehalten werden. Siehe. auch Antwort zu Kommentar Nr. 1252. Redaktionelle Anpassungen.	Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorien A bis C ausführen, sind unter möglichst realistischen Anlagen- und Einsatzbedingungen umfassend daraufhin getestet, ~~ob~~ alle zu unterstellenden Ereignisabläufe zu beherrschen~~t werden~~.
1252	7.1 (3) Teil 1	**Kommentar:** Der genannte Geltungsbereich der Anforderung („die leittechnischen Einrichtungen, die Leittechnik- Funktionen der Kategorien A bis C ausführen“) ist vor dem Hintergrund des in den RSK LL formulierten Geltungsbereichs der Anforderung („Sicherheitsleittechnik“) zu überprüfen.	**NEIN**	Der Geltungsbereiche der RSK-LL-DWR (siehe 7.3.1) lautet: „Die Sicherheitsleittechnik ist die Leittechnik des Sicherheitssystems und der anderen Systeme mit sicherheitstechnischer Bedeutung. Die Sicherheitsleittechnik umfasst die Leittechnik-Funktionen der Kategorien 1, 2 und 3. Sie wird durch Einrichtungen realisiert, bei denen Geräte Leittechnik-Funktionen ausführen.“ Der Geltungsbereich von Modul 5 lautet (Ziffer 1): „Die nachfolgenden Anforderungen gelten für leittechnische Einrichtungen, die auf den Sicherheitsebenen 1 bis 4 Leittechnik-Funktionen mit sicherheitstechnischer Bedeutung ausführen. Die Anforderungen werden durch Einrichtungen realisiert, bei denen Hard- und Software Leittechnik-Funktionen ausführen.“ Beide Geltungsbereiche sind u. E. übereinstimmend. Die Formulierung in Modul 5 entspricht der Anforderung in der RSK-LL 7.3.6.1 (4) und bezieht sich auf alle Kategorien der SILT 1bis 3 und der Geräte E1 und E2 (siehe RSK LL 7.3.2 (2) und (3)). Die Formulierung in Modul 5 Ziffer 7.1 (3) ist	

Nr. in DB	Kapitel in Modul	Kommentar	Änderung	Begründung	Vorschlag Textänderung
				daher sachgerecht und lässt ausreichend Spielraum für sinnvolle technische Lösungen. Daher sollte die Formulierung von Modul 5 Rev. B beibehalten werden.	
	7.1 (4) Teil 1			Redaktionelle Anpassung.	Nach Abschluss der Montage in der Anlage oder nach Änderungen an ~~in~~ den leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A bis C ausführen, wird eine Inbetriebsetzungsprüfung durchgeführt.
	7.1 (5) neu		**JA**	Folgewirkung aus Kommentar Nr. 1230: T5 hat bei der Überprüfung des Kommentars erkannt, dass die Ziffer 5 (4) nach Abschnitt 7 aus inhaltlichen Gründen verschoben werden sollten.	7.1 (5) Die Informationssysteme sind gemäß ihrer sicherheitstechnischen Bedeutung qualifiziert.
1250	7.3 Teil 1	**Kommentar:** Dieser Abschnitt versucht viel zu detailliert auf die Erstellung und Prüfung einzugehen. Dabei entsteht einerseits eine Einengung auf eine mögliche Variante der Software-Qualifizierung, andererseits werden die einzelnen Anforderungen so kurz formuliert, dass die Klarheit verloren geht.	**NEIN**	In Modul 5 sind übergeordnete Anforderungen an die Qualifizierung der Software enthalten. Eine Einengung auf ein bestimmtes Phasenmodell wie in der RSL-LL-DWR besteht u. E. nicht. Qualifizierung der Software nach einem Phasenmodell entspricht u. E. dem Stand von Wissenschaft und Technik (siehe hierzu auch IAEA-NS-G-1-1, RSK-LL-DWR, IEC 61508). Daher sollte der Text von Modul 5 unverändert bleiben.	
81	7.3.2.3 (1) Teil 1	**Modultext:** Der Einsatz vorgefertigter Software ist auf unverzichtbare Bestandteile beschränkt, wobei Softwareänderungen vermieden werden. Diese Teile sind Prüfungen und Tests unterzogen, die in Umfang und Tiefe den Nachweisen nach den Abschnitten 7.3.2.1 und 7.3.2.2 gleichwertig sind. **Vorschlag:** Der Einsatz vorgefertigter Software, sofern nicht entsprechend den Anforderungen 7.3.2.1 und 7.3.2.2 ausgelegt wurden, ist auf unverzichtbare Bestandteile beschränkt, wobei Softwareänderungen vermieden werden.	**JA**	Vorschlag wird übernommen, da hilfreiche Präzisierung.	Der Einsatz vorgefertigter Software, sofern nicht entsprechend den Anforderungen 7.3.2.1 und 7.3.2.2 ausgelegt, ist auf unverzichtbare Bestandteile beschränkt, wobei Softwareänderungen vermieden werden. Diese Teile sind Prüfungen und Tests unterzogen, die in Umfang und Tiefe den Nachweisen nach den Abschnitten 7.3.2.1 und 7.3.2.2 gleichwertig sind.
1708	7.3.2.3 (1) Teil 1	**Kommentar:** Einschränkungen sind nur dann geboten, wenn die vorgefertigte Software nicht nach den Anforderungen des kerntechnischen Regelwerkes entwickelt wurde, **Vorschlag:** Der Einsatz vorgefertigter Software**, sofern nicht entsprechend den Anforderungen 7.3.2.1 und 7.3.2.2 ausgelegt wurden**, ist auf unverzichtbare Bestandteile beschränkt, wobei Softwareänderungen vermieden werden.	**JA**	Vorschlag wird übernommen, siehe Kommentar Nr. 81.	
513	7.3.3.1 (1) Teil 1	**Modultext:** Für die Entwicklung und Qualifizierung der Software der Leittechnikfunktionen der Kategorie B sind Rechner gestützte Beschreibungen und Testverfahren angewendet, die den Nachweis der korrekten Arbeitsweise unterstützen. **Kommentar:** Die Formulierung muss lauten: Für die Entwicklung und Qualifizierung der Software der Leittechnikfunktionen der Kategorie B sind Beschreibungen und Rechner gestützte Testverfahren angewendet, die den Nachweis der korrekten Arbeitsweise unterstützen	**JA**	Vorschlag wird übernommen, da hilfreiche Präzisierung.	Für die Entwicklung und Qualifizierung der Software der Leittechnik-Funktionen der Kategorie B sind ~~rechnergestützte~~ Beschreibungen und rechnergestützte Testverfahren angewendet, die den Nachweis der korrekten Arbeitsweise unterstützen.

Nr. in DB	Kapitel in Modul	Kommentar	Änderung	Begründung	Vorschlag Textänderung
	7.3.3.2 (4) Teil 1			Entbehrlicher Einschub, da Modul 5 ausschließlich diese Funktionen behandelt.	Das anforderungsgerechte Verhalten des Hardware- und Softwaresystems ist ~~in seinen sicherheitsrelevanten Funktionen~~ validiert.
82	7.3.4.3 Teil 1	**Modultext:** Einsatz von vorgefertigter Software Eingesetzte vorgefertigte Software ist betriebsbewährt oder zertifiziert **Kommentar:** Widerspruch zu 3.1 (2) wo Betriebsbewährung nicht als Qualitätsnachweis akzeptiert ist.	**NEIN**	Durch den Änderungsvorschlag zum Text im 3.1(2) (siehe Kommentar Nr. 67) wird vermeintlicher Widerspruch behoben.	
514	7.3.4.3 Teil 1	**Kommentar:** Die Anerkennung von Betriebsbewährung für Software ist unüblich und bedarf dann zumindest weiterer Differenzierungen.	**JA**	Die Formulierung in Rev. B orientierte sich an den RSK-LL. Der neue Vorschlag orientiert sich vorrangig an der DIN IEC 62138: *Einsatz von vorgefertigter Software* *Für die vorgefertigte Software sind die Eigenschaften, die zur Beurteilung der Einsetzbarkeit erforderlich sind, präzise und verständlich dokumentiert. Das sind z.B. Funktionalität, Schnittstellen, Datenformate, unterschiedliche Betriebsmodi und Einsatzbeschränkungen der Software. Ergänzend werden zur Beurteilung projektspezifische Tests, belastbar dokumentierte Betriebserfahrung und/oder relevante Prüfzertifikate herangezogen.* Kommentar wurde im neuen Textvorschlag berücksichtigt.	~~Eingesetzte vorgefertigte Software ist betriebsbewährt oder zertifiziert.~~ Einsatz von vorgefertigter Software Für eingesetzte vorgefertigte Software ist die Betriebserfahrung dokumentiert oder die Software ist zertifiziert. Die zur Beurteilung der Einsetzbarkeit erforderlichen Eigenschaften sind dokumentiert.
515	8 (1) Teil 1	**Modultext:** Die zulässigen elektrischen, elektromagnetischen, thermischen, mechanischen und strahlungs- sowie Feuchtigkeitsbedingten Einwirkungen sind so festgelegt, dass die unterstellten Betriebs- und Störfallbedingungen zuverlässig abgedeckt werden. **Kommentar:** Die Formulierung muss lauten: Die Einrichtungen der LT sind so ausgeführt, dass Sie den elektrischen, elektromagnetischen, thermischen, mechanischen und Strahlungs- sowie Feuchtigkeitsbedingten Einwirkungen unter den unterstellten Betriebs- und Störfallbedingungen standhalten.	**JA**	Text wird unter Berücksichtigung des Kommentators präzisiert.	Die ~~zulässigen~~ elektrischen, elektromagnetischen, thermischen, mechanischen und strahlungs- sowie feuchtigkeitsbedingten Einwirkungen sind für leittechnische Einrichtungen so festgelegt, dass die unterstellten Betriebs- und Störfallbedingungen zuverlässig abgedeckt werden.
1239	8 (3) Teil 1	**Kommentar:** Zu den Maßnahmen des Notfallschutzes gibt es keine definierten Ereignisabläufe (sondern Ziele) und damit auch keine eindeutige Zuordnung leittechnischer Einrichtungen. (letzter Satz:) „… durch die Folgen dieser Ereignisse …:“ Was ist mit "diesen Ereignissen“ gemeint? Die Ereignisse, die zum Notfall geführt haben? Oder die Ereignisse, die aus den Notfall- Maßnahmen resultieren?... Alles sind unvorhergesehene Ereignisse, gegen die man daher auch nicht die Funktionsfähigkeit von Geräten und Einrichtungen auslegen kann.	**JA**	Kommentar wird durch Präzisierung der Anforderungen berücksichtigt.	Die leittechnischen Einrichtungen, die für die Durchführung der im Rahmen des anlageninternen Notfallschutzes vorgesehenen Maßnahmen erforderlich sind, ~~werden so ausgelegt~~sind so beschaffen, dass sie durch die Folgen der zugrunde gelegten~~dieser~~ Ereignisabläufe oder Anlagenzustände ihre erforderliche Funktionsfähigkeit nicht verlieren.
1240	8 (4) Teil 1	**Kommentar:** Was sind "hinreichende Reserven"? (5%, 20%, 200%?)	**NEIN**	Die Anforderung aus Modul 5 entspricht der Anforderung der RSK-LL 7.3.7 (4): “Die Sicherheitsleittechnik ist so auszulegen, dass hinrei-	

Nr. in DB	Kapitel in Modul	Kommentar	Änderung	Begründung	Vorschlag Textänderung
				chende Reserven gegenüber Alterungseffekten vorhanden sind." Eine weitergehende Konkretisierung der „hinreichenden Reserven" sollte Gegenstand einer entsprechenden KTA Regel sein. Daher sollte die Formulierung von Modul 5 Rev. B beibehalten werden.	
1241	8 (5) Teil 1	**Modultext:** Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A bis C ausführen, sind mit Toleranz gegenüber Über- und Unterschreitungen des zulässigen Spannungsbereichs der elektrischen Energieversorgung ausgelegt. **Kommentar:** "… unempfindlich gegenüber Über- und Unterschreitungen des zulässigen Spannungsbereichs …": Ohne Angabe, wie viel Toleranz gefordert wird, ist das technisch unsinnig.	**JA**	Präzisierungsvorschlag wird umgesetzt.	Der zulässige Spannungsbereich für ~~Die~~ die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A bis C ausführen, ~~sind mit Toleranz~~ ist unempfindlich gegenüber Über- und Unterschreitungen des ~~zulässigen~~ spezifizierten Spannungsbereichs der elektrischen Energieversorgung ~~ausgelegt~~.
516	8 (6) Teil 1	**Modultext:** Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A und B ausführen, sind fehlertolerant aufgebaut. Sie sind so ausgelegt, dass das Ausfallverhalten grundsätzlich definiert und möglichst sicherheitsgerichtet ist. **Kommentar:** Die Ausdrücke "fehlertolerant", "auslösegerichtet", "sicherheitsgerichtet", "fehlersicher" sind in der Leittechnik zum Teil belegt und schließen sich gegenseitig aus. Die Widersprüche sind zu beseitigen. Es ist zu prüfen, ob diese Forderungen nicht bereits in anderen Punkten enthalten sind.	**JA**	Die Formulierung in den RSK Leitlinien (Ziffer 7.3.7 (6) lautet: „Die Sicherheitsleittechnik ist fehlertolerant aufzubauen. Das Ausfallverhalten soll sicherheitsgerichtet sein." Diese Anforderung soll mit den Begrifflichkeiten von Modul 5 umgesetzt werden. Ein Widerspruch zwischen der Anforderung „fehlertoleranter Aufbau" und „sicherheitsgerichtetes Ausfallverhalten" besteht nicht. Die Anforderung richtet sich auf die Auslegung von leittechnischen Einrichtungen. Fehlertoleranz ist ein in der Technik eingeführter Begriff und wird an dieser Stelle widerspruchfrei eingesetzt. Eine redaktionelle Änderung wird vorgeschlagen.	Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A und B ausführen, sind fehlertolerant aufgebaut~~. Sie sind so ausgelegt, dass das Ausfallverhalten grundsätzlich definiert und möglichst sicherheitsgerichtet ist.~~ Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A und B ausführen, sind so ausgelegt, dass das Ausfallverhalten grundsätzlich definiert und möglichst sicherheitsgerichtet ist.
1229	9 Teil 1	**Kommentar:** Es sollen nur Leittechnik spezifische Anforderungen in Modul 5 aufgenommen werden. Es ist zu prüfen, inwieweit in Modul 5 Rev. B formulierte Anforderungen nicht Leittechnik spezifischer Natur sind und daher als Querschnittsthema an anderer Stelle dargestellt werden sollten.	**NEIN**	Kommentar richtet sich generell auf die Anforderungen hinsichtlich der Aspekte „Instandhaltung und Änderungen" im Modul 5. U. E. werden in diesem Abschnitt die für leittechnische Einrichtungen relevante Aspekte behandelt. Überlappungen der Anforderungen in den Modulen können u. E. Ziel führend sein und sind daher zulässig.	
1242	9 Teil 1	**Kommentar:** Mit welchem Ziel wird geprüft?, Der gesamte Abschnitt zu Prüfungen berücksichtigt selbst überwachende Systeme (mit aktiver Aussteuerung einer Fehlermeldung z.B. bei Abweichungen zwischen zwei redundanten Kanälen) nicht.	**NEIN**	Der Begriff „Instandhaltung" ist definiert als „Die Gesamtheit der Maßnahmen zur Bewahrung und Wiederherstellung des Soll-Zustands sowie zur Feststellung und Beurteilung des Ist-Zustands (einschließlich wiederkehrender Prüfung). Die Instandhaltung gliedert sich in Inspektion, Wartung und Instandsetzung." Der Begriff „Prüfung" ist definiert als „Maßnahme zur Feststellung, ob der Ist-Zustand dem Soll-Zustand entspricht".	

Nr. in DB	Kapitel in Modul	Kommentar	Ände-rung	Begründung	Vorschlag Textänderung
				Prüfung erfolgt somit mit dem Ziel die Funktionsfähigkeit bzw. auslegungsgerechtes Verhalten einer Einrichtung nachzuweisen. Dies gilt auch für die selbst überwachenden Einrichtungen (z.B. Funktionsweise von Abschlussgliedern, die durch WKP überprüft und nachgewiesen wird). Tests werden mit dem Ziel durchgeführt, um die erforderliche Funktionsfähigkeit leittechnischer Einrichtungen lückenlos nachzuweisen.	
	9 (4) Teil 1			Folgeanpassung aufgrund Neugliederung von M10	Die leittechnischen Einrichtungen sind grundsätzlich so ausgelegt, dass durch Prüfungen verursachte Veränderungen nach den Prüfungen rückgesetzt werden. Prüfungen werden automatisch oder manuell durchgeführt. Die Prüfungen sind so geplant und durchgeführt, dass die Anforderungen aus den „Sicherheitsanforderungen für Kernkraftwerke: Anforderungen an die Auslegung und den sicheren Betrieb von baulichen Anlagenteilen, Systemen und Komponenten“ (Modul 10) Abschnitt 1~~(2)~~.2 eingehalten werden.
1253	9 (5) Teil 1	**Modultext:** Prüfungen sind so gestaltet, dass sie grundsätzlich von zentralen Stellen durch verantwortliches Betriebspersonal überwachbar sind. **Kommentar:** Zumindest missverständlich. Soll nur die Tatsache der Prüfung angezeigt werden, oder soll der Prüfablauf tatsächlich überwacht werden?	**JA**	Der Text der RSK Leitlinie DWR (Ziffer 7.3.7(1)) lautet: „Prüfungen sollen von zentralen Stellen überwachbar sein.“ Hierzu ist in Modul 5 eine Präzisierung hinsichtlich der Überwachung durch verantwortliches Betriebspersonal erfolgt. Erkenntnisse aus der Betriebserfahrung zeigen, dass nicht die zentralen Stellen (s. auch KTA 3501) alleine, sondern die Überwachung durch verantwortliches Betriebspersonal sicherheitstechnische Bedeutung hat, und deshalb entsprechende Vorkehrungen vorzusehen sind. Weitere allgemeine Anforderungen an die Überwachung der Prozesse und Tätigkeiten sind im Modul 8, Abs. 3.5 (2) formuliert: „Der Betreiber überwacht alle sicherheitsrelevanten Tätigkeiten und Prozesse. Dazu gehören − die Verfügbarkeit und der Gebrauch geeigneter Überwachungs- und Messmittel, − die Durchführung von Überwachungen und Messungen sowie Freigabe des Prozessergebnisses.“ Mit der Anforderung in Modul 5 wird konkret gefordert, dass sowohl der Prüfablauf als auch das Prüfergebnis überwacht werden können. Die Formulierung „von zentralen Stellen“ ist bewusst im Plural gewählt, da hier neben der	Prüfungen an leittechnischen Einrichtungen ~~sind so gestaltet, dass sie grundsätzlich von~~ sollen von zentralen Stellen durch verantwortliches Betriebspersonal überwacht werden.~~bar sind~~.

Nr. in DB	Kapitel in Modul	Kommentar	Änderung	Begründung	Vorschlag Textänderung
				Warte auch die Notsteuerstelle oder auch örtliche Leitstände angesprochen werden sollen.	
	9 (6)		**JA**	Anpassung der Begrifflichkeit „Strang“ gemäß Antwort auf Kommentar Nr. 68.	Instandhaltungsarbeiten sind so gestaltet, dass sie ohne unzulässige Minderung der Sicherheit der Anlage durchführbar sind und Auswirkungen zu unterstellender Fehlhandlungen auf ~~einen Strang~~ eine Redundante beschränkt bleiben.
	9 (7)			Redaktionelle Änderung.	Bei Änderungen in den leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A bis C ausführen, werden mindestens die gleichen Qualitätsstandards angewendet wie bei ~~Er~~Herstellung der leittechnischen Einrichtungen.
	9 (9)			Folgeanpassung aufgrund Neugliederung von M10	Änderungen der Software der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A bis C ausführen, werden unter Einhaltung der Qualitätsanforderungen nach Abschnitt 7.3 vorgenommen. Änderungen der Software und dazu erforderliche Eingriffe in die leittechnischen Einrichtungen erfolgen so, dass die Anforderungen aus den „Sicherheitsanforderungen für Kernkraftwerke: Anforderungen an die Auslegung und den sicheren Betrieb von baulichen Anlagenteilen, Systemen und Komponenten“ (Modul 10) Abschnitt 1 ~~(2)~~.2 eingehalten werden. Alle Eingriffe in die Software sind dokumentiert.
	9 (10)			Redaktionelle Änderung.	Änderungen von Parametrierdaten und Software der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A bis C ausführen, werden so behandelt, dass sie rekonstruierbar sind. Dazu werden regelmäßig sowie bei Änderungen der Software Sicherungskopien angefertigt. Software- und Parametrierdatenbestände sind archiviert.
	10 (1)			Redaktionelle Änderung.	Eingriffe in die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A und B ausführen, werden auf der Warte angezeigt. In Fällen, in denen dies technisch nicht möglich ist, wird das Wartenpersonal ~~zeitnah~~ vor dem geplanten Eingriff über die Eingriffe informiert.
83	12 (1) Teil 1	**Modultext:** Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A bis C ausführen, werden von unterbrechungslosen Notstromanlagen mit Energiespeicherung versorgt. Die Kapazität des Energiespeichers ist unter der Annahme, dass der Leistungsbedarf des Stranges nur aus dem strangzugehörigen Energiespeicher gedeckt wird, so bemessen, dass die Versorgung mindestens 2 h aufrechterhalten wird, ohne dass die zulässige Mindestspannung unterschritten wird. Die Energieversorgung ist so ausgelegt, dass nach	**JA**	Vorschlag wird bei Präzisierung des Textes sinngemäß berichtigt.	Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A bis C ausführen, werden von unterbrechungslosen Notstromanlagen mit Energiespeicherung versorgt. Die Kapazität des Energiespeichers ist unter der Annahme, dass der Leistungsbedarf ~~des Stranges~~einer Redundante ~~strangzugehörigen~~ redundanzzugehörigen Energiespeicher gedeckt

Nr. in DB	Kapitel in Modul	Kommentar	Änderung	Begründung	Vorschlag Textänderung
		vollständigem Spannungsausfall oder Unterschreiten der Mindestspannung die leittechnischen Einrichtungen nach Spannungswiederkehr funktionsfähig sind. **Kommentar:** Präzisierung **Vorschlag:** Die leittechnischen Einrichtungen und deren Energieversorgung sind so ausgelegt, dass nach Unvollständigem Spannungsausfall oder Unterschreiten der Mindestspannung die leittechnischen Einrichtungen nach Spannungswiederkehr funktionsfähig sind.			wird, so bemessen, dass die Versorgung mindestens 2 h aufrechterhalten wird, ohne dass die zulässige Mindestspannung unterschritten wird. Die leittechnischen Einrichtungen und deren Energieversorgung ~~ist~~ sind so ausgelegt, dass nach vollständigem Spannungsausfall oder Unterschreiten der Mindestspannung die leittechnischen Einrichtungen nach Spannungswiederkehr funktionsfähig sind. Hinweis Siehe auch „Sicherheitsanforderungen für Kernkraftwerke: Anforderungen an Elektrische Energieversorgung“ (Modul ~~5, Teil 2~~12) Kapitel 1.
1710	12 (1) Teil 1	**Kommentar:** Die Anforderungen betreffen nicht nur die Energieversorgung, sondern auch die leittechnischen Einrichtungen. Nach der Spannungswiederkehr soll die Leittechnik wieder funktionsfähig sein. Präzisierung und ggf. Zuordnung prüfen. **Vorschlag:** **Die leittechnischen Einrichtungen und deren Energieversorgung** sind so ausgelegt, dass nach vollständigem Spannungsausfall oder Unterschreiten der Mindestspannung die leittechnischen Einrichtungen nach Spannungswiederkehr funktionsfähig sind	**JA**	Siehe vorausgehende Zeile.	
	13.3.1 (4) neu			Folgeanpassung aufgrund Änderungen in M7	13.3.1 (4) Es ist eine Weitbereichsanzeige für die Messgrößen vorgesehen, die die repräsentativen Ereignisabläufe und daraus abgeleiteten Anlagenzustände der Sicherheitsebenen 4b und 4c charakterisieren (siehe „Sicherheitsanforderungen für Kernkraftwerke: Anforderungen an den anlageninternen Notfallschutz“ (Modul 7, Ziffer ~~2 (3)~~3.3 (2)).
	Modul 5 Teil 2 Kapitel 1				
1244	Teil 2, Kap.1 2 (4) **jetzt** Modul 12, 2 (4)	**Modultext:** Es sind Einrichtungen zur automatischen Leistungsanpassung des Blockgenerators bei einer Abtrennung des Blockes vom Netz zur Sicherstellung der elektrischen Energieversorgung vorhanden. **Kommentar:** Gehört zu 2(3) a), sollte damit gemeinsam behandelt werden.	**NEIN**	Ziffer 2 (3) listet alle Möglichkeiten der Energieversorgung auf. Ziffern 2 (4) bis 2 (10) umfassen **Detaillierungen der Anforderungen an die Auslegung.** Ergebnis der Diskussion in der FARS-AG: Es sollte eine redaktionelle Anpassung vorgenommen werden, mit dem Ziel der Verdeutlichung des Zusammenhangs zwischen der Ziffer 2 (3) Modul 5 und den Ziffern 2 (4) - 2 (7). Diesem Vorschlag wurde nicht gefolgt, weil Text auch ohne Verweis in 2 (3)a lesbar ist und dann auch die weitere Querverweise eingefügt werden	

Nr. in DB	Kapitel in Modul	Kommentar	Ände-rung	Begründung	Vorschlag Textänderung
				müssten wodurch die Lesbarkeit verschlechtert wird.	
84	Teil 2, Kap.1 2 (4) **jetzt** Modul 12, 2 (4)	**Kommentar:** Präzisierung um Lastabwurf auf Eigenbedarf.	**NEIN**	Es besteht u. E. kein inhaltlicher Änderungsbedarf am Text, da aus dem Text hervorgeht, dass es sich um einen Lastabwurf auf Eigenbedarf handelt.	
85	Teil 2, Kap.1 2 (5) **jetzt** Modul 12, 2 (5)	**Modultext:** Die Haupt- und Reservenetzanschlüsse sind grundsätzlich an unterschiedlichen Spannungsebenen der externen Versorgungsnetze angebunden, um die Zuverlässigkeit der Energieversorgung auf Grund unterschiedlicher Energieerzeugungsanlagen sowie Schalt- und Vertei-lungsanlagen zu erhöhen. Ist diese Anforderung auf Grund von Netzgegebenheiten in Kraftwerksnähe nicht erfüllbar, so sind zumindest Haupt- und Reservenetzanschluss an getrennte Netzschaltanlagen angeschlossen. **Kommentar:** Klärung: Sind hierbei Netzkuppler eingeschlossen?	**NEIN**	Es besteht u. E. kein Änderungsbedarf. Die Forderung soll die Gesamtzuverlässigkeit der Energieversorgung aus den Netzen erhöhen. Die Netze der verschiedenen Spannungsebenen haben zum einen unterschiedliche Energieerzeugungsanlagen (Kraftwerke), sind aber gleichzeitig miteinander über Transformatoren gekuppelt. Der Stufenplan zur Auflösung des Verbundnetzes sieht vor, dass die Netze ggf. entkoppelt werden. Dadurch erhöht sich die Chance, dass eine der beiden Netze noch verfügbar ist. Sind die Netzschaltanlagen, an die der Haupt- und Reservenetzanschluss angeschlossen ist, direkt gekuppelt, ergeben sich hieraus sowohl Vor- als auch Nachteile für die Gesamtzuverlässigkeit der Netzanbindungen für das Kraftwerk. Welche Netzanbindung dann sinnvoll ist, muss im konkreten Fall geklärt werden. Entscheidend ist jedoch die Einhaltung des Ziels, dass durch die Anforderung des Moduls 5 formuliert ist.	
517	Teil 2, Kap.1 2 (5) **jetzt** Modul 12, 2 (5)	**Modultext:** Die Haupt- und Reservenetzanschlüsse sind grundsätzlich an unterschiedlichen Spannungsebenen der externen Versorgungsnetze angebunden, um die Zuverlässigkeit der Energieversorgung auf Grund unterschiedlicher Energieerzeugungsanlagen sowie Schalt- und Verteilungsanlagen zu erhöhen. Ist diese Anforderung auf Grund von Netzgegebenheiten in Kraftwerksnähe nicht erfüllbar, so sind zumindest Haupt- und Reservenetzanschluss an getrennte Netzschaltanlagen angeschlossen. **Kommentar:** Der Anschluss an getrennte Spannungsebenen alleine ist keine Gewähr dafür, dass die Zuverlässigkeit der Energieversorgung nennenswert erhöht wird. Bedeutsam ist, dass die beiden Netzanschlüsse getrennt und schutztechnisch entkoppelt ausgeführt sind. **Vorschlag:** Ist diese Anforderung auf Grund von Netzgegebenheiten in Kraftwerksnähe nicht erfüllbar, so sind zumindest Haupt- und Reservenetzanschluss an getrennte Netzschaltanlagen angeschlossen und schutztechnisch entkoppelt.	**JA**	Kommentar wird akzeptiert da Ziel führende Ergänzung. Vorschlag wird umgesetzt.	Die Haupt- und Reservenetzanschlüsse sind grundsätzlich an unterschiedlichen Spannungsebenen der externen Versorgungsnetze angebunden, um die Zuverlässigkeit der Energieversorgung der elektrischen Verbraucher auf Grund unterschiedlicher Energieerzeugungsanlagen sowie Schalt- und Verteilungsanlagen zu erhöhen. Ist diese Anforderung auf Grund von Netzgegebenheiten in Kraftwerksnähe nicht erfüllt~~bar~~, so sind zumindest Haupt- und Reservenetzanschluss an getrennte Netzschaltanlagen angeschlossen und schutztechnisch entkoppelt.~~.~~

Nr. in DB	Kapitel in Modul	Kommentar	Änderung	Begründung	Vorschlag Textänderung
1711	Teil 2, Kap.1 2 (5) **jetzt** Modul 12, 2 (5)	**Kommentar:** Die Netzanschlüsse eines Kraftwerkes müssen schutztechnisch so entkoppelt sein, dass sie unabhängig voneinander betrieben und bei Störungen selektiv herausgetrennt werden können. Dies kann nicht als Forderung nach einer Unabhängigkeit der Netze selbst interpretiert werden, da der Verbundbetrieb der Netze nur durch sinnvolle Abhängigkeit (insbesondere Leistungsausgleich) möglich ist. **Vorschlag:** ‚um die Zuverlässigkeit der Energieversorgung der Verbraucher des Sicherheitssystems zu erhöhen… …erfüllt ..	**Teilweise**	Die Forderung 2(5) beinhaltet u. E. keine Forderung an die Unabhängigkeit der externen Versorgungsnetze, sondern nur an unterschiedliche Spannungen, allerdings vor dem Hintergrund, dass die externe Versorgungsnetze zwar wegen des Leistungsausgleiches miteinander u.a. verkoppelt sind, aber eben unterschiedliche Energieerzeugungsanlagen und Schaltanlagen haben. Nicht zuletzt beruht der Stufenplan zur Auflösung des Verbundnetzes nach einer schweren Netzstörung auf diesen Hintergrund. Dem Änderungsvorschlag kann somit z. T. zugestimmt werden. Allerdings soll nicht nur die Energieversorgung der elektrischen Verbraucher des Sicherheitssystems (Sicherheitsebene 3 und höher) erhöht werden, sondern es soll auch durch 2(5) die Zuverlässigkeit der elektrischen Verbraucher der Sicherheitsebenen 1und 2 erhöht werden. Vorschlag zu Präzisierung der Anforderung wird übernommen (siehe vorausgehende Zeile).	
55	Teil 2, Kap.1 2 (6) **jetzt** Modul 12, 2 (6)	**Modultext:** Die räumliche Anordnung der Netzanschlüsse und der Eigenbedarfsanlage ist so ausgeführt, dass durch ein einzelnes versagen auslösendes Ereignis innerhalb des Kernkraftwerks oder durch ein einzelnes versagen auslösendes Ereignis innerhalb der elektrischen Energieversorgung im Kernkraftwerk oder im Bereich der Netzanschlüsse nicht alle netzseitigen Versorgungsmöglichkeiten längerfristig ausfallen können. Ein solches versagen auslösendes Ereignis, wie eine Einwirkung von außen oder von innen oder ein Zufallsausfall einschließlich mechanischer Folgeschäden, führt nicht zum mechanischen Ausfall der Energieversorgungsmöglichkeiten nach Ziffer 2 (3) b, c und e. **Kommentar:** Anforderung ist hinsichtlich Gültigkeit für den Lastfall "Erdbeben" hinterfragt worden. Ist nicht der Lastfall "Erdbeben" u. a. anforderungsbestimmend für "die Notstromversorgung hinsichtlich einer ausreichenden Energie für die erforderlichen Verbraucher für eine Zeit, in welcher keinerlei Versorgung von außerhalb der Anlage erwartet werden kann ?	**JA**	Der Ausfall der Netzanschlüsse infolge von Erdbeben kann tatsächlich nicht ausgeschlossen werden, weil die Auslegung der externen Energieversorgung außerhalb des Geltungsbereiches der Anforderungen des kerntechnischen Regelwerks liegt. Nur die Notstromanlage wird gegen Einwirkungen eines Erdbebens ausgelegt. T5 schlägt deshalb vor, die Ausnahme des Lastfalls „Erdbeben“ in den M5 Text aufzunehmen.	Die räumliche Anordnung der Netzanschlüsse und der Eigenbedarfsanlage ist so ausgeführt, dass durch ein einzelnes versagenauslösendes Ereignis innerhalb des Kernkraftwerks oder durch ein einzelnes versagenauslösendes Ereignis innerhalb der elektrischen Energieversorgung im Kernkraftwerk oder im Bereich der Netzanschlüsse nicht alle netzseitigen Versorgungsmöglichkeiten längerfristig ausfallen können. Ein solches versagenauslösendes Ereignis, wie ~~eine Einwirkung von außen oder von innen oder ein Zufallsausfall einschließlich mechanischer Folgeschäden, führt nicht zum mechanischen Ausfall der~~ ein Zufallsausfall einschließlich mechanischer Folgeschäden, eine Einwirkung von innen oder eine Einwirkung von außen, mit Ausnahme des Erdbebens, führt nicht zum langfristigen Ausfall aller Energieversorgungsmöglichkeiten nach Ziffer 2 (3) b, c und e.
518	Teil 2, Kap.1 2 (6) **jetzt** Modul 12, 2 (6)	**Kommentar:** Es ist zu überprüfen, inwieweit die Anforderungen hinsichtlich EVA durchgängig aufrecht erhalten werden können.	**JA**	Siehe Kommentar Nr. 55.	

Nr. in DB	Kapitel in Modul	Kommentar	Änderung	Begründung	Vorschlag Textänderung
86	Teil 2, Kap.1 2 (6) **jetzt** Modul 12, 2 (6)	**Kommentar:** Nicht erfüllbar im Erdbebenfall. Sollte geprüft werden.	**JA**	Siehe Kommentar Nr. 55.	
1717	Teil 2, Kap.1 2 (6) **jetzt** Modul 12, 2 (6)	**Kommentar:** Nicht erfüllbar im Erdbebenfall. Sollte überprüft werden. Siehe z. B. Regelung in KTA 3701 Anhang C (C 2.4). Sollte der Erdbebenfall ausgeschlossen werden, müsste dieser Fall separat geregelt werden (wie in KTA 3701).	**JA**	Text der Anforderung wurde geändert, in dem der Erdbebenfall ausgeschlossen wird. Außerdem wurde die Anforderung 2(17a) für die Einwirkungen von außen neu aufgenommen. Außerdem wurde eine Umstellung in der Reihenfolge der Aufzählung der versagensauslösenden Ereignisse durchgeführt, um Missinterpretationen bezüglich der Erdbebenfalls auszuschließen. Zur weiteren Präzisierung wurde „mechanischer Ausfall“ durch „langfristigen Ausfall“ ersetzt. Siehe auch Kommentar Nr. 55.	
	2 (6a) neu **jetzt** Modul 12, 2 (7)		**JA**	Folgewirkung aus dem Kommentar Nr. 521 zu Ziffer 2 (17) und der dort vorgeschlagenen Streichung von 2 (17a)	2 (~~6a~~7) Mindestens eine Verbindung zum Netz oder zu einem Kraftwerk ist im Nahbereich des Kernkraftwerks als erdverlegtes Kabel ausgeführt.
519	Teil 2, Kap.1 2 (7) **jetzt** Modul 12, 2 (8)	**Modultext:** Haupt- und Reservenetzanschluss sind so ausgelegt, dass die elektrische Energieversorgung der Einrichtungen, welche Funktionen auf den Sicherheitsebenen 1 bis 4c ausführen, sichergestellt ist,.... **Kommentar:** Eine Auslegung für die Funktionen der Sicherheitsebenen 4b und c kann nur erfolgen, wenn das Szenarium bekannt ist. Da z.B. ein Station blackout ein Ereignis der Ebene 4 ist, ist die Anforderung so nicht haltbar.	**JA**	Die Anforderung bezieht sich auf die leistungsmäßige Auslegung der Netzanschlüsse. Der Station Blackout selbst ist durch den Ausfall dieser beiden Netzanschlüsse bedingt. Die erforderlichen Funktionen auf der Sicherheitsebene 4 beim SBO sind nicht von einer Energieversorgung aus den Netzanschlüssen abhängig. Dem Einwand wird mit einer Textpräzisierung Rechnung getragen.	Haupt- und Reservenetzanschluss sind so ausgelegt, dass jeder für sich allein in der Lage ist, die elektrische Energieversorgung der Einrichtungen, welche die erforderlichen Funktionen auf den Sicherheitsebenen 1 bis 4a ausführen, sicherzustellen. ~~die elektrische Energieversorgung der Einrichtungen, welche Funktionen auf den Sicherheitsebenen 1 bis 4c ausführen, sichergestellt ist,~~ ~~der Kernkraftwerksblock unter Erhalt der Hauptwärmesenke abgefahren werden kann, eine langfristige Nachwärmeabfuhr sichergestellt ist~~ Haupt- und Reservenetzanschluss sowie die Energieversorgungsmöglichkeit nach Ziffer 2 (3) e) sind so bemessen, dass jeder für sich allein in der Lage ist, die elektrische Energieversorgung der Einrichtungen für anlageninterne Notfallmaßnahmen (Sicherheitsebenen 4b und 4c) zu ermöglichen.
87	Teil 2, Kap.1	**Modultext:** Die Umschaltung vom Hauptnetzanschluss auf den Reservenetzanschluss	**NEIN**	Keine Präzisierung erforderlich. Es ist eindeutig als Anforderungsfall definiert, dass die elektri-	

Nr. in DB	Kapitel in Modul	Kommentar	Änderung	Begründung	Vorschlag Textänderung
	2 (8) **jetzt** Modul 12, 2 (8)	erfolgt im Anforderungsfall automatisch. Der Anforderungsfall ist gegeben, wenn die elektrischen Versorgungsbedingungen bei einer elektrischen Energieversorgung über den Hauptnetzanschluss nicht mehr eingehalten werden können und das Reservenetz verfügbar ist. Die Anrege grenzwerte und die Zeitverzögerungen dieser Umschaltautomatik sind mit denen der Startautomatik der Notstromerzeugungsanlagen so abgestimmt, dass die Notstromerzeugungsanlagen nicht unnötig durch elektrische Transienten angefordert werden. **Kommentar:** Präzisierung erforderlich: Der vorliegende Fall deckt nur die Öffnung des Generatorschalters bei einem generatorseitigen Fehler ab, d.h.: Die Eigenbedarfsleistung wird über den Hauptnetzanschluss bezogen. Ansonsten erfolgt bei Ausfall des Hauptnetzanschlusses zuerst Lastabwurf auf Eigenbedarf und dann, wenn dieser nicht gelingt, Umschaltung auf das Reservenetz.		schen Versorgungsbedingungen bei einer elektrischen Energieversorgung über den Hauptnetzanschluss nicht mehr eingehalten werden können. Eine Energieversorgung über den Hauptnetzanschluss tritt nur dann auf, wenn die Versorgung aus dem Generator ausgefallen ist, zum Beispiel offener Generatorleistungsschalter oder unzureichend für eine Versorgung der EB-Anlage ist, zum Beispiel beim Hochfahren aus der Generatornulllast bis zur Eigenbedarfsleistung. Daher impliziert der Regeltext einen vorhergehenden Ausfall der Generatoreinspeisung.	
1718	Teil 2, Kap.1 2 (8) **jetzt** Modul 12, 2 (9)	**Kommentar:** Kürzung: Nur 1. und 3. Satz sollen stehen bleiben. **Vorschlag:** Die Umschaltung vom Hauptnetzanschluss auf den Reservenetzanschluss erfolgt im Anforderungsfall automatisch. Die Anregegrenzwerte und die Zeitverzögerungen dieser Umschaltautomatik sind mit denen der Startautomatik der Notstromerzeugungsanlagen so abgestimmt, dass die Notstromerzeugungsanlagen nicht unnötig durch elektrische Transienten angefordert werden.	**JA**	Vorschlag wurde sinngemäß umgesetzt, wobei 2. Satz beibehalten wurde.	Die Umschaltung vom Hauptnetzanschluss auf den Reservenetzanschluss erfolgt ~~im Anforderungsfall~~ automatisch. ~~Der Anforderungsfall ist gegeben, wenn~~ wenn die elektrischen Versorgungsbedingungen ~~bei einer elektrischen Energieversorgung~~ über den Hauptnetzanschluss nicht mehr eingehalten werden können und das Reservenetz verfügbar ist. Die Anregegrenzwerte und die Zeitverzögerungen dieser Umschaltautomatik sind mit denen der Startautomatik der Notstromerzeugungsanlagen so abgestimmt, dass die Notstromerzeugungsanlagen nicht unnötig durch elektrische Transienten angefordert werden.
88	Teil 2, Kap.1 2 (9) **jetzt** Modul 12, 2 (10)	**Modultext:** Für die Notstromversorgung sind Notstromanlagen vorgesehen, die strangweise redundant und unabhängig derart aufgebaut sind, dass sie die Anforderungen zur Beherrschung von Einzelfehlern gemäß „Sicherheitsanforderungen für Kernkraftwerke: Anforderungen an die Auslegung und den sicheren Betrieb von baulichen Anlagenteilen, Systemen und Komponenten“ (Modul 10) Abschnitt 1.1 erfüllen. Die Redundanz der Stränge der Notstromanlagen entspricht mindestens der Redundanz der zu versorgenden verfahrenstechnischen Systeme. **Vorschlag:** redundant und unabhängig derart aufgebaut sind, dass sie die Anforderungen zur Beherrschung des Einzelfehlers gemäß "Sicherheitsanforderungen für Kernkraftwerke".	**JA**	Vorschlag wird übernommen, da klarstellend. Der Anforderungstext wurde redaktionell umgestellt. Der Begriff „Strang“ wird im M5 nicht mehr verwendet (s. auch Antwort zu Kommentar Nr. 68).	Für die Notstromversorgung sind redundant aufgebaute Notstromanlagen vorgesehen.~~,~~ ~~die strangweise redundant~~Die Redundanten der Notstromanlagen sind voneinander ~~und~~ unabhängig. ~~derart aufgebaut sind, dass sie~~ Der Redundanzgrad der Notstromanlagen entspricht mindestens dem Redundanzgrad der zu versorgenden verfahrenstechnischen Systeme. Durch den Redundanzgrad werden die Anforderungen zur Beherrschung von Einzelfehlern gemäß „Sicherheitsanforderungen für Kernkraftwerke: Anforderungen an die Auslegung und den sicheren Betrieb von baulichen Anlagenteilen, Systemen und Komponenten“ (Modul 10) Abschnitt 1.1 ~~erfüllen.~~erfüllt. ~~Die Redundanz der Stränge der Notstromanlagen entspricht mindestens der Redundanz der zu versorgenden verfahrenstechnischen Systeme.~~
1724	Teil 2, Kap.1	**Kommentar:** Änderung	**JA**	Vorschlag wurde berücksichtigt. Siehe Antwort zu Kommentar Nr. 88.	

Nr. in DB	Kapitel in Modul	Kommentar	Änderung	Begründung	Vorschlag Textänderung
	2 (9) **jetzt** Modul 12, 2 (10)	**Vorschlag:** Für die Notstromversorgung sind Notstromanlagen vorgesehen, die strangweise redundant und unabhängig derart aufgebaut sind, dass sie die Anforderungen zur redundant und unabhängig derart aufgebaut sind, dass sie die Anforderungen zur **Beherrschung des Einzelfehlers** gemäß „Sicherheitsanforderungen für Kernkraftwerke …			
	Teil 2, Kap.1 2 (10) **jetzt** Modul 12, 2 (11)		**JA**	Der Begriff „Strang“ wird im M5 nicht mehr verwendet (siehe auch Antwort zu Kommentar Nr. 68).	Das Notstromsystem besteht grundsätzlich aus redundanten, unvermaschten ~~Strängen~~ Redundanten der~~von~~ Notstromanlagen, die aufgrund i~~in~~hre~~m~~ s Aufbaus eine funktionelle Unabhängigkeit zwischen den Redundanten gewährleisten. Wird dadurch eine vom zu versorgenden System geforderte Zuverlässigkeit nicht erreicht, dürfen Notstromverbraucher von mehr als ~~einem~~ einer Redundanten ~~Strang~~ einer Notstromanlage versorgt werden, wenn a) die Zuverlässigkeit des Notstromsystems dadurch nicht unzulässig gemindert wird und b) die Verbindungen so ausgeführt sind, dass keine in Betracht zu ziehende Versagensmöglichkeit mehr als ein~~en~~ ~~Strang~~ Redundante einer Notstromanlage ausfallen lassen kann.
520	Teil 2, Kap.1 2 (12) in Verb. mit 2 (15)+ 2 (17) **jetzt** Modul 12, 2 (13)	**Modultext:** 2 (12) Die redundanten Stränge von Notstromanlagen sind räumlich so getrennt oder so gegeneinander geschützt, dass versagen auslösende Ereignisse in der Notstromanlage nicht zum Ausfall von mehr als einer redundanten Notstromanlage führen. 2 (15) Die Voraussetzung zur Beendigung des Betriebs der Notstromanlagen ist dann gegeben, wenn die Versorgung aus dem Hauptnetzanschluss oder dem Reservenetzanschluss oder einer anderen Versorgung für die Verbraucher der Notstromanlagen wieder sicher verfügbar ist. Die Rückschaltung auf den verfügbaren Netzanschluss wird manuell eingeleitet. 2 (17) ... Stränge der Notstromanlage... **Kommentar:** Die Verwendung der Begriffe „Redundante Stränge von Notstromanlagen“, „Notstromanlage“, „Redundante Notstromanlage“, Stränge der Notstromanlagen“ ist irreführend. Es sollten einheitliche Begriffe verwendet werden.	**JA**	Einwand wird stattgegeben und Text präzisiert. Der Begriff „Strang“ wird im M5 nicht mehr verwendet (siehe auch Antwort zu Kommentar Nr. 68).	Die ~~redundanten Stränge von~~ Redundanten der Notstromanlagen sind räumlich so getrennt oder so gegeneinander geschützt, dass versagenauslösende Ereignisse in der Notstromanlage nicht zum Ausfall ~~von mehr als~~ mehrerer Redundanten einer ~~redundanten~~ Notstromanlage führen.
89	Teil 2, Kap. 1 2 (15) **jetzt** Modul 12, 2 (16)	**Kommentar:** Gemeint sind hier die Notstromerzeugungsanlagen. In der Definitionsliste: diesbezügliche Definition ändern, vorliegende nicht korrekt. **Vorschlag:** Die Voraussetzung zur Beendigung des Betriebs der Notstromerzeugungsanlagen ist dann gegeben, wenn die Versorgung aus dem Hauptnetzanschluss oder dem Reservenetzanschluss oder einer anderen Versorgung für die Verbraucher der Notstromerzeugungsanlagen wieder sicher verfügbar ist. Die Rückschaltung auf den verfügbaren Netzanschluss wird manuell eingeleitet.	**JA**	Hinweis ist richtig und wird umgesetzt (red. Änderung). Die Definitionen „Notstrom-Anlage“ und „Notstrom- Erzeugungsanlage“ in der Definitionsliste sind korrekt.	Die Voraussetzung zur Beendigung des Betriebs der Notstromerzeugungsanlagen ist dann gegeben, wenn die Versorgung aus dem Hauptnetzanschluss oder dem Reservenetzanschluss oder einer anderen Versorgung für die Verbraucher der Notstromanlagen wieder sicher verfügbar ist. Die Rückschaltung auf den verfügbaren Netzanschluss wird manuell eingeleitet.

Nr. in DB	Kapitel in Modul	Kommentar	Änderung	Begründung	Vorschlag Textänderung
1726	Teil 2, Kap. 1 2 (15) **jetzt** Modul 12, 2 (16)	**Kommentar:** Gemeint sind hier die Notstromerzeugungsanlagen. In der Definitionsliste: diesbezügliche Definition ändern, vorliegende nicht korrekt. Es sollten generell einheitliche Begriffe verwendet werden. **Vorschlag:** Die Voraussetzung zur Beendigung des Betriebs der **Notstromerzeugungs-anlagen** ist dann gegeben, wenn die Versorgung aus dem Hauptnetzanschluss oder dem Reservenetzanschluss oder einer anderen Versorgung für die Verbraucher der Notstromanlagen wieder sicher verfügbar ist. Die Rückschaltung auf den verfügbaren Netzanschluss wird manuell eingeleitet.	**JA**	Siehe vorhergehende Zeile.	
	Teil 2, Kap. 1 2 (16) **jetzt** Modul 12, 2 (19)		**JA**	Der Begriff „Strang“ wird im M5 nicht mehr verwendet (s. auch Antwort zu Kommentar Nr. 68).	Die Notstromanlagen sind so ausgelegt und geschützt, dass bei Einwirkungen von außen oder von innen nicht alle ~~Stränge von~~Redundanten der Notstromanlagen gleichzeitig außer Funktion gesetzt werden. Die nicht außer Funktion gesetzten ~~Stränge~~ Redundanten der Notstromanlagen sind zur Beherrschung von Ereignissen der Sicherheitsebenen 3 und 4a ausreichend wirksam.
521	Teil 2, Kap.1 2 (17) a) **jetzt** Modul 12, 2 (22)	**Modultext:** Zur Beherrschung eines Ausfalls der elektrischen Energieversorgung des Kernkraftwerkes einschließlich der Notstromerzeugungsanlagen sind folgende Maßnahmen und technische Vorkehrungen vorgesehen: a) mindestens eine zusätzliche Einspeisemöglichkeit über ein im Nahbereich des Kernkraftwerkes Erdverlegtes Kabel b) ... **Kommentar:** Nach dem bisherigen Stand von W&T sind Einspeisemöglichkeiten erforderlich. Es ist zu klären, ob Einspeisemöglichkeiten in das D1 und das D2-netz gemeint sind.	**Teilweise**	Für die geforderte zum Haupt- und Reservenetzanschluss zusätzliche Energieversorgungsmöglichkeit soll hier der Ort der Einspeisung an das Notstromsystem nicht näher konkretisiert werden. Die Forderung in M5 beruht auf dem Hintergrund, dass für diejenigen Komponenten, die zur Ausführung der entsprechend dem SE-Konzept erforderlichen Funktionen bei einem Ausfall der elektrischen Energieversorgung des Kernkraftwerkes einschließlich der Notstromerzeugungsanlagen benötigt werden, eine elektrische Energieversorgung vor Erschöpfung der Energiespeicher sichergestellt werden muss. Die im Kommentar angesprochene ausführungsorientierte Konkretisierung der Anbindung an das Notstromnetz richtet sich also danach, wo die benötigten Verbraucher angeschlossen sind. Diese Konkretisierung ist im Regelwerk nicht vorgesehen. Weder im übergeordneten Regelwerk (einschließlich Modul 5) noch im untergeordneten kerntechnischen Regelwerk (KTA-Regeln) werden ausführungsorientierte Forderungen bezüglich eines Aufbaus des Notstromnetzes aus einem D1-Netz bzw. D2-Netz erhoben. Die Forderung nach einer Vorhaltung von Ener-	Zur Beherrschung eines Ausfalls der elektrischen Energieversorgung des Kernkraftwerkes einschließlich der Notstromerzeugungsanlagen sind folgende Maßnahmen und Einrichtungen ~~technische Vorkehrungen~~ vorgesehen ~~bzw. vorhanden~~: ~~a) Mindestens eine zusätzliche Einspeisemöglichkeit über ein im Nahbereich des Kernkraftwerkes erdverlegtes Kabel.~~ a~~b~~) Vorhaltung von Energiespeichern mit ausreichender Kapazität, um ~~so dass~~ die notwendigen Funktionen bis zur Wiederherstellung der elektrischen Energieversorgung, mindestens jedoch für 2 Stunden, durch~~ge~~führ~~t werd~~en zu können. b) eine zusätzliche Einspeisemöglichkeit zum Haupt- und Reservenetzanschluss, mit der vor Erschöpfung der Energiespeicher die elektrische Energieversorgung der notwendigen Funktionen hergestellt werden kann.

Nr. in DB	Kapitel in Modul	Kommentar	Änderung	Begründung	Vorschlag Textänderung
				giespeichern mit ausreichender Kapazität (erste Forderung von 2(17)) soll durch die Forderung nach einer zusätzlichen Einspeisemöglichkeit ergänzt werden, mit der vor Erschöpfung der Energiespeicher die elektrische Energieversorgung der notwendigen elektrischen Funktionen bei einem Station Blackout hergestellt werden können.	
90	Teil 2, K1 2 (17) b) **jetzt** Modul 12, 2 (22)	**Modultext:** b) Vorhaltung Energiespeicher mit ausreichender Kapazität, so dass die notwendigen Funktionen bis zur Wiederherstellung der elektrischen Energieversorgung durchgeführt werden können. **Kommentar:** Präzisierung Vorhaltung Energiespeicher.	**JA**	Um den Zweck, die Durchführung der notwendigen Funktionen bis zur Wiederherstellung der elektrischen Energieversorgung sicherzustellen, ist Energie erforderlich. Diese Energie muss gespeichert sein, weil bei SBO keine elektrische Energie erzeugt wird und die Überbrückung ab Verlust der elektrischen Energieerzeugung bis zur Wiederversorgung aus Energieerzeugungsanlagen bzw. Netzen zu gewährleisten ist. Eine technische Lösung, Energiespeicher zu realisieren, sind Batterien, aber auch andere Energiespeicher sind denkbar wie z. B. Schwungräder (Verwendung in konventionellen Kraftwerken). Eine Präzisierung hinsichtlich der Mindestzeit für die Batteriekapazität wird in den Text aufgenommen. siehe Textvorschlag zu Kommentar Nr. 521.	
1915	Teil 2, Kap.1 2 (17c) neu **jetzt** Modul 12, 2 (20)	**Kommentar:** Die Anforderungen für eine elektrischen Wiederversorgung nach einer Einwirkung von außen, (z. B. Flugzeugabsturz, Explosion, also Ereignisse der SE 4a) bei denen unterstellt wird, dass die Eigenbedarfsanlage als auch die nicht gegen Einwirkung von außen geschützten Notstromanlagen nicht mehr zur Verfügung stehen, sind für den Langzeitbereich bislang im Modul 5 nicht definiert worden. Da in solchen Fällen die gegen Einwirkung von außen geschützten Notstromanlagen mit ihren Notstromerzeugungsanlagen die Stromversorgung für die notwendigen Sicherheitsfunktionen übernehmen, ergibt sich aufgrund der Betriebserfahrung, dass die Zuverlässigkeit der Aggregate mit zunehmender Betriebszeit abnimmt. Demzufolge ist eine Versorgung der gegen Einwirkung von außen geschützten Notstromanlagen über Anschlüsse zu einem externen Netz nach einer bestimmten Zeit (3 Tage) zu fordern. Die entsprechende Anforderung aus KTA701 Anhang C2.4 soll daher in das Modul 5 aufgenommen werden.	**JA**	Vor dem Hintergrund, dass bei bestimmten Einwirkungen von Außen (Notstandsfälle, Ereignisse der SE4a) die Eigenbedarfsanlage sowie das Notstromnetz 1 auslegungsgemäß als nicht mehr zur Verfügung stehend postuliert werden, ist u. E. nebenstehende Erweiterung vorzunehmen.	2 (17c) Soweit bei Einwirkungen von außen ein gleichzeitiger Ausfall aller Netzanschlüsse nicht ausgeschlossen werden kann, sind Maßnahmen und Einrichtungen dafür vorgesehen, dass spätestens nach 3 Tagen eine Versorgung über einen der nach Ziffer 2 (3) vorgesehenen Netzanschlüsse b) oder c) wieder hergestellt oder über eine Versorgungsmöglichkeit nach 2 (3) e) hergestellt werden kann.
522	Teil 2, Kap.1 2 (18) **jetzt** Modul 12, 2 (21)	**Modultext:** Der Schutz gegen externe und interne elektrische und elektromagnetische Einwirkungen ist so ausgelegt, dass die elektrischen Einrichtungen der Energieversorgung, die Funktionen auf den Sicherheitsebenen 1 bis 4 ausführen, nicht unzulässig beeinträchtigt werden. **Kommentar: Formulierungsvorschlag:** Der Schutz gegen externe und interne elektrische und elektromagnetische Einwirkungen ist so ausgelegt, dass die elektrischen Einrichtungen der Ener-	**Teilweise**	Dem 1.Satz im Vorschlag kann zugestimmt werden. Die Präzisierung wird übernommen. Eine Festlegung auf bestimmte externe und interne elektrische und elektromagnetische Einwirkungen entspricht nicht dem Detaillierungsgrad des Moduls.	Der Schutz gegen externe und interne elektrische und elektromagnetische Einwirkungen ist so ausgelegt, dass die elektrischen Einrichtungen der Energieversorgung, die Einrichtungen mit Funktionen auf den Sicherheitsebenen 1 bis 4 ~~ausführe~~versorgen, nicht unzulässig beeinträchtigt werden.

Nr. in DB	Kapitel in Modul	Kommentar	Änderung	Begründung	Vorschlag Textänderung
		gieversorgung, die Einrichtungen für Funktionen auf den Sicherheitsebenen 1 bis 4 versorgen, nicht unzulässig beeinträchtigt werden. Die hier relevanten externen Einwirkungen sollten genannt werden.			
1727	Teil 2, Kap. 1 2 (20) **jetzt** Modul 12, 2 (18)	**Modultext:** Es sind Maßnahmen und technische Vorkehrungen vorgesehen, die eine gleichzeitige Prüfung redundanter Notstromanlagen zuverlässig verhindern. **Kommentar:** Präzisierung erforderlich oder Kürzung: **Vorschlag:** Eine gleichzeitige Prüfung redundanter Notstromanlagen ist zuverlässig verhindert.	**JA**	Einwand ist richtig. Vorschlag zur Präzisierung wird übernommen.	Eine gleichzeitige Prüfung von Redundanten einer Notstromanlage ist zuverlässig verhindert. ~~Es sind Maßnahmen und technische Vorkehrungen vorgesehen, die eine gleichzeitige Prüfung redundanter Notstromanlagen zuverlässig verhindern.~~
523	Teil 2, Kap.1 2 (20) **jetzt** Modul 12, 2 (18)	**Kommentar:** Technische Maßnahmen, die eine gleichzeitige Prüfung redundanter Notstromanlagen zuverlässig verhindern sind bisher nicht gefordert und mit vertretbarem technischem Aufwand nur eingeschränkt realisierbar. Die Forderung ist zu weit gehend.	**JA**	Siehe vorhergehende Zeile.	
91	Teil 2, Kap. 1 2 (18)	**Kommentar:** Zu technische Vorkehrungen Erläuterung erforderlich **Vorschlag:** Anmerkung: Eine technische Maßnahme ist z.B. die Betätigung Prüfanwahl. Damit könnte dieser Punkt entfallen	**NEIN**	Technische Vorkehrungen können Geräte, Aufbauten sein, die in diesem Fall etwas verhindern (zum Beispiel Schlüssel oder Türverriegelungen zwischen den Redundanzen usw.). Das Wort „Maßnahmen“ ist der Durchführung einer Tätigkeit vorbehalten. Die Einhaltung einer administrativen Vorschrift, in der bestimmte Tätigkeiten vorgezeichnet sind, stellt für diesen Zweck eine wirkungsvolle Maßnahme dar. Die Gesamtheit „Maßnahmen und/oder technische Vorkehrungen“ bezeichnen allumfassend die Einhaltung der administrativen Vorschriften als auch notwendige Gerätschaften; Aufbauten, Türen, Schlösser etc, die für die Erfüllung des geforderten Zwecks geeignet sind. Siehe Kommentar Nr. 1727.	
1729	Teil 2, Kap. 1 3 (1) **jetzt** Modul 12, 3 (1)	**Kommentar:** Es fehlen Anforderungen an die Qualifizierung von elektrotechnischen Komponenten. **Vorschlag:** Qualitätssicherung und Prüfungen Die Eignung der elektrotechnischen Komponenten für den Einsatz in Kernkraftwerken ist durch Typprüfungen und Betriebsbewährung nachgewiesen. Für zusätzlich erforderliche sicherheitstechnische Eigenschaften, z. B. Auslegung für die Belastung durch Einwirkungen von außen und gegen Störfälle (Störfallfestigkeit), die durch Betriebsbewährung und Typprüfung nicht erfasst werden, sind zusätzliche Eignungsnachweise geführt.	**JA**	Der Vorschlag wird als 2. Satz in die Anforderung übernommen.	Die erforderliche Qualität der elektrischen Einrichtungen der Energieversorgung wird durch Qualitätssicherungsmaßnahmen sichergestellt. Die Eignung der elektrotechnischen Komponenten für den Einsatz in Kernkraftwerken ist durch Typprüfungen und Betriebsbewährung nachgewiesen. Für zusätzlich erforderliche sicherheitstechnische Eigenschaften, z.B. Auslegung für die Belastung durch Einwirkungen von außen und gegen Störfälle (Störfallfestigkeit), die durch Betriebsbewährung und Typprüfung nicht erfasst werden, sind zusätzliche Eignungsnachweise geführt.

Nr. in DB	Kapitel in Modul	Kommentar	Änderung	Begründung	Vorschlag Textänderung
1731	Teil 2, Kap. 1 3 (2) **jetzt** Modul 12, 3 (2)	**Kommentar:** Es fehlen Anforderungen an die Qualifizierung von elektrotechnischen Komponenten **Vorschlag:** **Der Erhalt** der erforderlichen Qualität der elektrischen Einrichtungen der Energieversorgung wird durch Qualitätssicherungsmaßnahmen sichergestellt.	**NEIN**	Der vorgeschlagene Text ist im 1.Satz des Abschnitts 3.1 enthalten.	
1254	Teil 2, Kap. 1 3 (3) **jetzt** Modul 12, 3 (3)	**Kommentar:** Prüfung des letzten Satzes im Hinblick auf Streichung bzw. Platzierung in anderem Modul.	**JA**	Da der letzte Satz übergeordnet in Modul 1 Ziffer 8 (4) 3. Absatz geregelt ist und zudem keine direkte Anforderung an die Auslegung der Einrichtungen darstellt, kann der letzte Satz gestrichen werden.	Die Einrichtungen im Notstromsystem werden auf ~~die Einhaltung ihrer Funktion durch Messungen und Meldungen überwacht, um deren~~ Funktionsbereitschaft und ihren Betriebszustand durch Messungen und Meldungen überwacht.~~zu erkennen. Unzulässige Abweichungen werden dokumentiert.~~
1732	Teil 2, Kap. 1 3 (3) **jetzt** Modul 12, 3 (3)	**Kommentar:** Es fehlen Anforderungen an die Qualifizierung von elektrotechnischen Komponenten **Vorschlag:** Die Einrichtungen des Notstromsystems werden regelmäßig wiederkehrend geprüft. Soweit aus Zuverlässigkeitsgründen notwendig, werden die Prüfungen auch im Leistungsbetrieb durchgeführt. Die Prüfungen werden dokumentiert.	**NEIN**	Siehe Antwort zu Kommentar Nr. 1254, 1729, 1731.	
	Modul 5 Teil 2 Kapitel 2				
94	Teil 2, Kap. 2 2 (3) **jetzt** Modul 5, 13	**Modultext:** Die Einrichtungen der Störfallinstrumentierung sind an eine unterbrechungslose Notstromversorgung des Notstromsystems angeschlossen. **Kommentar:** Diese Formulierung ist zu präzisieren. Begründung: Es sind Einrichtungen der Störfallinstrumentierung auch in der Notsteuerstelle installiert (siehe hierzu KTA 3502, Kap. 3.5 Stromversorgung).	**JA**	M5-Text wird unter Berücksichtigung der KTA 3502 präzisiert.	Die Einrichtungen der Störfallinstrumentierung sind an eine unterbrechungslose Notstromversorgung des Notstromsystems angeschlossen. Für Einrichtungen der Störfallinstrumentierung, bei denen aufgrund ihrer Aufgabenstellung eine kurzzeitige Nichtverfügbarkeit zulässig ist, muss die Stromversorgung nicht unterbrechungslos erfolgen.
524	Teil 2, Kap. 2 3.1 (1) **jetzt** Modul 5, 13	**Modultext:** Die Störfallanzeige ist so ausgelegt, dass Daten, die vor, während und nach Eintreten eines Ereignisses der Sicherheitsebenen 3 oder 4a für die Beurteilung der Anlagensicherheit, der Wirksamkeit des Sicherheitssystems und für die Entscheidung über Maßnahmen des anlageninternen Notfallschutzes erforderlich sind, zuverlässig und ausreichend genau angezeigt werden. Bei Auslegung der Störfallanzeige ist berücksichtigt, dass die Daten, die vor, während und nach Eintreten eines Ereignisablaufs bzw. Anlagenzustands, welche zu einer erhöhten Freisetzung radioaktiver Stoffe in die Kernkraftwerksumgebung führen können (Sicherheitsebenen 4b oder 4c), für die Entscheidung über Maßnahmen des anlageninternen Notfallschutzes erforderlich sind, unter den anzunehmenden Umgebungsbedingungen ausreichend genau angezeigt werden.	**JA**	Richtige Präzisierung.	Die Störfallanzeige ist so ausgelegt, dass Daten, die vor, während und nach Eintreten eines Ereignisses der Sicherheitsebenen 3 oder 4a für die Beurteilung der Anlagensicherheit, der Wirksamkeit des Sicherheitssystems und für die Entscheidung über Maßnahmen des anlageninternen Notfallschutzes erforderlich sind, zuverlässig und ausreichend genau angezeigt werden. Bei Auslegung der Störfallanzeige ist berücksichtigt, dass die Daten, die vor, während und nach Eintreten eines Ereignisablaufs bzw. Anlagenzustands, welche zu einer erhöhten Freisetzung radioaktiver Stoffe in die Kernkraftwerksumge-

Nr. in DB	Kapitel in Modul	Kommentar	Änderung	Begründung	Vorschlag Textänderung
		Kommentar: Formulierungsvorschlag: ...unter den anzunehmenden Umgebungsbedingungen mit der erforderlichen Genauigkeit angezeigt werden. Mit dieser Änderung können anforderungsgerechte Festlegungen von Fall zu Fall getroffen werden.			bung führen können (Sicherheitsebenen 4b oder 4c), für die Entscheidung über Maßnahmen des anlageninternen Notfallschutzes erforderlich sind, unter den anzunehmenden Umgebungsbedingungen mit der erforderlichen Genauigkeit ~~ausreichend genau~~ angezeigt werden.
1245	Teil 2, Kap. 2 3.1 (4) **jetzt** Modul 5, 13	**Modultext:** Die Weitbereichsanzeige ist so ausgelegt, dass bei Ereignisabläufen bzw. Anlagenzuständen der Sicherheitsebene 4b bzw. 4c die Annäherung von Anlagenparametern an Grenzwerte der aktivitätseinschliessenden Barrieren und die Überschreitung dieser Grenzwerte durch Messgrößen erfasst wird. **Kommentar:** Auch an dieser Stelle wird von der Kenntnis der Ereignisabläufe und Umgebungsbedingungen auf den SE 4b und 4c ausgegangen, gegen die ausgelegt werden soll. Das entspricht nicht der aktuellen Sicherheitsphilosophie.	**JA**	In den RSK-LL (Abschnitt 25.1) und in der KTA 3502 (Abschnitt 2 (5)) wird gefordert, dass die Störfallinstrumentierung vor während und nach einem Störfall oder einem Ereignis, dass zu einer erhöhten Freisetzung führen kann die Informationen über den Zustand der Anlage erfassen, anzeigen und aufzeichnen soll. In Bezug auf die Sicherheitsebene 4 ist hierzu die Weitbereichsanzeige vorgesehen. In Modul 5 werden diesbezüglich keine neuen Anforderungen gestellt. Es werden nebenstehende Präzisierungen vorgeschlagen.	~~Die~~ Es ist eine Weitbereichsanzeige ~~ist so ausgelegt~~für die Messgrößen vorgesehen, die die repräsentativen Ereignisabläufe und daraus abgeleiteten Anlagenzustände der Sicherheitsebenen 4b und 4c charakterisieren (siehe „Sicherheitsanforderungen für Kernkraftwerke: Anforderungen an den anlageninternen Notfallschutz“ (Modul 7,Ziffer 2 (3)). ~~dass bei Ereignisabläufen bzw. Anlagenzuständen der Sicherheitsebene 4b bzw. 4c die Annäherung von Anlagenparametern an Grenzwerte der aktivitätseinschliessenden Barrieren und die Überschreitung dieser Grenzwerte durch Messgrößen erfasst wird.~~
1246	Teil 2, Kap.2 3.1 (8) **jetzt** Modul 5, 13	**Kommentar:** Der Begriff „Notsteuerstelle“ wird hier konsistent zur als „neu“ bezeichneten Begriffsbestimmung dieses Regelwerkes benutzt. Diese Begriffsbestimmung ist aber sehr missverständlich, da damit allgemein dezentrale Steuereinrichtungen gemeint sind, die in Notfällen benutzt werden, sich aber nicht alle an ein und demselben Ort befinden. Der Zustand, in dem die „Notsteuerstelle“ zum Einsatz kommt heißt dann aber gemäß Begriffsdefinition „Notstandsfall“.	**NEIN**	Die Definition des Begriffs „Notsteuerstelle“ (Rev. B) lautet: „Einrichtung außerhalb der Warte, von der aus bei Ausfall der Warte der Reaktor unterkritisch gemacht, die Unterkritikalität aufrecht erhalten und die Wärmeabfuhr aus dem Reaktor nach dessen Abschaltung überwacht und gesteuert werden kann.“ Eine Änderung am Modultext oder in der Definition ist nicht erforderlich.	
	Teil 2, Kap.2 3.1 (12) **jetzt** Modul 5, 13			Redaktionelle Anpassung.	Die Einrichtungen der Störfallanzeige sind nach ergonomischen Gesichtspunkten so gestaltet, dass die Voraussetzungen für ein sicherheitstechnisch optimales Verhalten des Betriebspersonals ~~der Beschäftigten~~ gewährleistet sind.
92	Teil 2, Kap. 2 3.2 (1) **jetzt** Modul 5, 13	**Modultext:** Die Störfallaufzeichnung ist so ausgelegt, dass die Messgrößen, die vor, während und nach Eintreten - eines Ereignis der Sicherheitsebenen 3 oder 4a oder - eines Ereignisses, das zu einer erhöhten Freisetzung radioaktiver Stoffe in die Kernkraftwerksumgebung führen kann (Sicherheitsebenen 4b oder 4c), übersichtlich und in der richtigen zeitlichen Folge dokumentiert werden. **Kommentar:** Zeitdauer sollte festgelegt werden.	**NEIN**	Kommentar ist unverständlich. Welche Zeitdauer soll festgelegt werden? Zudem wäre eine Zeitangabe dem Detaillierungsgrad von Modul 5 nicht angemessen.	
1247	Teil 2,	**Modultext:**	**JA**	Angemessene Präzisierung, wird u. E. im aktuel-	Für die Aufzeichnung und Speicherung der

Nr. in DB	Kapitel in Modul	Kommentar	Änderung	Begründung	Vorschlag Textänderung
	Kap. 2 3.2 (6) **jetzt** Modul 5, 13	Für die Aufzeichnung und Speicherung der Störfallablaufdaten werden mindestens zwei gegen einen systematischen Ausfall ausgelegte Datenspeicher eingesetzt. Der Ausfall eines Datenspeichers wird angezeigt. **Kommentar:** Sollte hier wirklich Diversität im Sinne unterschiedlicher physikalischer Speicherarten gemeint sein, so ist dies nicht erforderlich. Vielleicht war ja Redundanz und räumliche Trennung gemeint.		len Vorschlag umgesetzt. Das Mittel zum Erreichen der erforderlichen Vorsorge soll in jedem konkreten Fall festgelegt werden.	Störfallablaufdaten werden zur Vorsorge gegen einen systematischen Ausfall mindestens zwei ~~gegen einen systemattischen Ausfall ausgelegte~~ Datenspeicher eingesetzt. Der Ausfall eines Datenspeichers wird angezeigt.
525	Teil 2, Kap. 2 3.2 (6) **jetzt** Modul 5, 13	**Kommentar:** Die Forderung nach Berücksichtigung des systematischen Ausfalls geht über den bisherigen Stand W&T hinaus.	**JA**	Siehe auch unter Kommentar Nr. 1247.	
1248	Teil 2, Kap. 2 3.2 (6) **jetzt** Modul 5, 13	**Kommentar:** Die Störfallablaufdaten sollten benannt werden.	**NEIN**	Die Auflistung der zu speichernden Störfallablaufdaten ginge über den in Modul 5 angestrebten Detaillierungsgrad hinaus. Daher sollte dem Vorschlag nicht gefolgt werden.	
93	Teil 2, Kap. 2 3.2 (6) **jetzt** Modul 5, 13	**Kommentar:** Zu klären ist, ob in der Warte und der Notsteuerstelle je zwei diversitäre Speichermedien vorzuhalten sind.	**NEIN**	Aus dem M5-Text ergibt sich nicht die explizite Anforderung zum Vorhandensein von zwei diversitären Speichern (nicht Speichermedien), auch nicht in der Warte bzw. in der Notsteuerstelle.	
1735	Teil 2, Kap. 2 3.2 (6) **jetzt** Modul 5, 13	**Kommentar:** Präzisierung erforderlich. Warte und Notsteuerstelle	**NEIN**	Die Anforderung richtet sich auf die Vorsorge gegen einen systematischen Ausfall der Aufzeichnung und der Speicherung der Störfallablaufdaten und nicht auf den Einbauort.	

Anhang 1: **Dr. Arndt Lindner,**
Garching, den 14.03.2008

Abweichende Auffassung zum Regeltextvorschlag zu den Ziffern 3.2 (11) und 3.2 (12) von Modul 5 Teil 1

Dem Regeltextvorschlag kann aus folgenden Gründen nicht zugestimmt werden:

1. Systematische Ausfälle können von unabhängigen Systemen beherrscht werden. Die im Regeltextvorschlag geforderte dissimilare Auslegung ist (neben anderen) nur ein Mittel, um Unabhängigkeit herzustellen.

2. Der Vorschlag grenzt die Anwendung von Diversität auf „unterschiedliche Soft- und Hardware sowie deren Entwicklungsprozess und Entwicklungswerkzeuge“ ein. Aus meiner Sicht ist es erforderlich, durch eine Analyse das Potential für GVA zu ermitteln und danach die Auslegungskriterien zur Sicherstellung der Unabhängigkeit abzuleiten. Dabei können sich andere Formen der Diversifizierung als wirksamer herausstellen. Die Anwendung von funktionaler Diversität, die mit dem Regeltextvorschlag bewusst ausgegrenzt werden soll, wird in unterschiedlichen Regelwerken als besonders wirksames Mittel gegen GVA bei software-basierter Leittechnik betont (siehe NRC PTB 19, VDI/VDE 2735, IEC 62340).

3. Der Vorschlag gibt konkrete technische Lösungen vor. Das Regelwerk sollte jedoch Anforderungen enthalten, die von den technischen Lösungen zu erfüllen sind.

4. Eine dreifach dissimilare Auslegung der Soft- und Hardware erhöht die Komplexität des Gesamtsystems in starkem Maß (z.B. Zusammenschaltung der unterschiedlichen Systeme, Berücksichtigung unterschiedlichen Zeitverhaltens, Wiederkehrende Prüfung und Wartung für drei unterschiedliche Systeme). Das daraus resultierende Fehlerpotential muss bei einer Gesamtbeurteilung einbezogen werden. Abschließend ist festzuhalten, dass eine dreifache Soft- und Hardwarediversität für Schutzsysteme in KKW nicht dem Stand von Wissenschaft und Technik entspricht.

5. Der in der Begründung zum Regeltextvorschlag angegebenen These, dass der Regeltextvorschlag einen in der Kerntechnik und in anderen sicherheitskritischen Anwendungen vorherrschenden Lösungsansatz darstellt, kann aus unseren Erkenntnissen zu den Entwicklungstrends bei der Anwendung software-basierter Leittechnik nicht gefolgt werden.

6. Deterministische Nachweise zur Beherrschung von GVA in software-basierten Leittechniksystemen sind auch für Systeme durchführbar, die auf einer Gerätefamilie (Geräteplattform) aufbauen.

Alternativer Regeltextvorschlag:

3.2 (11) Bei der Auslegung der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, sind Vorkehrungen gegen systematische Ausfälle der Hardware und systematisches Versagen der Software zu treffen. Dazu sind unabhängige Systeme oder Teilsysteme einzusetzen. Es ist nachzuweisen, dass ein angenommenes systematisches Versagen eines dieser Systeme die Funktion des jeweils anderen Systems nicht beeinträchtigt.

Für Leittechnik-Funktionen, deren aktives Versagen immer sicherheitsgerichtet wirkt, ist der Einsatz eines Systems ausreichend, wenn dessen passives Versagen sicher erkannt wird und dieses zur Auslösung der Schutzaktion führt.

3.2 (12) Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, sind so ausgelegt, dass sie ihre Aufgaben auch dann erfüllen, wenn im Anforderungsfall ein Zufallsausfall und ein systematischer Ausfall (systematischer Ausfall der Hardware oder systematisches Versagen der Software) und daraus resultierende Folgeausfälle eintreten. Während eines Instandhaltungsfalls wird im Anforderungsfall innerhalb einer Zeitspanne von 100 h das gleichzeitige Auftreten des systematischen Ausfalls und des Zufallsausfalls nicht unterstellt.