



Gesellschaft für Anlagen-
und Reaktorsicherheit
(GRS) mbH



Institut für
Sicherheitstechnologie
(ISTec) GmbH

- Textmodul -

„Sicherheitsanforderungen
für Kernkraftwerke:

Anforderungen an Leittechnik“

ENTWURF

Revision B

SR 2475

Ergebnisse Team 5 (Teil 1)

- Textmodul -

„Sicherheitsanforderungen
für Kernkraftwerke:
Anforderungen an Leittechnik“

Revision B ENTWURF

Dieser Bericht ist im Auftrag des BMU im Rahmen des Vorhabens SR 2475 erstellt worden. Die Arbeiten des Vorhabens SR 2475 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

September 2006

Auftrags-Nr.: 813071

Anmerkung:

Der Auftraggeber behält sich alle Rechte vor. Insbesondere darf dieser Bericht nur mit seiner Zustimmung zitiert, ganz oder teilweise vervielfältigt werden bzw. Dritten zugänglich gemacht werden.

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 werden zu bisher im kerntechnischen Regelwerk nicht verankerten oder erheblich überarbeitungsbedürftigen Sicherheitsaspekten modularisierte 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. Das Zusammenwirken aller Regeltextmodule und der weiteren kerntechnischen Regelungen ist in einem Wegweiser dargestellt.

Zu folgenden Sicherheitsaspekten wurden Regeltextmodule erstellt:

- Modul 1: „Sicherheitsanforderungen für Kernkraftwerke:
Grundlegende Sicherheitsanforderungen“
- Modul 2: „Sicherheitsanforderungen für Kernkraftwerke:
Anforderungen an die Auslegung 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 Leittechnik (Modul 5, Teil 1)“
„Sicherheitsanforderungen für Kernkraftwerke:
Anforderungen an Elektrische Energieversorgung, Störfallinstrumentierung (Modul 5, Teil 2)“
- Modul 6: „Sicherheitsanforderungen für Kernkraftwerke:
Anforderungen an 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 bautechnischen Anlagenteilen, Systemen und Komponenten“
- Modul 11 „Sicherheitsanforderungen für Kernkraftwerke:
Anforderungen an die Handhabung und Lagerung der Brennelemente“

Die vorangegangenen Entwürfe der Regeltextmodule Rev. A sind seit September 2005 im Internet (<http://regelwerk.grs.de>) verfügbar und wurden u. a. in Workshops, die vom 23. Januar bis 3. Februar 2006 im BMU durchgeführt wurden, zur Diskussion gestellt.

Alle bis Ende Februar 2006 zur Rev. A der Regeltextmodule eingegangenen Kommentare sowie die Hinweise aus den Workshops wurden bei der Erstellung der Rev. B ausgewertet.

Die vorliegende Unterlage des Regeltextmoduls in der Fassung Rev. B enthält dementsprechend in synoptischer Darstellung die Ergebnisse der Auswertung aller zum Modul 5 „Sicherheitsanforderungen für Kernkraftwerke: Anforderungen an Leittechnik (Teil 1)“ übermittelten Kommentare und Hinweise aus den Workshops. Zur besseren Lesbarkeit ist Rev. B von Modul 5, Teil 1 in einen Fließtext umgesetzt worden. Rev. B von Modul 5, Teil 1 ist wiederum im Internet unter <http://regelwerk.grs.de> verfügbar.

Gliederung

- 1 Geltungsbereich**
- 2 Kategorisierung**
- 3 Auslegung**
 - 3.1 Leittechnische Einrichtungen für Leittechnik-Funktionen der Kategorien A bis C
 - 3.2 Leittechnische Einrichtungen für Leittechnik-Funktionen der Kategorie A
 - 3.3 Leittechnische Einrichtungen für Leittechnik-Funktionen der Kategorie B
 - 3.4 Leittechnische Einrichtungen für Leittechnik-Funktionen auf der Sicherheitsebene 4
- 4 Anforderungsspezifikation für leittechnische Einrichtungen für Leittechnik-Funktionen der Kategorien A bis C**
- 5 Erfassung von Prozessvariablen**
- 6 Redundanz und Unabhängigkeit**
- 7 Qualifizierung**
 - 7.1 Qualifizierung der Hardware- und Software der leittechnischen Einrichtungen für Leittechnik-Funktionen der Kategorien A bis C
 - 7.2 Qualifizierung der Hardware
 - 7.3 Qualifizierung der Software
- 8 Robustheit**
- 9 Mensch-Maschine-Schnittstelle bei leittechnischen Einrichtungen**
- 910 Instandhaltungen und Änderungen**
- 1011 Anforderungen an die Zugriffskontrolle**
- 1112 Dokumentation**
- 1213 Elektrische Energieversorgung der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorien A bis C ausführen**
- ~~**14 Anforderungen für die Erstellung und Prüfung von Software**~~
 - ~~14.1 Software für Leittechnik-Funktionen der Kategorien A bis C~~
 - ~~14.2 Software für Leittechnik-Funktionen der Kategorie A~~
 - ~~14.3 Software für Leittechnik-Funktionen der Kategorie B~~
 - ~~14.4 Software für Leittechnik-Funktionen der Kategorie C~~

- Anhang 1:** Zusammenstellung der Textquellen zum TextmModul 5, Teil 21
 „Sicherheitsanforderungen für Kernkraftwerke: Anforderungen an
 Leittechnik“ sowie Teil 2 „Sicherheitsanforderungen für
 Kernkraftwerke: Anforderungen an Elektrische Energieversorgung,
 Störfallinstrumentierung“
- Anhang 2:** Relevanz der Empfehlungen und Stellungnahmen der RSK seit 1990
 (Auszug aus der Empfehlungsliste) für Modul 5, Teil 1 und 2
 „Leittechnik“
- Anhang 3:** Übersicht über Berücksichtigung von Erkenntnissen aus dem
 Vorhaben SR 2472 „Regelvergleich“ (Auszug aus der
 Empfehlungsliste) im Modul 5
- Anhang 4:** Übersicht über Berücksichtigung der Festlegungen der
 Sicherheitskonvention und von WENRA Aktivitäten im TextmModul
 5, Teil 2

Komm. Nr.	Kommen tator	Kommentar	Antwort Team 5
384	VGB /EnBW	<p>Zusammenfassung</p> <p>Das vom BMU initiierte Vorhaben SR 2475 erhebt den Anspruch (Zitat): <i>Das Vorhaben SR 2475 ist darauf ausgerichtet, zu bisher im kerntechnischen Regelwerk nicht verankerten oder erheblich überarbeitungsbedürftigen Sicherheitsaspekten modularitg Regeltextentwürfe im Detaillierungsgrad der „BMI-Sicherheitskriterien“ und „RSK-Leitlinien“ zu erstellen.</i></p> <p>Für das Textmodul „Leittechnik ist dazu festzustellen: Das Textmodul enthält 117 Punkte mit Forderungen. Davon stammen nahezu alle aus den derzeit gültigen RSK- Leitlinien und aus dem KTA- Regelwerk. Eine weitere Forderung wird als sinngemäße Übersetzung aus dem Regelwerk der IAEA angegeben, zwei weitere beziehen sich auf Untersuchungen der ISTec. Inhaltlich sind ca. 50 Forderungen gegenüber der Quelle unverändert übernommen oder nur redaktionell geändert worden. Bei den übrigen Forderungen sind über redaktionelle Änderungen und Ergänzungen hinausgehende Veränderungen vorgenommen worden, die, wie der Vergleich mit den bereits vorliegenden Modulen nahe legt, wenigstens teilweise durch Vorgaben wie:</p> <ul style="list-style-type: none"> • Gleichsetzung von „Sicherheitsebenen“ mit „sicherheitstechnischer Bedeutung“, • Undifferenzierte Forderungen nach jeweils unabhängigen und eigenständigen Maßnahmen für alle Einrichtungen der Sicherheitsebenen 1 bis 3, • Vermeiden des Begriffs „Schutzziel“, • Vermeiden der Begriffe „Störfälle“ und „Störungen“, • Streichen von sinnvollen Relativierungen, <p>bedingt sind. Hinzu kommen begriffliche Verschiebungen wie:</p> <ul style="list-style-type: none"> • Gleichsetzung von „Sicherheitsleittechnik“ mit „Leittechnik des Sicherheitssystems“, oder • Ersatz des Begriffs „Sicherheitsleittechnik“ durch den umfassenderen Begriff „Leittechnische Einrichtungen“. <p>Dadurch wird einerseits der Geltungsumfang ausgeweitet, zum anderen werden z. T. erhebliche Veränderungen der Inhalte oder Verschärfungen der Forderungen bewirkt, die überwiegend nicht gerechtfertigt und teilweise nicht erfüllbar sind.</p> <p>Damit wird keineswegs eine Erhöhung des Sicherheitsniveaus erreicht, weil sich die Erweiterungen im wesentlichen auf Einrichtungen der Sicherheitsebenen 1 und 2 und auf Funktionen ohne sicherheitstechnische Bedeutung erstrecken und die Verschärfungen überwiegend dadurch entstehen, dass Einrichtungen und Funktionen mit abgestuft geringerer sicherheitstechnischer Bedeutung mit Forderungen für Ein-</p>	<p>Der Kommentar vom Oktober 2005 bezieht sich noch auf das Modul 5 Rev. 6 (Internetfassung), die aufgrund von Änderungsvorschläge bereits durch die Rev. A abgelöst worden ist.</p> <p>Die in dem Kommentar enthaltenen übergeordneten Kritikpunkte wurden bereits durch die zu der Rev. 6 eingegangen Kommentare 327/RSK, 345/ Framatome ANP sinngemäß berücksichtigt.</p>

Komm. Nr.	Kommentator	Kommentar	Antwort Team 5
		<p>richtungen und Funktionen mit höchster sicherheitstechnischer Bedeutung belegt werden. In einem ausgewogenen Sicherheitskonzept kann sich aber die Verstärkung einzelner Elemente nicht signifikant auswirken.</p> <p>Das Modul stützt sich ganz überwiegend auf die RSK- Leitlinien in der Fassung 10. 1996 ab. Im Vorwort zur Veröffentlichung (BAnz. Nr. 158a vom 23. August 1996) wird die Neufassung begründet (Zitat): <i>Die Neufassung trägt der Entwicklung auf dem Gebiet der Leittechnik Rechnung. Die bisher gültige Fassung von 1981 war nur mittelbar auf die inzwischen entwickelte rechnerbasierte Leittechnik anwendbar. Die Neufassung soll Unsicherheiten bei der Anwendung auf solche Systeme beseitigen.</i></p> <p>Es ist nicht erkennbar, dass im Modul „Leittechnik“ bisher nicht geregelte oder erheblich änderungsbedürftige Sicherheitsaspekte behandelt werden. Ein Grund für die Neufassung des kerntechnischen Regelwerks ist zumindest aus dem Modul „Leittechnik“ nicht ableitbar.</p> <p>Auf die wesentlichen und übergreifenden Änderungen, wird nachfolgend eingegangen. Anschließend werden die Forderungen einzeln kommentiert.</p> <p>1) Gleichsetzung von Sicherheitsebenen mit sicherheitstechnischer Bedeutung</p> <p>Die RSK-LL definieren und kategorisieren die sicherheitstechnische Bedeutung einer Leittechnik- Funktion über deren Beitrag zur Beherrschung von Störfällen (Formulierung: „Funktionen zur Verhinderung der nichttolerablen Auswirkung der Störfälle“, „Funktionen zur Verhinderung der Ausweitung von Störungen zu Störfällen“ und „übrige Funktionen mit sicherheitstechnischer Bedeutung z. B. Strahlenschutz- Störfallinstrumentierung“) und damit über deren Beitrag zur Einhaltung der Schutzziele. Entsprechend dieser Kategorisierung werden für die Einrichtungen (Geräte), die diese Funktionen ausführen, abgestufte Forderungen abgeleitet. Für Funktionen (und die zugehörigen Einrichtungen) ohne sicherheitstechnische Bedeutung werden keine Anforderungen gestellt. Genau so verfährt DIN IEC 61226. Beide Regeln verfolgen das Konzept der gestuften Maßnahmen (Defence in Depth (DiD)). Die Kategorisierung entsprechend der sicherheitstechnischen Bedeutung der Funktionen und der Einrichtungen, die sie ausführen erfolgt in Erweiterung der in IAEA N-R-1 formulierten Klassifizierungs-Strategie. DIN IEC 61226 verweist zur Anwendung des DiD -Konzeptes auf Abschnitt A3 von DIN IEC 61513 (VDE 0491 Teil 2, die erst in 2002 in das nationale Regelwerk übernommen wurde. Dieses Vorgehen stellt somit den Stand von W&T dar.</p>	

Komm. Nr.	Kommentar	Antwort Team 5
	<p>In den KTA- Regeln werden Anforderungen ebenfalls nach dem Beitrag zur Beherrschung oder Vermeidung von Störfällen abgestuft. Allerdings werden statt der leittechnischen Funktionen und den zugehörigen Einrichtungen gleich die mit konkreten Geräten aufgebauten leittechnischen Systeme geregelt, die die entsprechenden Aufgaben wahrnehmen. Entsprechend diesen Anforderungen ergibt sich z. B. die Hierarchie der sicherheitstechnischen Bedeutung der automatisch arbeitenden Systeme der Sicherheitsleittechnik:</p> <ul style="list-style-type: none"> • Reaktorschutzsystem, • Schutzbegrenzung, • Zustandsbegrenzung. <p>Die den Zustandsbegrenzungen vorgelagert arbeitenden Reaktorregelungen haben keine sicherheitstechnische Bedeutung werden infolgedessen betrieblich eingestuft. Für diese werden im KTA-Regelwerk keine Auslegungsanforderungen gestellt. Gleichwohl ergeben sich funktionale Anforderungen z. B aus BMI-Sicherheitskriterien oder RSK-LL Abschnitt 6.</p> <p>Das mit dem Vorhaben SR 2475 verfolgte Konzept der gestaffelten Sicherheitsebenen, die durch Anlagenzustände festgelegt sind und deren Gleichsetzung mit sicherheitstechnischer Bedeutung, passt weder zur funktionalen Hierarchie der RSK-LL noch zu den Regeln DIN IEC 61226, DIN IEC 61513 (VDE 0491 Teil 2) und damit auch nicht zum Stand von W&T, noch zur Aufgaben- und Systemhierarchie der einschlägigen KTA- Regeln.</p> <p>Die meisten betrieblichen Einrichtungen der Sicherheitsebene 1 sind mit Schutzeinrichtungen versehen, die der Sicherheitsebene 2 zuzuordnen sind. Diese Schutzeinrichtungen zählen ebenfalls zur betrieblichen Leittechnik und haben nichts mit Sicherheit zu tun sondern nur mit Verfügbarkeit oder Schutz des eingesetzten Kapitals. Mit Ausnahme einiger weniger Einrichtungen -z. B. der Zustandsbegrenzungen- enthalten die SE 1 und SE 2 überwiegend Funktionen bzw. Einrichtungen ohne sicherheitstechnische Bedeutung. Es ist nicht akzeptabel für die in ihrer sicherheitstechnischen Bedeutung unterschiedlichen Funktionen, die derselben Sicherheitsebene zuzuordnen sind, einheitliche Anforderungen zu stellen, da diese sich dann nach denen mit der höchsten Bedeutung richten müssten.</p> <p>Zur Störfallbeherrschung auf der SE 3 ist aus Sicht der Leittechnik kurzfristig nur das Reaktorschutzsystem erforderlich wobei die Ausgangszustände für die zu berücksichtigenden Störfälle vor Störfalleintritt durch einige wenige Zustandsbegrenzungsfunktionen in den Grenzen gehalten wurden, die den Störfallanalysen zugrunde gelegt werden. Für die Do-</p>	

Komm. Nr.	Kommentator	Kommentar	Antwort Team 5
		<p>kumentation, die Analyse und für die mittel- und langfristige Beherrschung sind weitere Einrichtungen erforderlich und vorhanden z. B. Störfallinstrumentierung. Letztere sind zweifellos Einrichtungen der SE 3, gleichwohl aber mit gegenüber dem Reaktorschutzsystem abgestuften Anforderungen. Diese Anforderungen sind, wie oben ausgeführt, in den RSK-LL kategorisiert und differenziert im KTA- Regelwerk festgelegt.</p> <p>Zusammengefasst bleibt festzustellen: Die Gleichsetzung von SE d. h. Anlagenzuständen mit sicherheitstechnischer Bedeutung und daraus abgeleiteten Anforderungen wird den funktionalen und sicherheitstechnisch begründeten Anforderungen an Funktionen (Aufgaben) und den Einrichtungen, die diese Funktionen ausführen, nicht gerecht und entspricht nicht dem Stand von W&T.</p> <p>2) Gleichsetzung von „Sicherheitsleittechnik“ mit „Leittechnik des Sicherheitssystems“</p> <p>Der Begriff „Sicherheitsleittechnik“ wird im Abschnitt 7 der RSK-LL seit ihrer Neufassung in 1996 definiert. Er umfasst alle Einrichtungen, die Funktionen der Kategorien 1 bis 3 wahrnehmen. Unterscheidungskriterium für eine Abstufung der Anforderungen war bis dahin die sicherheitstechnische Bedeutung der leittechnischen Einrichtung, die zu der üblichen Unterscheidung: „betriebliche Leittechnik“, „Sicherheitsleittechnik“ und - im Graubereich – zu „Leittechnik mit sicherheitstechnischer Bedeutung“ geführt hat. Der Begriff „Sicherheitsleittechnik“ der RSK-LL umfasst die beiden letzten Begriffe.</p> <p>Die zum Sicherheitssystem der Kernkraftwerke gehörenden verfahrenstechnischen Systeme (z. B. das Not- und Nachkühlssystem TH) haben jeweils eine Leittechnik, die für ihren bestimmungsgemäßen Betrieb erforderlich ist (z. B. eine Nachkühlregelung). Unter „Leittechnik des Sicherheitssystems“ wird korrekterweise diese betrieblich, aber mit sicherheitstechnischer Bedeutung, eingestufte Leittechnik verstanden. Das Reaktorschutzsystem greift auf die Komponenten des Sicherheitssystems (z. B. Nachkühlpumpen) mit Vorrang zu. Befehle der betrieblichen Leittechnik werden dann unwirksam. Die Einrichtungen, mit denen dieser Vorrang sichergestellt wird und nur diese, gehören zur Sicherheitsleittechnik und werden nach den Anforderungen des Reaktorschutzsystems qualifiziert. Das Reaktorschutzsystem ist daher nicht Bestandteil der Leittechnik des Sicherheitssystems, sondern ein Teil der Sicherheitsleittechnik. Diese Unterscheidung kommt allerdings auch im vorhandenen Regelwerk nicht immer klar zum Ausdruck.</p> <p>Richtigerweise sind in den RSK-LL im Abschnitt 7.2 Anforderungen an die elektrischen Einrichtungen des Sicherheitssystems in Abgrenzung</p>	

Komm. Nr.	Kommentar	Antwort Team 5
	<p>zur Sicherheitsleittechnik gestellt, für die in Abschnitt 7.3 weitergehende Anforderungen formuliert werden.</p> <p>Die im Text des Moduls vorgenommene Auswechslung von Begriffen verwischt diese Unterscheidung zusätzlich. Darüber hinaus ist nicht klar, was damit bezweckt werden soll. Damit kann die Forderung gemeint sein, diese Leittechnik der verfahrenstechnischen Sicherheitssysteme nach Anforderungen für Sicherheitsleittechnik auszulegen. Falls das beabsichtigt ist stellt das eine massive Verschärfung der Anforderungen an die betriebliche Leittechnik dar. Das hat auch keinerlei Entsprechungen im internationalen Regelwerk und ist schon von daher abzulehnen. Falls das nicht beabsichtigt ist, sollten die Formulierungen eindeutig erkennen lassen, was stattdessen gemeint ist.</p> <p>Zur Klarstellung ist erforderlich, den Begriff „Leittechnik des Sicherheitsleitsystems“ in diesem Modul eindeutig zu definieren und dann einheitlich zu verwenden, oder bei den etablierten Begriffen zu bleiben.</p> <p>3) Erweiterung des Geltungsumfangs auf alle Sicherheitsebenen</p> <p>Bei einer großen Anzahl von Forderungen der RSK-LL wird durch Ersatz des in diesen Leitlinien eindeutig definierten Begriffs „Sicherheitsleittechnik“ durch den Begriff „leittechnische Einrichtungen“ der Geltungsbereich der jeweiligen Forderung auf alle Sicherheitsebenen und alle Einrichtungen ausgeweitet. Das ist potentiell eine massive Ausweitung des Geltungsbereichs dieses Moduls gegenüber den RSK-LL, die bisher Auslegungsanforderungen nur für die elektrischen Einrichtungen des Sicherheitssystems und die Sicherheitsleittechnik erhoben. Für die elektrischen Einrichtungen des Betriebssystems werden in den RSK-LL nur funktionale Anforderungen gestellt.</p> <p>Dieser Austausch des Begriffs „Sicherheitsleittechnik“ durch den Begriff „leittechnische Einrichtungen“ erweitert, sofern keine weiteren Einschränkungen im Text vorgenommen werden, die jeweiligen Forderungen auf alle Funktionen und Einrichtungen unabhängig von der sicherheitstechnischen Bedeutung der jeweiligen Funktion d. h. auf die gesamte Leittechnik des Kernkraftwerks. Die im Abschnitt 13. 1 für Software der SE 1 nicht vorgenommene Kategorisierung für Software ohne direkten Bezug zur Sicherheit für sich allein stellt keine solche Einschränkung dar, auch wenn der unter Nr. 1 im Geltungsbereich gemachte Verweis auf das Modul 1 in Forderung 3.2 (1) als vergleichbare Reduktion für die Hardware interpretiert werden kann. Falls diese Interpretation zutrifft heißt das nur, dass der Sicherheitsebene 1 zugeordnete Funktionen ohne jede sicherheitstechnische Bedeutung nicht kategorisiert werden müssen. Es bestehen aber immer noch die Auslegungsanforderungen, die ursprünglich für die Sicherheitsleittechnik erhoben</p>	

Komm. Nr.	Kommentar	Antwort Team 5
	<p>wurden für alle anderen Sicherheitsebenen. Das ist dann immer noch eine nicht akzeptable Verschärfung der generellen Anforderungen an Leittechnik. Das soll am Beispiel der SE 2 verdeutlicht werden.</p> <p>So fordert Abschnitt 2.3:</p> <p><i>„Die leittechnischen Einrichtungen der Sicherheitsebene 2 müssen ihre Aufgaben auch dann erfüllen, wenn zusätzlich zu einem Ereignis der Sicherheitsebene 2 ein Zufallsausfall und Folgeausfälle eintreten.“</i></p> <p>Diese Forderung nach redundantem Aufbau ist angemessen für eine Zustandsbegrenzungseinrichtung, für den Aggregateschutz einer betrieblichen Komponente oder die Schutzverriegelung eines betrieblichen Systems der SE 2 aber nicht.</p> <p>Selbst für Funktionen mit sicherheitstechnischer Bedeutung ist nicht notwendigerweise ein redundanter Aufbau erforderlich. So weisen Gefahrenmeldeeinrichtungen der Klasse 1 auf Störungen im Sicherheitssystem hin. Sie sind daher der SE 2 zuzurechnen. KTA 3501 fordert aber keineswegs einen redundanten Aufbau. Die Anforderungen müssen daher auch für die SE 2 nach der jeweiligen sicherheitstechnischen Bedeutung der leittechnischen Funktion und nicht nach Betriebszuständen (Sicherheitsebenen) erhoben werden.</p> <p>Die Verwendung von Sicherheitsebenen und die begründete Forderung nach Abstufung der zu stellenden Anforderungen an Funktionen nach deren sicherheitstechnischen Bedeutung macht eine Differenzierung der Anforderungen an die Leittechnik auf jeder Sicherheitsebene unvermeidlich.</p> <p>4.) Undifferenzierte Forderungen nach jeweils unabhängigen und eigenständigen Maßnahmen für alle Einrichtungen der Sicherheitsebenen 1 bis 3</p> <p>In Abschnitt 2.1 wird für die Hardware der SE 2 und in 13.1 für die Software der Ebenen 1 bis 3 sinngemäß gefordert:</p> <p>Die leittechnischen Einrichtungen (Hard und Software) einer Sicherheitsebene, deren Versagen Ereignisse auslöst, die nicht durch Maßnahmen und Einrichtungen der nächst höheren Sicherheitsebene beherrscht werden, sind nach den Anforderungen der nächst höheren Sicherheitsebene zu erstellen und zu prüfen.</p> <p>Entsprechende Forderungen sind auch im Modul 1 enthalten.</p> <p>Das grundsätzlich sinnvolle Vorgehen, die Auslegungsanforderungen an Funktionen und den zugeordneten Einrichtungen von den Auswirkungen bei einem unterstellten Ausfall abzuleiten, ist in der hier gewählten Formulierung insofern problematisch, als sie sich nur an Sicherheitsebenen festgemacht und nicht mit der sicherheitstechnischen Bedeutung einer Funktion und den daraus resultierenden Zuverlässigkeitsanforderungen</p>	

Komm. Nr.	Kommentator	Kommentar	Antwort Team 5
		<p>verbunden wird.</p> <p>Im Modul 5 wird das für die Hardware damit begründet, dass Zustandsbegrenzungen die Randbedingungen für die Beherrschung von Störfällen sicherstellen. Der Forderungstext selbst enthält diese Einschränkung nicht ebenso wenig wie der Forderungstext für die Software, die für die Ebenen bis 3 gelten. Er gilt damit für alle Einrichtungen der drei Ebenen 1 bis 3 und nicht nur für Zustandsbegrenzungen.</p> <p>Die Gleichsetzung von Sicherheitsebene mit sicherheitstechnischer Bedeutung ist nicht Ziel führend. Eine differenzierte Anwendung der Forderung in Abhängigkeit von der sicherheitstechnischen Bedeutung der jeweiligen Funktion ist erforderlich.</p> <p>Im Nachfolgenden werden die Forderungen einzeln kommentiert.</p>	
513	AREVA	<p><u>Begriffsdefinitionen Widerspruch</u></p> <ul style="list-style-type: none"> – Unsauber definierte Begriffe führen zu Widersprüchen und zu unklaren Anforderungen – Beispiel: <ul style="list-style-type: none"> • „Systematischer Ausfall“ ist über „Versagen“ definiert • „Versagen“ ist über „Verlust der Integrität“ definiert • „Integrität“ ist über die Einhaltung mechanischer Merkmale definiert (Festigkeit, Dichtigkeit, Bruchsicherheit) • Folgerung: Software besitzt keine mechanischen Merkmale, kann also die Integrität nicht verlieren, kann also nicht versagen, kann also nicht systematisch ausfallen. • ABER: Absatz 3.2 spricht vom „Versagen der Software“ <p><u>Begriffsdefinitionen - Unklare Abgrenzungen</u></p> <ul style="list-style-type: none"> – Präzisierung und Abgrenzung ist mindestens erforderlich zwischen folgenden Begriffen <ul style="list-style-type: none"> • Fehler, Ausfall, Versagen, systematischer Ausfall, systematisches Versagen, Mehrfachversagen, Ausfallkombinationen, Einzelfehlerkonzept • Funktion, Sicherheitsfunktion, grundlegende Sicherheitsfunktion, Leittechnik-Funktion, Funktion der leittechnischen Einrichtung, Aufgaben der Leittechnik, Teilaufgaben der Leittechnik, Anforderungen an die Leittechnik, Anforderungsspezifikation der Leittechnik • Einrichtungen des Sicherheitssystems, Einrichtungen für Leittechnik-Funktionen der Kategorie A • Eignungsprüfung • Robustheit, Unempfindlichkeit 	<p>In Modul 5 wurde „Versagen“ als Synonym für Ausfall verwendet: Verhalten, das nicht der Spezifikation entspricht. Ein Fehler, z. B. in der Software, kann unter bestimmten Umständen zu einem Versagen führen. „Verlust der Integrität“ wurde im Zusammenhang mit den Anforderungen an die leittechnischen Einrichtungen nicht angewendet.</p> <p>Begriffe in den Modulen 1 und 5 werden in der Revision B erneut zwischen allen Modulen abgestimmt und notwendige Anpassungen werden für die Begriffsdefinitionen vorgeschlagen. Hierbei werden in den Modulen 1 und 5 einheitliche Definitionen angewendet.</p>

Komm. Nr.	Kommentator	Kommentar	Antwort Team 5
		<ul style="list-style-type: none"> • Unabhängigkeit <p><u>Zusammenfassung</u></p> <ul style="list-style-type: none"> – Schlüsselbegriffe zur Formulierung der Auslegungsanforderungen müssen klarer formuliert und gegeneinander abgegrenzt werden – Die Vielfalt der Begriffe sollte deutlich reduziert werden – Es muss klar und verständlich formuliert werden, welche Ereigniskombinationen von welchen leittechnischen Einrichtungen zu beherrschen ist – Es sollte geprüft werden, wann Unabhängigkeiten sinnvoll und daher zu fordern sind 	
519	BfS	<p><u>Begründung zum Kommentar:</u> Ergänzungen, um in Anwendung auf Anforderungen an die E- und Leittechnik (insbes. Modul 5) die Begriffe „Ausfall“ und „Versagen“ der aktuellen Begriffsdefinition gemäß der DIN-IEC-Standards anzupassen; s. z. B. DIN-IEC 61513 (VDE 0491 Teil 2):2002-10</p> <p><u>Änderungsvorschlag:</u> Ausfall (failure): Abweichung der ausgeführten Funktion von der vorgesehenen Funktion Anm.: Ein Versagen ist das Ergebnis eines Hardwarefehlers, eines Softwarefehlers, eines System-Fehlers oder von Fehlverhalten bei Bedienung und Wartung, und einer damit verbundenen Signaltrajektorie, die zu dem Versagen führt. Nationale Fußnote: Wenn Hardware oder Teilsysteme (z.B. ein Strang eines redundanten Systems) betroffen sind, wird „failure“ mit „Ausfall“ übersetzt.</p>	<p>Begriffe in den Modulen 1 und 5 werden in der Revision B erneut abgestimmt und notwendige Anpassungen werden für die Begriffsdefinitionen vorgeschlagen. Siehe auch Antworten zu den Begriffsdefinitionen.</p> <p>Die Definition von Ausfall lautet (siehe Begriffsdefinitionen): „Eine oder mehrere <i>Auslegungsanforderungen</i> können derart nicht mehr erfüllt werden, dass die geforderte <i>Funktionsfähigkeit</i> der betroffenen <i>Einrichtung</i> nicht mehr gegeben ist.“</p> <p>Die Definition für Versagen lautet (siehe Begriffsdefinitionen): „Synonym für <i>Ausfall</i>.“</p>
538	UM / BW	<ul style="list-style-type: none"> • Der Detaillierungsgrad des Moduls ist uneinheitlich. Bei der weiteren Überarbeitung sollte vor dem Hintergrund, dass ein übergeordnetes Regelwerk erarbeitet werden soll, eine angemessene und einheitliche Regelungstiefe erzielt werden. • Die verwendeten Begriffe sollten einheitlich verwendet werden und eindeutig definiert sein. So ist z. B. der Begriff „Softwareversagen“ in Teil 1, 3.2 (11) unklar und nicht gebräuchlich. Definitionsketten sollten nach Möglichkeit vermieden werden. • Manche Passagen sind zu unpräzise formuliert und provozieren Missverständnisse. • Es gibt sowohl Doppelungen als auch Inkonsistenzen zwischen Modul 5 und dem entsprechenden Kapiteln in Modul 1, die korrigiert werden müssen. 	<ul style="list-style-type: none"> • Die teilweise unterschiedliche Detaillierung ergibt sich aus dem Detaillierungsgrad der durch das neue Regelwerk abzulösenden Regelungen in den bestehenden BMI Sicherheitskriterien und der RSK-LL-DWR. • Begriffe siehe Antwort zu 513/AREVA und 519/BFS • Inkonsistenzen bezüglich Zuordnung der leittechnischen Einrichtungen zu Sicherheitsebenen wurden in der Rev. B beseitigt: in Modul 5 (Rev. A) wurde Kategorisierung der Leittechnikfunktionen eingeführt, in Modul 1 (Rev. A) waren leittechnischen Einrichtungen der Sicherheitsebene zugeordnet. • Doppelungen zwischen M1 und M5 Rev. B wurden minimiert.

Komm. Nr.	Komm. tator	Kommentar	Antwort Team 5
		<ul style="list-style-type: none"> Es sollte generell überprüft werden, ob die in Modul 1 festgelegten Anforderungen die Bezeichnung „übergreifende technische Anforderungen“ verdienen. Beispielsweise wird in Modul 1 konkret das Auslegungsmerkmal Diversität für das Reaktorschutzsystem gefordert (3.2 (7a)). Hinsichtlich der Eindeutigkeit und Anwendbarkeit scheint es sinnvoller, alle Anforderungen in Modul 5 zu bündeln, um ein in sich geschlossenes Modul zu bilden. Andernfalls sollte der Umfang in Modul 1 auf ein Mindestmaß reduziert und ausschließlich Anforderungen mit grundlegender Bedeutung in Modul 1 aufgenommen werden. Mehrfach werden die „Umgebungsbedingungen“ der Ebenen 4b und 4c genannt, ohne dass diese eindeutig bestimmt sind bzw. im Fall 4c aus heutiger Sicht überhaupt benannt werden können. 	<p>Im Modul 5 wird zwar für Leittechnikfunktionen auf den SE 4b und 4c die Auslegung gegen Umgebungsbedingungen gefordert, allerdings mit der Einschränkung, dass nur die für die jeweilige Aufgabe zu unterstellenden Umgebungsbedingungen zu unterstellen sind. Das heißt, für vorgeplante Maßnahmen müssen die nach der Planung zu erwartenden Umgebungsbedingungen berücksichtigt werden. Hiervon sind keine Anforderungen an nicht vorgeplante Maßnahmen abzuleiten.</p>
593	RSK / Bandholz	<p>Ich möchte nur das unterstützen, was Herr Liemersdorf eben sagte. Wenn man das Kapitel 3.3 im Modul 1 sieht, da gibt es zwei wesentliche Unterscheidungen. Es gibt zum einen den Abschnitt 3.3, wo eben festgelegt ist, dass sie räumlich zu trennen sind, Warte und Notsteuerstelle, und dass sie derart zu schützen sind, dass eine von beiden überlebt. Daraus kann man natürlich nicht schließen, dass beide geschützt sein müssen, sondern nur eine von beiden, wenn sie die falsche treffen, haben Sie Pech so ungefähr. Es ist eindeutig so gefordert.</p> <p>Zum Zweiten ist es so, dass wenn Sie weitergehen in 3.5, dann steht da plötzlich, „Maßnahmen des anlageninternen Notfallschutzes werden“, das heißt, es wird eine Verknüpfung vorgenommen unter dem Thema Notsteuerstelle, wird plötzlich auch der anlageninterne Notfallschutz eingesteuert, obwohl es keine Anforderung eigentlich gibt, solange die Warte verfügbar ist.</p> <p>Unter 3.5 (Wickel 6) steht da, „...muss es lange genug aushalten können in der Notsteuerstelle“, sozusagen dass man sich da längere Zeit aufhalten kann. Hier wird auch wieder thematisch das Thema Notsteuerstelle mit Notfallschutz und Notstandsfall wieder verknüpft.</p> <p>Insofern, hier muss mal die Begrifflichkeit und die Aufgabenstellungen sicherlich noch einmal überdacht werden und dieses wird natürlich jetzt transportiert, sowohl punktuell in Modul 5, als auch in Modul 10. Nur an dieser Stelle muss man sich darüber einig sein, was man eigentlich will. Weil der anlageninterne Notfallschutz ist grundsätzlich natürlich von einer Notsteuerstelle, die nur für den äußeren Einwirkungsfall existiert oder für den Brand auf der Warte existiert. Dort kann man dann natürlich nicht die Möglichkeiten nutzen, die man auf der Warte hat für den anlageninternen Notfallschutz.</p>	<p>Die Anforderungen an die Unabhängigkeit bzgl. räumlicher Trennung der Warte und der Notsteuerstelle werden in Rev. B in Modul 10 formuliert.</p> <p>Die Anforderungen der leittechnischen Einrichtungen der Warte und der Notsteuerstelle sind im Modul 5 Teil 1 berücksichtigt.</p>

Komm. Nr.	Kommen tator	Kommentar	Antwort Team 5
		Ich weise noch mal darauf hin, wenn man sich mal dann mit der Freisetzung extern, wenn Sie dann externe Einrichtungen des KFÜ einbinden, das wird auf jeden Fall nicht in der Notstandstelle der Fall sein, um Freisetzung beobachten zu können. Das geht nur auf der Warte. Und deswegen sind die Begrifflichkeiten und die Ableitung, für welchen Fall ist was zuständig, die sollten tatsächlich überdacht werden hier.	
594	Bandholz / RSK	<p>Wenn die Anforderungen in den Modulen gegenüber gestellt werden, dann ist zum Beispiel nach dem Modul 5 auch in der Ebene 4c definiert worden, dass konkurrierende Maßnahmen des anlageninternen Notfallschutzes Vorrang vor Reaktorschutz haben. Gleichzeitig habe ich hier die Anforderung, dass sich alles sozusagen eben auch, hinsichtlich der sicherheitstechnischen Bedeutung immer daran orientieren soll. Und diese ganzen Anforderungen und das Übereinanderlegen der Ebene 4c, die Vorrang vor dem Schutz haben soll, also auch Leitechnikfunktion der Kategorie A, da kommen mir eben Zweifel, ob die ganzen Vorgaben aus Modul 1, Modul 7 und Modul 5 sich tatsächlich auch übereinander falten lassen. Und da sind meine großen Bedenken, dass hier zu viele abstrakte Begriffe sind, dass man in der Sicherheitsebene 2 so zuverlässig sein muss, dass die Ebene 3 nicht in Anspruch genommen wird, das ist natürlich auch eine Anforderung. Das würde bedeuten, dass die Kategorie B in der Leitechnik zuverlässiger sein muss als die Kategorie A. Als ganz generelle Folgen, das steht hier so wörtlich drin, dass Sie in der Ebene 2 so zuverlässig einrichten und aufbauen müssen, dass Sie Ebene 3 nicht erreichen. Modul 5 wird einfach überladen mit all diesen allgemeinen Anforderungen aus Modul 1 und auch aus anderen Modulen. Das ist meine große Sorge.</p> <p>Zum Zweiten komme ich eben dazu und sage, ich habe in Modul 3 auf der Sicherheitsebene 2 Ereignisse definiert, die das Sicherheitssystem anfordern, bspw. Ausfall der Hauptwärmesenke. Da gibt es Mehrere davon. Diese Ereignisse fordern also Einrichtungen der Ebene 3 an, nicht der Ebene 2 und auch nicht die Kategorie A und nicht die Kategorie B. Das passt aber nicht zusammen mit den Anforderungen aus Modul 1, dass sie ebenenweise auch die Einhaltung der Schutzziele oder der Sicherheitsanforderungen auf der einzelnen Ebene sicherstellen müssen. Und deswegen muss das Modul 5 sich an der Stelle, meines Erachtens nach, einfach als „Mittler zwischen diesen Modulen“ verstehen, in dem darauf hingewiesen wird, dass die Sicherheitsebenenanzuordnung aus dem Modul 3 und die Anforderung aus Modul 1 sich natürlich hier irgendwo in einem System auslegen lassen müssen. Sie haben echte Schwierigkeiten, diese Anforderungen</p>	<p>Die Kompatibilität der Texte der betroffenen Module wurde überprüft. Änderungen sind die Rev. B eingeflossen (Ziffer 3.2 (5) in Modul 1). Von der Sache her ist sicherzustellen, dass bei anlageninternen Notfallmaßnahmen (Ebenen 4b und 4c) zielführende Eingriffe bei allen Leitechnik-Funktionen, einschl. Reaktorschutz (<i>Kategorie A</i>), möglich und zulässig sind. Die Formulierung in Ziffer 2.1 (3) Modul 1 ist, dass das Eintreten von Störfällen vermieden wird. Diese Formulierung ist bewusst gewählt und bedeutet nicht, dass die Sicherheitsebene 3 „nicht in Anspruch genommen wird“. Es besteht die Anforderung, dass (gemäß Planung) Störungen grundsätzlich mit den Einrichtungen der Sicherheitsebene 2 beherrscht werden, ebenso wie Störfälle mit denen der Sicherheitsebene 3. Der im Kommentar gezogene Schluss, dass „die Kategorie B in der Leitechnik zuverlässiger sein muss als die Kategorie A“ ist daraus u. E. nicht ableitbar.</p> <p>Ziffer 2.1 (7) Modul 1 regelt die Bedingungen, unter denen Einrichtungen der Sicherheitsebene 3 bei Ereignissen der Ebene 2 in der Analyse herangezogen werden können. Eine Inkonsistenz zu den in Modul 3 definierten Ereignissen bzw. den Anforderungen in Modul 5 besteht u. E. nicht.</p>

Komm. Nr.	Kommentator	Kommentar	Antwort Team 5
		so übereinander zu falten, dass Sie das auch umsetzen können. Insofern hat das Modul 5 da auch an manchen Stellen einfach die Führungskappe aufzusetzen, um vielleicht das Modul 1 an vielen Stellen zu korrigieren. Es lässt sich so nicht auslegen, wenn Sie die Anforderungen aus den drei Modulen übereinander falten.	
598	VGB Power	<p>Die Detaillierung ist sehr unterschiedlich, mal KTA-Niveau mal übergeordnete Regel. Gleiche Sachverhalte werden zum Teil an verschiedenen Stellen behandelt und dabei widersprüchlich beschrieben. Mehrere Stellen sind zumindest missverständlich.</p> <p>Es bestehen Inkonsistenzen z. B. zum Modul 1: Im Modul 1 wird in 3.2 bis 3.4 noch von Einrichtungen gesprochen, die Sicherheitsebenen (SE) zugeordnet sind. Der zweite Satz unter 3.2(13d) des Moduls 1: „Hierbei ist ...“ ist nicht verständlich.</p> <p>Begrifflichkeiten wie Fehler, Ausfall, Versagen etc. werden nicht präzise definiert und gebraucht. So wird in der Begriffserklärung zu „Fehler“ dieser dadurch von „Ausfall“ abgegrenzt, dass ein „Ausfall“ dann vorliegt, wenn sich ein bestehender Fehler auf eine Funktion tatsächlich auswirkt. In der Begriffsdefinition für „Ausfall“ findet sich dieser Sachverhalt jedoch nicht wieder. Hier wird „Ausfall“ als Nichteinhaltung einer oder mehrerer Auslegungsanforderungen definiert, die faktische Auswirkung auf eine Funktion ist hier nicht gefordert.</p> <p>Die SE 4 wird insbesondere für die Unterebenen 4b und 4c praktisch nicht mehr als auslegungsüberschreitend betrachtet. Es wird die Kenntnis von Ereignisabläufen und Umgebungsbedingungen unterstellt, gegen die auszulegen ist. Dies widerspricht grundlos dem etablierten Verständnis und der allgemein anerkannten Sicherheitsphilosophie.</p>	<p>Hinsichtlich des Detaillierungsgrades siehe Antwort zum Kommentar 538.</p> <p>Im Modul 5 wurde die Kategorisierung der Leittechnikfunktionen eingeführt, wobei die Anforderungen der Sicherheitsebenen berücksichtigt werden. Die Verknüpfung zwischen leittechnischen Einrichtungen und der SE im Modul 1 wird in der Rev. B entsprechend der Kategorisierung im Modul 5 präzisiert und damit werden Inkonsistenzen beseitigt.</p> <p>Ohne Präzisierung der angesprochenen Stellen in Modul 5 lassen sich die Aussagen nicht sinnvoll beantworten.</p> <p>Zur Definition von „Ausfall“ und „Versagen“ siehe Antwort auf Kommentar 519. Unstimmigkeiten zur Definition von „Fehler“ sind nicht konkretisiert.</p>

Ziffer	Textvorschlag Modul 5/Teil 1 (Rev. A)	Komm. Nr.	Kommen-tator	Kommentar bzw. Antwort	Ziffer (Neu)	Textvorschlag Modul 5/Teil 1 (Rev. B)
1	Geltungsbereich				1	Geltungsbereich
	<p>Die nachfolgenden Anforderungen gelten für leittechnische Einrichtungen, die auf den Sicherheitsebenen 1 bis 4c Leittechnik-Funktionen ausführen.</p> <p>Die Anforderungen werden durch Einrichtungen realisiert, bei denen Hard- und Software Leittechnik-Funktionen ausführen.</p> <p>Hinweise: Die Anforderungen an die leittechnischen Einrichtungen der Sicherheitsebene 1 ohne direkte sicherheitstechnische Bedeutung sind im Modul 1 "Sicherheitsanforderungen für Kernkraftwerke", Abschnitt 3.2, festgelegt.</p>	384	VGB/EnBW	<p>Der Geltungsbereich umfasst alle Sicherheitsebenen 1 bis 4c. Die im Hinweis implizit gemachte Einschränkung für Ebene 1 auf leittechnische Einrichtungen mit direkter sicherheitstechnischer Bedeutung findet sich weder im Querverweis (Modul 1) noch im weiteren Text wieder. Lediglich im Abschnitt 13.1 wird für Softwarefunktionen der Leittechnik der Sicherheitsebene 1 ohne unmittelbare Sicherheitsrelevanz auf eine Kategorisierung verzichtet. Grundsätzlich gilt: Die vorhandene (und auch die neue) Leittechnik lässt sich nicht eindeutig Sicherheitsebenen zuordnen. Das geht nur für leittechnische Aufgaben (Terminus: Leittechnische Funktionen (LEFU)). Unterscheidungskriterium für eine Abstufung der Anforderungen war bisher die sicherheitstechnische Bedeutung, die zu der üblichen Unterscheidung: „betriebliche LT“, „Sicherheits- LT“ und - im Graubereich - zu „LT mit sicherheitstechnischer Bedeutung“ geführt hat. Die betriebliche Leittechnik ohne sicherheitstechnische Bedeutung ist bisher im kerntechnischen Regelwerk nur funktional geregelt. Insofern ist hier potentiell eine erhebliche Ausweitung des Regelungsumfangs vorgenommen worden.</p> <p>Team 5: Bereits in Modul 1 ist der Geltungsbereich der Anforderungen der Module begrenzt auf Maßnahmen und Einrichtungen mit sicherheitstechnischer Bedeutung, hinsichtlich der Sicherheitsebene 1 dahingehend, dass dort diejenigen betroffen sind, die den Eintritt von Störungen bzw. Störfällen betreffen. Es wird auch in Modul 5 eine Präzisierung vorgenommen.</p> <p>Hinweis wurde gestrichen, weil die Anforderungen in den Modulen 1 und 5 nur an die</p>		<p>Die nachfolgenden Anforderungen gelten für leittechnische Einrichtungen, die auf den Sicherheitsebenen 1 bis 4c Leittechnik-Funktionen mit sicherheitstechnischer Bedeutung ausführen.</p> <p>Die Anforderungen werden durch Einrichtungen realisiert, bei denen Hard- und Software Leittechnik-Funktionen ausführen.</p> <p>Hinweise: Die Anforderungen an die leittechnischen Einrichtungen der Sicherheitsebene 1 ohne direkte sicherheitstechnische Bedeutung sind im Modul 1 "Sicherheitsanforderungen für Kernkraftwerke", Abschnitt 3.2, festgelegt.</p>

Ziffer	Textvorschlag Modul 5/Teil 1 (Rev. A)	Komm. Nr.	Kommen-tator	Kommentar bzw. Antwort	Ziffer (Neu)	Textvorschlag Modul 5/Teil 1 (Rev. B)
				Einrichtungen mit sicherheitstechnischen Bedeutungen gestellt werden.		
		593	Bandholz / RSK	<p>Sie haben darauf hingewiesen, das ist die Schnittstelle zwischen zwei Teams, ich würde sagen, das ist zwischen vier Teams eine Schnittstelle. Aber fangen wir mit Modul 1 mal an, da steht unabhängig von den ganzen Definitionen aus Modul 5, wird hier noch das Wort „Reaktorschutzsystem“ usw. verwendet, was sicherlich im weiteren Prozesses angeglichen wird an die Terminologie.</p> <p>Hier (Modul1 Ziffer 3.2 (5)) steht zum Beispiel, dass auf der Sicherheitsebene 4c Eingriffe in den Reaktorschutz erlaubt sind und die Maßnahmen des anlageninternen Notfallschutz Vorrang vor dem Reaktorschutz haben. Wenn Sie dann versuchen, ihren Textvorschlag in die Systematik einer solchen Leittechnikfunktion der Kategorie A einzufügen, also, dass eine Kategorie A im Normalbetrieb von der Wertigkeit her eine Kategorie A Notfallschutz unterliegt, also von ihr dominiert wird, da tut man sich sehr schwer, Ihre Prozessvariablen einzuordnen. Insofern würde ich sagen, sollte man sich die Weiterführung dieses Textvorschlags auf der Ebene 4b und 4c noch einmal gut überlegen. Zumal es auf der Ebene 4c, wie wir im Modul 7 festgestellt haben, dann auch keine Maßnahmen mehr gibt.</p> <p>Team 5: Der Begriff Reaktorschutz wird in den Modulen (Revision B) synonym verwendet mit der Definition „Leittechnischen Einrichtungen für Leittechnik-Funktionen der Kategorie A“.</p> <p>Die Anforderungen an die Leittechnik-Funktionen der SE 4b und 4c wurden ent-</p>		

Ziffer	Textvorschlag Modul 5/Teil 1 (Rev. A)	Komm. Nr.	Kommentator	Kommentar bzw. Antwort	Ziffer (Neu)	Textvorschlag Modul 5/Teil 1 (Rev. B)
				sprechend dem SE-Konzept umgesetzt. In der Revision B werden Definitionen und Anforderungen hinsichtlich der Notfallmaßnahmen und -strategien präzisiert. Ziffer 3.2 (5) Modul 1 stellt keine Anforderung an die Auslegung der Leittechnik dar, sondern erlaubt bei der Planung von Notfallmaßnahmen Eingriffe in die Leittechnik. Eine unterschiedliche Wertigkeit der Einrichtungen ist daraus nicht abzuleiten. Siehe hierzu auch Modul 7 Ziffer 3.1 (9) Revision B.		
		598	VGB Power	<p>Der hier angegebene Geltungsbereich (Einrichtungen die Leittechnik-Funktionen (LF) auf den Sicherheitsebenen 1 bis 4c ausführen) wird unter 2 mit dem entsprechenden Hinweis sofort weiter eingeschränkt auf LF der Kategorien A bis C. Dabei bezieht sich der Hinweis wieder auf Anforderungen an Funktionen, nicht wie beabsichtigt auf Anforderungen an Einrichtungen die Funktionen ausführen.</p> <p>Team 5: Der Kommentar vom Oktober 2005 bezieht sich noch auf den Modul 5 Rev. 6 (Internetfassung), die aufgrund von Änderungsvorschläge bereits durch die Rev. A abgelöst worden ist. Die in dem Kommentar enthaltenen übergeordneten Kritikpunkte wurden bereits durch die zu der Rev. 6 eingegangenen Kommentare 327/RSK, 345/Framatom ANP sinngemäß berücksichtigt.</p>		
2	Kategorisierung				2	Kategorisierung
	Entsprechend ihrer sicherheitstechnischen Bedeutung sind die Leittechnik-Funktionen auf den Sicherheitsebenen in unterschiedliche Kategorien eingeordnet, für die abgestufte Sicherheitsanforderungen gelten: Kategorie A	519	BfS	<p><u>Begründung zum Kommentar:</u> In den aktuellen Versionen der DIN-IEC Standards zur E-und Leittechnik (z. B. DIN IEC 61513, 60880) wird begrifflich zwischen dem Versagen einer Funktion und dem Ausfall einer Einrichtung unterschieden. <u>Änderungsvorschlag:</u></p>		Entsprechend ihrer sicherheitstechnischen Bedeutung sind die Leittechnik-Funktionen auf den Sicherheitsebenen in unterschiedliche Kategorien eingeordnet, für die abgestufte Sicherheit sa Anforderungen gelten: Kategorie A

Ziffer	Textvorschlag Modul 5/Teil 1 (Rev. A)	Komm. Nr.	Kommentator	Kommentar bzw. Antwort	Ziffer (Neu)	Textvorschlag Modul 5/Teil 1 (Rev. B)
	<p>Die Leitechnik-Funktionen der Kategorie A umfassen alle Funktionen, die erforderlich sind, um Störfälle zu beherrschen sowie das Eintreten von Anlagenzuständen mit Mehrfachversagen von Sicherheitseinrichtungen zu verhindern;</p> <p>Kategorie B Die Leitechnik-Funktionen der Kategorie B umfassen alle Funktionen, die erforderlich sind, um Störungen zu beherrschen sowie das Eintreten von Störfällen zu vermeiden.</p> <p>Kategorie C Die Leitechnik-Funktionen der Kategorie C umfassen alle übrigen Funktionen mit sicherheitstechnischer Bedeutung.</p> <p>Nicht kategorisiert Leitechnik-Funktionen die keine unmittelbare sicherheitstechnische Bedeutung haben.</p>	592	Bandholz / RSK	<p>In Abschn. 2: Statt „Versagen der Sicherheitseinrichtungen“ „<i>Ausfall von Sicherheitseinrichtungen</i>“; bzw. in 3.2 (12) statt „systematisches Versagen“ „<i>systematischer Ausfall</i>“</p> <p>Team 5: Die Begriffe in den Modulen 1 und 5 werden in der Revision B erneuert abgestimmt und notwendige Änderungen (z.B. für Softwareversagen) vorgenommen.</p> <p>Die Formulierung, die im jetzigen Entwurf Revision A steht, dass die Leitechnikfunktionen, auch Funktionen umfassen, die das Eintreten von Anlagenzuständen mit Mehrfachversagen verhindern sollen. Ist das so zu verstehen, dass Sie das Mehrfachversagen von Komponenten darunter fassen? Oder sind das nur Ereignisse, die Sie darunter fassen? Ein ganz konkretes Beispiel, wie wollen Sie durch Leitechnikfunktion der Kategorie A vier Sicherheitseinspeisepumpen daran hindern, auszufallen?</p> <p>Team 5: Aufgrund dieses Kommentars wurde der Nachsatz zum Mehrfachversagen in den Anforderungen zur Kategorie A gestrichen.</p>		<p>Die Leitechnik-Funktionen der Kategorie A umfassen alle Funktionen, die erforderlich sind, um Ereignisse der Sicherheitsebene 3 Störfälle zu beherrschen sowie das Eintreten von Anlagenzuständen mit Mehrfachversagen von Sicherheitseinrichtungen zu verhindern;</p> <p>Kategorie B Die Leitechnik-Funktionen der Kategorie B umfassen alle Funktionen, die erforderlich sind, um Ereignisse der Sicherheitsebene 2 Störungen zu beherrschen sowie das Eintreten von Ereignissen der Sicherheitsebene 3 Störfällen zu vermeiden.</p> <p>Kategorie C Die Leitechnik-Funktionen der Kategorie C umfassen alle übrigen Funktionen mit sicherheitstechnischer Bedeutung.</p> <p>Nicht kategorisiert sind Leitechnik-Funktionen, die keine unmittelbare sicherheitstechnische Bedeutung haben.</p>
		598	VGB Power	<p>In den Kriterien für eine Einstufung von Leitechnik-Funktionen (LEFU) in die Kategorie A wird von LEFU ausgegangen, die das Eintreten von Anlagenzuständen mit Mehrfachversagen von Sicherheitseinrichtungen verhindern. Diese Anlagenzustände sind grundsätzlich auslegungsüberschreitend, d. h. ihnen sind keine LEFU zugeordnet.</p> <p>Team 5: Aufgrund dieses Kommentars wurde der Nachsatz zum Mehrfachversagen in den Anforderungen zur Kategorie A gestrichen.</p>		

Ziffer	Textvorschlag Modul 5/Teil 1 (Rev. A)	Komm. Nr.	Kommen-tator	Kommentar bzw. Antwort	Ziffer (Neu)	Textvorschlag Modul 5/Teil 1 (Rev. B)
Hinweis	Für nicht kategorisierte Leittechnik-Funktionen werden in diesem Modul keine Anforderungen gestellt.				Hinweis	Für leittechnische Einrichtungen , die nicht kategorisierte Leittechnik-Funktionen ausführen , werden im Folgenden in diesem Modul keine Anforderungen gestellt.
3	Auslegung				3	Auslegung
3.1	Leittechnische Einrichtungen für Leittechnik-Funktionen der Kategorien A bis C				3.1	Leittechnische Einrichtungen für Leittechnik-Funktionen der Kategorien A bis C
3.1 (1)	Leittechnische Einrichtungen, die für die Ausführung von Leittechnik-Funktionen in mehreren Kategorien vorgesehen sind, werden nach der Kategorie mit den höchsten Anforderungen geplant, ausgelegt und betrieben.	384	VGB / EnBW	Die Forderung, dass die LEFU mit der höchsten sicherheitstechnischen Bedeutung die Auslegung der Einrichtung bestimmt auf der diese LEFU ausgeführt werden, ist selbstverständlich. Die Betonung liegt aber auf Bedeutung und nicht auf Sicherheits-ebene. Da die leittechnischen Einrichtungen der SE 1 und 2 überwiegend in denselben Einrichtungen realisiert sind, bedeutet das, dass praktisch auch für die gesamte betriebliche Leittechnik die Anforderungen der SE 2 gelten. Team 5: Betrifft Vorläuferversion 2.2 (1). Der Einwand wurde durch die grundsätzliche Überarbeitung des M5 in der REV A u B sinngemäß berücksichtigt. Siehe z.B. Antwort zu 327/RSK „Alle“ zur REV A.	3.1 (1)	Leittechnische Einrichtungen, die für die Ausführung von Leittechnik-Funktionen unterschiedlicher in mehreren Kategorien vorgesehen sind, werden sind nach den Anforderungen der Kategorie mit der höchsten sicherheitstechnischen Bedeutung Anforderungen geplant, ausgelegt und werden nach den Anforderungen dieser Kategorien betrieben.
3.1 (2)	Eine auf ihre Eignung geprüfte oder für den Einsatzfall und für die unterstellten Einsatzbedingungen betriebsbewährte und möglichst wartungsfreie Hardware wird verwendet. Eine auf ihre Eignung geprüfte Software wird eingesetzt.	384	VGB / EnBW	Die RSK-LL erhebt diese Forderung nur für die elektrischen Einrichtungen des Sicherheitssystems und der anderen Systeme mit sicherheitstechnischer Bedeutung und nicht für die elektrischen Einrichtungen des Betriebssystems. Insofern ist hier eine vom Umfang her erhebliche Ausweitung des Regelungsumfangs vorgenommen worden. Team 5: Betrifft Vorläuferversion 2.1 (2). Der Einwand wurde durch die grundsätzliche Überarbeitung des M5 in der REV A sinngemäß berücksichtigt. (s. auch Antwort	3.1 (2)	Eine auf ihre Eignung geprüfte oder für den Einsatzfall und für die unterstellten Einsatzbedingungen betriebsbewährte und möglichst wartungsfreie Hardware wird verwendet ist eingesetzt. Eine auf ihre Eignung geprüfte Software wird ist eingesetzt.

Ziffer	Textvorschlag Modul 5/Teil 1 (Rev. A)	Komm. Nr.	Kommentator	Kommentar bzw. Antwort	Ziffer (Neu)	Textvorschlag Modul 5/Teil 1 (Rev. B)
				zum Kommentar 384 in Abs. 1)		
3.1 (3)	Leitungen und Kabel einschließlich Lichtwellenleiter sind nach Strängen getrennt und, soweit erforderlich, gegen Einwirkungen von innen und außen geschützt verlegt. Leitungen und Kabel zur Signalübertragung und Stromversorgung von redundanten Mess- und Steuereinrichtungen des Sicherheitssystems werden ohne Einschleifen in Warten oder zentrale Rangierverteiler zu den signalverarbeitenden Baugruppen geführt.	384	VGB / EnBW	<p>Die RSK-LL erhebt die ursprüngliche Forderung im Abschnitt 7 und daher nicht für die elektrischen Einrichtungen des Betriebssystems, die im Abschnitt 6 geregelt sind. Insofern ist hier eine vom Umfang her erhebliche Ausweitung des Regelungsumfangs vorgenommen worden. Die Begründung für Ersatz des Begriffs „äußeren Einwirkungen“ durch „übergreifende Einwirkungen“ speziell für LWL ist unverständlich. Was heißt unmittelbar bei einem Bus-System?</p> <p>Team 5: Betrifft Vorläuferversion 2.1 (3). Der Einwand zur Ausweitung des Anwendungsbereichs wurde bereits durch die grundsätzliche Überarbeitung des M5 in der REV A u B sinngemäß berücksichtigt. Siehe z.B. Antwort zu 327/RSK „Alle“ zur REV A. Der Begriff „übergreifende Einwirkungen“ wurde durch die definierten Begriffe Einwirkungen von innen und Einwirkungen von außen ersetzt. Textteil „unmittelbar“ wurde schon in der Rev. A gestrichen.</p>	3.1 (3)	<p>Leitungen und Kabel einschließlich Lichtwellenleiter sind nach Strängen getrennt und, soweit erforderlich, gegen Einwirkungen von innen und außen geschützt verlegt. Leitungen und Kabel zur Signalübertragung und Stromversorgung von redundanten Mess- und Steuereinrichtungen des Sicherheitssystems werden ohne Einschleifen in Warten oder zentrale Rangierverteiler zu den signalverarbeitenden Baugruppen geführt.</p>
		598	VGB Power	<p>Führung von Kabeln und Lichtwellenleitern zu detailliert: „... ohne Einschleifen ...“</p> <p>Team 5: Die Anforderung ist zu detailliert. Zweiter Absatz wird in Rev. B gestrichen und kann hier in der Tat gestrichen werden.</p>		
3.1 (4)	Die leittechnischen Einrichtungen sind so ausgelegt, montiert, abgeschirmt und geschützt, dass durch anlageninterne sowie durch äußere Störquellen, eine unzulässige Beeinflussung der Signale vermieden wird.	384	VGB/EnBW	<p>Verallgemeinerung der ursprünglichen Forderung an Kabel und Leitungen auf alle leittechnischen Einrichtungen und Komponenten stellt eine erhebliche Ausweitung des Regelungsumfangs dar.</p> <p>Team 5: Betrifft Vorläuferversion 2.1 (4). Es ist nicht ausreichend, nur die Kabel und Leitungen gegen Störquellen zu schützen. Aus</p>	3.1 (4)	<p>Die leittechnischen Einrichtungen sind so ausgelegt, montiert, abgeschirmt und geschützt, dass eine unzulässige Beeinflussung der Signale durch anlageninterne sowie durch äußere Störquellen, eine unzulässige Beeinflussung der Signale vermieden wird.</p>

Ziffer	Textvorschlag Modul 5/Teil 1 (Rev. A)	Komm. Nr.	Kommentator	Kommentar bzw. Antwort	Ziffer (Neu)	Textvorschlag Modul 5/Teil 1 (Rev. B)
				diesem Grunde wurde dieser Abschnitt ergänzt.		
3.1 (5)	Es sind Maßnahmen vorgesehen, die es ermöglichen, die Funktionsfähigkeit der leittechnischen Einrichtungen und deren Zusammenwirken mit den aktiven und passiven Komponenten des Sicherheitssystems zu überprüfen und den Zustand dieser sicherheitstechnischen Einrichtungen zu überwachen.	384	VGB / EnBW	Die RSK-LL erhebt diese Forderung nicht für die elektrischen Einrichtungen des Betriebssystems. Insofern ist hier eine vom Umfang her erhebliche Ausweitung des Regelungsumfangs vorgenommen worden. Team 5: Betrifft Vorläuferversion 2.1 (5). Der Einwand zur Ausweitung des Anwendungsbereichs wurde bereits durch die grundsätzliche Überarbeitung des M5 in der REV A u B sinngemäß berücksichtigt. Siehe z.B. Antwort zu 327/RSK „Alle“ zur REV A. Siehe auch Antwort zum Kommentar 384 in Abs. 1.	3.1 (5)	Es sind Maßnahmen und Einrichtungen vorhanden gesehen , die es ermöglichen, die Funktionsfähigkeit der leittechnischen Einrichtungen und ihr deren 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 Systemkomponenten, welche den Funktionsablauf der leittechnischen Einrichtungen mitbestimmen, werden vorzugsweise aus der Prozessvariablen abgeleitet oder unmittelbar am verfahrenstechnischen Stellglied abgegriffen.	384	VGB / EnBW	Für betriebliche Leittechnik sind in RSK-LL 6.1 (2) Anforderungen formuliert, die mit der Forderung nach Vorzug der Prozessvariablen vor Abgriff am Stellglied nicht übereinstimmen. Weiterhin stellen die RSK-LL diese Forderung nur für wichtige Stellungsanzeigen. Die Ausweitung der Forderung auf die gesamte Leittechnik ist unangemessen. Team 5: Betrifft Vorläuferversion 2.1 (6). Der Einwand zur Ausweitung des Anwendungsbereichs wurde bereits durch die grundsätzlich Überarbeitung des M5 in der REV A u. B sinngemäß berücksichtigt. Siehe z. B. Antwort zu 327/RSK „Alle“ zur REV A und Antwort zum Kommentar 384 in Abs. 1.	3.1 (6)	Meldungen von aktiven System k omponenten, welche den Funktionsablauf der leittechnischen Einrichtungen mitbestimmen, werden vorzugsweise aus der Prozessvariablen abgeleitet oder unmittelbar am verfahrenstechnischen Stellglied abgegriffen.
3.1 (7)	Die Funktionsfähigkeit der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorien A und B ausführen, ist unabhängig von Art und Umfang der zeitlichen Änderung ihrer	384	VGB / EnBW	Erweiterung des Geltungsumfangs auf die gesamte Leittechnik der SE 2 und 3. Die Verallgemeinerung der Forderung auf alle Einrichtungen der SE 2 und 3 ist unangemessen.	3.1 (7)	Die Funktionsfähigkeit der Leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorien A und B ausführen, sind so ausgelegt und

Ziffer	Textvorschlag Modul 5/Teil 1 (Rev. A)	Komm. Nr.	Kommentator	Kommentar bzw. Antwort	Ziffer (Neu)	Textvorschlag Modul 5/Teil 1 (Rev. B)
	<p>Eingangssignale gewährleistet.</p> <p>Hinweis: Ein Meldeschwall wird ohne Informationsverlust verarbeitet.</p>	519	BfS	<p>Team 5: Betrifft Vorläuferversion 2.1 (7). In der bestehenden RSK-LL-DWR wird die Forderung für die Sicherheitsleittechnik erhoben. Die Sicherheitsleittechnik umfasst dabei die Leittechnik des Sicherheitssystems und der anderen Systeme mit sicherheitstechnischer Bedeutung. Im Modul 5 wurden die Anforderungen für die Kategorien A und B gestellt. Das Team 5 kann keine Ausweitung des Anwendungsbereichs erkennen.</p> <p><u>Begründung zum Kommentar:</u> Beim Nachweis zur Beherrschung eines Meldeschalles liegt der Schwerpunkt auf den sicherheitsrelevanten Informationen. (Beispiel: Unterdrückung von Mehrfachinformationen infolge eines Fehlers im Informationssystem)</p> <p><u>Änderungsvorschlag:</u> Ein Meldeschwall ist ohne <i>Verlust an Informationen mit Sicherheitsbedeutung</i> zu verarbeiten.</p> <p>Team 5: Im M5 werden nur Anforderungen an Einrichtungen die Funktionen mit sicherheitstechnischer Bedeutung ausführen gestellt, siehe Abschnitt 1 Geltungsbereich (siehe auch Antwort zu 384/VGB). Aufgrund des Kommentars wird der Hinweis umformuliert und in einen Regeltext umgewandelt.</p>		<p>werden so betrieben, dass ihre Funktionsfähigkeit ist unabhängig von Art und Umfang der zeitlichen Änderung ihrer Eingangssignale gewährleistet wird.</p> <p>Hinweis: — Die Meldeanlagen sind so ausgelegt, dass Ein Meldeschwall wird ohne Informationsverlust Verlust sicherheitsrelevanter Informationen verarbeitet wird.</p>
3.1 (8)	Die leittechnischen Einrichtungen sind so ausgelegt bzw. auszulegen, dass notwendige Anpassungen an regelmäßig wiederkehrende Zustände des Normalbetriebs (z. B. Streckbetrieb) einfach und zuverlässig durchgeführt werden können.	384	VGB / EnBW	Erweiterung des Geltungsumfangs auf die gesamte Leittechnik. Die RSK-LL erhebt diese Forderung nur für die Sicherheitsleittechnik und damit weder für die elektrischen Einrichtungen des Sicherheitssystems noch des Betriebssystems. Insofern ist hier eine vom Umfang her erhebliche Ausweitung des Regelungsumfangs vorgenommen worden.	3.1 (8)	Die leittechnischen Einrichtungen sind so ausgelegt bzw. auszulegen , dass notwendige Anpassungen an regelmäßig wiederkehrende Zustände des Normalbetriebs (z.B. Streckbetrieb) einfach und zuverlässig durchführbar sind. geführt werden können.

Ziffer	Textvorschlag Modul 5/Teil 1 (Rev. A)	Komm. Nr.	Kommentator	Kommentar bzw. Antwort	Ziffer (Neu)	Textvorschlag Modul 5/Teil 1 (Rev. B)
				Team 5: Betrifft Vorläuferversion 2.1 (8). Der Einwand wurde durch die Überarbeitung des M5 in der REV A sinngemäß berücksichtigt		
3.1 (9)	Die in der Verfahrenstechnik vorhandene Unabhängigkeit und Fehlertoleranz wird durch leittechnische Einrichtungen nicht beeinträchtigt.				3.1 (9)	Die leittechnischen Einrichtungen sind so ausgelegt, dass die in der Verfahrenstechnik vorhandene Unabhängigkeit und Fehlertoleranz wird durch sie leittechnische Einrichtungen nicht beeinträchtigt werden .
3.1 (10)	Die Störfallfestigkeit der leittechnischen Einrichtungen wird, soweit erforderlich, nachgewiesen.	384	VGB / EnBW	Formale Erweiterung des Geltungsumfangs auf die gesamte Leittechnik Da sich die Forderung auf Störfallfestigkeit bezieht, sind faktisch nur Einrichtungen des Sicherheitssystems betroffen. Team 5: Betrifft Vorläuferversion 2.1 (10). Der Einwand wurde durch die Überarbeitung des M5 in der REV A sinngemäß berücksichtigt, s. auch Antwort zum Kommentar 384 in Abs. 1.	3.1 (10)	Die Störfallfestigkeit der leittechnischen Einrichtungen ist wird , soweit erforderlich, nachgewiesen.
3.1 (11)	Zur Absicherung gegen Bedienungsfehler werden technische Maßnahmen vorrangig vor administrativen vorgesehen.	384	VGB / EnBW	Erweiterung des Geltungsumfangs von den elektrischen Einrichtungen des Sicherheitssystems und den anderen Systemen mit sicherheitstechnischer Bedeutung auf die gesamte Leittechnik. Das ist in dieser allgemeinen Formulierung unangemessen. Team 5: Betrifft Vorläuferversion 2.1 (11). Der Einwand wurde durch die Überarbeitung des M5 in der REV A sinngemäß berücksichtigt, s. auch Antwort zum Kommentar 384 in Abs. 1.	3.1 (11)	Zur Absicherung gegen Bedienungsfehler sind werden technische Vorkehrungen Maßnahmen vorrangig vor organisatorischen Maßnahmen administrativen vorgesehen.
			Team 5	Text wurde aus dem Abs. 9.9 nach 3.1 (12) verschoben.	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 vor-

Ziffer	Textvorschlag Modul 5/Teil 1 (Rev. A)	Komm. Nr.	Kommentator	Kommentar bzw. Antwort	Ziffer (Neu)	Textvorschlag Modul 5/Teil 1 (Rev. B)
						handen sind. Die Eingriffsmöglichkeiten 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.
3.2	Leittechnischen Einrichtungen für Leittechnik-Funktionen der Kategorie A				3.2	Leittechnische Einrichtungen für Leittechnik-Funktionen der Kategorie A
		492	VGB / Powertech	<p>Nicht nur im Modul 5 sondern auch unter 3.2 im Modul 1 werden Anforderungen an leittechnische Einrichtungen formuliert. Dabei wird im Modul 1 von einer Zuordnung von Leittechnischen Einrichtungen zu Sicherheitsebenen (SE) ausgegangen, die nicht sachgerecht ist und im Modul 5 weitgehend vermieden wurde. Beispiel aus Modul 1, 3.2(2): „... muss in der Sicherheitsebene 2 leittechnische Einrichtungen vorsehen ...“</p> <p>Team 5: Modul 1 wurde überarbeitet und an die Kategorisierung im Modul 5 angepasst. (s. auch Antwort zum Kommentar 384 in Abs. 1).</p>		
3.2 (1)	Bei der Auslegung der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, werden versagensauslösende Ereignisse innerhalb und außerhalb des Sicherheitssystems in Betracht gezogen.	384	VGB / EnBW	<p>Nach KTA 3501 zählen Störfälle nicht zu den versagensauslösenden Ereignissen. Ist dieser Verzicht beabsichtigt?</p> <p>Team 5: Betrifft Vorläuferversion 2.2 (1). Aufgrund dieses Kommentars wurde der Text überarbeitet, wobei versagensauslösende Ereignisse im Sinne der KTA 3501 bei der Auslegung zu berücksichtigen sind: Versagensauslösende Ereignisse innerhalb des Reaktorschutzsystems, Versagensauslösende Ereignisse innerhalb der Reaktoranlage.</p>	3.2 (1)	Bei der Auslegung der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, sind werden versagensauslösende Ereignisse innerhalb und außerhalb des Sicherheitssystems berücksichtigt . in Betracht gezogen .

Ziffer	Textvorschlag Modul 5/Teil 1 (Rev. A)	Komm. Nr.	Kommentator	Kommentar bzw. Antwort	Ziffer (Neu)	Textvorschlag Modul 5/Teil 1 (Rev. B)
3.2 (2)	Werden die Bereitschaftsstellungen von Einrichtungen des Sicherheitssystems verändert, so ist sicherzustellen, dass diese Veränderungen nur durchgeführt werden, wenn entsprechende Freigabebedingungen erfüllt sind und dass diese Veränderungen automatisch oder durch betriebstechnische und administrative Maßnahmen wieder aufgehoben werden, wenn die Freigabebedingungen nicht mehr erfüllt sind. In dem sicherheitstechnisch geforderten Zustand werden die Einrichtungen gegen Eingriffe gesichert.	384	VGB / EnBW	Die Streichung des Beispiels trägt nicht zum besseren Verständnis bei. Die Streichung des Begriffs „weitgehend“ ist nicht akzeptabel und entspricht auch nicht, wie behauptet, dem Stand von W&T. Falls damit eine Qualitätsforderung verbunden werden soll, kann „weitgehend“ z. B. durch einen entsprechenden Qualitätsbegriff ersetzt werden. Team 5: Betrifft Vorläuferversion 2.2 (2). Modul 5 stellt an dieser Stelle übergeordnete Anforderungen an die elektrische und leittechnische Einrichtungen des Sicherheitssystems. Auf Anwendung des Adverbs „weitgehend“ kann im Zusammenhang mit dem Schutz gegen Fehleingriff verzichtet werden. Die begründeten Ausnahmen bei der Sicherung bleiben weiterhin möglich.	3.2 (2)	Werden Veränderungen an Bereitschaftsstellungen von Einrichtungen des Sicherheitssystems werden nur dann vorgenommen, wenn entsprechende Freigabebedingungen erfüllt sind und wenn diese Veränderungen automatisch oder durch betriebs technische Vorkehrungen bzw. organisatorische und administrative Maßnahmen wieder aufgehoben werden, wenn die Freigabebedingungen nicht mehr erfüllt sind. In dem sicherheitstechnisch geforderten Zustand sind werden die Einrichtungen gegen Eingriffe gesichert.
		598	VGB Power	Das sind allg. Anforderungen an das Sicherheitssystem bzw. die Betriebsführung des Kraftwerkes, nicht an die leittechnischen Einrichtungen. Das muss an anderer Stelle aufgeführt werden. Team 5: Modul 5 stellt an dieser Stelle übergeordnete Anforderungen an die elektrischen und leittechnischen Einrichtungen. Die Freigabebedingungen können sowohl automatisch als auch administrativ aufgehoben werden. Außerdem ist es u. E. zielführend, an dieser Stelle auch administrative Vorgaben, die zum Kontext gehören, anzuführen.		
3.2 (3)	Soweit bei Einrichtungen des Sicherheitssystems eindeutige Bereitschaftsstellungen von Stellgliedern bei Normalbetrieb vorgeschrieben sind, ist das Verlassen dieser Bereitschaftsstellung zu signalisieren.	384	VGB / EnBW	Soll die Streichung der Einschränkung für Handarmaturen heißen, dass diese eine Stellungserfassung und Signalisierung haben sollen? Bei den vorhandenen Anlagen, bei denen keine Stellungssignalgeber vorhanden sind, kann dies nicht mit vertretba-	3.2 (3)	Sind Soweit bei Einrichtungen des Sicherheitssystems eindeutige Bereitschaftsstellungen von Stellgliedern bei Normalbetrieb vorgeschrieben sind , so wird ist das Verlassen dieser Bereitschaftsstellung zu signalisiert. en-

Ziffer	Textvorschlag Modul 5/Teil 1 (Rev. A)	Komm. Nr.	Kommen-tator	Kommentar bzw. Antwort	Ziffer (Neu)	Textvorschlag Modul 5/Teil 1 (Rev. B)
	Handarmaturen werden in Bereitschaftsstellung möglichst eingriffsicher blockiert.	598	VGB Power	<p>revertretbarem Aufwand gemacht werden. Im Übrigen gilt das ganze nur für TMI- Armaturen.</p> <p>Siehe oben, Regelungen für Handarmaturen gehören nicht hier hin.</p> <p>Team 5: Betrifft Vorläuferversion 2.2 (3). Diese Anforderung wurde auf Grund der RSK/VdTÜV-Kommentierung (327/338) in der Rev. A des Moduls 5 wieder aufgenommen. Es ist u. E. zielführend, an dieser Stelle auch Vorgaben, die zum Kontext gehören, anzuführen.</p>		Handarmaturen sind werden -in Bereit-schaftsstellung möglichst eingriffsicher blockiert.
3.2 (4)	<p>Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, werden zur Sicherstellung ihrer Funktionsfähigkeit zuverlässig ausgelegt. Auch bei Prüfungen, Wartungsarbeiten oder Reparaturen der leittechnischen Einrichtungen, erfüllt das Sicherheitssystem seine Aufgabe mit ausreichender Zuverlässigkeit.</p> <p>a) Die leittechnischen Einrichtungen des Sicherheitssystems werden redundant sowie räumlich getrennt oder durch sicherheitstechnisch gleichwertige Maßnahmen geschützt und elektrisch unabhängig ausgeführt.</p> <p>b) Ein Ausfall in den leittechnischen Einrichtungen des Sicherheitssystems darf nur die Funktion des betroffenen Stranges des Sicherheitssystems beeinträchtigen.</p> <p>c) Die leittechnischen Einrichtungen, die für die Funktionsfähigkeit des Sicherheitssystems nach Eintritt</p>	<p>384</p> <p>592</p>	<p>VGB /. EnBW</p> <p>AREVA/ Dr. Graf (WSI)</p>	<p>In der ursprünglichen Formulierung der RSK-LL ist die Unterscheidung und Abgrenzung der Sicherheitsleittechnik, die im Abschnitt 7.3 definiert wird als die Leittechnik der Kategorien 1 bis 3, von der Leittechnik des Sicherheitssystems (Formulierung im Regeltext: „elektrische Einrichtungen des Sicherheitssystems“) vorgenommen worden. Die Forderungen selbst gelten für beide. Hier ist eine eindeutige Definition erforderlich! Abschnitte c und e werden in diesem Modul nicht geregelt.</p> <p>Team 5: Betrifft Vorläuferversion 2.2 (4). Der Kommentar bezieht sich auf die Formulierung aus dem Modul 5 Rev. 6, die aufgrund von Änderungsvorschläge bereits durch die Rev. A -(s. Abs. 2. Kategorisierung) abgelöst worden ist und in der Revision B (s. Begriffsdefinitionen) präzisiert wird.</p> <p>Im Kapitel „leittechnische Einrichtungen der Kategorie A“ werden zum einen Anforderungen an leittechnische Einrichtungen für Funktion der Kategorie A gestellt, parallel dazu gibt es auch leittechnische Einrichtung-</p>	3.2 (4)	<p>Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, sind werden-zur Sicherstellung ihrer Funktionsfähigkeit zuverlässig ausgelegt. Sie sind so ausgelegt, dass auch bei Instandhaltungsmaßnahmen an diesen Auch bei Prüfungen, Wartungsarbeiten oder Reparaturen der leittechnischen Einrichtungen,erfüllt 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).</p> <p>a) Die leittechnischen Einrichtungen des Sicherheitssystems, die Leittechnikfunktionen der Kategorie A ausführen, werden sind redundant ausgelegt. Sie sind sowie-räumlich getrennt oder durch sicherheitstechnisch gleichwertige Vorkehrungen Maßnahmen-geschützt und</p>

Ziffer	Textvorschlag Modul 5/Teil 1 (Rev. A)	Komm. Nr.	Kommentator	Kommentar bzw. Antwort	Ziffer (Neu)	Textvorschlag Modul 5/Teil 1 (Rev. B)
	von Ereignissen der Sicherheits-ebene 3 erforderlich sind, halten den jeweils ungünstigsten Umgebungs- und Störfallbedingungen stand, die im zugehörigen Aufstellungs- und Installationsbereich vorgegeben sind.	598	VGB Power	<p>gen des Sicherheitssystems. Es werden auch Anforderungen formuliert an leittechnische Einrichtungen des Sicherheitssystems. Für mich ist nicht klar, ist das korrespondierend, das heißt, sind die leittechnischen Einrichtungen des Sicherheitssystems gleichbedeutend mit den leittechnischen Einrichtungen der Kategorie A oder nicht? Dann sollte man es auch gleich benutzen oder es ist bewusst eine Zusatzantwort, dass man sagt, das Sicherheitssystem umfasst Funktionen der Kategorie A, B und C. Das ist ein dramatischer Unterschied und das kommt nicht klar raus.</p> <p>Team 5: In der Revision A wurde die Kategorisierung von Leittechnik-Funktionen eingeführt. Die Begriffe werden in der Revision B unter Berücksichtigung des Kommentars überprüft und angepasst.</p> <p>Der erste Satz ist unpräzise. Was bedeutet „...sind ... zuverlässig auszulegen“?</p> <p>Team 5: Die Anforderungen an die zuverlässige Auslegung sind in den weiteren Sätzen des Abschnitts formuliert.</p>		<p>elektrisch unabhängig ausgeführt.</p> <p>b) Ein Ausfall in den leittechnischen Einrichtungen des Sicherheitssystems darf nur hat höchstens Auswirkungen auf die Funktion des betroffenen Stranges des Sicherheitssystems. beeinträchtigen.</p> <p>c) Die leittechnischen Einrichtungen, die für die Funktionsfähigkeit des Sicherheitssystems nach Eintritt von Ereignissen der Sicherheits-ebene 3 erforderlich sind, halten sind so ausgelegt, dass sie den jeweils ungünstigsten Umgebungs- und Störfallbedingungen standhalten, die im zugehörigen Aufstellungs- und Installationsbereich auf-treten können. vorgegeben sind.</p>
3.2 (5)	Fehlerhaftes Ansteuern des Sicherheitssystems wird unter Berücksichtigung der Ausfallkombinationen nach dem Einzelfehlerkonzept verhindert, wenn dadurch Ereignisse der Sicherheitsebene 4 ausgelöst werden können.	384	VGB / EnBW	<p>RSK-LL 7.3.2 (6) hat weniger mit dem Einzelfehlerkonzept und mehr mit KTA 3501 zu tun. Der Inhalt von RSK-LL 7.3.2 (6) wird unter 2.2 (12) in diesem Modul geregelt.</p> <p>Team 5: Betrifft Vorläuferversion 2.2 (5). Die übergeordnete Anforderung zur Verhinderung der Ereignisse der SE 4 durch fehlerhaftes Ansteuern des Sicherheitssystems hat mit den Auslegungsanforderungen der Fachregeln zu tun. Das EFK wird in Modul 1 eingeführt, in Modul 10 ausgeführt und ist auch im Modul 5 anzuwenden.</p>	3.2 (5)	Die leittechnischen Einrichtungen sind so ausgelegt, dass f ehlerhaftes Ansteuern des Sicherheitssystems wird unter Berücksichtigung der Ausfallkombinationen nach dem Einzelfehlerkonzept verhindert wird , wenn dadurch Ereignisse der Sicherheitsebene 4 ausgelöst werden können.

Ziffer	Textvorschlag Modul 5/Teil 1 (Rev. A)	Komm. Nr.	Kommen-tator	Kommentar bzw. Antwort	Ziffer (Neu)	Textvorschlag Modul 5/Teil 1 (Rev. B)
					Hinweis	Anforderungen 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.
3.2 (6)	<p>Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, werden so ausgelegt, dass Schutzaktionen grundsätzlich automatisch ausgeführt werden.</p> <p>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, werden notwendige Schutzaktionen auch von Hand ausgelöst.</p> <p>Der Richtwert für die Zeitspanne, ab der Handmaßnahmen zulässig sind, beträgt 30 Minuten.</p>	384	VGB / EnBW	<p>Der Text ist weitgehend in Übereinstimmung mit KTA 3501 (und anderen), hat aber mit der angegebenen Quelle nur wenig Übereinstimmung.</p> <p>Team 5: Betrifft Vorläuferversion 2.2(6). In der Revision A wurde die Quelle für die Anforderung korrigiert (S. Dokumentation zur Rev. A). Diese Ziffer deckt die in Modul 1 Revision A enthaltende Ziffer 3.2 (7b) ab, die daher in Revision B von Modul 1 gestrichen wurde.</p>	3.2 (6)	<p>Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, sind werdenso ausgelegt, dass Schutzaktionen grundsätzlich automatisch ausgeführt werden.</p> <p>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, werdendürfen notwendige Schutzaktionen auch von Hand ausgelöst werden.</p> <p>Der Richtwert für die Zeitspanne, ab der Handmaßnahmen zulässig sind, beträgt 30 Minuten.</p>
3.2 (7)	<p>Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, werden grundsätzlich selbstüberwachend ausgelegt. Die Funktionen und Eigenschaften, die von der Selbstüberwachung nicht erfasst sind, werden einer regelmäßigen und lückenlosen Überprüfung unterzogen. Die Prüfzyklen werden auf Grundlage von Zuverlässigkeitsbetrachtungen festgelegt. Diese Prüfungen sollen mittels eingebauter Prüfhilfen leicht durchführbar sein. Prüf-</p>	384	VGB / EnBW	<p>Der Selbstüberwachung wird Vorrang vor Funktionsprüfungen gegeben. Das ist nur für neue digitale Leittechnik selbstverständlich. Für die vorhandenen konventionellen Einrichtungen ist diese Forderung, soweit bei der Auslegung geplant erfüllt. Nachrüstungen sind nicht erforderlich und auch nicht möglich.</p> <p>Team 5: Betrifft Vorläuferversion 2.2(7). Im Modul 5 werden übergeordnete Anforderungen gemäß dem Stand von W&T formuliert,</p>	3.2 (7)	<p>Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, sind werdengrundsätzlich selbstüberwachend ausgelegt. Die Funktionen und Eigenschaften, die von der Selbstüberwachung nicht erfasst sind, werden einer regelmäßigen und lückenlosen Überprüfung unterzogen. Die Prüfzyklen werden sind auf Grundlage von Zuverlässigkeitsbetrachtungen festgelegt. Diese Prüfungen sollen mittels eingebauter</p>

Ziffer	Textvorschlag Modul 5/Teil 1 (Rev. A)	Komm. Nr.	Kommen-tator	Kommentar bzw. Antwort	Ziffer (Neu)	Textvorschlag Modul 5/Teil 1 (Rev. B)
	eingriffe und Handbefehle dürfen notwendige Sicherheitsfunktionen weder verhindern noch die Zuverlässigkeit ihrer Anregung signifikant vermindern.			somit gilt Anforderung generell für LEFU der Kat. A. Der Satz zu den Prüfhilfen lässt sich nicht sinnvoll im Indikativ formulieren und wird deshalb gestrichen.		Prüfhilfen leicht durchführbar sein. Prüfeingriffe und Handbefehle dürfen sind so festgelegt, dass notwendige Sicherheitsfunktionen weder verhindert a werden noch die Zuverlässigkeit ihrer Anregung signifikant vermindert wird a .
					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 Anlagen-teilen, Systemen und Komponenten“ (Modul 10) Abschnitt 1.4.
3.2 (8)	Die Selbstüberwachung darf die Funktion der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, nicht beeinträchtigen. Es ist sicherzustellen, dass eine gleichzeitige Prüfung redundanter leittechnischen Einrichtungen verhindert wird. Der Abschnitt 3.2 (5) ist anzuwenden.	598	VGB Power	Der zweite und dritte Satz ("Es ist sicherzustellen... .. ist anzuwenden") bezieht sich auf Prüfungen (3.2(7)), nicht auf Selbstüberwachung wie der vorhergehende Satz. Team 5: Der entsprechende Textabschnitt wird für regelmäßige Überprüfungen präzisiert.	3.2 (8)	Die Selbstüberwachung ist so ausgelegt, dass sie darf die Funktion der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, nicht beeinträchtigen. Die regelmäßigen Überprüfungen nach Ziffer 3.2 (7) werden so geplant und werden so durchgeführt, Es ist sicherzustellen, dass eine gleichzeitige Prüfung redundanter leittechnischer Einrichtungen nicht stattfindet. verhin- dert wird. Der Abschnitt 3.2 (5) ist anzuwenden.
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 Maßnahmen der Sicherheitsebenen 1 oder 2 eingesetzt werden, sind die zugehörigen leittechnischen Einrichtungen so ausgelegt, dass die geforderte Zuverlässigkeit der Einrichtungen, die Leittechnik-Funktionen	513	AREVA	Unklare Anforderungen Absatz 3.2 (9) < - > Absatz 6(5) Welche Unabhängigkeit wird gefordert? Unabhängigkeit der Sicherheitsebenen ist wichtig, nicht aber Unabhängigkeit zwischen Funktionen verschiedener Kategorien. Team 5: Durch die Einführung von Kategorien in der Revision A des Moduls 5 wurde der Kommentar sinngemäß berücksichtigt.	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 Maßnahmen der Sicherheitsebenen 1 oder 2 eingesetzt werden, sind die zugehörigen leittechnischen Einrichtungen so ausgelegt, dass die geforderte Zuverlässigkeit

Ziffer	Textvorschlag Modul 5/Teil 1 (Rev. A)	Komm. Nr.	Kommentator	Kommentar bzw. Antwort	Ziffer (Neu)	Textvorschlag Modul 5/Teil 1 (Rev. B)
	der Kategorie A ausführen, nicht beeinträchtigt wird.					der Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, nicht beeinträchtigt wird.
3.2 (10)	Der Aufbau der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, soll einfach sein. Erforderliche Nachweise zur Qualifizierung der leittechnischen Einrichtungen des Sicherheitssystems werden dadurch zuverlässig möglich.	384	VGB / EnBW	<p>Diese Streichung ist missverständlich. Die Forderung gilt nur für das Reaktorschutzsystem. Das Reaktorschutzsystem ist aber nicht die Leittechnik des Sicherheitssystems. Dieser Begriff muss in diesem Modul genau so definiert werden wie der Begriff „Sicherheitsleittechnik der Kategorie 1“ in den zitierten RSK-LL. Bei Gleichsetzung ist die Forderung für die vorhandenen Anlagen kaum erfüllbar.</p> <p>Team 5: Betrifft Vorläuferversion 2.2(10). Der Kommentar bezieht sich auf die Formulierung aus dem Modul 5 Rev. 6, die aufgrund von Änderungsvorschläge bereits durch die Rev. A (s. Abs. 2. Kategorisierung) abgelöst worden ist und in der Revision B (s. Begriffsdefinitionen) präzisiert wird. Der 2. Satz wurde in den Anforderungstext integriert.</p>	3.2 (10)	<p>Es ist das Ziel, den Aufbau der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, so einfach zu gestalten sein, dass die Erforderliche erforderlichen Nachweise zur Qualifizierung der leittechnischen Einrichtungen des Sicherheitssystems werden dadurch zuverlässig möglich sind.</p>
		538	UM / BW	<p>Bezüglich der Qualifizierung von Einrichtungen des Sicherheitssystems, die Leittechnikfunktionen der Kategorie A betreffen, ist festzustellen, dass Zuverlässigkeitsnachweise für Software vergleichbar mit Hardwarenachweisen insbesondere mit probabilistischen Methoden nach heutigem Stand nicht machbar sind. Es gibt dafür bisher nach hiesigen Erkenntnissen kein anerkanntes Verfahren.</p> <p>Team 5: Der Kommentar lässt keinen eindeutigen Bezug zum Anforderungstext zu. Wir stimmen zu, dass es z. Z. keine anerkannten Methoden zur probabilistischen Zuverlässigkeitsbewertung der Software gibt. Trotzdem ist es im konkreten Fall erforder-</p>		

Ziffer	Textvorschlag Modul 5/Teil 1 (Rev. A)	Komm. Nr.	Kommentator	Kommentar bzw. Antwort	Ziffer (Neu)	Textvorschlag Modul 5/Teil 1 (Rev. B)
				lich, die Zuverlässigkeit der Nachweisführung zu fordern.		
3.2 (11)	Bei der Auslegung der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, sind Vorkehrungen gegen systematische Ausfälle der Hardware und Versagen der Software getroffen worden.	384	VGB / EnBW	Kommentar wie vorstehend. Der Text deutet auf eine Gleichsetzung von Reaktorschutzesystem mit leittechnischen Einrichtungen des Sicherheitssystems hin. Falls das nicht gemeint ist, bedeutet diese Forderung eine massive Verschärfung und ist kaum erfüllbar. Team 5: Betrifft Vorläuferversion 2.2 (11). Der Kommentar bezieht sich auf die Formulierung aus dem Modul 5 Rev. 6, die aufgrund von Änderungsvorschläge bereits durch die Rev. A (s. Abs. 2. Kategorisierung) abgelöst worden ist und in der Revision B (s. Begriffsdefinitionen) präzisiert wird.	3.2 (11)	Bei der Auslegung der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, werden den sind Vorkehrungen gegen systematische Ausfälle der Hardware und Versagen der Software derart getroffen-, dass ein systematischer Ausfall so unwahrscheinlich ist, dass er ausgeschlossen werden kann.
		538	UM / BW	Die verwendeten Begriffe sollten einheitlich verwendet werden und eindeutig definiert sein. So ist z. B. der Begriff „Softwareversagen“ in Teil 1, 3.2 (11) unklar und nicht gebräuchlich. Definitionsketten sollten nach Möglichkeit vermieden werden. Team 5: Die Begriffe in allen Modulen werden in der Revision B erneut abgestimmt und die Begriffeliste aufgenommen (u.a. Begriff „Versagen“, „Softwareversagen“. Siehe auch Antwort auf Kommentar 519 im Vorspann.		
3.2 (12)	Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, werden so ausgelegt, dass ein systematischer Ausfall so unwahrscheinlich ist, dass er ausgeschlossen werden kann. Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, erfüllen ihre Aufgaben auch	384	VGB / EnBW	Kommentar zur Gleichsetzung der Sicherheitsleittechnik der Kategorie 1 mit der Leittechnik des Sicherheitssystems wie vorstehend. Team 5: Betrifft Vorläuferversion 2.2(12). Der Satz „Ein systematischer Ausfall...“ wurde gestrichen, da er in der Indikativfassung inhaltlich durch den 1. Satz von 3.2	3.2 (12)	Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, werden so ausgelegt, dass ein systematischer Ausfall so unwahrscheinlich ist, dass er ausgeschlossen werden kann. Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, sind so ausgelegt, dass

Ziffer	Textvorschlag Modul 5/Teil 1 (Rev. A)	Komm. Nr.	Kommentator	Kommentar bzw. Antwort	Ziffer (Neu)	Textvorschlag Modul 5/Teil 1 (Rev. B)
	<p>dann, wenn zusätzlich zu einem Ereignis der Sicherheitsebene 3 ein Zufallsausfall und ein systematisches Versagen (systematisches Versagen der Hardware oder Versagen der Software) und Folgeausfälle eintreten.</p> <p>Ein systematisches Versagen wird dabei nicht angenommen, wenn ausreichende Maßnahmen zu seiner Vermeidung nachgewiesen sind.</p> <p>Während eines Instandhaltungsfalls wird auch ein Ereignis der Sicherheitsebene 3 unterstellt. Dabei brauchen innerhalb einer Zeitspanne von 100 h das systematische Versagen und der Zufallsausfall nicht unterstellt werden.</p>	519	BfS	<p>(12) abgedeckt ist. Der Kommentar bezieht sich auf die Formulierung aus dem Modul 5 Rev. 6, die aufgrund von Änderungsvorschläge bereits durch die Rev. A (s. Abs. 2. Kategorisierung) abgelöst worden ist und in der Revision B (s. Begriffsdefinitionen) präzisiert wird.</p> <p><u>Begründung zum Kommentar:</u> In den aktuellen Versionen der DIN-IEC Standards zur E-und Leittechnik (z.B. DIN IEC 61513, 60880) wird begrifflich zwischen dem Versagen einer Funktion und dem Ausfall einer Einrichtung unterschieden.</p> <p><u>Änderungsvorschlag:</u> In Abschn. 2: Statt „Versagen der Sicherheitseinrichtungen“ „Ausfall von Sicherheitseinrichtungen“; bzw. in 3.2 (12) statt „systematisches Versagen“ „systematischer Ausfall“</p> <p><u>Begründung zum Kommentar:</u> Es sind hier zwei Postulate zugleich zu erfüllen:</p> <ul style="list-style-type: none"> – Eine Leittechnikfunktion der Kategorie A darf nicht total *) versagen; dies ist notwendigerweise nachzuweisen. – Der systematische Ausfall von rechnergestützten Leittechnikeneinrichtungen infolge eines Software-Fehlers ist zu unterstellen, weil die Fehlerfreiheit von Software praktisch nicht nachgewiesen werden kann. <p>*) Die Spezifikation einer Leittechnikfunktion umfasst neben der Nutzfunktion (anforderungsgerechtes Verhalten) auch unverzichtbare Zusatzfunktionen wie Selbstüberwachung und sicheres Ausfallverhalten. Bei einem Totalversagen wären auch diese Zusatzfunktionen nicht mehr verfügbar. Außerdem kann die Nutzfunktion von mehreren Teilsystemen parallel ausgeführt werden.</p>		<p>sie erfüllen ihre Aufgaben auch dann erfüllen, wenn im Anforderungsfall zusätzlich zu einem Ereignis der Sicherheitsebene 3 ein Zufallsausfall (gemäß Einzelfehlerkonzept) und ein systematischer Ausfall Versagen (systematischer Ausfall Versagen der Hardware oder Versagen der Software) und daraus resultierende Folgeausfälle eintreten. Ein systematisches Versagen wird dabei nicht angenommen, wenn ausreichende Maßnahmen zu seiner Vermeidung nachgewiesen sind. Während eines Instandhaltungsfalls wird im Anforderungsfall auch ein Ereignis der Sicherheitsebene 3 unterstellt. Dabei werden innerhalb einer Zeitspanne von 100 h das gleichzeitige Auftreten des systematischen Versagen Ausfalls und des Zufallsausfalls nicht unterstellt.</p>

Ziffer	Textvorschlag Modul 5/Teil 1 (Rev. A)	Komm. Nr.	Kommen-tator	Kommentar bzw. Antwort	Ziffer (Neu)	Textvorschlag Modul 5/Teil 1 (Rev. B)
				<p>den. Die Leittechnikfunktion versagt dann total, wenn alle Teilsysteme ausfallen. Dies kann durch Diversifizierung auf Funktions-ebene oder – eingeschränkt - auf Leittechnik-ebene (Hardware/Software) verhindert werden.</p> <p><u>Änderungsvorschlag:</u> <i>Die Leittechnikfunktionen der Kategorie A sind durch leittechnische Einrichtungen der- art auszuführen, dass ein Totalversagen ausgeschlossen werden kann.</i> Die leittechnischen Einrichtungen, die Funktionen der Kategorie A ausführen, müssen ihre Aufgaben auch dann ausführen, wenn zusätzlich zu einem Ereignis der Sicherheitsebene 3 ein Zufallsausfall und ein systematisches Versagen <i>systematischer Ausfall</i> (systematischer Ausfall der Hardware oder <i>Wirksamwerden eines Software-Fehlers</i>) und Folgeausfälle eintreten. Ein systematischer Ausfall der Hardware braucht nicht angenommen zu werden, wenn ausreichende Maßnahmen zu seiner Vermeidung nachgewiesen sind. von 100 h das systematische Versagen <i>der systematische Ausfall</i></p> <p>Team 5: Die Begriffe in allen Modulen werden in der Revision B erneut abgestimmt und die Begriffeliste aufgenommen (u.a. Begriffe „Ausfall“, „Versagen“, „Softwareversagen“). Der Begriff „Totalausfall“ in Bezug auf leittechnische Einrichtungen wird nicht in die Formulierung aufgenommen.</p>		
		513	AREVA /	<p>Unklare Anforderungen: Ausschluss des systematischen Ausfalls aber Beherrschung systematischen Versagens !!!! Widerspruch?</p> <p>Team 5: Die Anforderung wird modifiziert.</p>		

Ziffer	Textvorschlag Modul 5/Teil 1 (Rev. A)	Komm. Nr.	Kommentator	Kommentar bzw. Antwort	Ziffer (Neu)	Textvorschlag Modul 5/Teil 1 (Rev. B)
		598	VGB Power	Die Ausfallkombinationen sind missverständlich und in der KTA 3501 klar dargestellt. Die Wirkungsweise des elektrischen Schutzes (grundsätzlich in 1 von 1; immer Vorrang vor Reaktorschutz) ist hier nicht ausreichend berücksichtigt. Team 5: Die Anforderung wird modifiziert. Die Anforderung gilt für die leittechnische Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen. Die Wechselwirkung mit dem elektrischen Schutz wird in den anderen Abschnitten des Moduls 5 (u. a. 13 (2), 13 (3)) geregelt.		
3.2 (13)	Einrichtungen des Aggregateschutzes werden so ausgelegt, dass bei Anforderung eines Aggregats durch die leittechnischen Einrichtungen des Sicherheitssystems der Aggregateschutz grundsätzlich nicht wirksam wird. Dies darf nicht erfolgen, wenn hierdurch Folgeschäden verursacht werden können, die die Sicherheit der Reaktoranlage mehr beeinträchtigen als der Ausfall des Aggregats. Der Vorrang der Leittechnik-Funktionen der Kategorie A vor dem Aggregateschutz wird durch die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, sichergestellt. 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	384	VGB / EnBW	Die Forderungen entsprechen inhaltlich der KTA- Regel 3501 gelten da aber nur für die Ansteuerung von Aggregaten durch das Reaktorschutzsystem. Team 5: Betrifft Vorläuferversion 2.2(13). Die Anforderung regelt Wechselwirkung zwischen leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen (Reaktorschutz), und dem Aggregateschutz.	3.2 (13)	Einrichtungen des Aggregateschutzes sind werden 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 –Dies darf nicht erfolgen, wenn hierdurch Folgeschäden verursacht werden können, die beeinträchtigen die Sicherheit der Reaktora Anlage mehr beeinträchtigen als der Ausfall des Aggregats. Der Vorrang der Leittechnik-Funktionen der Kategorie A vor dem Aggregateschutz wird durch die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, sichergestellt. Der Aggregateschutz ist so ausgelegt, dass der Vorrang der Leittechnik-Funktionen der Kategorie A vor dem Aggregateschutz sichergestellt ist. Ist im Aggregateschutz ein Vorrang
		513	AREVA	Unklare Anforderungen: Anforderungen der Kategorie A an Aggregateschutz und Redundanzforderung nach 6(1) !!! Widerspruch? Team 5: Die Anforderungen an Aggregateschutz sind abgestuft formuliert, so dass unmittelbar eine Redundanzanforderung abzuleiten ist (s. insbesondere den ersten und letzten Satz).		
		592	AREVA Dr. Graf	Ich habe noch eine Frage zu der jetzigen Formulierung, wie sie existiert. Die ist ja geändert worden. Ich bin mir immer noch nicht		

Ziffer	Textvorschlag Modul 5/Teil 1 (Rev. A)	Komm. Nr.	Kommen-tator	Kommentar bzw. Antwort	Ziffer (Neu)	Textvorschlag Modul 5/Teil 1 (Rev. B)
	die Einrichtungen des Aggregateschutzes werden nicht gestellt, wenn nachgewiesen wird, dass Fehler so unwahrscheinlich sind, dass eine dadurch verursachte Fehlauslösung nicht betrachtet werden braucht.			<p>ganz klar, ob das, was jetzt da steht, wirklich gewollt ist. Ich habe gesehen, dass jetzt in der neuen Formulierung zu dem Aggregateschutz einfach auf die Kategorie A der Leittechnik verwiesen wird. Also gleiche Anforderung der Leittechnik auch für den Aggregateschutz. Jetzt habe ich dazu das Problem, oder die Fragestellung, der Aggregateschutz ist normalerweise schon Komponenten zugeordnet, das heißt, wenn man vier maschinentechnische Systeme hat, hat jedes System seinen eigenen Aggregateschutz. Wenn ich jetzt die Kategorie A Anforderung an den Aggregateschutz reflektiere, dann heißt das, ich würde eine vierfache Redundanz für den Aggregateschutz einer einzelnen Komponente fordern, man könnte es so interpretieren. Ist das gewollt oder nicht gewollt?</p> <p>Team 5: Siehe Antwort auf Nr. 513</p>		<p>vor Leittechnik-Funktionen der Kategorie A notwendig, werden an den Aggregateschutz die Anforderungen der Kategorie A gestellt.</p> <p>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. nicht betrachtet werden braucht.</p>
		592	TÜV / ET / BW Hr. Weich	<p>Was mir nicht ganz klar ist, wenn Sie die Anforderung der Kategorie A reflektieren, heißt das ja auch räumliche Trennung. Das gilt natürlich für Aggregateschutz eigentlich nie, denn die räumliche Trennung kriegen Sie innerhalb des Aggregateschutzes nicht hin. Wenn Sie das nicht ändern hier, dann ist die Befürchtung natürlich da, dass man in Zukunft etwas interpretieren könnte, dass die räumliche Trennungsanforderung aus der Kategorie A auch im Aggregateschutz einzuhalten ist. Das müsste schon nochmal deutlich gestellt werden. Man müsste hier klar unterscheiden zwischen dem Aggregateschutz, wie er z. B. bei Dieselaggregaten aufgebaut wird, wo man leittechnische Funktionen beispielsweise „Überdrehzahl“ hat, die man dann 2- oder 3-kanalig aufbaut. Da zielt ja wohl Ihre Formulierung hin und das denke ich, ist auch in Ordnung. Sie</p>		

Ziffer	Textvorschlag Modul 5/Teil 1 (Rev. A)	Komm. Nr.	Kommen-tator	Kommentar bzw. Antwort	Ziffer (Neu)	Textvorschlag Modul 5/Teil 1 (Rev. B)
				<p>muss dann so hochwertig sein, dass die Schutzaktion selber nicht infrage gestellt wird. Man muss natürlich auch andererseits die vorhin angesprochenen starkstromtechnischen Schutzeinrichtungen sehen, die also 1-kanalig sind und wo der Nachweis, dass sie also so hochwertig sind, wahrscheinlich nicht immer geführt werden kann. Wenn man in diese Richtung etwas differenzieren könnte, denke ich, dann würde das nichts Neues bringen.</p> <p>Team 5: siehe Antwort auf Nr. 513, 384.</p>		
		592	RSK / Hr. Steckenborn	<p>Wenn man reinschreiben würde, dass das System, was jetzt geschützt wird, in der Verfügbarkeit nicht wesentlich beeinträchtigt wird, dann wäre das etwas, da könnten alle mit leben.</p> <p>Team 5: Siehe Antwort auf Nr. 513, 384, bezüglich Verfügbarkeit siehe insbesondere den 1. Satz.</p>		
3.2 (14)	Die leittechnischen Einrichtungen bestimmen nicht die Unverfügbarkeit des Sicherheitssystems.	384	VGB / EnBW	<p>Die Ausweitung der Forderung von der Sicherheitsleittechnik auf die gesamte Leittechnik ist unverständlich. Bisher war das eine Auslegungsanforderung an das Reaktorschutzsystem (s. auch 4.9 (1) aus KTA-3501). Soll damit eine inhaltliche Änderung erreicht werden?</p> <p>Team 5: Betrifft Vorläuferversion 2.2(14). Der Einwand zur Ausweitung des Anwendungsbereichs wurde bereits durch die grundsätzliche Überarbeitung des M5 in der REV A u B sinngemäß berücksichtigt. Siehe z.B. Antwort zu 327/RSK „Alle“ zur REV A</p>	3.2 (14)	Die leittechnischen Einrichtungen sind so ausgelegt, dass sie bestimmen nicht die Unverfügbarkeit des Sicherheitssystems nicht bestimmen .
			Team 5	Text wurde im Modul 1, Abs. 3.2 (7c) gestrichen und inhaltlich nach Modul 5, Abs. 3.2 (15) verlagert.	3.2 (15)	In den Betriebsphasen, in denen die Verfügbarkeit der Reaktorschnellabschaltung erforderlich ist, ist jederzeit

Ziffer	Textvorschlag Modul 5/Teil 1 (Rev. A)	Komm. Nr.	Kommen-tator	Kommentar bzw. Antwort	Ziffer (Neu)	Textvorschlag Modul 5/Teil 1 (Rev. B)
						eine Die -Reaktorschnellabschaltung kann jederzeit von Hand möglich. ausgelöst werden.
			Team 5	Text wurde im Modul 1, Abs. 3.2 (7d) gestrichen und vollständig nach Modul 5, Abs. 3.2 (16) verlagert.	3.2 (16)	In Betriebsphasen außerhalb der Betriebsphasen A und B, in denen Teile von Leittechnikfunktionen 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.
			Team 5	Text wurde im Modul 1, Abs. 3.2 (12) gestrichen und nach Modul 5, Abs. 3.2 (17) verlagert.	3.2 (17)	Die leittechnischen Einrichtungen, die Leittechnikfunktionen der Kategorie A ausführen, sind so ausgelegt, dass auch beim Auftreten von Fehlern in diesen Einrichtungen keine Aktionen ausgelöst werden, die die Anlage in einen Störfall überführen können.
			Team 5	Diese Anforderung wird in der Rev. B aus dem Abs. 9 (5) nach Abs. 3.2 (18) verschoben.	3.2 (18)	Die Anregekriterien für Leittechnik-Funktionen der Kategorie A und die dadurch ausgelösten Schutzaktionen und Maßnahmen werden in der Warte übersichtlich angezeigt.
			Team 5	Diese Anforderung wird in der Rev. B aus dem Abs. 9 (6) nach Abs. 3.2 (19) verschoben.	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				3.3	Leittechnische Einrichtungen für Leittechnik-Funktionen der Kategorie B
	Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie B	384	VGB / EnBW	Ungeeignete Gleichsetzung der Sicherheitsleittechnik der Kategorie 2. mit der Sicher-		Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie

Ziffer	Textvorschlag Modul 5/Teil 1 (Rev. A)	Komm. Nr.	Kommen-tator	Kommentar bzw. Antwort	Ziffer (Neu)	Textvorschlag Modul 5/Teil 1 (Rev. B)
	<p>ausführen, erfüllen ihre Aufgaben auch dann, wenn zusätzlich zu einem Ereignis der Sicherheitsebene 2 ein Zufallsausfall und Folgeausfälle eintreten.</p> <p>Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie B ausführen und deren Versagen Ereignisse auslöst, die nicht durch Maßnahmen und Einrichtungen der Sicherheitsebene 3 beherrscht werden, werden nach den Anforderungen der Kategorie A ausgelegt und geprüft.</p>			<p>heitsebene 2. s. auch Kommentar zu 13.1. Die neu aufgenommene Textpassage wird erst durch die Erläuterung verständlich, nach der Zustandsbegrenzungen die Randbedingungen zur Beherrschung von Ereignissen der SE 3 sicherstellen. Damit wird implizit die Forderung erhoben, Zustandsbegrenzungen nach Kriterien des Reaktorschutzes auszulegen, sofern sie ausfallen können. Das ist weder angemessen noch nach KTA 3501 nötig. Wegen der hohen Zuverlässigkeit, die durch Auslegung nach Kapitel 7 der KTA 3501 erreicht wird, braucht der gleichzeitige Ausfall der Zustandsbegrenzung und der Störfall für dessen Beherrschung die Randbedingungen sichergestellt werden sollen nicht unterstellt zu werden. Die hier gestellte Forderung entspricht weder den bisherigen RSK-LL, dem KTA- Regelwerk noch dem internationalen IEC- Regelwerk.</p> <p>Team 5: Betrifft Vorläuferversion 2.3. In dieser Anforderung wurde für die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie B ausführen, der Konzept der Sicherheitsebenen umgesetzt und wird Revision B unter Berücksichtigung des Kommentars präzisiert.</p>		<p>B ausführen, sind so ausgelegt, dass sie erfüllen ihre Aufgaben auch dann erfüllen, wenn im Anforderungsfall zusätzlich zu einem Ereignis der Sicherheitsebene 2 ein Zufallsausfall und daraus resultierende Folgeausfälle eintreten.</p> <p>Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie B ausführen und deren Wirksamkeit für die Störfallbeherrschung erforderlich ist, Versagen Ereignisse auslöst, die nicht durch Maßnahmen und Einrichtungen der Sicherheitsebene 3 beherrscht werden, werden sind nach den Anforderungen der Kategorie A ausgelegt und werden dementsprechend geprüft.</p>
		515	TÜV-Süd	<p>Der Text in der Fassung der Rev. A, wird dem gestaffelten Sicherheitskonzept gemäß Modul 1 nicht gerecht und sollte wie folgt abgeändert werden:</p> <p><u>Den leittechnischen Einrichtungen, die Leittechnikfunktionen der Kategorie B ausführen und deren Versagen Störfälle der Sicherheitsebene 3 auslösen können, sind zur Vermeidung eines Störfalls Leittechnikfunktionen der Kategorie A zu überlagern.</u></p>		

Ziffer	Textvorschlag Modul 5/Teil 1 (Rev. A)	Komm. Nr.	Kommen-tator	Kommentar bzw. Antwort	Ziffer (Neu)	Textvorschlag Modul 5/Teil 1 (Rev. B)
				<p><u>Begründung:</u></p> <p>Wenn Funktionen der Kategorie B (Sicherheitsebene 2) das Potenzial haben, bei einem aktiven Versagen, einen Störfall der Ebene 3 zu initiieren, so muss eine Funktion der Kategorie A vorhanden sein, die das durch das Versagen betätigte Stellglied wieder in den sicheren Zustand überführt; d. h. in der Lage ist, den initiierten Störfall zu <u>verhindern</u>. Es muss hier der Grundsatz gelten, dass technische Einrichtungen einer niedrigen Sicherheitsebene niemals einen Störfall produzieren dürfen. Darüber hinaus sind auslegungsgemäß auch Funktionen der Kategorie A für andere Störfallszenarien vorhanden, um den Störfall selbst zu <u>beherrschen</u>. Im Sinne des defence-in-depth-Prinzips muss aber für Funktionen der Kategorie B mit dem Potenzial für die Auslösung eines Störfalls immer eine Kategorie-A- Funktion zur <u>Verhinderung</u> eines aktiven Versagens einer Kategorie-B-Funktion vorhanden sein. Diesem Aspekt wird der Text in der vorliegenden Fassung, Rev. A, nicht gerecht.</p> <p>Beispielhaft für ein derartiges mögliches Ereignis bzw. Versagen möchten wir das fehlerhafte Öffnen oder Offenbleiben des Abblasestranges am Druckhalter von DWR-Anlagen anführen. Ein derartiges Versagen könnte durch ein aktives Versagen (fehlerhafter AUF-Befehl aufgrund eines systematischen Fehlers) in den Begrenzungseinrichtungen (Kategorie-B-Funktionen) hervorgerufen werden. Ein derartiges Ereignis führt, ohne Maßnahmen zum Schließen des Abblasestranges (Störfallvermeidung) zu einem kleinen Leck. Gemäß den vorstehenden genannten Grundsätzen ist daher bei einem Offenbleiben bzw. fehlerhaften Öffnen des Abblasestranges am Druckhalter</p>		

Ziffer	Textvorschlag Modul 5/Teil 1 (Rev. A)	Komm. Nr.	Kommen-tator	Kommentar bzw. Antwort	Ziffer (Neu)	Textvorschlag Modul 5/Teil 1 (Rev. B)
				<p>durch eine Kategorie-A-Funktion das sichere Schließen des Abblasestranges sicherzustellen, um den Störfall „kleines Leck“ zu vermeiden. Eine Realisierung dieser Maßnahmen mit Funktionen der Kategorie B würde den Anforderungen nicht gerecht werden, da Kategorie-B-Funktionen nicht gegen den systematischen Fehler ausgelegt werden. Sollten die Absperrmaßnahmen (Störfall-vermeidung) versagen, müssen die Maßnahmen zur Störfallbeherrschung wirksam werden.</p> <p>Im Übrigen möchten wir anmerken, dass bis Ende der 70'er Jahre das Schließen des Druckhalte-rabblasestranges Bestandteil der Reaktorschutzmaßnahme „Primärkreisabschluss“ (KWB B YZ 37, KKG YZ 43) war. Aus auslegungstechnischen Gründen wurde die Teilfunktion „Druckhalterabblaseventil Schließen“ in die Kühlmitteldruckbegrenzung (KMD-Begrenzung) integriert, die alle Anforderungen für Funktionen des Reaktorschutzsystems (Kategorie A) ebenfalls erfüllt (Aufbau in Iskamatic A und B).</p> <p>Bezüglich der Eintrittswahrscheinlichkeit eines Ereignisses „kleines Leck“ verweisen wir auf die internationale Bewertungsskala für bedeutsame Ereignisse in kerntechnischen Einrichtungen (INES). Danach gehört ein „kleines Leck“ zu den möglichen Ereignissen, für die eine Häufigkeit des Auftretens von $3 \cdot 10^{-2}$ bis $3 \cdot 10^{-4}$ pro Jahr angenommen wird. Durch die Auslegung von Funktionen, die das Potenzial zur Auslösung dieses Ereignisses und eine Zuverlässigkeit haben, die geringer als für Kategorie-A-Funktionen ist, kann die Annahme für eine so geringe Häufigkeit nicht aufrecht erhalten werden.</p> <p>Team 5: Dem Kommentar wird inhaltlich</p>		

Ziffer	Textvorschlag Modul 5/Teil 1 (Rev. A)	Komm. Nr.	Kommen-tator	Kommentar bzw. Antwort	Ziffer (Neu)	Textvorschlag Modul 5/Teil 1 (Rev. B)
				hinsichtlich der Umsetzung des defence-in-depth Konzepts zugestimmt. Der betroffene 2. Absatz wird gestrichen. Die entsprechende Vorsorge und die damit verbundenen Anforderungen sind über die zu beherrschenden Ereignissen bzw. die grundlegenden Auslegungsanforderungen formuliert. ##		
		592	TÜV Süd / Hr. Kaminski	<p>Eine Anmerkung zu den leittechnischen Einrichtungen der Sicherheitsebene 2 unter dem Punkt 3.3 wird ausgeführt, „dass die leittechnischen Einrichtungen, die Leittechnikfunktionen der Kategorie B ausführen und deren Versagen Ereignisse auslöst, die nicht durch Maßnahmen der Einrichtung der Sicherheitsebene 3 beherrscht werden, nach den Anforderungen der Kategorie A auszulegen und zu prüfen sind.“</p> <p>Ich sehe hier gewissen philosophischen Widerspruch, weil das „defence in-depth“-Prinzip, dass wir ja philosophisch bearbeiten, auf der einen Seite sagt, wenn ich ein Ereignis auf einer niedrigeren Ebene auslösen kann, das in die nächsthöhere reicht, dann muss ich erst einmal Maßnahmen zur Vermeidung vorsehen, die in der gleichen Ebene mit einer, aber höheren Zuverlässigkeit gemacht werden müssen, und ich muss dann immer noch eine Maßnahme zur Beherrschung in der Sicherheitsebene 3 haben. Auf die kann ich nicht verzichten, weil sonst ist das ganze System in sich nicht konsistent. Daher ist, aus meiner Sicht, dieser Satz „die nicht durch Maßnahmen und Einrichtungen der Sicherheitsebene 3 beherrscht werden“ nicht richtig an dieser Stelle. Das kann ich nicht machen, ich muss immer etwas auf der Ebene 3 haben, was diesen Störfall beherrscht.</p> <p>Wir haben ja hier, das Versagen einer Leittechnikfunktion der Sicherheitsebene 2 un-</p>		

Ziffer	Textvorschlag Modul 5/Teil 1 (Rev. A)	Komm. Nr.	Kommen-tator	Kommentar bzw. Antwort	Ziffer (Neu)	Textvorschlag Modul 5/Teil 1 (Rev. B)
				<p>terstellt. Was ja auch möglich ist. Dann müssen wir erst mal Maßnahmen zur Vermeidung haben, die auch in der gleichen Ebene sind, nur mit einer höheren Zuverlässigkeit und das steht ja hier auch: „Die nach den Anforderungen der Kategorie A auszu-legen und zu prüfen sind“.</p> <p>Aber die Ebene 3 muss ich immer noch zur Beherrschung behalten. Zur Beherrschung!</p> <p>Team 5: Siehe Antwort auf Nr. 515.</p>		
		592	RSK / Hr. Bandholz (WSI)	<p>Was hier steht, ist ja, dass ich ein Versagen der Leittechnik der Kategorie B unterstelle und dann sage ich, ich springe auf die Ebene 4. Die Frage ist einfach, ob ich das durch die Kategorie A verhindern kann, das heißt, ob durch das Vorgehen der Leittechnik „Qualifikation Ebene A“ beim Versagen eben nicht mehr die Ebene 4 erreicht wird. Weil, ich kann nicht hingehen und sagen, ich unterstelle, dass die Kategorie A nicht versagt. Also da hilft auch die Qualifizierung nichts, wenn ich den Weg verfolge. Das Versagen einer Einrichtung können Sie grundsätzlich unterstellen, ob Kategorie B oder A. Es fragt sich nur: Bei B ist es so, wir nehmen an, dass Sie auf der Ebene 3 landen und bei Kategorie A sagt dieser Text implizit, dass wir auf Ebene 4 landen, das musste wohl gar nicht sein. Also noch mal, man kann die Verknüpfung „das Versagen der Ereignisse“ und „das Überspringen der Ebene 3“ nicht an der Qualifizierung festmachen. Das geht nicht. Dann würden wir einen Absolutheitsanspruch stellen, dass Kategorie A nie versagt. Das wollen wir nicht erheben. Das geht nicht.</p> <p>Team 5: Siehe Antwort auf Kommentar 515.</p>		
		598	VGB Power	Es darf keine Ereignisse geben, die durch		

Ziffer	Textvorschlag Modul 5/Teil 1 (Rev. A)	Komm. Nr.	Kommen-tator	Kommentar bzw. Antwort	Ziffer (Neu)	Textvorschlag Modul 5/Teil 1 (Rev. B)
				<p>Versagen von Leittechnik-Funktionen der Kategorie B ausgelöst werden und nicht von Einrichtungen der Sicherheitsebene 3 beherrscht werden können. Was ist hier wirklich gemeint?</p> <p>Team 5: Siehe Antwort auf Nr. 515.</p>		
3.4	Leittechnische Einrichtungen für Leittechnik-Funktionen der Sicherheitsebene 4				3.4	Leittechnische Einrichtungen für Leittechnik-Funktionen auf der Sicherheitsebene 4
	<p>Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Sicherheitsebene 4a, 4b und 4c ausführen, werden so ausgelegt, dass sie unter den für die jeweilige Aufgabe zu unterstellenden Umgebungsbedingungen ihre Aufgaben mit ausreichender Zuverlässigkeit erfüllen können. Hierfür werden ist es zulässig, Einrichtungen für Leittechnik-Funktionen der Kategorien A bis C zu verwenden.</p> <p>Hinweis: Anforderungen an die Auslegung von Maßnahmen des anlageninternen Notfallschutzes gemäß Kapitel 4 in Modul 7 werden auf die Auslegung der Leittechnik-Funktionen der Sicherheitsebenen 4b und 4c angewendet.</p>	<p>384</p> <p>593</p>	<p>VGB / EnBW</p> <p>RSK / Hr. Bandholz</p>	<p>Die Kommentierung der Ausweitung des Regelwerks auf die Sicherheitsebene 4 erfolgte bereits in verschiedenen Betreiberstellungnahmen, auf die hier verwiesen wird.</p> <p>Team 5: Betrifft Vorläuferversion. In Modul 5 wurde der Konzept der Sicherheitsebenen für die leittechnischen Einrichtungen umgesetzt.</p> <p>Wenn sie das Modul1 vergleichen, da ist eindeutig gesagt, dass diese Funktionalitäten, die in Modul 5 beschrieben sind, für die Umgebungsbedingungen auszulegen sind, die sich aus der Analyse ergeben. Wir verbinden nämlich die Anforderungen an die Leittechnik Kategorie A mit der Ebene 4c, fordern eine hohe Zuverlässigkeit und das im Rahmen der zugrunde liegenden Umgebungsbedingungen. Da sage ich einfach nur, da häuft man zu viele Forderungen aufeinander, dass man wirklich diese Funktionalitäten so nicht erbringen kann. In 3.2 (6) / M1 steht das nämlich drin, dass die Umgebungsbedingungen zusätzlich erfüllt werden können. Also die einzelnen Anforderungen sind durchaus schlüssig und nachvollziehbar, nur wenn Sie sie übereinander falten, kommen Sie dahin, dass Sie eine diversitäre Anregung 3-kanalig in Kategorie A „Ausle-</p>		<p>Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Sicherheitsebenen 4a, 4b und 4c ausführen, sind werden so ausgelegt, dass sie unter den für die jeweilige Aufgabe zu unterstellenden Umgebungsbedingungen ihre Aufgaben mit ausreichender Zuverlässigkeit erfüllen können. Für Maßnahmen des anlageninternen Notfallschutzes können alle leittechnischen Einrichtungen eingesetzt werden, die dazu geeignet sind. Hierfür werden ist es zulässig, Einrichtungen für Leittechnik-Funktionen der Kategorien A bis C zu verwenden.</p> <p>Hinweis: Anforderungen an die Auslegung von Maßnahmen des anlageninternen Notfallschutzes gemäß Kapitel 4 in Modul 7 werden auf die Auslegung der Leittechnik-Funktionen der Sicherheitsebenen 4b und 4c angewendet.</p>

Ziffer	Textvorschlag Modul 5/Teil 1 (Rev. A)	Komm. Nr.	Kommen-tator	Kommentar bzw. Antwort	Ziffer (Neu)	Textvorschlag Modul 5/Teil 1 (Rev. B)
				<p>gung für den Fall Kernschmelze“ bräuchten.</p> <p>Team 5: Der Text in 3.2 (6) Modul 1 ist entfallen. Die Formulierungen in Modul 5 Ziffer 3.4 lassen die im Kommentar angesprochene Interpretationsmöglichkeit nicht zu.</p>		
		598	VGB Power	<p>Hier werden die Ereignisse der Sicherheits-ebene 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.</p> <p>Team 5: Für die vorgeplanten Maßnahmen ist zu zeigen, dass diese unter den für die vorgeplanten Fälle erwarteten Bedingungen ihre Aufgabe erfüllen. Eine „Verschiebung“, in Richtung „Auslegungsstörfälle“ erfolgt hier nicht. Es wird nicht formuliert, dass es Leittechnikfunktionen der Sicherheitsebenen 4b und 4c gibt, wohl aber Funktionen, die dort ausgeführt werden sollen.</p>		
4	Anforderungsspezifikation für leittechnische Einrichtungen für Leittechnik-Funktionen der Kategorien A bis C	598	VGB Power	<p>Es wird eine konsequente Ereignisorientierung verfolgt, das etablierte zielgerichtete Vorgehen nach Schutzzielen wird nicht erwähnt.</p> <p>Team 1: Die Schutzziele sind Bestandteil der ereignisorientierten Vorgehensweise (siehe bspw. Modul 3). Sofern sich hierzu Unterschiede zum im Kommentar angesprochenen Vorgehen ergeben, wären diese vom Kommentator zu präzisieren.</p>	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 werden in einer Anforderungsspezifikation in übersichtlicher Darstellung dokumentiert.	384	VGB / EnBW	Ausweitung des Geltungsumfangs auf die gesamte Leittechnik. Das ist für alle Anwendungen weder nötig noch machbar. Faktisch verbietet diese Forderung den Einsatz von Off the Shelf Produkten, da deren Entwicklungsdokumentation nicht beschaffbar ist.	4 (1)	Sämtliche Anforderungen an Leittechnik-Funktionen der Kategorien A bis C sind werden in einer Anforderungsspezifikation in übersichtlicher Darstellung dokumentiert.

Ziffer	Textvorschlag Modul 5/Teil 1 (Rev. A)	Komm. Nr.	Kommentator	Kommentar bzw. Antwort	Ziffer (Neu)	Textvorschlag Modul 5/Teil 1 (Rev. B)
				Team 5: Betrifft Vorläuferversion 3 (1). Die Anforderungsspezifikation bezieht sich auf die Leittechnik-Funktionen und nicht auf Off the Shelf Produkte.		
4 (2)	<p>Die Aufgaben der Leittechnik-Funktionen der Sicherheitsebenen 2, 3, 4a und 4b werden aufgrund einer Analyse von Ereignisabläufen ermittelt, die die in den Sicherheitsebenen 2, 3 und 4b zu unterstellenden Ereignisse umfasst.</p> <p>Für Notfallmaßnahmen und Notfallstrategien der Sicherheitsebene 4c werden Betrachtungen zur Nutzung der verfügbaren leittechnischen Einrichtungen angestellt.</p>	384	VGB / EnBW	<p>Erweiterung des Geltungsumfangs auf die gesamte Leittechnik der Ebenen 2, 3 und 4b. Die Analyse von betrieblichen Einrichtungen der SE 2 ist weder notwendig, noch angemessen. Kommentare zur Sicherheitsebene 4c wurden bereits an anderer Stelle gemacht (s. o.).</p> <p>Team 5: Betrifft Vorläuferversion 3 (2). Im Modul 5 wurde das Konzept der Sicherheitsebenen für die leittechnischen Einrichtungen umgesetzt. Die Leittechnik-Funktionen der Kategorie B (Zustandsbegrenzungen) werden aufgrund von Analysen ermittelt. Funktionen, die nicht in Ereignisabläufen angefordert werden, sind hiervon nicht betroffen.</p>	4 (2)	<p>Die Aufgaben der Leittechnik-Funktionen, die auf den -der Sicherheitsebenen 2, 3, 4a und 4ab eingesetzt werden, sind auf Basis grund einer Analyse der von Ereignisabläufen ermittelt, die die in den Sicherheitsebenen 2, 3 und 4a zu unterstellenden den Ereignisse umfasst.</p> <p>Für Maßnahmen des anlageninternen Notfallschutzes maßnahmen und Notfallstrategien der Sicherheitsebene 4c werden sind Betrachtungen zur Nutzung der verfügbaren leittechnischen Einrichtungen angestellt.</p>
		492	VGB / Powertech	<p>Anforderungen bezüglich der Sicherheitsebenen 4b und 4c unter der Voraussetzung bekannter Ereignisabläufe und Prozesse. Die Anforderungen die z. B. im Teil 1 in 4(2) oder 5(1) formuliert sind, gehen von der nicht zutreffenden Voraussetzung aus, dass Ereignisse der SE 4b und 4c in einer Sammlung von Abläufen bzw. Prozessen beschrieben sind.</p> <p>Team 5: Die Anforderung wird in der Revision B unter Berücksichtigung des Kommentars präzisiert.</p>		
		598	VGB Power	Für Sicherheitsebenen 4b und 4c gibt es keine "zu unterstellenden Ereignisabläufe" und damit auch keine Leittechnik, die diese beherrscht.		

Ziffer	Textvorschlag Modul 5/Teil 1 (Rev. A)	Komm. Nr.	Kommentator	Kommentar bzw. Antwort	Ziffer (Neu)	Textvorschlag Modul 5/Teil 1 (Rev. B)
				Team 5: Die Anforderung wird in der Revision B unter Berücksichtigung des Kommentars präzisiert.		
4 (3)	In der Anforderungsspezifikation ist die verfahrenstechnische Aufgabenstellung der Leittechnik-Funktionen der Kategorien A und B in klar abgegrenzte Teilaufgaben gegliedert. Diese Teilaufgaben werden in Leittechnik-Funktionen dargestellt. Die Teilaufgaben der softwarebasierten leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, haben einen geringen Funktionsumfang. Die Gesamtheit aller Leittechnik-Funktionen ist übersichtlich strukturiert dokumentiert.	384	VGB / EnBW	Erweiterung des Geltungsumfangs auf die gesamte Leittechnik der SE 2 und 3. Das ist nicht für alle Einrichtungen dieser Ebenen notwendig. Warum diese Streichung? Die Verwendung von Leittechnikfunktionen entspricht dem Stand von W&T und hat sich in der Praxis bewährt. Das ist nicht für alle Funktionen notwendig. Team 5: Betrifft Vorläuferversion 3 (3). Der Kommentar bezieht sich auf die Formulierung aus dem Modul 5 Rev. 6, die aufgrund von Änderungsvorschläge bereits durch die Rev. A (s. Abs. 2. Kategorisierung) abgelöst worden ist.	4 (3)	In der Die Anforderungsspezifikation ist die verfahrenstechnische Aufgabenstellung der 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 werden in Leittechnik-Funktionen dargestellt. Die Teilaufgaben der softwarebasierten leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, sind so ausgelegt, dass diese haben einen geringen Funktionsumfang haben . Die Gesamtheit aller Leittechnik-Funktionen ist übersichtlich strukturiert dokumentiert.
4 (4)	Für die Leittechnik-Funktionen werden die Aufgabe, 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.	384	VGB / EnBW	Die Bedeutung einer LEFU richtet sich nicht nach SE, sondern nach dem Beitrag zum Einhalten der Schutzziele. Die geforderten Angaben ergeben sich aus den üblicherweise verwendeten Funktionsplänen von selbst. Sind eigenständige Datenzusammenstellungen gemeint? Die Anforderung an die Datenspeicherung ist unverständlich. Die Art und der Ort der Datenspeicherung sind vom verwendeten Leittechniksystem abhängig und nicht von der Funktion. Team 5: Betrifft Vorläuferversion 3 (4). Nein, es sind keine eigenständige Datenzusammenstellungen gefordert. Die Datenspeicherung kann ein Bestandteil der LEFU sein und sollte angegeben werden.	4 (4)	Für die Leittechnik-Funktionen sind werden 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.

Ziffer	Textvorschlag Modul 5/Teil 1 (Rev. A)	Komm. Nr.	Kommentator	Kommentar bzw. Antwort	Ziffer (Neu)	Textvorschlag Modul 5/Teil 1 (Rev. B)
4 (5)	Es ist nachgewiesen, dass die grundlegenden Sicherheitsfunktionen mit den Leittechnik-Funktionen entsprechend der Anforderungsspezifikation bei allen zu unterstellenden Ereignissen und Ereignisabläufen sichergestellt sind.	384	VGB / EnBW	Das ist ein Rückschritt, der möglicherweise auf die Vorgabe der Vermeidung des Begriffs „Schutzziel“ zurückzuführen ist. Wie soll eine Validierung der Anforderungsspezifikation gelingen, wenn nicht gegen Schutzziele geprüft wird? Team 5: Betrifft Vorläuferversion 3 (5). Der Begriff grundlegenden Sicherheitsfunktionen war als Synonym für „Schutzziele“ im Modul 1 eingeführt worden und wird nunmehr auch direkt verwendet.	4 (5)	Es ist nachgewiesen, dass die Schutzziele grundlegenden Sicherheitsfunktionen mit den Leittechnik-Funktionen entsprechend der Anforderungsspezifikation bei allen zu unterstellenden Ereignissen und Ereignisabläufen sichergestellt sind.
5	Erfassung von Prozessvariablen	598	VGB Power	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. Team 5: Der eingeführte Begriff „Prozessvariable“ hat nach wie vor Gültigkeit und beschreibt Information über den Zustand der Anlage. Auch Zustände werden über Prozessvariable erfasst.	5	Erfassung von Prozessvariablen
5 (1)	Für die unterstellten Ereignisse der Sicherheitsebenen 2 bis 4a sowie für die Notfallmaßnahmen der Sicherheitsebenen 4b und 4c werden die erforderlichen Prozessvariablen erfasst.	384	VGB / EnBW	Erweiterung des Geltungsbereichs auf Sicherheitsebenen 2 bis 4. Dieser Forderung liegt offenbar die Überlegung zu Grunde, dass alle Maßnahmen, Einrichtungen, Signale eindeutig Sicherheitsebenen zugeordnet werden können. Das geht möglicherweise mit Mehrfachzuordnung auf den SE1 bis 4a und gar nicht für die Sicherheitsebenen 4b und 4c. In den Notfallhandbüchern werden die Erkennungsmerkmale zusammen mit den dann möglichen Maßnahmen benannt. Das kann nicht an vorherbestimmten definierten Signalen aus Prozessvariablen festgemacht werden. Die Forderung ist so nicht erfüllbar.	5 (1)	Für die unterstellten Ereignisse der Sicherheitsebenen 2 bis 4a sowie für die vorgeplanten Maßnahmen des anlageninternen Notfall schutzes maßnahmen der Sicherheitsebenen 4b und 4c werden die erforderlichen Prozessvariablen erfasst.

Ziffer	Textvorschlag Modul 5/Teil 1 (Rev. A)	Komm. Nr.	Kommen-tator	Kommentar bzw. Antwort	Ziffer (Neu)	Textvorschlag Modul 5/Teil 1 (Rev. B)
				Team 5: Betrifft Vorläuferversion 4 (1). Siehe auch Antwort zu Nr. 598, Abs. 5.		
		492	VGB / Powertech	Anforderungen bezüglich der Sicherheits-ebenen 4b und 4c unter der Voraussetzung bekannter Ereignisabläufe und Prozesse. Die Anforderungen die z. B. im Teil 1 in 4(2) oder 5(1) formuliert sind, gehen von der nicht zutreffenden Voraussetzung aus, dass Ereignisse der SE 4b und 4c in einer Sammlung von Abläufen bzw. Prozessen beschrieben sind. Team 5: Siehe Antwort zu Nr. 598, Abs. 5.		
5 (2)	Für jedes von den leittechnischen Einrichtungen zu beherrschende Ereignis der Sicherheitsebene 3 werden mindestens zwei unterschiedliche Anregekriterien herangezogen, die aus physikalisch unterschiedlichen Prozessvariablen gebildet werden sollen. Wenn dies technisch nicht realisierbar ist, werden andere Maßnahmen zum Erreichen hoher Zuverlässigkeit getroffen.	384	VGB / EnBW	Diese Forderung gilt nur für das Reaktorschutzsystem. Für die übrigen Einrichtungen der SE 3 ist sie weder erforderlich, noch erfüllbar. Team 5: Betrifft Vorläuferversion 4(2). Die Anforderung wird in der Rev. B für die LEFU der Kategorie A präzisiert.	5 (2)	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 sollen . Wenn dies technisch nicht realisierbar ist, sind werden andere Maßnahmen und Einrichtungen zum Erreichen hoher Zuverlässigkeit vorgesehen . getroffen .
			Team 5	Text wurde aus dem Abs. 9.3 nach 5 (3) verschoben.	5 (3)	Die sicherheitstechnisch relevanten Ziele In der Spezifikation der Prozessführungs- und der Informationseinrichtungen sind in ihrer Spezifikation werden deren sicherheitsrelevante Ziele festgelegt.
			Team 5	Text wurde aus Ziffer 9 (8) nach 5 (4) verschoben.	5 (4)	Wird das Informationssystem in ein Sicherheits- und in ein Prozessinformationssystem aufgeteilt, dann sind beide Teile in voneinander unabhängigen Einrichtungen realisiert. Die Informationssysteme sind gemäß ihrer sicherheitstechnischen Bedeutung

Ziffer	Textvorschlag Modul 5/Teil 1 (Rev. A)	Komm. Nr.	Kommentator	Kommentar bzw. Antwort	Ziffer (Neu)	Textvorschlag Modul 5/Teil 1 (Rev. B)
						qualifiziert.
6	Redundanz und Unabhängigkeit	598	VGB Power	Hierzu sind bereits Regelungen in 3.2(4) getroffen. Team 5: In diesem Abschnitt wird die Umsetzung der Anforderung aus 3.2 (4) erläutert.	6	Redundanz und Unabhängigkeit
6 (1)	Die leittechnischen Einrichtungen sind so aufgebaut, dass die in den aktiven Einrichtungen des Sicherheitssystems vorgegebene Redundanz gewahrt bleibt.	384	VGB / EnBW	Formale Erweiterung des Geltungsumfangs auf die gesamte Leittechnik. Die Forderung ist für die Leittechnik des Sicherheitssystems sinnvoll und in den RSK-LL im den Abschnitten 7.1 und 7.2 enthalten. Ist diese Leittechnik wirklich gemeint? Team 5: Betrifft Vorläuferversion 5(1). Der Einwand zur Ausweitung des Geltungsumfangs wurde bereits durch die grundsätzliche Überarbeitung des M5 in der Rev. A u B sinngemäß berücksichtigt. Dabei ist zu beachten, dass die Anforderungen an die Redundanz und Unabhängigkeit der leittechnischen Einrichtungen nur im Zusammenhang mit Leittechnik-Funktionen gelten.	6 (1)	Die leittechnischen Einrichtungen sind so aufgebaut, dass die in den aktiven Einrichtungen des Sicherheitssystems vorgegebene Redundanz gewahrt bleibt.
6 (2)	Die redundanten Stränge der leittechnischen Einrichtungen sind voneinander so unabhängig, dass ein anlageninternes versagensauslösendes Ereignis nicht zum Ausfall mehrerer redundanter Stränge des Sicherheitssystems führen kann. Bei Ausfall einzelner Stränge leittechnischer Einrichtungen des Sicherheitssystems durch Einwirkungen von außen reichen die übrigen Stränge zur Beherrschung dieses Ereignisses aus.	384	VGB / EnBW	Ist eine formale Erweiterung des Geltungsumfangs auf die gesamte Leittechnik beabsichtigt? Team 5: Betrifft Vorläuferversion 5(2). Der Einwand zur Ausweitung des Geltungsumfangs wurde bereits durch die grundsätzliche Überarbeitung des M5 in der Rev. A u B sinngemäß berücksichtigt. Dabei ist zu beachten, dass die Anforderungen an die Redundanz und Unabhängigkeit der leittechnischen Einrichtungen nur im Zusammenhang mit Leittechnik-Funktionen gelten.	6 (2)	Die redundanten Stränge der leittechnischen Einrichtungen sind voneinander so unabhängig ausgelegt , dass ein anlageninternes versagensauslösendes Ereignis nicht zum Ausfall mehrerer redundanter Stränge des Sicherheitssystems führt. Bei Ausfall einzelner Stränge leittechnischer Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, des Sicherheitssystems durch Einwirkungen von außen reichen die übrigen Stränge zur Beherrschung dieses Ereignisses aus.
6 (3)	Zum Schutz gegen versagensauslösen-	384	VGB /	Erweiterung des Geltungsumfangs auf die	6 (3)	Zum Schutz gegen redundanzüber-

Ziffer	Textvorschlag Modul 5/Teil 1 (Rev. A)	Komm. Nr.	Kommentator	Kommentar bzw. Antwort	Ziffer (Neu)	Textvorschlag Modul 5/Teil 1 (Rev. B)
	de Ereignisse innerhalb der leittechnischen Einrichtungen und innerhalb der Reaktoranlage sollen zueinander redundante Stränge räumlich getrennt angeordnet werden.		EnBW	gesamte Leittechnik. In dieser allgemeinen Formulierung für die gesamte Leittechnik weder erforderlich, noch erfüllbar. Team 5: Betrifft Vorläuferversion 5 (3). Der Einwand zur Ausweitung des Geltungsumfangs wurde bereits durch die grundsätzliche Überarbeitung des M5 in der Rev. A u B sinngemäß berücksichtigt.		greifende versagensauslösende Ereignisse innerhalb der leittechnischen Einrichtungen und innerhalb der Reaktor Anlage sollen-sind zueinander redundante Stränge grundsätzlich räumlich getrennt angeordnet -werden .
6 (4)	Verbindungen der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A und B ausführen, zu anderen Datenverarbeitungs- oder Datenübertragungseinrichtungen sind auf ein Minimum begrenzt und nachweislich rückwirkungsfrei gestaltet.	384	VGB / EnBW	Die Gleichsetzung der SE mit den Kategorien der RSK-LL (und damit auch der DIN IEC 61226) ist falsch. S. oben. Die Streichung ist nicht akzeptabel. Es ist nur notwendig die Rückwirkungsfreiheit einer leittechnischen Einrichtung in Richtung der sicherheitstechnisch höherwertigen Einrichtung sicherzustellen. Genau das sagte die alte Formulierung aus. Team 5: Betrifft Vorläuferversion 5(4). Der Kommentar bezieht sich auf die Formulierung aus dem Modul 5 Rev. 6, die aufgrund von Änderungsvorschläge bereits durch die Rev. A (s. Abs. 2. Kategorisierung) abgelöst worden ist.	6 (4)	Verbindungen der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A und B ausführen, zu nicht kategorisierten oder anderen Datenverarbeitungs- oder Datenübertragungseinrichtungen der Kategorie C sind werden 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, dass bei versagensauslösenden Ereignissen in den Einrichtungen sicherheitstechnisch niederwertigeren Kategorie die Funktionen der sicherheitstechnisch höherwertigeren Kategorie erhalten bleiben.	384	VGB / EnBW	Bisher sollte die Unabhängigkeit der Einrichtung mit der höheren sicherheitstechnischen Bedeutung (Kategorie) gegenüber niederwertigen Kategorien sichergestellt werden. Die Gleichsetzung von SE 1 bis 3 und Kategorien 1 bis 3 führt zu deutlichen inhaltlichen Verschiebungen. Team 5: Betrifft Vorläuferversion 5 (5). Der Kommentar bezieht sich auf die Formulierung aus dem Modul 5 Rev. 6, die aufgrund von Änderungsvorschläge bereits durch die Rev. A (s. Abs. 2. Kategorisierung) abgelöst worden ist. In der Revision wird entsprechender Text im Modul 1, 3.2 (9) gestrichen	6 (5)	Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorien A bis C ausführen, sind werden von einander so unabhängig ausgelegt , dass bei versagensauslösenden Ereignissen in den Einrichtungen sicherheitstechnisch niederwertigeren Kategorien die Funktionen der sicherheitstechnisch höherwertigeren Kategorie erhalten bleiben.

Ziffer	Textvorschlag Modul 5/Teil 1 (Rev. A)	Komm. Nr.	Kommentator	Kommentar bzw. Antwort	Ziffer (Neu)	Textvorschlag Modul 5/Teil 1 (Rev. B)
				und inhaltlich durch die modifizierten Anforderungen im M5 Abschnitt 6 (5) berücksichtigt.		
6 (6)	Innerhalb der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorien A bis C ausführen, haben Ausgangssignale von Einrichtungen einer sicherheitstechnisch höherwertigeren Kategorie Priorität vor den Ausgangssignalen von Einrichtungen einer sicherheitstechnisch niederwertigeren Kategorie.	384	VGB / EnBW	Erweiterung des Geltungsbereichs auf die gesamte Leittechnik bis Sicherheitsebene 3. Im übrigen s. Kommentar zu 5.4 Team 5: Betrifft Vorläuferversion 5 (6). Der Kommentar bezieht sich auf die Formulierung aus dem Modul 5 Rev. 6, die aufgrund von Änderungsvorschläge bereits durch die Rev. A (s. Abs. 2. Kategorisierung) abgelöst worden ist.	6 (6)	Innerhalb der Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorien A bis C ausführen, sind so ausgelegt, dass die haben Ausgangssignale von Einrichtungen einer sicherheitstechnisch höherwertigeren Kategorie Priorität vor den Ausgangssignalen von Einrichtungen einer sicherheitstechnisch niederwertigeren Kategorie haben .
7	Qualifizierung				7	Qualifizierung
7.1	Qualifizierung der Hard- und Software der leittechnischen Einrichtungen für Leittechnik-Funktionen der Kategorien A bis C				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, sind administrative, konstruktive und analytische Maßnahmen einschließlich praktischer Prüfungen im Rahmen der Qualitätssicherung durchgeführt und dokumentiert.	384	VGB / EnBW	Erweiterung des Geltungsumfangs auf die gesamte Leittechnik. In dieser umfassenden und für alle Funktionen und Einrichtungen gültigen Form weder erforderlich noch machbar. Team 5: Betrifft Vorläuferversion 6.1 (1). Der Kommentar bezieht sich auf die Formulierung aus dem Modul 5 Rev. 6, die aufgrund von Änderungsvorschläge bereits durch die Rev. A (s. Abs. 2. Kategorisierung) abgelöst worden ist.	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 sind 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 leit-	384	VGB / EnBW	Erweiterung des Geltungsumfangs auf die gesamte Leittechnik. In dieser umfassenden und für alle Funktionen und Einrichtungen gültigen Form weder erforderlich noch machbar. Team 5: Betrifft Vorläuferversion 6.1 (2). Der Kommentar bezieht sich auf die Formu-	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

Ziffer	Textvorschlag Modul 5/Teil 1 (Rev. A)	Komm. Nr.	Kommen-tator	Kommentar bzw. Antwort	Ziffer (Neu)	Textvorschlag Modul 5/Teil 1 (Rev. B)
	technischen Anforderungen erfüllt werden.			lierung aus dem Modul 5 Rev. 6, die aufgrund von Änderungsvorschläge bereits durch die Rev. A (s. Abs. 2. Kategorisierung) abgelöst worden ist.		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, ob alle zu unterstellenden Ereignisabläufe beherrscht werden.	384	VGB / EnBW	Erweiterung des Geltungsumfangs auf die gesamte Leittechnik. In dieser umfassenden und für alle Funktionen und Einrichtungen gültigen Form weder erforderlich noch machbar. Team 5: Betrifft Vorläuferversion 6.1 (3). Der Kommentar bezieht sich auf die Formulierung aus dem Modul 5 Rev. 6, die aufgrund von Änderungsvorschläge bereits durch die Rev. A (s. Abs. 2. Kategorisierung) abgelöst worden ist.	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, ob alle zu unterstellenden Ereignisabläufe beherrscht werden.
		598	VGB Power	Welche Tests sind gemeint und wie ‚realistisch sollte ein KMV‘ sein? Team 5: Die Formulierung „möglichst realistische Anlagen- und Einsatzbedingungen“ lässt ausreichend Spielraum für sinnvolle technische Lösungen.		
7.1 (4)	Nach Abschluss der Montage der leittechnischen Einrichtungen in der Anlage ist eine Inbetriebsetzungsprüfung durchgeführt worden.	384	VGB / EnBW	Erweiterung des Geltungsumfangs auf die gesamte Leittechnik. In dieser umfassenden und für alle Funktionen und Einrichtungen gültigen Form weder erforderlich noch machbar. Team 5: Betrifft Vorläuferversion 6.1 (4). Der Kommentar bezieht sich auf die Formulierung aus dem Modul 5 Rev. 6, die aufgrund von Änderungsvorschläge bereits durch die Rev. A (s. Abs. 2. Kategorisierung) abgelöst worden ist.	7.1 (4)	Nach Abschluss der Montage in der Anlage oder nach Änderungen in den der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A bis C ausführen, in der Anlage ist wird eine Inbetriebsetzungsprüfung durchgeführt worden .
7.2	Qualifizierung der Hardware				7.2	Qualifizierung der Hardware
7.2 (1)	Für leittechnische Einrichtungen, die Leittechnik-Funktionen der Kategorie A	384	VGB / EnBW	Für SE 2 nur zum Teil berechtigt.	7.2 (1)	Für leittechnische Einrichtungen, die Leittechnik-Funktionen der Kategorie

Ziffer	Textvorschlag Modul 5/Teil 1 (Rev. A)	Komm. Nr.	Kommen-tator	Kommentar bzw. Antwort	Ziffer (Neu)	Textvorschlag Modul 5/Teil 1 (Rev. B)
	und B ausführen, wird zuverlässige, typgeprüfte oder für die unterstellten Einsatzbedingungen betriebsbewährte sowie möglichst wartungsfreie Hardware zu verwenden.			Team 5: Betrifft Vorläuferversion 6.2 (1). Im Modul 5 werden generelle übergeordnete Anforderungen entsprechend dem Geltungsbereich gestellt.		A und B ausführen, ist wird ist zuverlässige, typgeprüfte oder für die unterstellten Einsatzbedingungen betriebsbewährte sowie möglichst wartungsfreie Hardware zu verwendetn eingesetzt .
7.2 (2)	Für leittechnische Einrichtungen, die Leittechnik-Funktionen der Kategorie C ausführen, ist zuverlässige und für die unterstellten Einsatzbedingungen geeignete Hardware verwendet.	384	VGB / EnBW	Für SE 1 nur zum geringen Teil berechtigt. Team 5: Betrifft Vorläuferversion 6.2 (2). Im Modul 5 werden generelle übergeordnete Anforderungen entsprechend dem Geltungsbereich gestellt.	7.2 (2)	Für leittechnische Einrichtungen, die Leittechnik-Funktionen der Kategorie C ausführen, ist zuverlässige und für die unterstellten Einsatzbedingungen geeignete Hardware verwendet eingesetzt .
7.2 (3)	Die anlagenbezogene Eignung wird durch den Vergleich der Eigenschaften der Hardware mit den für den Einsatzfall spezifizierten Anforderungen nachgewiesen.				7.2 (3)	Die anlagenbezogene Eignung ist wird durch den Vergleich der Eigenschaften der Hardware mit den für den Einsatzfall spezifizierten Anforderungen nachgewiesen.
7.3	Qualifizierung der Software				7.3	Qualifizierung der Software
	Die Software ist nach den Anforderungen des Abschnitts 14 qualifiziert.			Team 5: Text aus dem Abschnitt 14 wird hier eingefügt.		Die Software wird nach den Anforderungen des Abschnitts 14 qualifiziert.
14	Anforderungen für die Erstellung und Prüfung von Software	384	VGB / EnBW	Alter und neuer Text haben miteinander nur wenig gemein. Deshalb wird auf Gegenüberstellung verzichtet. Die RSK-LL gelten für Hard- und Software, die hier gestellten Forderungen gelten nur für Software, sind aber teilweise auch für die Hardware im Abschnitt 2.3 erhoben. Die Kategorisierung sollte daher im Text nur einmal und dann für Hard- und Software gemeinsam erfolgen. Die RSK- LL orientieren sich an der sicherheitstechnischen Bedeutung der Leittechnikfunktionen d. h. an deren Beitrag zur Einhaltung der Schutzziele. Das ist in Übereinstimmung mit dem internationalen Regelwerk, entspricht dem Stand von W&T, ist mit DIN IEC 61226 auch in das unterlagerte deutsche Regelwerk eingegangen. Die hier vorgeschlagene Kategorisierung orientiert	14	Anforderungen für die Erstellung und Prüfung von Software

Ziffer	Textvorschlag Modul 5/Teil 1 (Rev. A)	Komm. Nr.	Kommen-tator	Kommentar bzw. Antwort	Ziffer (Neu)	Textvorschlag Modul 5/Teil 1 (Rev. B)
				<p>sich an Sicherheitsebenen. Um die Konsistenz mit W&T herzustellen wird von den Verfassern dieses Moduls offenbar eine Gleichsetzung der SE mit der sicherheitstechnischen Bedeutung vorgenommen. Die Gleichsetzung von SE mit sicherheitstechnischer Bedeutung ist nicht sinnvoll möglich. Nicht akzeptabel sind die offensichtlich deterministisch gemeinten Forderungen nach der die Software (Hardware s. Abschnitt 2.3) für Leittechnik-Funktionen einer Sicherheitsebene, deren Versagen Ereignisse auslöst, die nicht durch Maßnahmen und Einrichtungen der nächst höheren Sicherheitsebene beherrscht werden, nach den Anforderungen der nächst höheren Kategorie zu erstellen und zu prüfen sind. Im Abschnitt 2.3 sind in der Begründung die Zustandsbegrenzungen genannt. Die bisherige Auslegung ist so, dass durch Redundanz, Qualität, Prüfindervall für WKP usw. eine so hohe Zuverlässigkeit erreicht wird, dass die Überlagerung von Ausfall der Begrenzung und Störfall, für den die Zustandsbegrenzungen die Ausgangsbedingungen sicherstellen, nicht erforderlich ist. Die gegenüber dem Reaktorschutzsystem reduzierten Auslegungsanforderungen für die mit Hilfe Elektronikbaugruppen realisierten Zustandsbegrenzungen sind in KTA 3501 festgelegt. Für die in einigen Anlagen bereits realisierten rechnerbasierten Systeme wurde diese Regel ebenfalls angewendet, wobei zusätzlich die RSK-LL sowie internationale Regeln zur Anwendung kamen.</p> <p>Team 5: Betrifft Vorläuferversion 13.1. Der Kommentar bezieht sich auf die Formulierung aus dem Modul 5 Rev. 6, die aufgrund von Änderungsvorschläge bereits durch die</p>		

Ziffer	Textvorschlag Modul 5/Teil 1 (Rev. A)	Komm. Nr.	Kommentator	Kommentar bzw. Antwort	Ziffer (Neu)	Textvorschlag Modul 5/Teil 1 (Rev. B)
				Rev. A (s. Abs. 2. Kategorisierung) abgelöst worden ist.		
		598	VGB Power	<p>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</p> <p>Team 5: Die teilweise unterschiedliche Detaillierung ergibt sich aus dem Detaillierungsgrad der durch das neue Regelwerk abzulösenden Regelungen in den bestehenden RSK-LL-DWR. Es sind unterschiedliche Varianten für die Qualifizierung neu entwickelter und vorgefertigter Software berücksichtigt.</p>		
14.1	Software für Leittechnik-Funktionen der Kategorien A bis C				7.3.1	Software für Leittechnik-Funktionen der Kategorien A bis C
14.1 (1)	Die Software wird in verifizierbaren Schritten in einem Phasenmodell entwickelt.				7.3.1 (1)	Die Software ist wird in verifizierbaren Schritten nach einem Phasenmodell entwickelt.
14.1 (2)	<p>Die Funktionen der Anwendersoftware und der Systemsoftware sind in eigenständigen Softwareeinheiten realisiert. In der Softwarearchitektur ist die Anwendersoftware von der Systemsoftware getrennt.</p> <p>Hinweis: Zur Systemsoftware gehören z.B. das Betriebssystem und bei Mehrrechnersystemen die Software zur Kommunikation der Rechner</p>	384	VGB / EnBW	<p>Erweiterung des Geltungsumfangs auf die gesamte Leittechnik.</p> <p>Team 5: Betrifft Vorläuferversion 13.2 (2). Der Kommentar bezieht sich auf die Formulierung aus dem Modul 5 Rev. 6, die aufgrund von Änderungsvorschläge bereits durch die Rev. A (s. Abs. 2. Kategorisierung) abgelöst worden ist.</p>	7.3.1 (2)	<p>Die Softwarearchitektur ist so gestaltet, dass dDie Funktionen der Anwendersoftware und der Systemsoftware sind in eigenständigen Softwareeinheiten realisiert sind und -In der Softwarearchitektur ist die Anwendersoftware von der Systemsoftware getrennt ist.</p> <p>Hinweis: —Zur Systemsoftware gehören z.B. das Betriebssystem und bei Mehrrechnersystemen die Software zur Kommunikation der Rechner.</p>
14.1 (3)	Die Software ist so ausgelegt, dass keine unzulässigen Rückwirkungen von leit-				7.3.1 (3)	Die Software ist so ausgelegt, dass keine unzulässigen Rückwirkungen

Ziffer	Textvorschlag Modul 5/Teil 1 (Rev. A)	Komm. Nr.	Kommen-tator	Kommentar bzw. Antwort	Ziffer (Neu)	Textvorschlag Modul 5/Teil 1 (Rev. B)
	technischen Einrichtungen der sicherheitstechnisch niederwertigeren Kategorie auf die leittechnischen Einrichtungen der sicherheitstechnisch höherwertigeren Kategorie auftreten.					von leittechnischen Einrichtungen der sicherheitstechnisch niederwertigeren Kategorie auf die leittechnischen Einrichtungen der sicherheitstechnisch höherwertigeren Kategorie auftreten.
14.1 (4)	Der anforderungsgerechte Ablauf der Programme ist unabhängig von Art und Umfang der zeitlichen Änderung ihrer Eingangssignale gewährleistet.				7.3.1 (4)	Die Software ist so gestaltet, dass deren Der -anforderungsgerechter Ablauf der Programme ist unabhängig von Art und Umfang der zeitlichen Änderung ihrer Eingangssignale gewährleistet ist.
14.2	Software für Leittechnik-Funktionen der Kategorie A				7.3.2	Software für Leittechnik-Funktionen der Kategorie A
14.2.1	Grundsätze				7.3.2.1	Grundsätze
14.2.1 (1)	Die Entwicklung und Qualifizierung der Software für Leittechnikfunktionen 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 Prüfmethode n entsprechend dem internationalen Stand von Wissenschaft und Technik durchgeführt. Diese Methoden werden auch in den anderen Entwicklungsphasen verwendet.				7.3.2.1 (1)	Die Entwicklung und Qualifizierung der Software für Leittechnikfunktionen 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 Prüfmethode n entsprechend dem in- internationalen Stand von Wissenschaft und Technik durchgeführt. Diese Methoden werden auch in den anderen Entwicklungsphasen verwendet.
14.2.1 (2)	Die Software für Leittechnik-Funktionen der Kategorie A ist einfach aufgebaut.				7.3.2.1 (2)	Die Software für Leittechnik-Funktionen der Kategorie A ist grundsätzlich einfach aufgebaut.
14.2.1 (3)	Der Funktionsumfang der Software für Leittechnik-Funktionen der Kategorie A ist auf das für jeweilige Funktion notwendige Maß begrenzt.				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.
14.2.1 (4)	Die Programme sind robust und selbstüberwachend ausgelegt.	513	AREVA	Unklare Anforderung: Selbstüberwachung der Programme ist faktisch nicht möglich.	7.3.2.1 (4)	Die Software ist Programme sind robust und selbstüberwachend

Ziffer	Textvorschlag Modul 5/Teil 1 (Rev. A)	Komm. Nr.	Kommentator	Kommentar bzw. Antwort	Ziffer (Neu)	Textvorschlag Modul 5/Teil 1 (Rev. B)
		598	VGB Power	Was bedeutet "robuste" Auslegung von Programmen? Team 5: Die Anforderung entspricht dem Text RSK-LL-DWR, 7.6.1.2.1 (4). In der Informatik wird der Begriff „Robustheit“ verwendet, um die Eigenschaft eines Verfahrens zu beschreiben, das auch unter ungünstigen Bedingungen noch zuverlässig funktioniert. U. a. kann die „robuste“ Software die Fehlersituation erkennen und weiterhin zuverlässig funktionieren.		ausgelegt.
14.2.2	Qualitätssicherung				7.3.2.2	Qualitätssicherung
14.2.2.1	Konstruktive Qualitätssicherung				14.2.2.1	Konstruktive Qualitätssicherung
14.2.2.1 (1)	Die Software wird nach einem Phasenmodell durchgängig mit rechnergestützten Werkzeugen erstellt.				7.3.2.2 (1)	Die Software ist wird nach einem Phasenmodell durchgängig mit rechnergestützten Werkzeugen erstellt.
14.2.2.1 (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 zu einer übersichtlichen Programmstruktur zu integriert.				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 zu in eine f übersichtliche a Programmstruktur zu integriert.
14.2.2.2	Analytische Qualitätssicherung				14.2.2.2	Analytische Qualitätssicherung
14.2.2.2 (1)	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 (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.
14.2.2.2	Nach Installation der Software auf den				7.3.2.2	Nach Installation der Software auf den

Ziffer	Textvorschlag Modul 5/Teil 1 (Rev. A)	Komm. Nr.	Kommen-tator	Kommentar bzw. Antwort	Ziffer (Neu)	Textvorschlag Modul 5/Teil 1 (Rev. B)
(2)	Rechnern wird das anforderungsgerechte Verhalten des Hardware- und Softwaresystems validiert. Wird die Validierung in mehreren Schritten durchgeführt, so erfolgen die einzelnen Validierungsschritte überlappend.				(4)	Rechnern wird das anforderungsgerechte Verhalten des Hardware- und Softwaresystems validiert. Wird die Validierung in mehreren Schritten durchgeführt, so erfolgen die einzelnen Validierungsschritte überlappend.
14.2.2.3	Organisation und Administration				14.2.2.3	Organisation und Administration
14.2.2.3 (1)	Die Organisation und Administration der Softwareentwicklung und der Qualitätssicherung stellt sicher, dass die Software nach vollständigen Entwicklungs-, Prüf-, Wartungs- und Qualitätssicherungsplänen erstellt und eingesetzt wird. Die Unabhängigkeit zwischen Konstruktion und Qualitätssicherung wird durchgehend gewahrt. Es wird eine vollständige Entwicklungs-, Qualitätssicherungs- und Benutzerdokumentation erstellt.				7.3.2.2 (5)	Die Organisation und Administration der Softwareentwicklung und der Qualitätssicherung ist so gestaltet, stellt sicher, 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 wird eine vollständige Entwicklungs-, Qualitätssicherungs- und Benutzerdokumentation vorhanden. erstellt.
14.2.2.3 (2)	Die konsistente Konfiguration der Programme wird sichergestellt. Die Sicherstellung der konsistenten Konfiguration der Programme wird mit geeigneten Verfahren und Methoden nachgewiesen (Konfigurationsmanagement).				7.3.2.2 (6)	Die konsistente Konfiguration der Programme wird sichergestellt. Die Sicherstellung der konsistenten Konfiguration der Programme wird mit geeigneten Es sind werden Verfahren und Methoden angewandt, die die konsistenten Konfigurationen der Software sicherstellen nachgewiesen (Konfigurationsmanagement).
14.2.2.4	Einsatz von vorgefertigter Software	598	VGB Power	Vorgefertigte Software soll auf unverzichtbare Bestandteile beschränkt werden, gleichzeitig soll eine Änderung vermieden werden. Das ist widersprüchlich. Team 5: Kommentar wurde sinngemäß berücksichtigt.	7.3.2.3	Einsatz von vorgefertigter Software
14.2.2.4	Bei vorgefertigter Software wird eine Be-	384	VGB /	Ist es beabsichtigt, die Verwendung von	7.3.2.3	Der Einsatz Bei vorgefertigter Soft-

Ziffer	Textvorschlag Modul 5/Teil 1 (Rev. A)	Komm. Nr.	Kommentator	Kommentar bzw. Antwort	Ziffer (Neu)	Textvorschlag Modul 5/Teil 1 (Rev. B)
(1)	schränkung auf unverzichtbare Bestandteile vorgenommen, wobei Softwareänderungen vermieden werden. Diese Teile sind Prüfungen und Tests unterzogen, die in Umfang und Tiefe den Nachweisen nach den Abschnitten 14.1 und 14.2.1 bis 14.2.2 gleichwertig sind.		EnBW	Standardprodukten damit weitgehend auszuschließen? Team 5: Betrifft Vorläuferversion 13.3.3 (1). Nein.	(1)	ware wird ist auf unverzichtbare eine Beschränkung auf unverzichtbare Bestandteile beschränkt , vorgenommen , wobei Softwareänderungen vermieden werden. Diese Teile sind Prüfungen und Tests unterzogen, die in Umfang und Tiefe den Nachweisen nach den Abschnitten 14.2.1 bis 14.2.2 7.3.2.1 und 7.3.2.2 gleichwertig sind.
14.2.2.4 (2)	Zur Bewertung der Gleichwertigkeit sind herangezogen: – Referenzen über den Hersteller der Software, – die Entwicklungs-, Anwenderdokumentation und QS-Dokumentation der Software, – die Ergebnisse unabhängiger Begutachtung (Zertifikate) der Software, die Betriebserfahrung der Software unter Berücksichtigung der Anwendungsprofile, zusätzliche Softwaretests.	384	VGB / EnBW	Ergänzung zum vorigen Abschnitt mit Verweis auf Forschungsvorhaben der ISTec Team 5: Betrifft Vorläuferversion 13.3.3 (2). Dieser Kommentar bezieht sich nicht auf den Regeltext sondern auf die Erläuterungen in der Synopse in der Rev. 6.	7.3.2.3 (2)	Zur Bewertung der Gleichwertigkeit sind werden herangezogen: – Referenzen über den Hersteller der Software, – die Entwicklungs dokumentation -, Anwenderdokumentation und QS-Dokumentation der Software, – die Ergebnisse unabhängiger Begutachtung (Zertifikate) der Software, – die Betriebserfahrung der Software unter Berücksichtigung der Anwendungsprofile, – zusätzliche Softwaretests.
14.3	Software für Leitechnik-Funktionen der Kategorie B				7.3.3	Software für Leitechnik-Funktionen der Kategorie B
14.3.1	Grundsätze				7.3.3.1	Grundsätze
14.3.1 (1)	Für die Entwicklung und Qualifizierung der Software der Leitechnik-Funktionen der Kategorie B werden rechnergestützte Beschreibungen und Testverfahren angewendet, die den Nachweis der korrekten Arbeitsweise unterstützen.				7.3.3.1 (1)	Für die Entwicklung und Qualifizierung der Software der Leitechnik-Funktionen der Kategorie B sind werden rechnergestützte Beschreibungen und Testverfahren angewendet, die den Nachweis der korrekten Arbeitsweise unterstützen.
14.3.1 (2)	Die Programme sind robust und selbstüberwachend ausgelegt.	519	BfS	Begründung zum Kommentar: Die Antwort von Team 5 sollte umgesetzt werden. <u>Änderungsvorschlag:</u> Die Software ist Programme sind robust und	7.3.3.1 (2)	Die Software ist Programme sind robust und selbstüberwachend ausgelegt.

Ziffer	Textvorschlag Modul 5/Teil 1 (Rev. A)	Komm. Nr.	Kommentator	Kommentar bzw. Antwort	Ziffer (Neu)	Textvorschlag Modul 5/Teil 1 (Rev. B)
				selbstüberwachend auszulegen. Team 5: Der Änderungsvorschlag wird in der Rev. B umgesetzt.		
14.3.2	Qualitätssicherung				7.3.3.2	Qualitätssicherung
14.3.2.1	Konstruktive Qualitätssicherung				14.3.2.1	Konstruktive Qualitätssicherung
14.3.2.1 (1)	Die Softwareerstellung folgt einem methodisch abgestimmten Phasenmodell und wird weitgehend mit rechnergestützten Werkzeugen durchgeführt.	598	VGB Power	"... und weitgehend mit rechnergestützten Werkzeugen durchgeführt werden": Was ist weitgehend? über 50 % / über 90 % ...? Team 5: Dies ist eine Anforderung die abgestuft ist zur Anforderung für die Kategorie A. Die Anforderungen an die Software der Leitechtechnik- Funktionen der Kategorie B sind gegenüber der Anforderungen der Kategorie A durch den Begriff „weitgehend“ anstelle von „durchgehend“ abgestuft und stellen einen Zielsetzung dar. Ob 50% oder 90% der Software der Kategorie B mit rechnergestützten Werkzeugen erstellt wird, ist in jedem Einzelfall zu entscheiden.	7.3.3.2 (1)	Die Softwareerstellung erfolgt nach einem methodisch abgestimmten Phasenmodell und wird weitgehend mit rechnergestützten Werkzeugen durchgeführt.
14.3.2.1 (2)	Die Software ist aus hinsichtlich der Funktion funktionell klar abgegrenzten Einheiten aufgebaut. Diese Softwareeinheiten sind auf unverzichtbare Anweisungen und Schnittstellen beschränkt und zu einer übersichtlichen Programmstruktur integriert.				7.3.3.2 (2)	Die Software ist aus hinsichtlich der Funktion funktionell klar abgegrenzten Einheiten aufgebaut. Diese Softwareeinheiten sind auf unverzichtbare Anweisungen und Schnittstellen beschränkt und zu in einer übersichtlichen Programmstruktur integriert.
14.3.2.2	Analytische Qualitätssicherung				14.3.2.2	Analytische Qualitätssicherung
14.3.2.2 (1)	Die Ergebnisse der einzelnen Phasen der Softwareentwicklung sind einer Prüfung zu unterziehen und zu dokumentieren. Alle sicherheitsrelevanten Programmteile sind durch eine Kombination von Testverfahren zu prüfen, wobei				7.3.3.2 (3)	Die Ergebnisse der einzelnen Phasen der Softwareentwicklung sind einer dokumentierten Prüfung unterzogen. zu unterziehen und zu dokumentieren. Es ist Alle sicherheitsrelevanten Programmteile sind durch eine Kombina-

Ziffer	Textvorschlag Modul 5/Teil 1 (Rev. A)	Komm. Nr.	Kommentator	Kommentar bzw. Antwort	Ziffer (Neu)	Textvorschlag Modul 5/Teil 1 (Rev. B)
	eine vollständige Funktionstestüberdeckung zu erreichen ist.					tion von Testverfahren angewandt, so dass für alle sicherheitsrelevanten Programmteile zu prüfen, wobei eine vollständige Funktionstestüberdeckung zu erreicht wird. en ist.
14.3.2.2 (2)	Das anforderungsgerechte Verhalten des Hardware- und Softwaresystems ist in seinen sicherheitsrelevanten Funktionen zu validieren.				7.3.3.2 (4)	Das anforderungsgerechte Verhalten des Hardware- und Softwaresystems ist in seinen sicherheitsrelevanten Funktionen zu validierten.
14.3.2.3	Organisation und Administration				14.3.2.3	Organisation und Administration
14.3.2.3 (1)	Die Organisation und Administration der Softwareentwicklung und der Qualitätssicherung stellt sicher, 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 erstellt.				7.3.3.2 (5)	Die Organisation und Administration der Softwareentwicklung und der Qualitätssicherung ist so gestaltet, dass sichergestellt ist, sicher, 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. erstellt.
14.3.2.3 (2)	Die konsistente Konfiguration der Programme ist sichergestellt.				7.3.3.2 (6)	Die konsistente Konfiguration der Programme ist sichergestellt.
14.3.3	Einsatz von vorgefertigter Software				7.3.3.3	Einsatz von vorgefertigter Software
14.3.3 (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 13.4.1 und 13.4.2 gleichwertig sind.	384	VGB / EnBW	s. Kommentar zu 13.3.3 (1) Team 5: Betrifft Vorläuferversion 13.4.3 (1). Siehe Antwort und Kommentar zu 7.3.2.1 (1).	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 13.4.1 und 13.4.2 7.3.3.1 und 7.3.3.2 gleichwertig sind.
14.3.3 (2)	Zur Bewertung der Gleichwertigkeit werden herangezogen:	384	VGB / EnBW	Ergänzung zum vorigen Abschnitt mit Verweis auf Forschungsvorhaben der ISTec.	7.3.3.3 (2)	Zur Bewertung der Gleichwertigkeit sind werden werden herangezogen:

Ziffer	Textvorschlag Modul 5/Teil 1 (Rev. A)	Komm. Nr.	Kommen-tator	Kommentar bzw. Antwort	Ziffer (Neu)	Textvorschlag Modul 5/Teil 1 (Rev. B)
	<ul style="list-style-type: none"> – Referenzen über den Hersteller der Software, – die Entwicklungs-, Anwenderdokumentation und QS-Dokumentation der Software, – die Ergebnisse unabhängiger Begutachtung (Zertifikate) der Software, – die Betriebserfahrung der Software unter Berücksichtigung der Anwendungsprofile, – zusätzliche Softwaretests. 			Team 5: Betrifft Vorläuferversion 13.4.3 (2). Dieser Kommentar bezieht sich nicht auf den Regeltext sondern auf die Erläuterungen in der Synopse in der Rev. 6.		<ul style="list-style-type: none"> – 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.
14.4	Software für Leitechnik-Funktionen der Kategorie C				7.3.4	Software für Leitechnik-Funktionen der Kategorie C
14.4.1	Grundsatz				7.3.4.1	Grundsatz
	Die Software für Leitechnik-Funktionen der Kategorie C wird nach anerkannten Methoden der Softwaretechnik qualifiziert.					Die Software für Leitechnik- Funktionen der Kategorie C ist wird nach anerkannten Methoden der Softwaretechnik qualifiziert.
14.4.2	Qualitätssicherung				7.3.4.2	Qualitätssicherung
14.4.2.1	Konstruktive Qualitätssicherung				14.4.2.1	Konstruktive Qualitätssicherung
	Bei der Softwareerstellung sind die Entwicklungsschritte einzeln ausgewiesen. Hinweis: Nach Möglichkeit werden bei wesentlichen Entwicklungsschritten Software-Werkzeuge genutzt.				7.3.4.2 (1)	Bei der Softwareerstellung sind die Entwicklungsschritte einzeln ausgewiesen. Hinweis: Nach Möglichkeit sind werden bei wesentlichen Entwicklungsschritten Software-Werkzeuge genutzt.
14.4.2.2	Analytische Qualitätssicherung				14.4.2.2	Analytische Qualitätssicherung
14.4.2.2 (1)	Das Erreichen der Phasenziele ist durch Prüfungen nachgewiesen und dokumentiert.				7.3.4.2 (2)	Das Erreichen der Phasenziele ist durch Prüfungen nachgewiesen und dokumentiert.
14.4.2.2 (2)	Das anforderungsgerechte Verhalten des Hardware- und Softwaresystems				7.3.4.2 (3)	Das anforderungsgerechte Verhalten des Hardware- und Softwaresystems

Ziffer	Textvorschlag Modul 5/Teil 1 (Rev. A)	Komm. Nr.	Kommentator	Kommentar bzw. Antwort	Ziffer (Neu)	Textvorschlag Modul 5/Teil 1 (Rev. B)
	wird in seinen sicherheitsrelevanten Funktionen validiert.					ist wird in seinen sicherheitsrelevanten Funktionen validiert.
14.4.2.3	Organisation und Administration					Organisation und Administration
	Die Software ist nach einem anerkannten Qualitätssicherungsplan erstellt. Es ist eine vollständige Entwicklungs-, Qualitätssicherungs- und Benutzerdokumentation erstellt.	598	VGB Power	"Die Software ist nach einem anerkannten Qualitätssicherungsplan zu erstellen. ..." Wer muss den QS-Plan anerkennen? Gutachter? Überwachungsbehörde? Besteller? Oder muss er nur den anerkannten Regeln der Technik (also IEC) entsprechen? Team 5: Siehe Textergänzung.	7.3.4.2 (4)	Die Software ist nach einem anerkannten Qualitätssicherungsplan gemäß den anerkannten Regeln der Technik erstellt. Es ist wird eine vollständige Entwicklungs-, Qualitätssicherungs- und Benutzerdokumentation vorhanden. erstellt.
14.4.3	Einsatz von vorgefertigter Software				7.3.4.3	Einsatz von vorgefertigter Software
	Eingesetzte vorgefertigte Software ist zertifiziert oder betriebsbewährt.					Eingesetzte vorgefertigte Software ist soll ist betriebsbewährt oder zertifiziert sein. oder betriebsbewährt.
8	Robustheit				8	Robustheit
8 (1)	Die zulässigen elektrischen, elektromagnetischen, thermischen, mechanischen und strahlungs- sowie feuchtigkeitsbedingten Belastungen sind so festgelegt, dass die zu unterstellenden Betriebs- und Störfallbedingungen zuverlässig abgedeckt werden. Ausfälle und Fehlverhalten der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A bis C ausführen, treten erst bei deutlichen Überschreitungen dieser Belastungen auf.	384	VGB / EnBW	Erweiterung des Geltungsumfangs auf die gesamte Leittechnik. In dieser umfassenden und für alle Funktionen und Einrichtungen gültigen Form weder erforderlich noch machbar. Team 5: Betrifft Vorläuferversion 7 (1). Der Kommentar bezieht sich auf die Formulierung aus dem Modul 5 Rev. 6, die aufgrund von Änderungsvorschläge bereits durch die Rev. A (s. Abs. 1 Geltungsbereich und 2. Kategorisierung) abgelöst worden ist.	8 (1)	Die zulässigen elektrischen, elektromagnetischen, thermischen, mechanischen und strahlungs- sowie feuchtigkeitsbedingten Einwirkungen Belastungen sind so festgelegt, dass die zu unterstellenden Betriebs- und Störfallbedingungen zuverlässig abgedeckt werden. Ausfälle und Fehlverhalten der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A bis C ausführen, treten erst bei deutlichen Überschreitungen dieser Belastungen auf.
		598	VGB Power	(letzter Satz) "... dürfen erst bei deutlichen Überschreitungen dieser Belastungen auftreten": Was ist gemeint? (5 % 20 % oder 200 % Überschreitung) Team 5: Der zweite Satz hat Empfehlungscharakter und kann im Indikativ entfallen.		

Ziffer	Textvorschlag Modul 5/Teil 1 (Rev. A)	Komm. Nr.	Kommentator	Kommentar bzw. Antwort	Ziffer (Neu)	Textvorschlag Modul 5/Teil 1 (Rev. B)
8 (2)	Die Funktionssicherheit der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A bis C ausführen, wird durch Bedienung und Instandhaltung nicht unzulässig beeinträchtigt.				8 (2)	Bedienung und Instandhaltung sind so gestaltet, dass die Funktionssicherheit der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A bis C ausführen, wird durch Bedienung und Instandhaltung nicht unzulässig beeinträchtigt wird.
8 (3)	Die leittechnischen Einrichtungen, die für die Durchführung der im Rahmen des anlageninternen Notfallschutzes vorgesehenen Maßnahmen erforderlich sind, verlieren durch die Folgen dieser Ereignisse nicht ihre erforderliche Funktionsfähigkeit.	598	VGB Power	<p>Zu den Maßnahmen des Notfallschutzes gibt es keine definierten Ereignisabläufe (sondern Ziele) und damit auch keine eindeutige Zuordnung leittechnischer Einrichtungen.</p> <p>(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.</p> <p>Team 5: Hier geht es um die Ereignisabläufe oder Anlagenzustände der Sicherheits-ebene 4b und 4c. Text wurde unter Berücksichtigung des Kommentars präzisiert.</p>	8 (3)	Die leittechnischen Einrichtungen, die für die Durchführung der im Rahmen des anlageninternen Notfallschutzes vorgesehenen Maßnahmen erforderlich sind, werden so ausgelegt, dass sie verlieren durch die Folgen dieser Ereignisabläufe oder Anlagenzustände nicht ihre erforderliche Funktionsfähigkeit nicht verlieren.
8 (4)	Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A bis C ausführen, sind so ausgelegt, dass hinreichende Reserven gegenüber Alterungseffekten vorhanden sind.	384	VGB / EnBW	<p>Erweiterung des Geltungsumfangs auf die gesamte Leittechnik. In dieser umfassenden und für alle Funktionen und Einrichtungen gültigen Form weder erforderlich noch machbar.</p> <p>Team 5: Betrifft Vorläuferversion 7 (4). Der Kommentar bezieht sich auf die Formulierung aus dem Modul 5 Rev. 6, die aufgrund von Änderungsvorschläge bereits durch die Rev. A (s. Abs. 1 Geltungsbereich und 2. Kategorisierung) abgelöst worden ist.</p>	8 (4)	Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A bis C ausführen, sind so ausgelegt, dass hinreichende Reserven gegenüber Alterungseffekten vorhanden sind.

Ziffer	Textvorschlag Modul 5/Teil 1 (Rev. A)	Komm. Nr.	Kommentator	Kommentar bzw. Antwort	Ziffer (Neu)	Textvorschlag Modul 5/Teil 1 (Rev. B)
		598	VGB Power	Was sind „hinreichende Reserven“? (5 %, 20 %, 200 %?) Team 5: Die Anforderung entspricht inhaltlich dem Text RSK-LL-DWR, 7.3.7 (4) und erfordert keine weitere Präzisierung in der Detaillierung des Moduls 5.		
8 (5)	Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A bis C ausführen, sollen unempfindlich gegenüber Über- und Unterschreitungen des zulässigen Spannungsbereichs der elektrischen Energieversorgung sein.	384	VGB / EnBW	Erweiterung des Geltungsumfangs auf die gesamte Leittechnik. In dieser umfassenden und für alle Funktionen und Einrichtungen gültigen Form weder erforderlich noch machbar. Team 5: Der Kommentar bezieht sich auf die Formulierung aus dem Modul 5 Rev. 6, die aufgrund von Änderungsvorschläge bereits durch die Rev. A (s. Abs. 1 Geltungsbereich und 2. Kategorisierung) abgelöst worden ist.	8 (5)	Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A bis C ausführen, sind mit Toleranz sollen unempfindlich gegenüber Über- und Unterschreitungen des zulässigen Spannungsbereichs der elektrischen Energieversorgung ausgelegt. sein.
		598	VGB Power	"... unempfindlich gegenüber Über- und Unterschreitungen des zulässigen Spannungsbereichs ...": Ohne Angabe, wie viel Toleranz gefordert wird, ist das technisch unsinnig. Team 5: Die Anforderung entspricht inhaltlich dem Text RSK-LL-DWR, 7.3.7 (5) und erfordert keine weitere Präzisierung in der Detaillierung des Moduls 5.		
8 (6)	Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A und B ausführen, sind fehlertolerant aufgebaut. Das Ausfallverhalten ist grundsätzlich definiert und soll möglichst sicherheitsgerichtet sein.				8 (6)	Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A und B ausführen, sind fehlertolerant aufgebaut. Sie sind so ausgelegt, dass d Das Ausfallverhalten ist grundsätzlich definiert und soll ist. sein. möglichst sicherheitsgerichtet ist.
8 (7)	Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorien A	384	VGB / EnBW	Erweiterung des Geltungsumfangs auf die gesamte Leittechnik. In dieser umfassenden	8 (7)	Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorien

Ziffer	Textvorschlag Modul 5/Teil 1 (Rev. A)	Komm. Nr.	Kommentator	Kommentar bzw. Antwort	Ziffer (Neu)	Textvorschlag Modul 5/Teil 1 (Rev. B)
	bis C ausführen, werden grundsätzlich so ausgelegt, dass während des Leistungsbetriebs keine Wartungsarbeiten durchgeführt werden müssen.			und für alle Funktionen und Einrichtungen gültigen Form weder erforderlich noch machbar. Team 5: Betrifft Vorläuferversion 7 (7). Der Kommentar bezieht sich auf die Formulierung aus dem Modul 5 Rev. 6, die aufgrund von Änderungsvorschläge bereits durch die Rev. A (s. Abs. 1 Geltungsbereich und 2. Kategorisierung) abgelöst worden ist.		A bis C ausführen, sind werden grundsätzlich so ausgelegt, dass während des Leistungsbetriebs keine Wartungsarbeiten erforderlich sind. durchgeführt werden müssen.
9	Mensch-Maschine-Schnittstelle bei leittechnischen Einrichtungen	598	VGB Power	Weitere Festlegungen sind unter Teil 2 Kap. 4 getroffen. Sollte zusammengeführt werden. Team 5: Dieser Abschnitt wird in der Rev. B derart verändert, dass die meisten Inhalte im Modul 10 berücksichtigt und die Anforderungen an die leittechnischen Einrichtungen nach Abschnitt 3 verschoben werden.	9	Mensch-Maschine-Schnittstelle bei leittechnischen Einrichtungen
9 (1)	Arbeitsplätze, Arbeitsmittel, Arbeitsabläufe und Arbeitsumgebung sind unter Berücksichtigung ergonomischer Gesichtspunkte so gestaltet und Aufgaben sind auf Personal und leittechnische Einrichtungen so aufgeteilt, dass die Voraussetzungen für ein sicherheitstechnisch optimales Verhalten der Beschäftigten geboten werden.	384	VGB / EnBW	Text gegenüber Quelle nicht vollständig übernommen. Team 5: Betrifft Vorläuferversion 8(1). Diese Anforderung wird in der Rev. B inhaltlich im Modul 10 berücksichtigt.	9 (1)	Arbeitsplätze, Arbeitsmittel, Arbeitsabläufe und Arbeitsumgebung werden unter Berücksichtigung ergonomischer Gesichtspunkte so gestaltet und Aufgaben werden auf Personal und leittechnische Einrichtungen so aufgeteilt, dass die Voraussetzungen für ein sicherheitstechnisch optimales Verhalten der Beschäftigten geboten sind.
9 (2)	Auf der Warte sind alle Informationen und Bedienmöglichkeiten verfügbar, die zum Beobachten des Anlagenzustandes und zum Bedienen in allen Betriebsphasen und -zuständen erforderlich sind.		Team 5	Diese Anforderung wird in der Rev. B inhaltlich im Modul 10 berücksichtigt.	9 (2)	Die Warte wird so gestaltet, dass alle Informationen und Bedienmöglichkeiten, die zum Beobachten des Anlagenzustandes und zum Bedienen in allen Betriebsphasen und -zuständen erforderlich sind, verfügbar sind.
9 (3)	In der Spezifikation der Prozessführungs- und der Informationseinrichtungen sind deren sicherheitsrelevante Ziele festgelegt.	384	VGB / EnBW	Redaktionelle Änderung oder soll der Inhalt verändert werden? Team 5: Betrifft Vorläuferversion 2.4. Re-	9 (3)	In der Spezifikation der Prozessführungs- und der Informationseinrichtungen werden deren sicherheitsrelevante Ziele festgelegt.

Ziffer	Textvorschlag Modul 5/Teil 1 (Rev. A)	Komm. Nr.	Kommen-tator	Kommentar bzw. Antwort	Ziffer (Neu)	Textvorschlag Modul 5/Teil 1 (Rev. B)
				daktionelle Änderung. Diese Anforderung wird in der Rev. B nach Abs. 5.3 verschoben.		
9 (4)	Die Informationsdarbietung ist ergonomisch so gestaltet, dass sie die Beurteilung und Diagnose des Anlagenzustandes durch das Betriebspersonal unterstützt. Bei hoher Informationsverdichtung bleibt der Zugriff auf sicherheitstechnisch relevante Einzelinformationen gewahrt.		Team 5	Diese Anforderung wird in der Rev. B inhaltlich im Modul 10 berücksichtigt.	9 (4)	Die Informationsdarbietung wird ergonomisch so gestaltet, dass sie die Beurteilung und Diagnose des Anlagenzustandes durch das Betriebspersonal unterstützt.
9 (5)	Anregekriterien für Leitechnik-Funktionen der Kategorie A und die dadurch ausgelösten Maßnahmen sind in der Warte übersichtlich angezeigt.	384	VGB / EnBW	Das ist eine Verschlimmbesserung des Textes falls damit wie in der alten Formulierung die Reaktorschutztafel gemeint sein sollte. Sollte das nicht gemeint sein ist die Forderung weder notwendig noch angemessen. Team 5: Betrifft Vorläuferversion 8 (5). Hier ist die Reaktorschutztafel gemeint. Diese Anforderung wird in der Rev. B nach Abs. 3.2 (18) verschoben.	9 (5)	Die Warte wird so gestaltet, dass Anregekriterien für Leitechnik-Funktionen der Kategorie A und die dadurch ausgelösten Maßnahmen in der Warte übersichtlich angezeigt werden.
9 (6)	Die durch die Leitechnik-Funktionen der Kategorie A ausgelösten Maßnahmen sind 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.	384	VGB / EnBW	Erweiterung des Geltungsumfangs auf die gesamte Leitechnik. Für die Notsteuerstelle nur für deren spezifische Funktionen? Team 5: Betrifft Vorläuferversion 8 (6). s. Antwort zum Geltungsumfang bzw. Kategorisierung. Diese Anforderung wird in der Rev. B nach Abs. 3.2 (19) verschoben.	9 (6)	Die durch die Leitechnik-Funktionen der Kategorie A ausgelösten 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.
		598	VGB Power	Die Aufgabe der „Notsteuerstelle“ erfordert nicht die Darstellung der Informationen bezüglich aller Leitechnik-Funktionen der Kat. A. Team 5: Es sind die notwendigen Informationen zur Überprüfung des Anlagenzustandes angesprochen.		

Ziffer	Textvorschlag Modul 5/Teil 1 (Rev. A)	Komm. Nr.	Kommentator	Kommentar bzw. Antwort	Ziffer (Neu)	Textvorschlag Modul 5/Teil 1 (Rev. B)
9 (7)	Zur Überwachung der grundlegenden Sicherheitsfunktionen sind ergonomische Grundsätze angewendet.	384	VGB / EnBW	Das ist eine völlige Veränderung des Sinns der ursprünglichen Forderung. Durch die bildhafte Darstellung von Schutzziele wird der Übergang vom ereignisorientierten Vorgehen nach BHB zum schutzzielorientierten Vorgehen nach „Schutzziel BHB“ erleichtert. Team 5: Betrifft Vorläuferversion 8(7). Dieser Themenkomplex in der Rev. B inhaltlich im Modul 10 berücksichtigt. Diese Anforderung entfällt jedoch gänzlich.	9 (7)	Zur Überwachung der grundlegenden Sicherheitsfunktionen werden ergonomische Grundsätze angewandt.
9 (8)	Wird das Informationssystem in ein Sicherheits- und in ein Prozessinformationssystem aufgeteilt, dann sind beide Teile in voneinander unabhängigen Einrichtungen realisiert. Die Informationssysteme sind gemäß ihrer sicherheitstechnischen Bedeutung qualifiziert.	598	VGB Power	Der erste Satz hat keine Aussage: Wenn Sicherheits- und Prozessinformationssystem getrennt sind, müssen sie getrennt sein, wenn nicht, dann nicht. Satz kann ersatzlos entfallen. Team 5: Diese Anforderung wird in der Rev. B nach Abs. 5.4 verschoben. Der Vorschlag wird berücksichtigt und der erste Satz wird gestrichen.	9 (8)	Wird das Informationssystem in ein Sicherheits- und in ein Prozessinformationssystem aufgeteilt, dann werden beide Teile in voneinander unabhängigen Einrichtungen realisiert. Die Informationssysteme werden gemäß ihrer sicherheitstechnischen Bedeutung qualifiziert.
9 (9)	Die für die Beherrschung von Ereignissen und für die Durchführung von anlageninternen Notfallmaßnahmen erforderlichen Eingriffsmöglichkeiten in die leittechnischen Einrichtungen werden vorgesehen. Diese dürfen nicht die Funktionsfähigkeit der leittechnischen Einrichtungen beeinträchtigen, die Leittechnik-Funktionen der Kategorie A und B ausführen, und werden gegen Fehlbedienung gesichert.	384	VGB / EnBW	Erweiterung des Geltungsumfangs auf die gesamte Leittechnik und auf alle Ereignisse. In dieser umfassenden und für alle Funktionen und Einrichtungen gültigen Form weder erforderlich noch machbar. Team 5: Betrifft Vorläuferversion 8(9). Der Kommentar bezieht sich auf die Formulierung aus dem Modul 5 Rev. 6, die aufgrund von Änderungsvorschläge bereits durch die Rev. A (s. Abs. 1 Geltungsbereich und 2. Kategorisierung) abgelöst worden ist. Diese Anforderung wird in der Rev. B nach Abs. 3.1 (12) verschoben.	9 (9)	Die leittechnischen Einrichtungen werden so ausgelegt, dass die für die Beherrschung von Ereignissen und für die Durchführung von anlageninternen Notfallmaßnahmen erforderlichen Eingriffsmöglichkeiten vorhanden sind. Die Eingriffsmöglichkeiten werden so ausgelegt, dass sie die Funktionsfähigkeit der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A und B ausführen, nicht beeinträchtigen und sie werden gegen Fehlbedienung gesichert.
		492	VGB / Powertech	Nicht verständliche Anforderung: Unter anderem werden auf der einen Seite im Teil 1 unter 9(9) Eingriffsmöglichkeiten in leittechnische Einrichtungen zur Durchführung von		

Ziffer	Textvorschlag Modul 5/Teil 1 (Rev. A)	Komm. Nr.	Kommentator	Kommentar bzw. Antwort	Ziffer (Neu)	Textvorschlag Modul 5/Teil 1 (Rev. B)
				<p>anlageninternen Notfallmaßnahmen gefordert. Auf der anderen Seite sollen Handeingriffe nicht dazu führen, dass Einrichtungen, die Leittechnische Funktionen der Kategorie A oder B ausführen, beeinträchtigt werden.</p> <p>Team 5: Im Modul 5 werden Anforderungen an die leittechnischen Einrichtungen (s. Geltungsbereich und Kategorisierung) formuliert. In den Anforderungen des Modul 5 wird unterschieden zwischen den vorgeplanten Maßnahmen und entsprechenden Möglichkeiten zu deren Durchführung und sonstigen Eingriffen in die leittechnischen Einrichtungen.</p>		
		598	VGB Power	<p>Die Forderung nach (Hand-) Eingriffsmöglichkeiten für Notfallmaßnahmen, die aber leittechnische Einrichtungen für Leittechnik-Funktionen der Kat. A und B nicht beeinträchtigen dürfen, ist widersprüchlich. Handeingriffe im Notfall müssen immer Vorrang haben. Dieses Thema ist in Modul 1, Punkt 3.2 (5) verständlicher behandelt.</p> <p>Team 5: Im Modul 1, Punkt 3.2 (5) ist die übergeordnete Anforderung formuliert. Im Modul 5 wird Berücksichtigung der Eingriffsmöglichkeiten bei der Auslegung geregelt.</p>		
9 (10)	Für den Fall, dass die Warte nicht zur Verfügung steht, wird die Anlage von einer anderen Stelle in einen langfristig sicheren Zustand überführt und dort gehalten.		Team 5	Diese Anforderung wird in der Rev. B inhaltlich im Modul 10 berücksichtigt.	9 (10)	Für den Fall, dass die Warte nicht zur Verfügung steht, wird die Anlage von einer anderen Stelle in einen langfristig sicheren Zustand überführt und dort gehalten.
10	Instandhaltung und Änderungen	598	VGB Power	<p>Mit welchem Ziel wird geprüft? Der gesamte Abschnitt zu Prüfungen berücksichtigt selbstüberwachende Systeme (mit aktiver Aussteuerung einer Fehlermeldung z.B. bei Abweichungen zwischen zwei redundanten Kanälen) nicht.</p>	10 9	Instandhaltung und Änderungen

Ziffer	Textvorschlag Modul 5/Teil 1 (Rev. A)	Komm. Nr.	Kommentator	Kommentar bzw. Antwort	Ziffer (Neu)	Textvorschlag Modul 5/Teil 1 (Rev. B)
				Team 5: Ziel der Prüfung ist die Funktionsfähigkeit der Einrichtung nachzuweisen und die Feststellung spezifikationsgerechter Eigenschaften.		
10 (1)	Die Funktionsfähigkeit der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A bis C ausführen, ist während der Nutzungsdauer der Anlage durch Prüfungen nachgewiesen. Diese Prüfungen erfassen alle funktionswichtigen Einrichtungen.	384	VGB / EnBW	Erweiterung des Geltungsumfangs auf die gesamte Leittechnik. In dieser umfassenden und für alle Funktionen und Einrichtungen gültigen Form weder erforderlich noch machbar. Team 5: Betrifft Vorläuferversion 9(1). Der Kommentar bezieht sich auf die Formulierung aus dem Modul 5 Rev. 6, die aufgrund von Änderungsvorschläge bereits durch die Rev. A (s. Abs. 1 Geltungsbereich und 2. Kategorisierung) abgelöst worden ist.	940 (1)	Die Funktionsfähigkeit der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A bis C ausführen, ist während der Betrieb Nut- zungsdauer der Anlage durch Prüfungen nachgewiesen. Diese Prüfungen erfassen alle funktionswichtigen Einrichtungen.
10 (2)	Art und Umfang der Prüfungen und die Zeitabstände zwischen den Prüfungen sind festgelegt. Diese Festlegungen sind in regelmäßigen Abständen u. a. anhand der Betriebserfahrungen überprüft.				940 (2)	Art und Umfang der Prüfungen und die Zeitabstände zwischen den Prüfungen sind festgelegt. Diese Festlegungen werden sind in regelmäßigen Abständen u. a. anhand der Betriebserfahrungen überprüft.
10 (3)	Die Ergebnisse der Prüfungen werden dokumentiert.				940 (3)	Die Ergebnisse der Prüfungen werden dokumentiert.
10 (4)	Während des bestimmungsgemäßen Betriebs soll die Durchführung der Prüfungen möglich sein, mit denen die einwandfreie Funktion der gesamten leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A bis C ausführen, nachgewiesen werden kann. Die leittechnischen Einrichtungen werden grundsätzlich so ausgelegt, dass durch Prüfungen verursachte Veränderungen nach den Prüfungen rückgesetzt werden. Es können automatische und manuelle Prüfungen vorgesehen wer-	384	VGB / EnBW	Erweiterung des Geltungsumfangs auf die gesamte Leittechnik. Diese Forderung ist für die Gesamtheit der Leittechnik nicht erfüllbar. Team 5: Betrifft Vorläuferversion 9 (4). Der Kommentar bezieht sich auf die Formulierung aus dem Modul 5 Rev. 6, die aufgrund von Änderungsvorschläge bereits durch die Rev. A (s. Abs. 1 Geltungsbereich und 2. Kategorisierung) abgelöst worden ist. Der erste Satz wird gestrichen, da die Anforderung durch (1) abgedeckt ist.	940 (4)	Während des bestimmungsgemäßen Betriebs soll die Durchführung der Prüfungen möglich sein, mit denen die einwandfreie Funktion der gesamten leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A bis C ausführen, nachgewiesen werden kann. Die leittechnischen Einrichtungen sind werden grundsätzlich so ausgelegt, dass durch Prüfungen verursachte Veränderungen nach den Prüfungen rückgesetzt werden. Prüfungen werden Es können automati-

Ziffer	Textvorschlag Modul 5/Teil 1 (Rev. A)	Komm. Nr.	Kommentator	Kommentar bzw. Antwort	Ziffer (Neu)	Textvorschlag Modul 5/Teil 1 (Rev. B)
	den. Durch eine Prüfung tritt keine unzulässige Minderung der Sicherheit der Reaktoranlage ein.					sche oder und-manuell durchgeführt. e Prüfungen vorgesehen werden. Die Prüfungen sind so geplant und durchgeführt, dass durch sie Durch eine Prüfung tritt keine unzulässige Minderung der Sicherheit der ReaktoraAnlage eintritt. 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.
10 (5)	Prüfungen sind grundsätzlich von zentralen Stellen durch verantwortliches Betriebspersonal überwachbar.	598	VGB Power	Zumindest missverständlich. Soll nur die Tatsache der Prüfung angezeigt werden, oder soll der Prüfablauf tatsächlich überwacht werden? Team 5: Die Anforderung entspricht inhaltlich dem Text RSK-LL-DWR, 7.3.9 (2) und erfordert keine weitere Präzisierung in der Detaillierung bzgl. der Überwachung der Prüfungen.	940 (5)	Prüfungen sind so gestaltet, dass sie grundsätzlich von zentralen Stellen durch verantwortliches Betriebspersonal überwachbar sind.
10 (6)	Erforderliche Instandhaltungsarbeiten sind ohne unzulässige Minderung der Sicherheit der Reaktoranlage durchführbar. Die Überprüfung des ordnungsgemäßen Zustandes nach Ausführung der Tätigkeit soll leicht durchführbar sein oder automatisch erfolgen. Auswirkungen zu unterstellender Fehlhandlungen bleiben auf einen Strang beschränkt.		Team 5	Redaktionelle Anpassung und Straffung des Inhalts.	940 (6)	Erforderliche Instandhaltungsarbeiten sind so gestaltet, dass sie ohne unzulässige Minderung der Sicherheit der ReaktoraAnlage durchführbar sind und Auswirkungen zu unterstellender Fehlhandlungen auf einen Strang beschränkt bleiben. Die Überprüfung des ordnungsgemäßen Zustandes nach Ausführung der Tätigkeit soll leicht durchführbar sein oder automatisch erfolgen. Auswirkungen zu unterstellender Fehlhandlungen bleiben auf einen Strang beschränkt.
10 (7)	Bei Änderungen in den leittechnischen Einrichtungen, die Leittechnik- Funktionen der Kategorie A bis C ausführen,	384	VGB / EnBW	Erweiterung des Geltungsumfangs auf die gesamte Leittechnik.	940 (7)	Bei Änderungen in den leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A bis C ausführen,

Ziffer	Textvorschlag Modul 5/Teil 1 (Rev. A)	Komm. Nr.	Kommentator	Kommentar bzw. Antwort	Ziffer (Neu)	Textvorschlag Modul 5/Teil 1 (Rev. B)
	werden mindestens die gleichen Qualitätsstandards angewendet wie bei Erstellung der leittechnischen Einrichtungen.			Team 5: Betrifft Vorläuferversion 9(7). Der Kommentar bezieht sich auf die Formulierung aus dem Modul 5 Rev. 6, die aufgrund von Änderungsvorschläge bereits durch die Rev. A (s. Abs. 1 Geltungsbereich und 2. Kategorisierung) abgelöst worden ist.		werden mindestens die gleichen Qualitätsstandards angewendet wie bei Erstellung der leittechnischen Einrichtungen.
10 (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.				940 (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.
10 (9)	Änderungen der Software der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A bis C ausführen, werden unter Einhaltung der Qualitätsanforderungen nach Abschnitt 14 vorgenommen. Durch Änderungen der Software der leittechnischen Einrichtungen und durch fehlerhafte Eingriffe wird keine unzulässige Minderung der Sicherheit der Reaktoranlage hervorgerufen. Alle Eingriffe in die Software werden dokumentiert und sind vollständig nachvollziehbar.	384	VGB / EnBW	Erweiterung des Geltungsumfangs auf die gesamte Leittechnik. Die RSK-LL erhebt diese Forderung nur für die Sicherheitsleittechnik und damit weder für die elektrischen Einrichtungen des Sicherheitssystems noch des Betriebssystems. Insofern ist hier eine vom Umfang her erhebliche Ausweitung des Regelungsumfangs vorgenommen worden. . In dieser umfassenden und für alle Funktionen und Einrichtungen gültigen Form weder erforderlich noch machbar. Team 5: Betrifft Vorläuferversion 9(9). Der Kommentar bezieht sich auf die Formulierung aus dem Modul 5 Rev. 6, die aufgrund von Änderungsvorschläge bereits durch die Rev. A (s. Abs. 1 Geltungsbereich und 2. Kategorisierung) abgelöst worden ist.	940 (9)	Änderungen der Software der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A bis C ausführen, werden unter Einhaltung der Qualitätsanforderungen nach Abschnitt 14-7.3 vorgenommen. Durch Änderungen der Software der leittechnischen Einrichtungen und durch fehlerhafte und dazu erforderliche Eingriffe in die leittechnischen Einrichtungen erfolgen so, dass dadurch wird keine unzulässige Minderung der Sicherheit der Reaktoranlage hervorgerufen wird. 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 w er den - und sind vollständig nachvollziehbar.
10 (10)	Parametrierdaten und Software der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A bis C	384	VGB / EnBW	Erweiterung des Geltungsumfangs auf die gesamte Leittechnik. In dieser umfassenden und für alle Funktionen und Einrichtungen	940 (10)	Parametrierdaten und Software der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A

Ziffer	Textvorschlag Modul 5/Teil 1 (Rev. A)	Komm. Nr.	Kommentator	Kommentar bzw. Antwort	Ziffer (Neu)	Textvorschlag Modul 5/Teil 1 (Rev. B)
	ausführen, sind rekonstruierbar: hierzu werden regelmäßig sowie bei Änderungen der Software Sicherungskopien angefertigt. Software- und Parametrierdatenbestände werden archiviert.			gültigen Form weder erforderlich noch machbar. Team 5: Betrifft Vorläuferversion 9 (10). Der Kommentar bezieht sich auf die Formulierung aus dem Modul 5 Rev. 6, die aufgrund von Änderungsvorschläge bereits durch die Rev. A (s. Abs. 1 Geltungsbereich und 2. Kategorisierung) abgelöst worden ist.		bis C ausführen, werden so behandelt, dass sie sind rekonstruierbar sind . hier Dazu werden regelmäßig sowie bei Änderungen der Software Sicherungskopien angefertigt. Software- und Parametrierdatenbestände sind werden archiviert.
11	Anforderungen an die Zugriffskontrolle				10 4	Anforderungen an die Zugriffskontrolle
11 (1)	Eingriffe in die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A und B ausführen, werden auf der Warte angezeigt. In Fällen, in denen das technisch nicht möglich ist, wird das Wartenpersonal zeitnah über die Eingriffe informiert.	384	VGB / EnBW	Ungeeignete Gleichsetzung von Kategorien der RSK-LL mit Sicherheitsebenen. Team 5: Betrifft Vorläuferversion 10 (1). Der Kommentar bezieht sich auf die Formulierung aus dem Modul 5 Rev. 6, die aufgrund von Änderungsvorschläge bereits durch die Rev. A (s. Abs. 1 Geltungsbereich und 2. Kategorisierung) abgelöst worden ist.	10 4 (1)	Eingriffe in die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A und B ausführen, werden auf der Warte angezeigt. In Fällen, in denen das technisch nicht möglich ist, wird das Wartenpersonal zeitnah über die Eingriffe informiert.
11 (2)	Eingriffe von Unbefugten in die leittechnischen Einrichtungen einschließlich Software sind vorzugsweise durch technische Einrichtungen so weit wie möglich erschwert oder verhindert. Eine Absicherung durch administrative Maßnahmen ist auf solche Bereiche beschränkt, die durch technische Maßnahmen nicht sinnvoll abgesichert werden können. Die Wirksamkeit und Zuverlässigkeit der vorgesehenen Maßnahmen entspricht der sicherheitstechnischen Bedeutung der leittechnischen Einrichtungen.	384	VGB / EnBW	Erweiterung des Geltungsbereichs auf die gesamte Leittechnik. In dieser umfassenden und für alle Funktionen und Einrichtungen gültigen Form weder erforderlich noch machbar. Team 5: Betrifft Vorläuferversion 10(2). Der Kommentar bezieht sich auf die Formulierung aus dem Modul 5 Rev. 6, die aufgrund von Änderungsvorschläge bereits durch die Rev. A (s. Abs. 1 Geltungsbereich und 2. Kategorisierung) abgelöst worden ist.	10 4 (2)	Eingriffe von Unbefugten Die unberechtigten Zugriffe in die leittechnischen Einrichtungen einschließlich der Software sind vorzugsweise durch technische Vorkehrungen Einrichtungen so weit wie möglich erschwert oder verhindert . Eine Absicherung durch organisatorische administrative Maßnahmen ist auf solche Bereiche beschränkt, die durch technische Vorkehrungen Maßnahmen nicht sinnvoll abgesichert werden können. Die Wirksamkeit und Zuverlässigkeit der vorgesehenen Maßnahmen und technischen Vorkehrungen entspricht der sicherheitstechnischen Bedeutung der leittechnischen Einrichtungen.
12	Dokumentation				11 2	Dokumentation

Ziffer	Textvorschlag Modul 5/Teil 1 (Rev. A)	Komm. Nr.	Kommentator	Kommentar bzw. Antwort	Ziffer (Neu)	Textvorschlag Modul 5/Teil 1 (Rev. B)
12 (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.	384	VGB / EnBW	Erweiterung des Geltungsbereichs für die gesamte Leittechnik. In dieser umfassenden und für alle Funktionen und Einrichtungen gültigen Form weder erforderlich noch machbar. Team 5: Betrifft Vorläuferversion 11(1). Der Kommentar bezieht sich auf die Formulierung aus dem Modul 5 Rev. 6, die aufgrund von Änderungsvorschläge bereits durch die Rev. A (s. Abs. 1 Geltungsbereich und 2. Kategorisierung) abgelöst worden ist.	112 (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.
12 (2)	Die Instandhaltungsvorgänge und Eingriffe in die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A bis C ausführen, sind dokumentiert.	384	VGB / EnBW	Erweiterung des Geltungsumfangs auf die gesamte Leittechnik. In dieser umfassenden und für alle Funktionen und Einrichtungen gültigen Form weder erforderlich noch machbar. Team 5: Betrifft Vorläuferversion 11(2). Der Kommentar bezieht sich auf die Formulierung aus dem Modul 5 Rev. 6, die aufgrund von Änderungsvorschläge bereits durch die Rev. A (s. Abs. 1 Geltungsbereich und 2. Kategorisierung) abgelöst worden ist.	112 (2)	Die Instandhaltungsvorgänge und Eingriffe in die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A bis C ausführen, sind dokumentiert.
12 (3)	Die Betriebserfahrung aus der Instandhaltung der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A bis C ausführen, wird erfasst, dokumentiert und systematisch ausgewertet.				112 (23)	Die Betriebserfahrung aus der Instandhaltung der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A bis C ausführen, wird erfasst, dokumentiert und systematisch ausgewertet.
13	Elektrische Energieversorgung der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A bis C ausführen				123	Elektrische Energieversorgung der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A bis C ausführen
13 (1)	Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A bis C ausführen, werden von unterbrechungslosen Notstromanlagen mit Energiespeicherung versorgt. Die Kapazität	384	VGB / EnBW	Die Gleichsetzung von SE und Kategorien entspricht nicht dem Stand von W&T. Team 5: Betrifft Vorläuferversion 12 (1). Der Kommentar bezieht sich auf die Formulierung	123 (1)	Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A bis C ausführen, werden von unterbrechungslosen Notstromanlagen mit Energiespeicherung versorgt. Die Ka-

Ziffer	Textvorschlag Modul 5/Teil 1 (Rev. A)	Komm. Nr.	Kommentator	Kommentar bzw. Antwort	Ziffer (Neu)	Textvorschlag Modul 5/Teil 1 (Rev. B)
	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 werden kann, ohne dass die zulässige Mindestspannung unterschritten wird. Nach vollständigem Spannungsausfall oder Unterschreiten der Mindestspannung sind die leittechnischen Einrichtungen nach Spannungswiederkehr funktionsfähig.	598	VGB Power	<p>rung aus dem Modul 5 Rev. 6, die aufgrund von Änderungsvorschläge bereits durch die Rev. A (s. Abs. 1 Geltungsbereich und 2. Kategorisierung) abgelöst worden ist.</p> <p>Soll die Streichung des Begriffs Batterie bedeuten, dass auch andere Speichermöglichkeiten zuzulassen sind?</p> <p>Team 5: Prinzipiell ja, wenn die Anforderungen an die Energieversorgung der leittechnischen Einrichtungen erfüllt werden.</p> <p>Anforderungen an die (Not-) Stromversorgung sollten ausschließlich an anderer Stelle stehen.</p> <p>Team 5: Die, wie hier, im Kontext stehenden Zusammenhänge können und sollten u. E. gemeinsam formuliert werden.</p>		<p>pazität 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 werden kann wird, ohne dass die zulässige Mindestspannung unterschritten wird. Die Energieversorgung ist so ausgelegt, dass nNach vollständigem Spannungsausfall oder Unterschreiten der Mindestspannung sind die leittechnischen Einrichtungen nach Spannungswiederkehr funktionsfähig sind.</p>
			Team 5		Hinweis:	Siehe auch „Sicherheitsanforderungen für Kernkraftwerke: Anforderungen an Elektrische Energieversorgung, Störfallinstrumentierung“ (Modul 5, Teil 2), Kapitel 1.
13 (2)	Bei der Auslegung der elektrischen Energieversorgung der leittechnischen Einrichtungen, die Leittechnik- Funktionen der Kategorie A bis C ausführen, sind die gleichen Ausfallkombinationen zugrunde gelegt wie bei der Auslegung der zu versorgenden leittechnischen Einrichtungen (vgl. für Kategorie A: Abschnitt 3.2 (12) und vgl. für Kategorie B: Abschnitt 3.3.	384	VGB / EnBW	<p>Erweiterung des Geltungsumfangs auf die gesamte Leittechnik. Gleichsetzung von SE und Kategorien. Kommentar s. oben.</p> <p>Team 5: Betrifft Vorläuferversion 12 (2). Der Kommentar bezieht sich auf die Formulierung aus dem Modul 5 Rev. 6, die aufgrund von Änderungsvorschläge bereits durch die Rev. A (s. Abs. 1 Geltungsbereich und 2. Kategorisierung) abgelöst worden ist.</p>	123 (2)	Bei der Auslegung der elektrischen Energieversorgung der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A bis C ausführen, sind die gleichen Ausfallkombinationen zu g Grunde gelegt wie bei der Auslegung der zu versorgenden leittechnischen Einrichtungen (vgl. für Kategorie A: Ziffer Abschnitt 3.2 (12) und vgl. für Kategorie B: Abschnitt 3.3).
13 (3)	Die Auslegung der einspeisenden Erzeugungsanlagen, der Verteilernetze und der leittechnischen Einrichtungen ist so aufeinander abgestimmt, dass die für die leittechnischen Einrichtungen	384	VGB / EnBW	<p>Erweiterung des Geltungsumfangs auf die gesamte Leittechnik s. o.</p> <p>Team 5: Betrifft Vorläuferversion 12 (3). Der Kommentar bezieht sich auf die Formulierung</p>	123 (3)	Die Auslegung der einspeisenden Erzeugungsanlagen, der Verteilernetze und der leittechnischen Einrichtungen ist so aufeinander abgestimmt, dass die für die leittechnischen Einrichtungen

Ziffer	Textvorschlag Modul 5/Teil 1 (Rev. A)	Komm. Nr.	Kommentator	Kommentar bzw. Antwort	Ziffer (Neu)	Textvorschlag Modul 5/Teil 1 (Rev. B)
	zugrunde gelegten Beanspruchungen nicht überschritten werden. Insbesondere werden die statischen und dynamischen Grenzwerte der für die leittechnischen Einrichtungen spezifizierten zulässigen Versorgungsspannungen nicht überschritten.			rung aus dem Modul 5 Rev. 6, die aufgrund von Änderungsvorschläge bereits durch die Rev. A (s. Abs. 1 Geltungsbereich und 2. Kategorisierung) abgelöst worden ist.		gen zu g Grunde gelegten Beanspruchungen nicht überschritten werden. Insbesondere werden und die statischen und dynamischen Grenzwerte der für die leittechnischen Einrichtungen spezifizierten zulässigen Versorgungsspannungen nicht überschritten werden.:-
13 (4)	Dynamische Spannungsänderungen in einem Stromkreis werden nicht zu Fehlfunktionen von leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A bis C ausführen, in benachbarten Stromkreisen führen.	384	VGB / EnBW	Änderung unverständlich. Erweiterung des Geltungsumfangs auf die gesamte Leittechnik Team 5: Betrifft Vorläuferversion 12 (4). Diese Anforderung ist inhaltlich in Abs. 3.1 (4) bereits berücksichtigt und wird an dieser Stelle gestrichen.	13 (4)	Die Energieversorgung wird so ausgelegt, dass dynamische Spannungsänderungen in einem Stromkreis nicht zu Fehlfunktionen von leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A bis C ausführen, oder in benachbarten Stromkreisen führen
13 (5)	Ausfälle der elektrischen Energieversorgung für die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A bis C ausführen, sind durch Überwachungseinrichtungen erfasst und gemeldet.	384	VGB / EnBW	Die Gleichsetzung von SE2 und 3 mit Sicherheitsleittechnik entspricht nicht dem Stand von W&T. Team 5: Betrifft Vorläuferversion 12 (5). Der Kommentar bezieht sich auf die Formulierung aus dem Modul 5 Rev. 6, die aufgrund von Änderungsvorschläge bereits durch die Rev. A (s. Abs. 1 Geltungsbereich und 2. Kategorisierung) abgelöst worden ist.	123 (45)	Ausfälle der elektrischen Energieversorgung für die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A bis C ausführen, werden durch Überwachungseinrichtungen erfasst und gemeldet.

Gliederung

1	Geltungsbereich	1
2	Kategorisierung.....	1
3	Auslegung.....	2
3.1	Leittechnische Einrichtungen für Leittechnik-Funktionen der Kategorien A bis C	2
3.2	Leittechnischen Einrichtungen-für Leittechnik-Funktionen der Kategorie A	3
3.3	Leittechnische Einrichtungen für Leittechnik-Funktionen der Kategorie B	8
3.4	Leittechnische Einrichtungen für Leittechnik-Funktionen auf der Sicherheitsebene 4	8
4	Anforderungsspezifikation für leittechnische Einrichtungen für Leittechnik-Funktionen der Kategorien A bis C	8
5	Erfassung von Prozessvariablen.....	9
6	Redundanz und Unabhängigkeit	10
7	Qualifizierung	11
7.1	Qualifizierung der Hard- und Software der leittechnischen Einrichtungen für Leittechnik-Funktionen der Kategorien A bis C.....	11
7.2	Qualifizierung der Hardware	12
7.3	Qualifizierung der Software	12
7.3.1	Software für Leittechnik-Funktionen der Kategorien A bis C.....	12
7.3.2	Software für Leittechnik-Funktionen der Kategorie A.....	13
7.3.3	Software für Leittechnik-Funktionen der Kategorie B.....	15
7.3.4	Software für Leittechnik-Funktionen der Kategorie C.....	16
8	Robustheit	17
9	Instandhaltung und Änderungen.....	18
10	Anforderungen an die Zugriffskontrolle	20
11	Dokumentation	20
12	Elektrische Energieversorgung der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorien A bis C ausführen	21

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 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.
- 3.1 (3) Leitungen und Kabel einschließlich Lichtwellenleiter sind nach Strängen 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 der Verfahrenstechnik 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 sind technische Vorkehrungen vorrangig vor organisatorischen Maßnahmen vorgesehen.
- 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, die Leittechnik-Funktionen der Kategorien A und B ausführen, nicht 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 die Einrichtungen gegen Eingriffe gesichert.

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

Handarmaturen sind in Bereitschaftsstellung möglichst eingriffssicher blockiert.

- 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 elektrisch unabhängig ausgeführt.

b) Ein Ausfall in den leittechnischen Einrichtungen des Sicherheitssystems hat höchstens Auswirkungen auf die Funktion des betroffenen Stranges 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 Ausfallkombi-

nationen nach dem Einzelfehlerkonzept verhindert wird, wenn dadurch Ereignisse der Sicherheitsebene 4 ausgelöst werden können.

Hinweis Anforderungen 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.

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 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.

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 leicht durchführbar sein.

Prüfeingriffe und Handbefehle 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 ausfüh-

ren, 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) 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.

- 3.2 (11) Bei der Auslegung der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, sind Vorkehrungen gegen systematische Ausfälle der Hardware und Versagen der Software derart getroffen, dass ein systematischer Ausfall so unwahrscheinlich ist, dass er ausgeschlossen werden kann.

- 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 (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 und des Zufallsausfalls nicht unterstellt.

- 3.2 (13) 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 Fehlauflösung 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.
- 3.2 (16) 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.
- 3.2 (17) Die leittechnischen Einrichtungen, die Leittechnikfunktionen der Kategorie A ausführen, sind so ausgelegt, dass auch beim Auftreten von Fehlern 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.

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.

3.4 Leittechnische Einrichtungen für Leittechnik-Funktionen auf der Sicherheitsebene 4

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.

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.

5 Erfassung von Prozessvariablen

- 5 (1) Für die unterstellten Ereignisse der Sicherheitsebenen 2 bis 4a sowie für die vorgeplanten Maßnahmen des anlageninternen Notfallschutzes 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 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.
- 5 (3) Die sicherheitstechnisch relevanten Ziele der Prozessführungs- und der Informationseinrichtungen sind in ihrer Spezifikation festgelegt.
- 5 (4) Die Informationssysteme sind gemäß ihrer sicherheitstechnischen Bedeutung qualifiziert.

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) Die redundanten Stränge der leittechnischen Einrichtungen sind voneinander so unabhängig ausgelegt, dass ein anlageninternes versagensauslösendes Ereignis nicht zum Ausfall mehrerer redundanter Stränge des Sicherheitssystems führt. Bei Ausfall einzelner Stränge leittechnischer Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, durch Einwirkungen von außen reichen die übrigen Stränge zur Beherrschung dieses Ereignisses aus.
- 6 (3) Zum Schutz gegen redundanzübergreifende versagensauslösende Ereignisse innerhalb der leittechnischen Einrichtungen und innerhalb der Anlage sind zueinander redundante Stränge grundsätzlich räumlich getrennt angeordnet.
- 6 (4) Verbindungen der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A und B ausführen, zu nicht kategorisierten oder Datenverar-

beitungs- 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, ob alle zu unterstellenden Ereignisabläufe beherrscht werden.

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

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 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 Leitechnik-Funktionen der Kategorie B

7.3.3.1 Grundsätze

7.3.3.1 (1) Für die Entwicklung und Qualifizierung der Software der Leitechnik-Funktionen der Kategorie B sind rechnergestützte Beschreibungen und 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 in seinen sicherheitsrelevanten Funktionen 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 Leitechnik-Funktionen der Kategorie C

7.3.4.1 Grundsatz

Die Software für Leitechnik-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

Eingesetzte vorgefertigte Software ist betriebsbewährt oder zertifiziert.

8 Robustheit

- 8 (1) Die zulässigen elektrischen, elektromagnetischen, thermischen, mechanischen und strahlungs- sowie feuchtigkeitsbedingten Einwirkungen sind 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, werden so ausgelegt, dass sie durch die Folgen dieser

Ereignisabläufe oder Anlagenzustände ihre erforderliche Funktionsfähigkeit nicht verlieren.

- 8 (4) Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A bis C ausführen, sind so ausgelegt, dass hinreichende Reserven gegenüber Alterungseffekten vorhanden sind.
- 8 (5) 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.
- 8 (6) 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.
- 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 rückge-

setzt 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 sind so gestaltet, dass sie grundsätzlich von zentralen Stellen durch verantwortliches Betriebspersonal überwachbar sind.
- 9 (6) Instandhaltungsarbeiten sind so gestaltet, dass sie ohne unzulässige Minderung der Sicherheit der Anlage durchführbar sind und Auswirkungen zu unterstellender Fehlhandlungen auf einen Strang 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 Erstellung 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) 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 Ände-

rungen 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 Wartpersonal zeitnah 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 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 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) Kapitel 1.

- 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.