

**Sicherheitsanforderungen für Kernkraftwerke: Anforderungen an Leittechnik“
Fassung vom September 2006 (Revision B)**

Originaltext (<i>betroffene Passage in fett</i>)	Änderungsvorschlag	Einwände bzw. Anmerkungen
	Anforderungen an die Leittechnik sind nicht doppelt und alle in Modul 5 zu formulieren. Ist es unvermeidlich, Anforderungen an die Leittechnik auch in anderen Modulen zu formulieren, dann sind in Modul 5 Querverweise auf diese Anforderungen aufzunehmen.	Die Anforderungen an die Leittechnik sind über mehrere Module gestreut. Es finden sich beispielsweise Aussagen bzgl. der zu unterstellenden Fehlerpostulate in den Modulen 1,5 und 10. So wird für die Sicherheitsebene 2 beispielsweise in Modul 1 (3.2 (2)) eine n+0, in Modul 5 (3.3) eine n+1 und in Modul 10 (1.1.1.2 (1)) eine n+2 Auslegung gefordert.
	Die Begriffsdefinitionen sollten derart präzisiert werden, dass klar unterschieden werden kann, ob sich ein Fehler spontan funktional auswirkt oder nicht.	Die derzeitige Definition der Begriffe Ausfall und Versagen erlaubt keine Unterscheidung, ob sich ein Fehler spontan funktional auswirkt oder nicht. Diese Unterscheidung ist jedoch sicherheitstechnisch von zentraler Bedeutung. Auch die Definition zu „Fehler“ ist aus Sicht der Leittechnik zu überdenken, z. B. bei unvollständiger oder fehlerhafter Anforderungsspezifikation, Herstellungsfehler. AG5-M5 wird einen Änderungsvorschlag erarbeiten.
	Siehe unten	Grundsätzlich sind die Anforderungen aus Modul 1 und 5 zueinander konsistent mit folgenden Einschränkungen Die Anforderung 3.2(6) in Modul 1 und die Anforderung 3.1(12) in Modul 5 sind widersprüchlich

<p>1 Geltungsbereich</p> <p>Die nachfolgenden Anforderungen gelten für leittechnische Einrichtungen, die auf den Sicherheitsebenen 1 bis 4 Leittechnik-Funktionen mit sicherheitstechnischer Bedeutung ausführen.</p> <p>Die Anforderungen werden durch Einrichtungen realisiert, bei denen Hard- und Software Leittechnik-Funktionen ausführen.</p>	<p>Anforderungen an leittechnische Funktionen:</p> <ol style="list-style-type: none"> 1. Die leittechnischen Funktionen sind derart festzulegen, dass die Schutzziele (die in Modul 1 definiert werden) in allen Betriebszuständen der Anlage und bei allen zu unterstellenden Ereignissen sichergestellt werden. 2. Es ist sicherzustellen, dass die verfahrenstechnischen Aufgabenstellungen vollständig durch leittechnische Funktionen in jeder Sicherheitsebene abgebildet sind. 3. Die leittechnischen Funktionen sind einfach strukturiert und vollständig spezifiziert. 4. Die Spezifikation der leittechnischen Funktionen umfasst mindestens <ul style="list-style-type: none"> • Die funktionalen Merkmale (Art und Weise, wie Messsignale von Sicherheitsvariablen zu Auslösesignale für Sicherheitssysteme verarbeitet werden) • Die Leistungsmerkmale (Antwortzeit, Genauigkeit usw.) sowie • Die Sicherheitsmerkmale (Sicherheitskategorie, relevante Störfälle, Unabhängigkeitanforderungen) 	<p>In Modul 5 finden sich nahezu keine Anforderung an die Festlegung der leittechnischen Funktionen (nur in 4 (2) aber ohne Anforderungen an Inhalte, Struktur, Verständlichkeit, Vollständigkeit, Korrektheit etc.). Bezüglich des zentralen Stellenwertes, der der Festlegung dieser Funktionen in Modul 1 eingeräumt wird, erscheint das unzureichend und sollte ergänzt werden. Im Rahmen dieser Ergänzungen sollte auch die Forderung 3.1 (6), 3.2 (1) und 8.6 aus Modul 1, die sich derzeit in Modul 5 nicht wieder finden, berücksichtigt werden.</p>
<p>2 Kategorisierung</p> <p>Entsprechend ihrer sicherheitstechnischen Bedeutung sind die Leittechnik-Funktionen in unterschiedliche Kategorien eingeordnet, für die abgestufte Anforderungen gelten:</p>		<p>Inkonsistenz zwischen Modul 1 und Modul 5.</p> <p>Ein Angleich an Modul 1 wurde vorgenommen (siehe Info-1_AG5_Modul5-3)</p>

<p>Kategorie A Die Leittechnik-Funktionen der Kategorie A umfassen alle Funktionen, die erforderlich sind, um Ereignisse der Sicherheitsebene 3 zu beherrschen.</p> <p>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.</p> <p>Kategorie C Die Leittechnik-Funktionen der Kategorie C umfassen alle übrigen Funktionen mit sicherheitstechnischer Bedeutung.</p> <p>Nicht kategorisiert sind Leittechnik-Funktionen, die keine unmittelbare sicherheitstechnische Bedeutung haben</p>	<p>Kategorie A Die Leittechnik-Funktionen der Kategorie A umfassen alle Funktionen, deren Versagen zu einer nicht beherrschbaren Verletzung von Barrieren führt sowie die Funktionen, die erforderlich sind um Ereignisse der Sicherheitsebene 3 zu beherrschen</p> <p>Kategorie B Die Leittechnik Funktionen der Kategorie B umfassen die Funktionen, die erforderlich sind zur wirksamen und zuverlässigen Störfallvermeidung, sowie zur Beherrschung von Ereignissen der Sicherheitsebene 2.</p> <p>Kategorie C Die Leittechnik Funktionen der Kategorie C umfassen alle übrigen Funktionen mit sicherheitstechnischer Bedeutung.</p>	
<p>3.1 (11) Zur Absicherung gegen Bedienungsfehler sind technische Vorkehrungen vorrangig vor organisatorischen Maßnahmen vorgesehen.</p>	<p>.. Vorkehrungen vorzugsweise vor organisatorischen Maßnahmen...</p>	<p>In Leitlinien: statt vorrangig „vorzugsweise“ Begriffsdefinitionen:</p>
<p>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</p>	<p>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 Wirksamkeit der anla-</p>	<p>Präzisierung erforderlich (durch Indikativ kommt es zu Missverständnissen). Zur Durchführung von Notfallmaßnahmen wird es auch notwendig sein, ggf. Sicherheitsfunktionen der Kategorie A oder B unwirksam zu machen.</p>

<p>sind. Die Eingriffsmöglichkeiten sind so ausgelegt, dass sie die Funktionsfähigkeit der leittechnischen Einrichtungen, die Leittechnikfunktionen der Kategorien A und B ausführen, nicht beeinträchtigen. Die Eingriffsmöglichkeiten sind gegen Fehlbedienung gesichert.</p>	<p>geninternen Notfallmaßnahmen ist auch bei beliebigem Versagen der Sicherheitsleittechnik sichergestellt. Die Eingriffsmöglichkeiten sind dezentral angeordnet, gegen Fehlbedienung gesichert und soweit erforderlich automatisiert.</p>	<p>Ansonsten Widerspruch zu Modul 1 3.2 (6)</p>
	<p>3.1(13) Können Fehler in leittechnischen Einrichtungen einer Sicherheitsebene zu Ereignissen (siehe Modul 3) führen, die nur durch Einrichtungen der nächsten Sicherheitsebene beherrscht werden, dann ist durch die Auslegung sicherzustellen, dass der Beitrag der Leittechnik zu diesen Ereignissen nicht relevant ist.</p>	<p>Die in dem Abschnitt über Fehlfunktionen angesprochenen Ereignisse sind in Modul 3 aufgeführt. (siehe Info1_AG5_Modul5-4)</p>
<p>3.2 (4) 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.</p>	<p>3.2 (4) 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.</p>	<p>Unnötige Einschränkung. Die Forderung nach Unabhängigkeit soll allgemein gefordert werden. Z.B die Vermeidung von datentechnischer Kopplung.</p>
<p>3.2 (5) Die leittechnischen Einrichtungen sind so ausgelegt, dass fehlerhaftes Ansteuern des Sicherheitssystems unter Berücksichtigung der Ausfallkombinationen nach dem Einzelfehlerkonzept verhindert wird, wenn dadurch Ereignisse der Sicherheitsebene 4 ausgelöst werden können</p>	<p>3.2 (5) Die leittechnischen Einrichtungen sind so ausgelegt, dass fehlerhaftes Ansteuern des Sicherheitssystems unter Berücksichtigung der Ausfallkombinationen nach dem Einzelfehlerkonzept verhindert wird, wenn dadurch Ereignisse der Sicherheitsebene 4 ausgelöst werden können</p>	<p>Hinsichtlich der Auswirkung von Fehlanregungen sind die Funktionen in immer sicherheitsgerichtet und nicht immer sicherheitsgerichtet zu unterscheiden. Immer sicherheitsgerichtete Funktionen z. B. RESA können durch Fehlauflösungen nie eine Verschlechterung des Sicherheitsniveaus zu Folge haben. Eine nicht immer sicherheitsgerichtete Funktion kann dagegen das Potential haben durch Fehlauflösungen selbst einen Störfall zu</p>

		indizieren, der durch eine andere Funktion beherrscht werden muss, um nicht tolerable Auswirkungen zu verhindern. Für diese ist gemäß RSK-LL 7.3.2 (9), was als Quelle für die Anforderung angegeben ist, durch eine entsprechende Auslegung Fehlanregungen zu verhindern.
3.2 (6) ... - Der Richtwert für die Zeitspanne, ab der Handmaßnahmen zulässig sind, beträgt 30 Minuten.	3.2 (6)... Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, sind so ausgelegt, dass innerhalb von 30 min nach Erkennen des Ereignisses keine Handmaßnahme erforderlich ist. Handmaßnahmen sind jederzeit zulässig. Die Inbetriebnahme und Zuschaltung der Notstromerzeugungsanlagen erfolgen im Anforderungsfall automatisch, so dass innerhalb von 30 min keine Handmaßnahme erforderlich ist. Eine manuelle Inbetriebnahme und Zuschaltung der Notstromerzeugungsanlagen ist jederzeit möglich.	Irreführend, Text aus Modul 5 Teil 2 zitieren 2 (14)
3.2 (7) ..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	3.2 (7) ...Diese Prüfungen sollen mittels eingebauter Prüfhilfen ohne Eingriff in die Anlage leicht durchführbar sein ... Prüfeingriffe und Handbetätigungen sind so festgelegt, dass notwendige Sicherheitsfunktionen weder verhindert werden noch die Zuverlässigkeit ihrer Anregung signifikant vermindert wird	Unnötige Einschränkung. Präzisierung erforderlich Stattdessen Handbetätigungen
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 Quali-	3.2 (10) ...leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, sind einfach aufgebaut	Welches Ziel? Irreführend durch Indikativ. Ansonsten Änderung:

fizierung 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 <i>Ausfälle</i> der Hardware und <i>Versagen</i> der Software derart getroffen, dass ein systematischer Ausfall so unwahrscheinlich ist, dass er ausgeschlossen werden kann.	<p>3.2(11) Bei der Auslegung der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, sind Auslegungsfehler nicht grundsätzlich auszuschließen.</p> <p>3.2(11a) Mögliche Auswirkungen von zu unterstellenden Auslegungsfehlern¹ sind unter Berücksichtigung der systemimmanenten Versagensmechanismen zu analysieren.</p> <p>3.2 (11b) Ergibt die Analyse, dass ein nicht gerichtetes Versagen der leittechnischen Einrichtungen mit systematischem Charakter zu unterstellen ist, dann ist die Auslegung zu ändern.</p>	(siehe Info-1_AG5_Modul5-3 und Info-1_AG5_Modul5-4)
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 systemati-	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 daraus resultierende Folgeausfälle und ein systematisches Versagen mit den unter 3.2 (11a) analysierten Auswirkungen eintreten. Während eines Instandhaltungsfalls wird im Anforderungsfall innerhalb einer Zeitspanne von 100 h das gleichzeitige Auftreten des systematischen Versagens nicht unterstellt.	<p>Definition Versagen/Ausfall</p> <p>Die derzeitige Definition der Begriffe Ausfall und Versagen erlaubt keine Unterscheidung, ob sich ein Fehler spontan funktional auswirkt oder nicht. Diese Unterscheidung ist jedoch sicherheitstechnisch von zentraler Bedeutung. Die Präzisierung ist für Sonderfälle in der Leittechnik notwendig, die Definitionen gelten jedoch allgemein.</p> <p>Versagen: Abweichung der ausgeführten Funktion im Anforderungsfall</p>

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

<p>schen <u>Ausfalls</u> und des Zufallsausfalls nicht unterstellt</p>		<p>rungsfall von der geforderten Funktion.</p> <p>Ausfall: Verlust einer oder mehrerer Auslegungsanforderungen derart, dass die geforderte Funktionsfähigkeit nicht mehr gegeben ist</p>
<p>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.</p> <p>Der Aggregateschutz ist so ausgelegt, dass der Vorrang der Leittechnik-Funktionen der Kategorie A vor dem Aggregateschutz sichergestellt ist.</p> <p>Ist im Aggregateschutz ein Vorrang 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.</p>		<p>Abschnitt zu detailliert. Detaillierung sollte entsprechender KTA-Regel vorbehalten sein. Auch Widerspruch zwischen Satz 2 und 3 (indikativ)</p> <p>Hier sollten nur allgemeine Anforderungen gestellt werden.</p> <p>Es liegt KTA 3504 vor</p> <p>Definition für Aggregateschutz erforderlich</p>

3.2 (16) In Betriebsphasen außerhalb der Betriebsphasen A und B, in denen Teile von Leittechnik-Funktionen der Kategorie A		Unglückliche Formulierung wegen gleicher Buchstaben
3.3 2. Satz 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.	Wird eine Funktion, die im Störfallablauf notwendige Maßnahmen zur Störfallbeherrschung auslöst, in leittechnischen Einrichtungen der Sicherheitsebene 2 implementiert, dann ist diese Funktion höherwertig (N+2) aufzubauen.	Nach Ansicht der Arbeitsgruppe sollten Schutzbegrenzungen, die für die Störfallbeherrschung erforderlich sind, nach den Anforderungen der Kategorie A ausgelegt werden, wobei ein systematischer Ausfall nicht zu unterstellen ist (Schutzqualität und n+2-Auslegung). Wird umformuliert (siehe Info-1_AG5_Modul5-4)
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	Für jedes von den leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, zu beherrschende Ereignis der Sicherheitsebene 3 werden grundsätzlich mindestens zwei unterschiedliche Anregekriterien...	1. und 2. Satz widersprechen sich in der vorliegenden Fassung. Im 1. Satz ist daher noch „grundsätzlich“ einzufügen, um die Möglichkeit von Ausnahmen gemäß dem 2. Satz darzustellen
7.3.2.3 (1) Einsatz von vorgefertigter Software 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.	Der Einsatz vorgefertigter Software, sofern nicht entsprechend den Anforderungen 7.3.2.1 und 7.3.2.2 ausgelegt wurden , ist auf unverzichtbare Bestandteile beschränkt, wobei Softwareänderungen vermieden werden.	Einschränkungen sind nur dann geboten, wenn die vorgefertigte Software nicht nach den Anforderungen des kerntechnischen Regelwerkes entwickelt wurde,

<p>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.</p>	<p>.....</p> <p>Die leittechnischen Einrichtungen und deren Energieversorgung sind so ausgelegt, dass nach vollständigem Spannungsausfall oder Unterschreiten der Mindestspannung die leittechnischen Einrichtungen nach Spannungswiederkehr funktionsfähig sind</p>	<p>Die Anforderungen betreffen nicht nur die Energieversorgung, sondern auch die leittechnischen Einrichtungen.</p> <p>Nach der Spannungswiederkehr soll die Leittechnik wieder funktionsfähig sein. Präzisierung und ggf. Zuordnung prüfen.</p>
--	--	--