

**Zusammenstellung des Abgleichs der KTA 3501 (2015-11)
mit den „Sicherheitsanforderungen an Kernkraftwerke“ und deren Interpretationen**

KTA-Dok.-Nr. 3501/15/3

- (1) Nach Beschlüssen des KTA-Präsidiums auf seiner 94., 95. und 97. Sitzung am 19.03.2014, 19.03.2015 und am 23.09.2015 soll für alle KTA-Regeln ein Abgleich mit den Sicherheitsanforderungen an Kernkraftwerke (SiAnf) und deren Interpretationen erfolgen. Es sollen die Anforderungen der jeweiligen KTA-Regel mit den Anforderungen der SiAnf und der zugehörigen Interpretationen verglichen und auf Konsistenz überprüft werden.
- (2) Der vorliegende SiAnf-Abgleich für KTA 3501 (2015-11) wurde von der KTA-GS vorbereitet und vom Unterausschuss ELEKTRO- UND LEITTECHNIK (UA-EL) auf seiner 78. Sitzung am 01.09.2015 diskutiert und einstimmig zur Vorlage an den KTA verabschiedet.
- (3) Der KTA nahm den vorliegenden Abgleich auf seiner 70. Sitzung am 10.11.2015 zustimmend zur Kenntnis.
- (4) In den „Sicherheitsanforderungen an Kernkraftwerke“ (SiAnf) sind folgende Anforderungen enthalten, die den Anwendungsbereich der Regel KTA 3501 betreffen:
- a) Anforderung 2 „Technisches Sicherheitskonzept“
 - aa) Anforderung „2.4 Schutzkonzept gegen Einwirkungen von innen und außen sowie gegen Notstandsfälle“
 - b) Anforderung 3 „Technische Anforderungen“,
 - ba) Anforderung 3.1 „Übergeordnete Anforderungen“,
 - bb) Anforderung 3.7 „Anforderungen an die Leittechnik“,
 - d) Anforderung 5 „Anforderungen an die Nachweisführung“ und
 - e) Anforderung 7 „Anforderungen an die Dokumentation“.
- (5) Die Anforderungen nach (4) b) bis e) werden in der Interpretation I-3 „Anforderungen an die Leittechnik“ präzisiert.
- (6) Die Konkretisierungen der Festlegungen aus den SiAnf sowie deren Interpretationen in KTA 3501 sind in der nachfolgenden **Tabelle 1** dargestellt.
- (7) Inkompatibilitäten zwischen den SiAnf und den Anforderungen der Regel KTA 3501 (2015-11) bestehen nicht.

Verweise

SiAnf	2015-03	Sicherheitsanforderungen an Kernkraftwerke in der Fassung der Bekanntmachung vom 3. März 2015 (BAnz AT 30.03.2015 B2)
Interpretationen	2015-03	Interpretationen zu den Sicherheitsanforderungen an Kernkraftwerke vom 22. November 2012, geändert am 3. März 2015 (BAnz AT 30.03.2015 B3)

Anforderungen nach SiAnf	Anforderungen nach den Interpretationen	Umsetzung in KTA 3501 (2015-11)	Bewertung bezüglich KTA 3501
2.4 Schutzkonzept gegen Einwirkungen von innen und außen sowie gegen Notstandsfälle 2.4 (3) Die zueinander redundanten Teilsysteme von Sicherheitseinrichtungen sind räumlich getrennt aufzustellen oder so zu schützen, dass bei Einwirkungen von innen ein redundanzüber-greifender Ausfall verhindert wird.		4.1.1 Grundsätzliche Anforderungen	In Abschnitt 4.1.1 werden grundsätzliche Auslegungsanforderungen an das Sicherheitssystem gestellt: 1. Das Sicherheitssystem muss nichttolerierbare Auswirkungen von Störfällen und Einwirkungen von innen und außen verhindern. 2. Das Auftreten eines der benannten versagensauslösenden Ereignisse und deren Auswirkungen auf eine leittechnische Funktion darf nicht dazu führen, dass im Anforderungsfall (Störfall) das Sicherheitssystem versagt. Die angesprochene Forderung nach räumlicher Trennung von Redundanzen ist nur eine Maßnahme aus einem Strauß von Maßnahmen, die sich aus diesen Auslegungsprinzipien ableiten. Die harte Forderung nach räumlicher Trennung von Redundanzen ist nicht immer nötig (z. B. LT0¹, Redundanzgruppen) bzw. nicht immer möglich (FSA-Station). Ein Brand an einer beliebigen Stelle ist Teil der Analyse und sollte beherrscht werden, die Störfallbeherrschung darf nicht eingeschränkt werden. Entweder wird der Brand zugelassen, da die Einrichtung eindeutig sicherheitsgerichtet auslöst, oder der Brand wird beherrscht durch Brandschutzmaßnahmen (z. B. Löschanlage), Redundanztrennung.
3.1 Übergeordnete Anforderungen 3.1 (2) Auf Maßnahmen und Einrichtungen der Sicherheitsebenen	I-3 3.1 Leittechnische Einrichtungen einschließlich der Stör-	5.1.4 und 5.2.4 Umgebungseinflüsse	Erfüllt.

¹ LT0 ist ein Logikteil dem nur Signale zugeordnet werden, die eindeutig sicherheitsgerichtete Schutzaktionen auslösen. Auf eine räumliche Trennung kann deshalb verzichtet werden.

Anforderungen nach SiAnf	Anforderungen nach den Interpretationen	Umsetzung in KTA 3501 (2015-11)	Bewertung bezüglich KTA 3501
1 bis 4a sowie die Maßnahmen und Einrichtungen, die für Einwirkungen von innen und außen sowie bei Notstandsfällen erforderlich sind, sind bezüglich aller Betriebsphasen sicherheitsfördernde Auslegungs-, Fertigungs- und Betriebsgrundsätze anzuwenden (siehe auch Nummer 2.1 (13)), wie insbesondere: a) begründete Sicherheitszuschläge bei der Auslegung von Komponenten, in Abhängigkeit von deren sicherheitstechnischer Bedeutung; hierbei können in Bezug auf den Anwendungsfall anerkannte Regeln und Standards angewendet werden; b) Bevorzugung von inhärent sicher wirkenden Mechanismen bei der Auslegung; c) Verwendung qualifizierter Werkstoffe, Fertigungs- und Prüfverfahren sowie betriebsbewährter oder ausreichend geprüfter Einrichtungen; d) instandhaltungs- und prüffreundliche Gestaltung von Einrichtungen unter besonderer Berücksichtigung der Strahlenexposition des Personals; e) ergonomische Gestaltung der Arbeitsplätze; f) Sicherstellung und Erhalt der Qualitätsmerkmale bei Fertigung, Errichtung und Betrieb; g) Durchführung von wiederkehrenden Prüfungen in dem sicherheitstechnisch notwendigen Umfang; h) zuverlässige Überwachung der in den jeweiligen Betriebsphasen relevanten Betriebszustände; i) Aufstellung und Anwendung eines Überwachungskonzepts mit Überwachungseinrichtungen zur Erkennung und Beherrschung betriebs- und alterungsbedingter Schäden; j) Aufzeichnung, Auswertung und sicherheitsbezogene Verwertung von Betriebserfahrungen.	fallinstrumentierung, die Leittechnik-Funktionen der Kategorien A bis C ausführen 3.1 (4) Die leittechnischen Einrichtungen müssen so ausgelegt, montiert, abgeschirmt und geschützt werden, dass eine unzulässige Beeinflussung der Signale durch anlageninterne sowie durch äußere Störquellen vermieden wird. 3.1 (10) Für leittechnische Einrichtungen, die auslegungsgemäß Funktionen auch unter Störfallbedingungen ausführen, muss die Störfallfestigkeit nachgewiesen werden. I-3 3.2 Leittechnische Einrichtungen zur Ausführung von Leittechnik-Funktionen der Kategorie A 3.2 (1) Bei der Auslegung der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, müssen versagensauslösende Ereignisse innerhalb und außerhalb des Sicherheitssystems berücksichtigt werden. 3.2 (4) Ein Ausfall in den leittechnischen Einrichtungen des Sicherheitssystems darf höchstens Auswirkungen auf die Funktion der betroffenen Redundante des Sicherheitssystems haben. Die leittechnischen Einrichtungen, die für die Funktionsfähigkeit des Sicherheitssystems nach Eintritt von Ereignissen der Sicherheitsebene 3 erforderlich sind, sind so auszulegen, dass sie den jeweils ungünstigsten Umgebungs- und Störfallbedingungen standhalten, die im zugehörigen Aufstellungs- und Installationsbereich auftreten können. Die leittechnischen Einrichtungen sind so auszulegen, dass ein fehlerhaftes Auslösen von Schutzaktionen unter Berücksichtigung der Nummer 3.2 (11) verhindert wird, wenn dies zu auslegungsüberschreitenden Anlagenzuständen führen kann. 3.2 (5) Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, sind grundsätzlich selbstüberwachend auszulegen. Deren Funktionen und Eigenschaften, die von der Selbstüberwachung nicht erfasst sind, sind einer regelmäßigen und lückenlosen Überprüfung zu unterziehen. Die Prüfzyklen sind auf	4.1.2 Versagensauslösende Ereignisse 5.1.4.1 Beanspruchung bei bestimmungsgemäßen Betrieb 5.1.4.3 Beanspruchung bei Störfällen 5.2.4.1 Beanspruchung bei bestimmungsgemäßen Betrieb 5.2.4.2 Beanspruchung bei Störfällen 4.1.9.1 Überwachung auf Funktionsbereitschaft	Der Absatz enthält keinen Mehrwert und passt nicht zur Struktur des Abschnittes 4.1.2. Er wurde deshalb nicht aufgenommen. Erfüllt. Erfüllt. Der Absatz wurde durch die Interpretationen I-3, 3.2(5) mit redaktionellen Änderungen ersetzt.

Anforderungen nach SiAnf	Anforderungen nach den Interpretationen	Umsetzung in KTA 3501 (2015-11)	Bewertung bezüglich KTA 3501
	Grundlage von Zuverlässigkeitsbetrachtungen festzulegen. Diese Prüfungen sollen mittels Prüfhilfen an für diesen Zweck vorgesehenen Schnittstellen leicht durchführbar sein. 3.2 (11) Bei der Auslegung der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, sind Vorkehrungen gegen systematische Ausfälle der leittechnischen Einrichtungen zur Minderung der Eintrittswahrscheinlichkeit derart zu treffen, dass ein systematischer Ausfall auf der Sicherheitsebene 3 nicht mehr unterstellt werden muss. Kann für rechnerbasierte oder programmierbare leittechnische Einrichtungen diese Nachweisführung nach dem Stand von Wissenschaft und Technik nicht erfolgen, sind Vorkehrungen derart zu treffen, dass ein systematischer Ausfall von Hardware und Software auf der Sicherheitsebene 3 beherrscht wird. Beim Einsatz rechnerbasierter oder programmierbarer Leittechnik sind grundsätzlich diversitäre leittechnische Einrichtungen unter Beachtung der folgenden Bedingungen zu verwenden. Es bestehen keine Vorgaben hinsichtlich des Einsatzes diversitärer Einrichtungen, wenn für die jeweils auszuführende Leittechnik-Funktion ein aktiver systematischer Ausfall sicherheitsgerichtet ist. Beim Einsatz von rechnerbasierter oder programmierbarer Leittechnik ist für Schutzaktionen, die nicht für jeden Anlagenzustand sicherheitsgerichtet sind, in Abhängigkeit von den Auswirkungen von passiven oder aktiven systematischen Ausfällen in den leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, eine zweifache oder dreifache diversitäre Ausführung der Leittechnik einzusetzen. Eine mindestens zweifache diversitäre Ausführung ist einzusetzen, – wenn mit den noch verfügbaren Sicherheitseinrichtungen der Störfall beherrscht wird oder – wenn jede der beiden diversitären leittechnischen Einrichtungen für sich alleine die erforderliche Schutzaktion auslöst. Trifft beim Einsatz von rechnerbasierter oder programmierbarer Leittechnik eine der beiden genannten Voraussetzungen für den Einsatz einer zweifach diversitären Ausführung	4.1.3.1 Grundannahmen	Erfüllt. Kein Widerspruch.

Anforderungen nach SiAnf	Anforderungen nach den Interpretationen	Umsetzung in KTA 3501 (2015-11)	Bewertung bezüglich KTA 3501
	Vorrang der Leittechnik-Funktionen der Kategorie A vor den Schutzeinrichtungen sichergestellt wird. Ist in einer Schutzeinrichtung ein Vorrang vor Leittechnik-Funktionen der Kategorie A notwendig, müssen an die Schutzeinrichtungen die Anforderungen an leittechnische Einrichtungen gestellt werden, die Kategorie A Funktionen ausführen. Die Anforderungen an leittechnische Einrichtungen, die Funktionen der Kategorie A ausführen, müssen an die Schutzeinrichtungen nicht gestellt werden, wenn nachgewiesen wird, dass Fehler der Schutzeinrichtung so unwahrscheinlich sind, dass eine dadurch verursachte Fehlauslösung nicht mehr unterstellt werden muss. I-3 3.7 Erfassung von Prozessvariablen 3.7 (2) Für jedes von den leittechnischen Einrichtungen, die Leittechnik Funktionen der Kategorie A ausführen, zu beherrschende Ereignis der Sicherheitsebene 3 müssen grundsätzlich mindestens zwei unterschiedliche Anregekriterien herangezogen werden, die aus physikalisch unterschiedlichen Prozessvariablen gebildet werden. Wenn dies technisch nicht realisierbar ist, sind andere Maßnahmen und Einrichtungen zum Erreichen hoher Zuverlässigkeit vorzusehen. I-3 3.4.2.2 Störfallaufzeichnung 3.4.2.2 (2) Die Störfallaufzeichnung ist so auszulegen, dass für jede erfasste Messgröße der Störfallinstrumentierung der Zeitbezug aus den zugehörigen Dokumentationsunterlagen so genau bestimmt werden kann, dass eine zeitliche Zuordnung zu Daten aus anderen Informationsquellen möglich ist. I-3 3.8 Redundanz und Unabhängigkeit 3.8 (3) Zum Schutz gegen redundanzübergreifende versagensauslösende Ereignisse innerhalb der leittechnischen Einrichtungen und innerhalb der Anlage sollen Redundanten der leittechnischen Einrichtungen, die Leittechnik-	3.4 Erfassung von Störfällen 4.1.4.4 Protokollierung 4.1.5 Redundanz und Unabhängigkeit 4.2.6 Redundanz und Unabhängigkeit	Die Formulierung aus I-3, 3.7 (2) wurde nicht übernommen, da eine unbedingt einzuhaltende Forderung (Absatz 2) im Widerspruch zur Ausnahme (Absatz 3) stünde. Der Inhalt von Absatz 2 und 3 ist allerdings konsistent mit I-3, 3.7.2. Die gefundene Formulierung verstößt aber nicht gegen das KTA-Merkblatt (2011-11). Anforderungen an die Störfallinstrumentierung liegen nicht im Focus der KTA 3501 sondern der KTA 3502. Die Formulierung wurde deshalb nicht übernommen. Wird in der KTA 3502 abgebildet. In diesem Sonderfall wird durch räumliche Trennung die Sicherheit der Anlage nicht verbessert. Der ursprüngliche Regeltext ergänzt die Interpretationen an dieser Stelle.

Anforderungen nach SiAnf	Anforderungen nach den Interpretationen	Umsetzung in KTA 3501 (2015-11)	Bewertung bezüglich KTA 3501
	Funktionen der Kategorie A oder B ausführen, räumlich getrennt angeordnet werden. 3.8 (4) Verbindungen der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A und B ausführen, zu nicht kategorisierten oder Datenverarbeitungs- oder Datenübertragungseinrichtungen der Kategorie C sind unter Berücksichtigung des technisch und betrieblich Notwendigen zu minimieren. Sie sind rückwirkungsfrei auszuführen. 3.8 (5) Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorien A bis C ausführen, sind voneinander so unabhängig auszulegen, dass bei versagensauslösenden Ereignissen in den Einrichtungen, die sicherheitstechnisch niederwertigere Leittechnik-Funktionen ausführen, die Leittechnik-Funktionen der sicherheitstechnisch höherwertigeren Kategorie erhalten bleiben. I3 3.10 Elektrische Energieversorgung der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorien A bis C ausführen 3.10 (1) Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorien A bis B sowie die erforderlichen Leittechnik-Funktionen der Kategorie C ausführen, müssen von unterbrechungslosen Notstromanlagen mit Energiespeicherung versorgt werden. Die Kapazität des Energiespeichers ist unter der Annahme, dass der Leistungsbedarf einer Redundante nur aus dem redundanzzugehörigen Energiespeicher gedeckt wird, so zu bemessen, dass die Versorgung mindestens 2 h aufrechterhalten wird, ohne dass die zulässige Mindestspannung unterschritten wird. Die leittechnischen Einrichtungen und deren Energieversorgung sind so auszulegen, dass nach vollständigem Spannungsausfall oder Unterschreiten der Mindestspannung die leittechnischen Einrichtungen nach Spannungswiederkehr funktionsfähig sind. 3.10 (2) Bei der Auslegung der elektrischen Energieversorgung der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorien A bis C ausführen, sind die gleichen Ausfallkombinationen zu Grunde zu legen wie bei der	4.1.6 Trennung der A-Funktions-Einrichtungen von anderen Systemen 4.2.6 Trennung der B-Funktions-Einrichtungen von anderen Systemen 4.1.6 Trennung der A-Funktions-Einrichtungen von anderen Systemen 4.2.6 Trennung der B-Funktions-Einrichtungen von anderen Systemen 8. Elektrische Energieversorgung	Ein Beispiel hierfür ist die RESA-Auslösekette. Erfüllt. Der Absatz wurde durch Interpretation der SiAnf, I-3, 3.8 (4) ergänzt. Die in den SiAnf verwendeten Begriffe „Datenverarbeitungs- oder Datenübertragungseinrichtungen“ wurde allerdings durch „leittechnischen Einrichtungen“ ersetzt, um keine neue Begrifflichkeiten einzuführen. Erfüllt. Kein Widerspruch. Erfüllt. Kein Widerspruch

Anforderungen nach SiAnf	Anforderungen nach den Interpretationen	Umsetzung in KTA 3501 (2015-11)	Bewertung bezüglich KTA 3501
	Auslegung der zu versorgenden leittechnischen Einrichtungen (siehe für Kategorie A in der Nummer 3.2 (12) und siehe für Kategorie B: Abschnitt 3.3). 3.10 (3) Die Auslegung der einspeisenden Erzeugungsanlagen, der Verteilernetze und der leittechnischen Einrichtungen sind so aufeinander abzustimmen, 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. 4 Qualifizierung 4.1 Qualifizierung von Hard- und Software der leittechnischen Einrichtungen für Leittechnik-Funktionen der Kategorien A bis C 4.2 Qualifizierung der Hardware 4.2 (1) Für leittechnische Einrichtungen, die Leittechnik-Funktionen der Kategorien A und B ausführen, ist zuverlässige, typgeprüfte oder für die unterstellten Einsatzbedingungen betriebsbewährte Hardware einzusetzen. Diese Hardware soll während des Leistungsbetriebs wartungsfrei sein. 4.3 Qualifizierung der Software 4.3.1 Software für Leittechnik-Funktionen der Kategorien A bis C 4.3.1 (1) Die Software ist in verifizierbaren Schritten nach einem Phasenmodell zu entwickeln. 4.3.1 (2) Die Softwarearchitektur von leittechnischen Einrichtungen ist so zu gestalten, 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 Mehrrechner-systemen die Software zur Kommunikation der Rechner. 4.3.1 (3) Die Software ist so auszulegen, dass keine unzulässigen Rückwirkungen von leittechnischen Einrichtungen, die Leittechnik-Funktionen der sicherheitstechnisch niederwertigeren Kategorie ausführen, auf die leittechnischen Einrichtungen, die Leittech-	5.1.2.1/5.2.2.1 Grundsätze (1) 5.1.2.1/5.2.2.1 Grundsätze (2) 5.1.2.1/5.2.2.1 Grundsätze (3)	Erfüllt. Erfüllt. Erfüllt.

Anforderungen nach SiAnf	Anforderungen nach den Interpretationen	Umsetzung in KTA 3501 (2015-11)	Bewertung bezüglich KTA 3501
	4.3.2.2 (4) Nach Installation der Software auf den Rechnern soll das anforderungsgerechte Verhalten des Hardware- und Software-systems validiert werden. Wird die Validierung in mehreren Schritten durchgeführt, so sollen die einzelnen Validierungsschritte überlap-pend sein.	5.1.2.2.2/5.2.2.2.2 Analytische Qualitätssi- cherung (2)	Erfüllt.
	4.3.2.2 (5) Die Organisation und Administration der Softwareent-wicklung und der Qualitätssiche-rung ist so zu gestalten, dass si- chergestellt wird, dass die Soft- ware nach vollständigen Entwick- lungs-, Prüf-, Wartungs- und Qua- litätssicherungsplänen erstellt und eingesetzt wird. Die Unabhängig- keit zwischen Konstruktion und Qualitätssicherung muss durchge- hend gewahrt werden. Es muss eine vollständige Entwicklungs-, Qualitätssicherungs- und Benut- zerdokumentation vorhanden sein.	5.1.2.2.3/5.2.2.2.3 Organisation und Admi- nistration (1)	Erfüllt.
	4.3.2.2 (6) Es sind Verfahren und Methoden anzuwenden, die die konsistenten Konfigurationen der Software sicherstellen (Konfigura- tionsmanagement).	5.1.2.2.3/5.2.2.2.3 Organisation und Admi- nistration (2)	Erfüllt.
	4.3.2.3 Einsatz von vorgefertigter Software 4.3.2.3 (1) Der Einsatz vorgefertig- ter Software, sofern nicht entspre- chend den Anforderungen der Ab- schnitte 4.3.2.1 und 4.3.2.2 ausge- legt, muss auf unverzichtbare Be- standteile beschränkt sein, wobei Softwareänderungen vermieden werden sollen. Diese Teile sind Prüfungen und Tests zu unterzie- hen, die in Umfang und Tiefe den Nachweisen nach den Abschnitten 4.3.2.1 und 4.3.2.2 gleichwertig sind. 4.3.2.3 (2) Zur Bewertung der Gleichwertigkeit sollen herangezogen werden: – Referenzen über den Hersteller der Software, – die Entwicklungsdokumentation, Anwenderdokumentation und Qualitätssicherungsdokumenta-tion der Software, – die Ergebnisse unabhängiger Begutachtung (Zertifikate) der Software, – die Betriebserfahrung der Soft-ware unter Berücksichtigung der Anwendungsprofile und – zusätzliche Softwaretests. 4.3.3 Software für Leitechnik-Funktionen der Kategorie B	5.1.2.3/5.2.2.3 Einsatz vorgefertigter Software (1)	Erfüllt.

Anforderungen nach SiAnf	Anforderungen nach den Interpretationen	Umsetzung in KTA 3501 (2015-11)	Bewertung bezüglich KTA 3501
	4.3.3.1 Grundsätze 4.3.3.1 (1) Für die Entwicklung und Qualifizierung der Software der Leittechnik-Funktionen der Kategorie B sind Beschreibungen und rechnergestützte Testverfahren anzuwenden, die den Nachweis der korrekten Arbeitsweise unterstützen. 4.3.3.1 (2) Die Software für Leittechnik-Funktionen der Kategorie B ist robust auszulegen. Eine Selbstüberwachung der Leittechnik-Funktionen der Kategorie B ist vorzusehen. 4.3.3.2 Qualitätssicherung 4.3.3.2 (1) Die Softwareerstellung muss nach einem Phasenmodell weitgehend mit rechnergestützten Werkzeugen erfolgen. 4.3.3.2 (2) Die Software ist aus hinsichtlich der Funktion klar abgegrenzten Einheiten aufzubauen. Diese Softwareeinheiten sollen mit Beschränkung auf unverzichtbare Anweisungen und Schnittstellen programmiert und in eine übersichtliche Programmstruktur integriert werden. 4.3.3.2 (3) Die Ergebnisse der einzelnen Phasen der Softwareentwicklung sind einer dokumentierten Prüfung zu unterziehen. Alle sicherheitsrelevanten Programmteile sind durch eine Kombination von Testverfahren zu prüfen, wobei eine vollständige Funktionsüberdeckung erreicht werden soll. 4.3.3.2 (4) Das anforderungsgerechte Verhalten des Hardware- und Softwaresystems ist zu validieren. 4.3.3.2 (5) Die Organisation und Administration der Softwareentwicklung und der Qualitätssicherung ist so zu gestalten, dass sichergestellt ist, dass die Software nach vollständigen Entwicklungs-, Prüf-, Wartungs- und Qualitätssicherungsplänen erstellt und eingesetzt wird. Die Unabhängigkeit zwischen Konstruktion und Qualitätssicherung muss durchgehend gewahrt werden. Es ist eine vollständige Entwicklungs-, Qualitätssicherungs- und Benutzerdokumentation zu erstellen. 4.3.3.2 (6) Die konsistente Konfiguration der Programme ist sicherzustellen (Konfigurationsmanagement).		

Anforderungen nach SiAnf	Anforderungen nach den Interpretationen	Umsetzung in KTA 3501 (2015-11)	Bewertung bezüglich KTA 3501
	4.3.3.3 Einsatz von vorgefertigter Software 4.3.3.3 (1) Der Einsatz vorgefertigter Software, sofern nicht entsprechend den Anforderungen in den Abschnitten 4.3.3.1 und 4.3.3.2 ausgelegt, muss auf unverzichtbare Bestandteile beschränkt sein, wobei Softwareänderungen vermieden werden sollen. Diese Teile sind Prüfungen und Tests zu unterziehen, die in Umfang und Tiefe den Nachweisen nach den Abschnitten 4.3.3.1 und 4.3.3.2 gleichwertig sind. 4.3.3.3 (2) Zur Bewertung der Gleichwertigkeit sollen herangezogen werden: – Referenzen über den Hersteller der Software, – die Entwicklungsdokumentation, Anwenderdokumentation und Qualitätssicherungsdokumentation der Software, – die Ergebnisse unabhängiger Begutachtung (Zertifikate) der Software, – die Betriebserfahrung der Software unter Berücksichtigung der Anwendungsprofile und – zusätzliche Softwaretests. I-3 5 Instandhaltung und Änderungen 5 (3) Prüfungen an leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorien A bis C ausführen, sollen von zentralen Stellen aus überwachbar sein. I-3 6 Spezifische Anforderungen zur Dokumentation zu leittechnischen Einrichtungen der Kategorie A bis C einschließlich Störfallinstrumentierung 6 (3) Die Betriebserfahrung aus der Instandhaltung der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorien A bis C ausführen, muss entsprechend der sicherheitstechnischen Bedeutung der leittechnischen Einrichtungen erfasst, dokumentiert und systematisch ausgewertet werden.	4.1.9.2 Prüfbarkeit der A-Funktions-Einrichtungen 4.2.10.2 Prüfbarkeit der B-Funktions-Einrichtungen 4.1.7 Instandhaltung	Erfüllt. Kein Widerspruch. Erfüllt. Der Absatz wurde aus den Interpretationen, I-3, 6(3) mit redaktionellen Änderungen ergänzt.
3.7 Anforderungen an die Leittechnik	I-3: Abschnitt 3 Auslegungsanforderungen	5 Aufbau und Ausführung	Erfüllt.

Anforderungen nach SiAnf	Anforderungen nach den Interpretationen	Umsetzung in KTA 3501 (2015-11)	Bewertung bezüglich KTA 3501
3.7 (3) Das Kernkraftwerk ist mit zuverlässigen leittechnischen Einrichtungen mit Leittechnik-Funktionen auf der Sicherheitsebene 3, dem Reaktorschutzsystem, auszurüsten, deren Leittechnik-Funktionen bei Erreichen festgelegter Ansprechwerte Schutzaktionen auslösen. Diese Einrichtungen sind nach folgenden Grundsätzen auszulegen: - redundante Auslegung von Komponenten, Baugruppen und Teilsystemen, - Diversität (siehe Nummer 3.1 (5)), - räumlich getrennte Installation entsprechend dem Wirkungsbereich möglicher versagensauslösender Ereignisse, - selbsttätige Überwachung auf einen Ausfall hin, - Anpassung der Komponenten an die möglichen Umgebungsbedingungen, - einfache Struktur der Software, - Begrenzung des Funktionsumfangs von Hard- und Software auf das sicherheitstechnisch notwendige Maß sowie - Einsatz fehlervermeidender, fehlerentdeckender und fehlerbeherrschender Maßnahmen und Einrichtungen. Hinweise: Für rechnerbasierte oder programmierbare leittechnische Einrichtungen werden zukünftig auch Anforderungen durch das Regelwerk der Sicherung gestellt werden, die auch Auslegungsanforderungen enthalten. Die nachweisliche Erfüllung aller Sicherungsanforderungen ist Voraussetzung für die Genehmigung dieser Systeme. Rechnerbasierte oder programmierbare leittechnische Einrichtungen werden danach auf der Sicherheitsebene 3 nur eingesetzt werden, wenn für den gesamten Lebenszyklus nachgewiesen werden kann, dass eine Manipulation dieser Einrichtungen durch geeignete Maßnahmen der Auslegung oder der Sicherung verhindert wird, oder wenn verhindert wird, dass Manipulationen einzelner oder verschiedener rechnerbasierter oder programmierbarer Einrichtungen Auswirkungen auf die Sicherheit der Anlage haben.	I-3:Abschnitt 3.1 Leittechnische Einrichtungen einschließlich der Störfallinstrumentierung, die Leittechnik-Funktionen der Kategorien A bis C ausführen I-3: Abschnitt 3.2 Leittechnische Einrichtungen zur Ausführung von Leittechnik-Funktionen der Kategorie A		
3.7 (4) Bei der Auslegung der leittechnischen Einrichtungen gemäß	I-3 3.2 (11) Bei der Auslegung der leittechnischen Einrichtungen, die	4.1.3 Ausfallkombinationen 4.1.3.1 Grundannahmen	Erfüllt. Die Formulierung wurde aus den SiAnf

Anforderungen nach SiAnf	Anforderungen nach den Interpretationen	Umsetzung in KTA 3501 (2015-11)	Bewertung bezüglich KTA 3501
Nummer 3.7 (3) sind die Potentiale für und die Auswirkungen von systematischem Versagen der leittechnischen Einrichtungen auf die Ereignisabläufe der Sicherheitsebene 3 unter Berücksichtigung der verfahrenstechnischen Vorgaben zu analysieren. Es sind Vorkehrungen gegen systematisches Versagen zur Minderung von dessen Eintrittswahrscheinlichkeit derart zu treffen, dass es auf der Sicherheitsebene 3 nicht mehr unterstellt werden muss.	Leittechnik-Funktionen der Kategorie A ausführen, sind Vorkehrungen gegen systematische Ausfälle der leittechnischen Einrichtungen zur Minderung der Eintrittswahrscheinlichkeit derart zu treffen, dass ein systematischer Ausfall auf der Sicherheitsebene 3 nicht mehr unterstellt werden muss. Kann für rechnerbasierte oder programmierbare leittechnische Einrichtungen diese Nachweisführung nach dem Stand von Wissenschaft und Technik nicht erfolgen, sind Vorkehrungen derart zu treffen, dass ein systematischer Ausfall von Hardware und Software auf der Sicherheitsebene 3 beherrscht wird. Beim Einsatz rechnerbasierter oder programmierbarer Leittechnik sind grundsätzlich diversitäre leittechnische Einrichtungen unter Beachtung der folgenden Bedingungen zu verwenden. Es bestehen keine Vorgaben hinsichtlich des Einsatzes diversitärer Einrichtungen, wenn für die jeweils auszuführende Leittechnik-Funktion ein aktiver systematischer Ausfall sicherheitsgerichtet ist. Beim Einsatz von rechnerbasierter oder programmierbarer Leittechnik ist für Schutzaktionen, die nicht für jeden Anlagenzustand sicherheitsgerichtet sind, in Abhängigkeit von den Auswirkungen von passiven oder aktiven systematischen Ausfällen in den leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, eine zweifache oder dreifache diversitäre Ausführung der Leittechnik einzusetzen. Eine mindestens zweifache diversitäre Ausführung ist einzusetzen, – wenn mit den noch verfügbaren Sicherheitseinrichtungen der Störfall beherrscht wird oder – wenn jede der beiden diversitären leittechnischen Einrichtungen für sich alleine die erforderliche Schutzaktion auslöst. Trifft beim Einsatz von rechnerbasierter oder programmierbarer Leittechnik eine der beiden genannten Voraussetzungen für den Einsatz einer zweifach diversitären Ausführung nicht zu, ist eine dreifach diversitär ausgeführte Leittechnik einzusetzen. 3.2 (12) Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, sind grundsätzlich so auszulegen,		3.7 (4) übernommen. Die „Sicherheitsebene 3“ wurde, wie in Abschnitt 2.2 <i>Kategorisierung</i>, durch den etablierten Begriff „Störfall“ ersetzt.

Anforderungen nach SiAnf	Anforderungen nach den Interpretationen	Umsetzung in KTA 3501 (2015-11)	Bewertung bezüglich KTA 3501
	dass sie ihre Aufgaben im Anforderungsfall unter Berücksichtigung folgender Annahmen erfüllen: Es liegt a) ein Zufallsausfall durch einen Einzelfehler, b) und ein systematischer Ausfall (systematischer Ausfall der Hardware oder systematisches Softwareversagen); dies gilt nicht, wenn die Voraussetzung der Nummer 3.2 (11) erfüllt ist, c) und Folgeausfälle d) und ein Instandhaltungsfall vor. Während eines Instandhaltungsfalls muss innerhalb einer Zeitspanne von 100 h das gleichzeitige Auftreten des systematischen Ausfalls und des Zufallsausfalls nicht unterstellt werden. Bei rechnerbasierten und programmierbaren leittechnischen Einrichtungen mit einem ausreichend hohen Selbstüberwachungsgrad und nachgewiesenen Instandhaltungszeiten kleiner als 8 h muss gleichzeitig mit dem systematischen Ausfall das Auftreten eines Zufallsausfalls oder des Instandhaltungsfalls nicht unterstellt werden. Hinweis: Zum Ausfall durch Einzelfehler und Unverfügbarkeit durch Instandhaltung sind weitere Anforderungen in Anhang 4 der „Sicherheitsanforderungen an Kernkraftwerke“ festgelegt.		
3.7 (5) In den Betriebsphasen, in denen die Verfügbarkeit der Reaktorschnellabschaltung erforderlich ist, muss jederzeit eine Reaktorschnellabschaltung von Hand möglich sein, auch beim unterstellten systematischen Versagen rechnerbasierter und programmierbarer leittechnischer Einrichtungen einschließlich systematischen Softwareversagens. Die manuelle Auslösung von Schutzaktionen ist unabhängig von automatischen leittechnischen Einrichtungen aufzubauen.		4.1.4.3 Automatisierungsgrad	Erfüllt. Kein Widerspruch.
3.7 (7) Das Kernkraftwerk muss mit Überwachungs- und Meldeeinrichtungen ausgerüstet sein, die auf den Sicherheitsebenen 1 und 2 jederzeit einen ausreichenden Überblick über den sicherheitsrelevanten Zustand der Anlage und die ablaufenden relevanten Prozesse ermöglichen und alle sicherheitstechnisch wichtigen Be-		9 Gefahrenmeldeeinrichtungen	Erfüllt.

Anforderungen nach SiAnf	Anforderungen nach den Interpretationen	Umsetzung in KTA 3501 (2015-11)	Bewertung bezüglich KTA 3501
triebsparameter anzeigen und registrieren können. Es müssen Gefahrenmeldeeinrichtungen vorhanden sein, die Veränderungen des Betriebszustandes, aus denen sich eine Verminderung der Sicherheit ergeben könnte, so frühzeitig anzeigen, dass die Einhaltung der jeweiligen sicherheitstechnischen Nachweisziele gewährleistet werden kann.			
3.7 (8) Das Kernkraftwerk muss mit einer Instrumentierung ausgerüstet sein, die bei Ereignisabläufen und Anlagenzuständen der Sicherheitsebenen 3 und 4 sowie bei Einwirkungen von innen oder außen sowie aus Notstandsfällen a) ausreichende Informationen über den Zustand der Anlage liefert, um die erforderlichen Schutzmaßnahmen für Personal und Anlage ergreifen und deren Wirksamkeit feststellen zu können, b) die Verfolgung des Ereignisablaufes und die Dokumentation der Ereignisse ermöglicht, c) eine Abschätzung der Auswirkungen auf die Umgebung gestattet, d) für mindestens 10 Stunden (auch bei Ausfall der nicht durch Batterien gepufferten elektrischen Energieversorgung) stromversorgt wird und e) die redundante Signalverarbeitung vornimmt. Die Einrichtungen zur Erfassung und Aufzeichnung der jeweils erforderlichen Informationen sollen diversitär und störfallfest aufgebaut sein. Für die Sicherheitsebenen 4b und 4c sollen ausreichende Informationen über den Zustand der Anlage geliefert werden, um die geplanten Notfallmaßnahmen ergreifen und deren Wirksamkeit feststellen zu können sowie eine Abschätzung der Auswirkungen auf die Umgebung zu ermöglichen.	3.1 (10) Für leittechnische Einrichtungen, die auslegungsgemäß Funktionen auch unter Störfallbedingungen ausführen, muss die Störfallfestigkeit nachgewiesen werden.	5.1.4 Umgebungseinflüsse 5.2.4 Umgebungseinflüsse	Erfüllt.
3.7 (10) Die von leittechnischen Einrichtungen auszuführenden Funktionen sind entsprechend ihrer sicherheitstechnischen Bedeutung gemäß der Nummer 3.1 (4) zu klassifizieren. Die Anforderungen an Entwurf, Implementierung, Qualifizierung, Inbetriebsetzung, Betrieb und Modifizierung der Software und an Auslegung, Fertigung, Errichtung und Betrieb der Hardware (Komponenten, Baugruppen und Teilsysteme) für leit-	2 Kategorisierung Entsprechend ihrer sicherheitstechnischen Bedeutung müssen Leittechnik-Funktionen, einschließlich Leittechnik-Funktionen der Störfallinstrumentierung, in unterschiedliche Kategorien eingeordnet werden, für die abgestufte Anforderungen gelten. Kategorie A	2.2 Kategorisierung der Funktionen der Sicherheitsleittechnik Entsprechend ihrer sicherheitstechnischen Bedeutung müssen Leittechnik-Funktionen, einschließlich Leittechnik-Funktionen der Störfallinstrumentierung, in unterschiedliche Kategorien eingeordnet werden, für die abgestufte Anforderungen gelten.	Erfüllt. Die Kategorisierung wurde aus den Interpretationen I-3, Abschnitt 2 übernommen. Die Sicherheitsebenen wurden inhaltlich übernommen und durch etablierte Begriffe ersetzt, die in den SiAnf definiert sind.

Anforderungen nach SiAnf	Anforderungen nach den Interpretationen	Umsetzung in KTA 3501 (2015-11)	Bewertung bezüglich KTA 3501
technische Einrichtungen sind entsprechend der sicherheitstechnischen Klassifizierung der von ihnen ausgeführten Funktionen festzulegen. Für leittechnische Einrichtungen, die nicht kategorisierte Leittechnik-Funktionen ausführen, werden in den „Sicherheitsanforderungen an Kernkraftwerke“ keine Anforderungen aufgestellt.	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 sicherheitstechnisch wichtigen Funktionen. Nicht kategorisiert sind Leittechnik Funktionen, die keine sicherheitstechnisch wichtigen Funktionen ausführen.	Kategorie A Die Leittechnik-Funktionen der Kategorie A umfassen alle Funktionen, die erforderlich sind, um Störfälle zu beherrschen. Kategorie B Die Leittechnik-Funktionen der Kategorie B umfassen alle Funktionen, die erforderlich sind, um anomale Betriebszustände (vgl. SiAnf Anhang 1) zu beherrschen, so dass das Eintreten von Störfällen vermieden wird. Kategorie C Die Leittechnik-Funktionen der Kategorie C umfassen alle übrigen sicherheitstechnisch wichtigen Funktionen. Nicht kategorisiert sind Leittechnik-Funktionen, die keine sicherheitstechnisch wichtigen Funktionen ausführen.	
5 Anforderungen an die Nachweisführung 5 (1) Der Genehmigungsinhaber muss über Nachweise zur Sicherheit der Anlage verfügen. Die Nachweisführungen müssen vollständig und nachvollziehbar dokumentiert werden. Sie sind, soweit geboten, zu aktualisieren. Hinweis: Konkretisierungen hierzu sind in Anhang 5 dargestellt. 5 (2) Zur Nachweisführung der Erfüllung der technischen Sicherheitsanforderungen sind deterministische Methoden sowie die probabilistische Sicherheitsanalyse heranzuziehen: Die deterministischen Methoden umfassen a) die rechnerische Analyse von Ereignissen oder Zuständen, b) die Messung oder das Experiment, c) die ingenieurmäßige Bewertung. 5 (3) Als Grundlage für Nachweisführungen müssen vorliegen: a) eine aktuelle Zusammenstellung der sicherheitstechnisch wichtigen		10 Prüfungen 11 Konfigurations- und Identifikations-Dokumentation	Erfüllt.

Anforderungen nach SiAnf	Anforderungen nach den Interpretationen	Umsetzung in KTA 3501 (2015-11)	Bewertung bezüglich KTA 3501
Informationen über den bestehenden Zustand der betroffenen Maßnahmen und Einrichtungen sowie b) eine Dokumentation, dass der bestehende Zustand der betroffenen sicherheitstechnisch wichtigen Maßnahmen und Einrichtungen die aktuell geltenden Anforderungen erfüllt. 5 (4) Bei der rechnerischen Analyse von Ereignisabläufen oder Zuständen müssen a) für den jeweiligen Anwendungsbereich validierte Berechnungsverfahren verwendet sowie b) mit der Berechnung verbundene Unsicherheiten quantifiziert oder durch geeignete Verfahren abgedeckt werden. 5 (6) Eine Messung oder ein Experiment kann als Nachweis herangezogen werden, wenn a) die Übertragbarkeit der experimentellen Bedingungen auf die Anlagenzustände des jeweiligen Anwendungszusammenhangs qualifiziert ist und b) die mit der Messung verbundenen Unsicherheiten quantifiziert sind. 5 (7) Ingenieurmäßige Bewertungen können bei Nachweisführungen herangezogen werden, wenn hierzu ein Bewertungsmaßstab vorliegt, der auf technisch-wissenschaftlich nachvollziehbaren Grundlagen beruht.			
6 Anforderungen an das Betriebsreglement 6 (4) Entsprechend ihrer sicherheitstechnischen Bedeutung müssen für alle sicherheitstechnisch wichtigen Einrichtungen Spezifikationen, Auslegungsvorschriften, Werkstoffvorschriften, Bauvorschriften und Prüfvorschriften sowie Betriebsvorschriften und Instandhaltungsvorschriften vorhanden sein. In den Prüfvorschriften sind Vorprüfungen, Werkstoffprüfungen, Bauprüfungen, Druckprüfungen, Abnahmeprüfungen und Funktionsprüfungen sowie regelmäßig wiederkehrende Prüfungen im Einzelnen festzulegen. Die Einhaltung dieser Vorschriften ist im Rahmen eines Qualitätsgewährleistungsprogramms zu überwachen. Das Ergebnis der Qualitätsüberwachung mit den Ergebnissen der Prüfungen ist zu dokumentieren. Die zur Beurteilung der Qualität notwendigen Unterlagen		Anforderungen, die übergeordnet mit der KTA 3501 in Verbindung stehen	Erfüllt.

Anforderungen nach SiAnf	Anforderungen nach den Interpretationen	Umsetzung in KTA 3501 (2015-11)	Bewertung bezüglich KTA 3501
über Auslegung, Fertigung, Errichtung und Prüfungen sowie Betrieb und Instandhaltung der sicherheitstechnisch wichtigen Einrichtungen sind bis zum Abbau der Einrichtungen verfügbar zu halten.			
7 Grundlegende Anforderungen an die Dokumentation 7 (1) Alle Unterlagen, die bei der Planung, der Errichtung und dem Betrieb einer Anlage für das Genehmigungs- und Aufsichtsverfahren verwendet wurden oder werden, sind systematisch zu dokumentieren. Der Detaillierungsgrad der Dokumentation muss an die sicherheitstechnische Bedeutung des Inhalts der Dokumente angepasst sein. 7 (2) Die Dokumentation hat folgende Anforderungen zu erfüllen: a) Anwendung eines Freigabe-/ Genehmigungsverfahrens, das der Bedeutung des jeweiligen Dokuments angemessen ist, b) eindeutige Kennzeichnung von Dokumenten, c) zeitnahe Aktualisierung von Dokumenten, insbesondere bei Änderungen an der Anlage, d) Kennzeichnung von Änderungen und des Überarbeitungsstatus von Dokumenten, e) Sicherstellung der Verfügbarkeit gültiger Dokumente an den jeweiligen Einsatzorten, f) zeitnahe Anpassung der zur Betriebsführung benötigten Dokumentation an den aktuellen Anlagenzustand und Bereitstellung im Bereich der Warte, g) Sicherstellung der Lesbarkeit und Erkennbarkeit, h) eindeutige und widerspruchsfreie Gestaltung sicherheitsrelevanter operativer Anweisungen, i) Kennzeichnung und Verteilung externer Dokumente an die jeweiligen Einsatzorte, j) Verhinderung der Verwendung veralteter oder nicht gültiger Dokumente. 7 (3) Die Dokumentation ist nach festgelegten Regeln zu pflegen und archivieren. Es sind auch Regelungen für Pflege und Archivierung der sonstigen Dokumentation zu treffen.		7 Prüfdokumentation	Erfüllt.

Anforderungen nach SiAnf	Anforderungen nach den Interpretationen	Umsetzung in KTA 3501 (2015-11)	Bewertung bezüglich KTA 3501
7 (4) In einem Dokumentationssystem sind Festlegungen zu Dokumentenart, Dokumentation, Unterlagenpflege, Archivierung, Verantwortlichkeiten und Prüfung zu treffen.			
Anhang 1 Begriffsbestimmungen Ausfall Verlust der Fähigkeit einer Einrichtung die geforderte Funktion zu erfüllen. Hinweis: Das Ereignis Ausfall markiert den Zeitpunkt des Übergangs von der Korrektheit zu einem Fehler. Mit einem Ausfall kann gleichzeitig ein Versagen auftreten, muss aber nicht. Zum Beispiel kann ein Aggregat, das nicht angefordert wird, ausgefallen sein, versagen wird es erst, wenn es angefordert wird und seine Funktion nicht mehr erbringt.		2 Begriffe (10) Ausfall Verlust der Fähigkeit einer Einrichtung die geforderte Funktion zu erfüllen. Hinweis: Das Ereignis Ausfall markiert den Zeitpunkt des Übergangs von der Korrektheit zu einem fehlerhaften Zustand. Mit einem Ausfall kann gleichzeitig ein Versagen auftreten, muss aber nicht. Zum Beispiel kann ein Aggregat, das nicht angefordert wird, ausgefallen sein, versagen wird es erst, wenn es angefordert wird und seine Funktion nicht mehr erbringt.	Erfüllt. Wurde aus SiAnf Anhang 1 übernommen. Zu Fehlern werden auch latente Fehler gezählt, die sich nicht als Ausfall zeigen. Der Begriff „Fehler“ wurde deshalb durch „fehlerhaften Zustand“ ersetzt.
Ausfall, systematischer <i>Ausfall</i> aufgrund der gleichen Ursache.		(1) Ausfall, systematischer Der systematische Ausfall ist das Versagen von Komponenten aufgrund der gleichen Ursache. Hinweis: Ein systematischer Ausfall kann z. B. durch falsche Auslegung oder Fehler in einer Fertigungsserie hervorgerufen werden.	Erfüllt. Übernahme aus den SiAnf Anhang 1. Ergänzung eines Hinweises, um auf besondere Aspekte in der Leittechnik aufmerksam zu machen.
Betrieb, bestimmungsgemäßer Der Betrieb, für den eine Anlage nach ihrem technischen Zweck bestimmt, ausgelegt und geeignet ist, umfasst die Betriebszustände und Betriebsvorgänge - bei funktionsfähigem Zustand der Einrichtungen, (ungestörter Betriebszustand, Normalbetrieb, Sicherheitsebene 1), - des anomalen Betriebs (gestörter Betriebszustand, Störung, Sicherheitsebene 2) sowie - bei Instandhaltungsvorgängen (Inspektion, Wartung, Instandsetzung).		(13) Bestimmungsgemäßer Betrieb Der Betrieb, für den eine Anlage nach ihrem technischen Zweck bestimmt, ausgelegt und geeignet ist, umfasst die Betriebszustände und Betriebsvorgänge a) bei funktionsfähigem Zustand der Einrichtungen, (ungestörter Betriebszustand, Normalbetrieb), b) des anomalen Betriebs (gestörter Betriebszustand, Störung) sowie c) bei Instandhaltungsvorgängen (Inspektion, Wartung, Instandsetzung).	Erfüllt. Übernahme aus den SiAnf Anhang 1. Der Bezug zu den Sicherheitsebenen erfolgt im Abschnitt Grundlagen, in denen auf die SiAnf verwiesen wird und kann an dieser Stelle entfallen.

Anforderungen nach SiAnf	Anforderungen nach den Interpretationen	Umsetzung in KTA 3501 (2015-11)	Bewertung bezüglich KTA 3501
Diversität Vorhandensein von zwei oder mehr funktionsbereiten Einrichtungen zur Erfüllung der vorgesehenen Funktion, die physikalisch oder technisch verschiedenartig ausgelegt sind.		(18) Diversitäre leittechnische Einrichtungen Vorhandensein von zwei oder mehr funktionsbereiten Einrichtungen zur Erfüllung der vorgesehenen Funktion, die physikalisch oder technisch verschiedenartig ausgelegt sind.	Erfüllt. Übernahme aus den SiAnf Anhang 1. „Vorhandensein“ und „funktionsbereit“ wird hinterfragt. Sind diese Attribute tatsächlich geeignet für diese Definition?
Inspektion Maßnahme zur Feststellung und Beurteilung des Ist-Zustandes von Einrichtungen.		(34) Inspektion Inspektionen sind Maßnahmen zur Feststellung und Beurteilung des Ist-Zustandes von Einrichtungen. (s. a. DIN 31051)	Erfüllt. Übernahme aus den SiAnf Anhang 1.
Instandhaltung Die Gesamtheit der Maßnahmen zur Bewahrung und Wiederherstellung des Soll-Zustands sowie zur Feststellung und Beurteilung des Ist-Zustands (einschließlich wiederkehrender Prüfung). Die Instandhaltung gliedert sich in die Vorbeugende Instandhaltung mit den zugehörigen Elementen Inspektion und Wartung, sowie Instandsetzung (Reparatur).		(35) Instandhaltung Die Instandhaltung ist die Gesamtheit der Maßnahmen zur Bewahrung und Wiederherstellung des Sollzustandes sowie zur Feststellung und Beurteilung des Ist-Zustandes. Die Instandhaltung gliedert sich in die Vorbeugende Instandhaltung mit den zugehörigen Elementen, Inspektionen (insbesondere Wiederkehrende Prüfungen) und Wartung, sowie Instandsetzung (Austausch und Reparatur).	Erfüllt. Übernahme aus den SiAnf Anhang 1. Redaktionelle Anpassung. Die WKP wurde in Klammern bei den „Inspektionen“ ergänzt und im 1. Satz gestrichen.
Komponente Ein nach baulichen oder funktionellen Gesichtspunkten abgegrenzter Teil eines Systems. Komponenten bestehen aus Betriebsmitteln. Betriebsmittel sind die kleinsten Einheiten, die in sich funktionsfähig sind. Betriebsmittel bestehen aus Bauteilen.		(36) Komponente Eine Komponente ist ein nach baulichen oder funktionellen Gesichtspunkten abgegrenzter Teil eines Systems, der noch selbstständige Teilfunktionen erfüllt.	Erfüllt. Die Änderungen, die sich aus den SiAnf Anhang 1 ergeben hätten, wurden nicht übernommen, da diese speziell für die Verfahrenstechnik gelten.
Leittechnik Gesamtheit der leittechnischen Einrichtungen zum Ausführen von Leittechnik-Funktionen. Leittechnische Einrichtungen umfassen sowohl automatische Einrichtungen als auch die Einrichtungen zur Prozessführung durch einen Operator.		(37) Leittechnik Gesamtheit der leittechnischen Einrichtungen zum Ausführen von Leittechnik-Funktionen. (38) Leittechnische Einrichtungen Leittechnische Einrichtungen sind Geräte und Systeme zur Ausführung von Leittechnik-Funktionen vom Messwertgeber bis zu den den Einzelantrieben zugeordneten Teilen der Steuerung zur Auslösung von Schutzaktionen. Leittechnische Einrichtungen	Erfüllt. Die Definition wurde überarbeitet. Der Aspekt, dass auch Einrichtungen zur Prozessführung durch einen Operator zur Leittechnik gezählt werden, ist in der Definition „Leittechnische Einrichtungen“ enthalten und wurde deshalb gestrichen.

Anforderungen nach SiAnf	Anforderungen nach den Interpretationen	Umsetzung in KTA 3501 (2015-11)	Bewertung bezüglich KTA 3501
		gen umfassen sowohl automatische Einrichtungen als auch die Einrichtungen zur Prozessführung durch einen Operator.	Die Definition Leittechnische Einrichtungen wurde redaktionelle angepasst.
Reaktorschutzsystem Die Einrichtungen des Reaktorschutzsystems sind für Ausführung der Leittechnik-Funktionen der Kategorie A vorgesehen. Das Reaktorschutzsystem ist Teil des Sicherheitssystems, welcher die für die Sicherheit wesentlichen Prozessvariablen zur Verhinderung von unzulässigen Einwirkungen und zur Erfassung von Störfällen überwacht, verarbeitet und Schutzaktionen auslöst, um den Zustand der Reaktoranlage in sicheren Grenzen zu halten. Das Reaktorschutzsystem umfasst als Teil des Sicherheitssystems alle Einrichtungen der Messwerterfassung, der Signalaufbereitung, der Logikebene und die den Einzelantrieben zugeordneten Teile der Steuerung zur Auslösung von Schutzaktionen sowie die Funktionsgruppensteuerungen.		(45) Reaktorschutzsystem Das Reaktorschutzsystem ist Teil des Sicherheitssystems, welcher die für die Sicherheit wesentlichen Prozessvariablen zur Verhinderung von unzulässigen Einwirkungen und zur Erfassung von Störfällen überwacht, verarbeitet und Schutzaktionen auslöst, um den Zustand der Reaktoranlage in sicheren Grenzen zu halten. Das Reaktorschutzsystem umfasst als Teil des Sicherheitssystems alle Einrichtungen der Messwerterfassung, der Signalaufbereitung, der Logikebene und die den Einzelantrieben zugeordneten Teile der Steuerung zur Auslösung von Schutzaktionen. Die Leittechnik-Funktionen des Reaktorschutzsystems sind typischerweise der Kategorie A zugeordnet. Hinweise: Die Festlegungen der Anzahl und der Art der vom Reaktorschutzsystem zu erfassenden Prozessvariablen und der daraus zu bildenden Sicherheitsvariablen, die Festlegung ihrer Grenzwerte sowie die Festlegung der Anzahl und der Art der Schutzaktionen erfolgen aufgrund der Störfallanalyse. Das Reaktorschutzsystem umfasst als Teil des Sicherheitssystems einer Reaktoranlage alle Geräte und Einrichtungen der Messwerterfassung, der Signalaufbereitung, der Logikebene und den den Einzelantrieben zugeordneten Teilen der Steuerung zur Auslösung von Schutzaktionen.	Erfüllt. Die Definition wurde redaktionell überarbeitet. Das Reaktorschutzsystem sollte nicht über die Kategorie A definiert werden, deshalb wurde der erste Satz gelöscht und am Ende des Absatzes der folgende Satz eingefügt: „Die Leittechnik-Funktionen des Reaktorschutzsystems sind typischerweise der Kategorie A zugeordnet“. Weiterhin wurden die Funktionsgruppensteuerungen gestrichen, da sie nicht mehr Stand der Technik sind. Das Reaktorschutzsystem umfasst nicht nur die Sicherheitsleittechnik, sondern auch verfahrenstechnische Komponenten.
Redundanz Vorhandensein von mehr funktionsbereiten Einrichtungen, als zur Erfüllung der vorgesehenen Funktion notwendig ist.		(47) Redundanz Die Redundanz ist das Vorhandensein von mehr funktionsbereiten Einrichtungen, als zur Erfüllung	Erfüllt. Übernahme aus den SiAnf Anhang 1.

Anforderungen nach SiAnf	Anforderungen nach den Interpretationen	Umsetzung in KTA 3501 (2015-11)	Bewertung bezüglich KTA 3501
		der vorgesehenen Funktion notwendig ist. Hinweis: In dieser Regel wird die Forderung nach Redundanz als erfüllt angesehen, wenn gleichartige Einrichtungen eingesetzt werden.	
Schutzaktion Die Betätigung oder der Betrieb von aktiven Sicherheitseinrichtungen, die zur Beherrschung von Ereignissen erforderlich sind.		(50) Schutzaktion Die Betätigung oder der Betrieb von aktiven Sicherheitseinrichtungen, die zur Beherrschung von Störfällen erforderlich sind.	Erfüllt. KTA-spezifischer Anwendungsbereich. Einige Ereignisse werden nicht durch den Reaktorschutz beherrscht. (z. B. FLAB, deren Auswirkungen können nur gemindert werden.)
Sicherheitsabstand Abstand zwischen dem gemäß eines Nachweiskriteriums zulässigen Wert einer Größe und dem Wert, bei dem der Verlust der geforderten Eigenschaften zu unterstellen ist.		(60) Sicherheitsabstand Der Sicherheitsabstand ist die Differenz zwischen dem am Grenzsinalgeber eingestellten Auslösewert und dem bei der Störfallanalyse festgelegten Gefährdungsgrenzwert.	Erfüllt. Präzisierung. Die Änderung, die sich aus den SiAnf Anhang 1 ergibt wurde abgelehnt. Der Begriff muss für diese Regel präziser gefasst werden. Der ursprüngliche Regeltext bildet dies adäquat ab.
Sicherheitseinrichtung, aktive Einrichtung des Sicherheitssystems, die Schutzaktionen ausführt.		(61) Sicherheitseinrichtung, aktive Die aktive Sicherheitseinrichtung ist eine technische Einrichtung des Sicherheitssystems, die Schutzaktionen ausführt. Hinweis: Aktive Sicherheitseinrichtungen sind z. B. Einrichtungen zur Abschaltung des Reaktors, zur Nachwärmeabfuhr, zum Durchdringungsabschluss des Reaktorsicherheitsbehälters. Sicherheitseinrichtungen, die eine Schutzfunktion ohne Stellglieder oder ohne Aggregate ausüben, z. B. Kernkühlmitteleinschluss, Sicherheitsbehälter, Abschirmung, werden als passive Sicherheitseinrichtungen bezeichnet.	Erfüllt. Die Präzisierung, dass es sich um eine „technische“ Einrichtung handeln muss, ist an dieser Stelle korrekt und sollte nicht verloren gehen.
Sicherheitssystem Gesamtheit aller Einrichtungen, die die Aufgabe haben, die Anlage vor unzulässigen Einwirkungen zu schützen und bei auftretenden Störfällen deren Auswirkungen auf		(62) Sicherheitssystem Das Sicherheitssystem ist die Gesamtheit aller Einrichtungen einer Reaktoranlage, die die Aufgabe	Erfüllt. Präzisierung. Die Definition aus den SiAnf Anhang 1 konnte nicht vollständig übernommen werden. Mit der

Anforderungen nach SiAnf	Anforderungen nach den Interpretationen	Umsetzung in KTA 3501 (2015-11)	Bewertung bezüglich KTA 3501
das Betriebspersonal, die Anlage und die Umgebung in vorgegebenen Grenzen zu halten.		haben, die Anlage vor unzulässigen Beanspruchungen zu schützen und bei auftretenden Störfällen deren Auswirkungen auf das Betriebspersonal, die Anlage und die Umgebung in vorgegebenen Grenzen zu halten.	Definition aus den SiAnf würden alle Sicherungsanlagen dem Sicherheitssystem zugeordnet, die nicht im KTA behandelt werden. Die ursprüngliche KTA-Definition wurde deshalb beibehalten.
Sicherheitsvariable Sicherheitstechnisch relevanter Betriebsparameter oder sicherheitstechnisch relevante Prozessvariable.		(64) Sicherheitsvariable Die Sicherheitsvariable ist eine aus einer oder mehreren Prozessvariablen gewonnene Größe, deren Wert die Sicherheit der Anlage kennzeichnet und die zur Auslösung von Schutzaktionen benötigt wird.	Erfüllt. Die Definition in den SiAnf Anhang 1 greift zu kurz (Die Sicherheitsvariable kann auch eine Rechengröße sein). Die ursprüngliche Definition präzisiert die Definition aus den SiAnf und steht nicht im Widerspruch zu ihr.
Verifizierung Bestätigung durch Bereitstellung eines objektiven Nachweises, dass festgelegte Kriterien erfüllt worden sind.		(67) Validierung: Bestätigung durch Prüfung und Nachweis, dass die Anforderungsspezifikation wie vorgesehen erfüllt ist. (68) Verifikation: Bestätigung durch Prüfung und Nachweise, dass die Resultate einer Tätigkeit die Ziele und Anforderungen erfüllen, die für diese Tätigkeit definiert wurden. Hinweis: Im Rahmen des Phasenmodells werden die einzelnen Phasen durch die Verifikation abgeschlossen.	Erfüllt. Die Validierung und Verifikation wird in KTA 3501 in einem anderen Kontext verwendet und weicht deshalb von der Definition in den SiAnf Anhang 1 ab. (s. a. Phasenmodell, Verifikation) Die ursprüngliche Definition wurde beibehalten.
Verriegelung Vorkehrung, mittels derer Funktionen von Einrichtungen, die bei spezifizierten Betriebs- oder Störfallbedingungen unzulässig sind, leit- oder verfahrenstechnisch blockiert werden.			Erfüllt. Der Neuaufnahme der Definition von Verriegelung aus den SiAnf Anhang 1 wurde nicht zugestimmt, da Verriegelungen in der KTA 3501 in einem anderen Kontext verwendet werden.
Versagen Nicht- oder Fehlfunktion bei Anforderung aktiver Systeme bzw. Verlust der <i>Integrität</i> bzw. <i>Funktionsfähigkeit</i> bei passiven Systemen.		(70)Versagen Nicht- oder Fehlfunktion bei Anforderung aktiver Systeme. Hinweis: Ursache des Versagens einer Funktion können Ausfälle von Komponenten oder Geräten sein, aber auch latente Fehler,	Erfüllt. Definition von Versagen wurde aus den SiAnf Anhang 1 neu aufgenommen zur Verdeutlichung des Unterschiedes zwischen Ausfall und Versagen.

Anforderungen nach SiAnf	Anforderungen nach den Interpretationen	Umsetzung in KTA 3501 (2015-11)	Bewertung bezüglich KTA 3501
		die unter besonderen Randbedingungen wirksam werden.	
Anhang 2 Zu berücksichtigende Ereignisse		3.2 Ereignisabläufe und ihre Auswirkungen	Erfüllt. Tab 5-3 Ereignisliste Brennelement-Lagerbeckenkühlung ist nicht im Anwendungsbereich der KTA 3501 und wurde deshalb ausgeschlossen.
Anhang 4 Grundsätze für die Anwendung des Einzelfehlerkriteriums und für die Instandhaltung 4 Sicherstellung der Funktionsbereitschaft sicherheitstechnisch wichtiger Einrichtungen 4 (1) Die Funktion von sicherheitstechnisch wichtigen Einrichtungen ist unter Bedingungen, die möglichst dem Anforderungsfall entsprechen, im erforderlichen Umfang wiederkehrend zu prüfen. 4 (10) Die Funktionsbereitschaft und die anforderungsgerechte Funktion sicherheitstechnisch wichtiger Einrichtungen sind nach abgeschlossener Instandhaltungsmaßnahme durch qualifizierte Funktionsprüfungen sicherzustellen.		4.1.2.2 Versagensauslösende Ereignisse innerhalb der Reaktoranlage 4.1.7 Instandhaltung 4.2.8 Instandhaltung	Erfüllt.
Anhang 5 7 Grundlegende Anforderungen an die Dokumentation 7 (1) Alle Unterlagen, die bei der Planung, der Errichtung und dem Betrieb einer Anlage für das Genehmigungs- und Aufsichtsverfahren verwendet wurden oder werden, sind systematisch zu dokumentieren. Der Detaillierungsgrad der Dokumentation muss an die sicherheitstechnische Bedeutung des Inhalts der Dokumente angepasst sein. 7 (2) Die Dokumentation hat folgende Anforderungen zu erfüllen: a) Anwendung eines Freigabe-/ Genehmigungsverfahrens, das der Bedeutung des jeweiligen Dokuments angemessen ist, b) eindeutige Kennzeichnung von Dokumenten, c) zeitnahe Aktualisierung von Dokumenten, insbesondere bei Änderungen an der Anlage,	6 Spezifische Anforderungen zur Dokumentation zu leittechnischen Einrichtungen der Kategorie A bis C einschließlich Störfallinstrumentierung 6 (1) Die anlagenspezifische Konfiguration der Hard- und Software leittechnischer Einrichtungen, die Leittechnik-Funktionen der Kategorien A bis C ausführen, muss während ihres gesamten Lebenszyklus hinsichtlich des aktuellen Zustands und durchgeführter Änderungen dokumentiert werden. 6 (2) Die Instandhaltungsvorgänge und Eingriffe in die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorien A bis C ausführen, sind zu dokumentieren. 6 (3) Die Betriebserfahrung aus der Instandhaltung der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorien A bis C ausführen, muss entsprechend der sicherheitstechnischen Bedeutung der leittechnischen Einrichtungen erfasst, dokumentiert und systematisch ausgewertet werden.	10 Prüfungen 11 Konfigurations- und Identifikations-Dokumentation	Erfüllt.

Anforderungen nach SiAnf	Anforderungen nach den Interpretationen	Umsetzung in KTA 3501 (2015-11)	Bewertung bezüglich KTA 3501
d) Kennzeichnung von Änderungen und des Überarbeitungsstatus von Dokumenten, e) Sicherstellung der Verfügbarkeit gültiger Dokumente an den jeweiligen Einsatzorten, f) zeitnahe Anpassung der zur Betriebsführung benötigten Dokumentation an den aktuellen Anlagenzustand und Bereitstellung im Bereich der Warte, g) Sicherstellung der Lesbarkeit und Erkennbarkeit, h) eindeutige und widerspruchsfreie Gestaltung sicherheitsrelevanter operativer Anweisungen, i) Kennzeichnung und Verteilung externer Dokumente an die jeweiligen Einsatzorte, j) Verhinderung der Verwendung veralteter oder nicht gültiger Dokumente. 7 (3) Die Dokumentation ist nach festgelegten Regeln zu pflegen und archivieren. Es sind auch Regelungen für Pflege und Archivierung der sonstigen Dokumentation zu treffen. 7 (4) In einem Dokumentationssystem sind Festlegungen zu Dokumentenart, Dokumentation, Unterlagenpflege, Archivierung, Verantwortlichkeiten und Prüfung zu treffen.			

Tabelle 1: Abgleich der KTA 3501 (2015-11) mit den „Sicherheitsanforderungen an Kernkraftwerke“ und deren Interpretationen