

**KTA 3506****Systemprüfung der Sicherheitsleittechnik von Kernkraftwerken**

Bisheriger Titel:

„Systemprüfung der leittechnischen Einrichtungen des Sicherheitssystems von Kernkraftwerken“

**Vorbemerkung**

Der Kerntechnische Ausschuss (KTA) beabsichtigt, die zurzeit in der Fassung 1990-06 vorliegende Regel KTA 2201.2 zu ändern. Der Entwurf dieser Änderung wird hiermit der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt, damit er erforderlichenfalls verbessert werden kann. Es wird darauf hingewiesen, dass die endgültige Fassung von dem vorliegenden Entwurf abweichen kann.

**Änderungsvorschläge sind innerhalb einer Frist von drei Monaten,  
beginnend am 1. Januar 2012,**

bei der Geschäftsstelle des Kerntechnischen Ausschusses beim Bundesamt für Strahlenschutz, Postfach 10 01 49, 38201 Salzgitter, einzureichen.

Frühere Fassung der Regel:

1984-11 (BAnz. Nr. 40a vom 27. Februar 1985)

**Änderungsentwurf****Inhalt**

	Seite
Grundlagen .....	2
1 Anwendungsbereich .....	2
2 Begriffe .....	2
3 Übergeordnete Prüfanforderungen .....	2
3.1 Allgemeines .....	2
3.2 Zu prüfende Systeme .....	2
3.3 Konfigurations-Management und Konfigurations-Identifikations-Dokumentation .....	2
4 Inbetriebsetzungsprüfungen der Sicherheitsleittechnik.....	3
4.1 Prüfungen ohne Betrieb der verfahrenstechnischen Systeme .....	3
4.2 Prüfungen des Zusammenwirkens mit den verfahrenstechnischen Systemen .....	4
4.3 Anforderungen an Prüfhilfsmittel.....	5
4.4 Prüfer.....	5
4.5 Dokumentation.....	5
4.6 Prüfungen nach Instandsetzung .....	5
4.7 Prüfungen nach Systemänderungen.....	5
5 Wiederkehrende Prüfungen der Sicherheitsleittechnik.....	6
5.1 Allgemeine Anforderungen .....	6
5.2 Voraussetzung für die Durchführung der Prüfung.....	7
5.3 Prüfintervalle.....	7
5.4 Prüfliste.....	7
5.5 Prüfanweisungen .....	7
5.6 Anforderungen an Prüfhilfsmittel.....	7
5.7 Prüfer.....	7
5.8 Dokumentation.....	7
5.9 Prüfungen nach Instandsetzung .....	7
5.10 Prüfungen nach Freischaltungen und Simulationen.....	8
5.11 Prüfungen nach Systemänderungen.....	8
Anhang: A Bestimmungen, auf die in dieser Regel verwiesen wird.....	9
Anhang B: (informativ) Begriffe, die in dieser Regel verwendet werden.....	10
Dokumentationsunterlage zur Regeländerung .....	11

## Grundlagen

(1) Die Regeln des Kerntechnischen Ausschusses (KTA) haben die Aufgabe, sicherheitstechnische Anforderungen anzugeben, bei deren Einhaltung die nach dem Stand von Wissenschaft und Technik erforderliche Vorsorge gegen Schäden durch die Errichtung und den Betrieb der Anlage getroffen ist (§ 7 Absatz 2 Nr. 3 AtG), um die im AtG und in der Strahlenschutzverordnung (StrlSchV) festgelegten sowie in den Sicherheitskriterien und den Störfall-Leitlinien weiter konkretisierten Schutzziele zu erreichen.

(2) Gesetze, Verordnungen und Vorschriften des Bundes und der Länder sowie nachgeordnete behördliche Bestimmungen, wie die Sicherheitskriterien für Kernkraftwerke, verabschiedet im Länderausschuss für Atomkernenergie, oder die Leitlinien der Reaktorsicherheitskommission werden bei der Erstellung von KTA-Regeln berücksichtigt.

(3) In dieser KTA-Regel wird die Einhaltung von Vorschriften und Normen (z. B. Unfallverhütungsvorschriften, DIN-Normen und VDE-Bestimmungen) vorausgesetzt, wenn nicht kernkraftwerksspezifisch bedingt andere Anforderungen gestellt werden.

(4) Basierend auf den Sicherheitskriterien Abschnitt 2.1 „Qualitätsgewährleistung“ und 2.2 „Prüfbarkeit“ werden für die leittechnischen Einrichtungen des Sicherheitssystems nach Abschnitt 7 der RSK-Leitlinien die Anforderungen an Umfang, Vorbereitung und Durchführung der Systemprüfungen für Kernkraftwerke in dieser Regel behandelt.

(5) Diese Regel steht in engem Zusammenhang mit der Regel KTA 3501. Weiter sind von Bedeutung die Regeln KTA 3507, KTA 3503 sowie KTA 3505.

(6) Die Anforderungen der Regel KTA 3403 an die Funktionsprüfungen sind in KTA 3506 berücksichtigt worden.

(7) Zu den Schaltanlagen und elektrischen Antrieben wird im Anwendungsbereich eine Abgrenzung vorgenommen, die sich in Übereinstimmung mit den Regeln KTA 3701 bis 3705 und KTA 3504 befindet.

(8) Die Anforderungen der Regel KTA 3904 sind in KTA 3506 berücksichtigt worden.

(9) Übergeordnet für das gesamte Kernkraftwerk sind die KTA 1401, REV KTA 1402, RE KTA 1403, die KTA 1404 und KTA 1202 anzusehen.

## 1 Anwendungsbereich

(1) Diese Regel ist anzuwenden auf die Sicherheitsleittechnik von Kernkraftwerken. Sie gilt für leittechnische Einrichtungen, die Funktionen der Kategorien A, B und C ausführen.

### Hinweis:

(1) Bis zur Fertigstellung des Gründruckes der Regel KTA 3501 erfolgt die Definition der Kategorien im informativen Anhang B.

(2) Diese Regel beschreibt nicht die Anforderungen an die konventionelle Sicherheitstechnik, z. B. Arbeitsschutz.

(2) Die Systemprüfungen der Sicherheitsleittechnik umfassen Systemprüfungen im Testfeld, Inbetriebsetzungsprüfungen (IBS-Prüfungen) und wiederkehrende Prüfungen. Sie beinhalten nicht die baubegleitenden Prüfungen während der Montage sowie die in KTA 3701 bis 3705 behandelten elektrischen Systeme der Energieversorgung.

## 2 Begriffe

(1) Integrale Funktionsprüfungen

Prüfungen, bei denen die ordnungsgemäße Funktion eines leittechnischen Systems mit vorrangig rechnergestützten Prüf-

hilfsmitteln durch Vorgabe an den Signaleingängen und Abfrage der Reaktion an den Signalausgängen nachgewiesen wird.

(2) Sachverständiger

Sachverständiger ist eine aufgrund von § 20 Atomgesetz durch die atomrechtliche Genehmigungsbehörde oder Aufsichtsbehörde zugezogene fachkundige Person oder Organisation.

## 3 Übergeordnete Prüfanforderungen

### 3.1 Allgemeines

(1) Durch Systemprüfungen ist lückenlos nachzuweisen, dass die Sicherheitsleittechnik nach den vom Sachverständigen geprüften Unterlagen erstellt wurde und die vorgesehenen Funktionen erfüllt.

(2) Bei schrittweiser Durchführung der Prüfungen muss die Funktion der leittechnischen Einrichtungen mit überlappend aufeinander abgestimmten Prüfungsteilen nachgewiesen werden. Hierbei darf der Selbsttest des Systems belastet werden, sofern seine Wirksamkeit nachgewiesen ist. Die Funktionsprüfungen sollen die Betätigung und den Betrieb der Antriebe (z. B. Elektromotore, Stellantriebe, Magnetventile) soweit einschließen, dass die Rückmeldungen geprüft werden können.

(3) Werden bei der Prüfung Fehler erkannt, sind deren Ursache und Auswirkung zu analysieren und die Ursache zu beseitigen.

(4) Durch wiederkehrende Prüfungen ist in festzulegenden Zeitabständen nachzuweisen, dass die Sicherheitsleittechnik ihre spezifizierte Aufgabenstellung erfüllt. Bei A-Funktionseinrichtungen und B-Funktionseinrichtungen sind in den Umfang der wiederkehrenden Prüfungen auch integrale Funktionsprüfungen mit einzubeziehen. Die Prüfintervalle für die integralen Funktionsprüfungen sind in Abhängigkeit von der Wirksamkeit der Selbstüberwachungsfunktionen festzulegen.

### 3.2 Zu prüfende Systeme

Zu prüfen sind leittechnische Einrichtungen, die Funktionen der Kategorie A, B oder C ausführen.

#### Hinweis:

Dazu gehören:

- Reaktorschutzsystem,
- Schutzbegrenzungen,
- Zustandsbegrenzungen,
- Sicherheitstechnisch wichtige Regel- und Steuereinrichtungen,
- Steuerebene für sicherheitstechnisch wichtige Antriebe,
- Gefahrenmeldungen der Klasse S und
- Gefahrenmeldungen der Klasse I.

### 3.3 Konfigurations-Management und Konfigurations-Identifikations-Dokumentation

#### 3.3.1 Konfigurations-Management

(1) Es sind die funktionalen und technischen Eigenschaften des Systems nach Abschnitt 1 zu identifizieren und zu dokumentieren sowie Änderungen an diesen Eigenschaften zu erfassen. Hierzu sind die technischen und administrativen Anleitungen und Kontrollmaßnahmen festzulegen.

(2) Das Konfigurations-Management darf in administrativen Regelungen (z. B. Instandhaltungsordnung, Fachanweisung) enthalten sein.

(3) Durch das Konfigurations-Management ist eine laufende Aktualisierung der Konfigurations-Identifikations-Dokumentation sicherzustellen.

(4) Für softwarebasierte Leittechnik soll nachprüfbar sein, dass

- a) die Funktionalität dem aktuellen Stand der Anforderungsspezifikation entspricht und durch Tests geprüft wurde,
- b) der typgeprüfte Ausgabestand der Systemsoftware und der Hardware tatsächlich zum Einsatz kommt,
- c) die auf Basis der gültigen Anforderungsspezifikation generierte Anwendersoftware zum Einsatz kommt und
- d) das Konfigurations-Management auf einem aktuellen Stand gehalten wird.

(5) Es ist sicherzustellen, dass das Konfigurations-Management bei allen Instandhaltungsmaßnahmen einschließlich Inbetriebsetzung zu Grunde gelegt wird.

### 3.3.2 Konfigurations-Identifikations-Dokumentation

(1) Es sind die Merkmale zur Identifikation der Systemstruktur einschließlich Schnittstellen, der Hardware-Komponenten, der System- und Anwendersoftware-Komponenten sowie der eingesetzten Projektierungs- und Service-Werkzeuge zu dokumentieren.

(2) Es sind die zur eindeutigen Identifikation der Konfiguration eines Leittechniksystems erforderlichen Informationen anzugeben. Bei Altsystemen darf die Erstaufnahme im Rahmen von Instandhaltungsmaßnahmen erfolgen. In Abhängigkeit vom eingesetzten Leittechniksystem sind dies z. B.:

- a) Bestückungsliste der Leittechnik-Schränke mit Ausgabestand / Seriennummer der Baugruppen (Hardware / Firmware),
- b) Inhaltsverzeichnis der Pläne der Hardware-Konfiguration (Schrankdispositionspläne, Netzpläne, Stromlaufpläne, etc.),
- c) Liste der Hardware-Parameter, z. B. Adress- und Jumper-einstellungen der Hardware-Baugruppen, sowie der Software-Parameter, z. B. Grenzwerte, Hysteresen, Zeitkonstanten,
- d) Software-Konfiguration (Anwendersoftware, Systemsoftware, Projektierungssoftware, Servicewerkzeuge) in Form einer Liste aller Softwarekomponenten unter Angabe der Versionsbezeichnung und der zugehörigen Prüfsummen und
- e) Liste der Benutzergruppen einschließlich der zugehörigen Zugriffs-Rechte.

(3) Die in der Konfigurations-Identifikations-Dokumentation festgelegte Konfiguration eines Leittechniksystems muss in der Einsatzumgebung überprüfbar sein.

(4) Die Konfigurations- und Identifikations-Dokumentation darf aus unterschiedlichen Dokumenten bestehen oder auf weitere nach geordnete Dokumente referenzieren.

## 4 Inbetriebsetzungsprüfungen der Sicherheitsleittechnik

### 4.1 Prüfungen ohne Betrieb der verfahrenstechnischen Systeme

#### 4.1.1 Allgemeine Anforderungen

(1) Die Prüfungen ohne Betrieb der verfahrenstechnischen Systeme sind in den beiden Teilabschnitten Sichtprüfungen und Funktionsprüfungen durchzuführen.

Hinweis:

Die Prüfungen ohne Betrieb der verfahrenstechnischen Systeme können in Prüfungen im Testfeld und in Prüfungen am endgültigen Aufstellungsort aufgeteilt werden.

(2) Für die Prüfungen im Testfeld und die Inbetriebsetzungsprüfungen auf der Anlage dürfen Simulatoren eingesetzt werden. Die Eignung der verwendeten Simulatoren und Simulationsmodelle ist nachzuweisen.

#### 4.1.2 Sichtprüfungen

(1) Zu Beginn der Prüfungen ohne Betrieb der verfahrenstechnischen Systeme sind sowohl im Testfeld als auch auf der Anlage Sichtprüfungen der Sicherheitsleittechnik anhand der vom Sachverständigen geprüften Unterlagen durchzuführen.

(2) Mit den Prüfungen ist nachzuweisen, dass der Aufbau der leittechnischen Einrichtungen auch unter Berücksichtigung der Anordnung der anderen Kraftwerkskomponenten (z. B. maschinenbauliche, elektrotechnische und lüftungstechnische Einrichtungen) eine einwandfreie Funktion erwarten lässt und dass Instandhaltungsmöglichkeiten vorhanden sind. Prüfkriterien sind zum Beispiel:

- a) Fertigstellung sowie vollständige Bestückung und Software-Implementierung entsprechend der gültigen Konfigurations-Identifikations-Dokumentation des zu prüfenden Teils der leittechnischen Einrichtungen,
- b) Unversehrtheit des zu prüfenden Teils der leittechnischen Einrichtungen,
- c) funktionsgerechter Aufbau des mechanischen Teils der Messanordnungen (z. B. Messwertgeber, Entnahmeleitung, Messumformer),
- d) vollständige Kennzeichnung der Geräte, Baugruppen und Schränke sowie Zuordnung zu den Redundanzgruppen,
- e) Schutz des zu prüfenden Teils der leittechnischen Einrichtungen gegen mechanische Einwirkungen (z. B. durch Instandhaltungsarbeiten in der Anlage) und
- f) Zugänglichkeit der Geräte, Baugruppen und Messanordnungen für Prüfungen, Wartung und Instandsetzung.

(3) Die Sichtprüfungen auf der Anlage dürfen erst dann durchgeführt werden, wenn für die zu prüfenden Teile der Sicherheitsleittechnik die baubegleitenden Prüfungen zum Abschluss gebracht worden sind und die Montagearbeiten in den Räumen mit den zu prüfenden leittechnischen Einrichtungen soweit abgeschlossen sind, dass zusätzliche Montagearbeiten die geprüften Einrichtungen in Bezug auf die in 4.1.2 (2) genannten Prüfkriterien nicht mehr beeinträchtigen können.

#### 4.1.3 Funktionsprüfungen

(1) Die Funktionsprüfungen am endgültigen Aufstellungsort müssen den Nachweis erbringen, dass die leittechnischen Einrichtungen die in den vom Sachverständigen geprüften Unterlagen (z. B. Übersichtspläne, Funktionspläne, Stromlaufpläne, Messkennblätter, Funktionsbeschreibungen, Spezifikationen, Erläuterungsberichte) geforderten Funktionen erfüllen.

(2) Es sind Integrationstests mit den leittechnischen Einrichtungen der Anlage (z. B. Prozessrechner, Gefahrenmeldeanlage, Wartenanzeige, Rückmeldung) durchzuführen.

(3) Funktionsprüfungen sollen mit den maschinentechnischen und elektrotechnischen Komponenten durchgeführt werden, indem die Rückmeldesignale von Stellantrieben, Magnetventilen und Leistungsschaltern durch Ansteuerung der Komponenten gebildet werden. Die verfahrenstechnischen Systeme brauchen bei diesen Prüfungen nicht betrieben zu werden. Bei von Medien abgeleiteten Signalen (z. B. Druck und Durchfluss) dürfen die physikalischen Größen mit Prüfhilfen vorgegeben werden.

(4) Es sind die spezifizierten Eigenschaften des Systems zu überprüfen, insbesondere

- a) die Einhaltung des spezifizierten Zeitverhaltens, z. B. Verzögerungs- und Totzeiten,
- b) die Einhaltung der spezifizierten Auslastungswerte, z. B. CPU, Netzwerk,
- c) das spezifizierte Fehler- und Wiederanlaufverhalten und
- d) die Wirksamkeit der Zugriffsschutzmaßnahmen.

(5) Bereits als Prüfungen im Testfeld durchgeführte Verdrahtungs- und Funktionsprüfungen an Systemteilen sowie durchgeführte integrale Systemprüfungen brauchen am endgültigen Aufstellungsort nicht wiederholt zu werden, wenn

- a) Umfang und Dokumentation der Prüfungen den Anforderungen nach 4.1 genügen,
- b) sich durch den Transport, die Montage und die Integration der leittechnischen Einrichtungen auf der Anlage keine Rückwirkungen auf die bereits überprüften Eigenschaften und das Verhalten von Leittechniksystemen ergeben,
- c) bei Änderungen überlappende Prüfungen nach 4.7 durchgeführt wurden.

**Hinweis:**

Werkprüfungen sind in KTA 3507 geregelt.

#### 4.1.4 Inbetriebsetzungsprogramm

Vor Beginn der Prüfungen ohne Betrieb der verfahrenstechnischen Systeme muss ein Inbetriebsetzungsprogramm erstellt und mit dem Sachverständigen abgestimmt werden. Dieses Inbetriebsetzungsprogramm muss die zu prüfenden Systeme oder Systemteile, die durchzuführenden Prüfungen, die zugehörigen Inbetriebsetzungsprüfanweisungen sowie die Beteiligung von Sachverständigen angeben. Dieses Inbetriebsetzungsprogramm darf mit den Inbetriebsetzungsprogrammen für die Prüfungen elektrotechnischer und verfahrenstechnischer Systeme in gemeinsamen Inbetriebsetzungsprogrammen zusammengefasst werden.

#### 4.1.5 Inbetriebsetzungsprüfanweisungen

(1) Vor Beginn der Prüfungen ohne Betrieb der verfahrenstechnischen Systeme müssen für den zu prüfenden Teil der Sicherheitsleittechnik Inbetriebsetzungsprüfanweisungen erstellt und mit dem Sachverständigen abgestimmt werden.

(2) Eine Inbetriebsetzungsprüfanweisung besteht aus einer Vorgangsbeschreibung und aus Prüfprotokoll-Formblättern.

(3) Die Vorgangsbeschreibung muss enthalten:

- a) eine Bezeichnung einschließlich Änderungsstand, die eine Zuordnung der Vorgangsbeschreibung zum Inbetriebsetzungsprogramm sicherstellt,
- b) eine Beschreibung des Prüfverfahrens, in der das Prüfverfahren und der Arbeitsablauf der Prüfungsdurchführung festgelegt und der messtechnische Prüfaufbau unter Verwendung einer Schaltskizze dargestellt sind (die Angaben zum Prüfaufbau dürfen bei einfachen Messaufbauten entfallen),
- c) die Prüfkriterien für die Sichtprüfungen nach 4.1.2,
- d) die Unterlagen, die der Prüfung zugrunde liegen und
- e) die zu verwendenden Prüfhilfsmittel mit Angabe der erforderlichen technischen Daten.

(4) Das Prüfprotokoll-Formblatt muss enthalten:

- a) den Prüfgegenstand mit Angabe des Einbau- oder Prüfortes und des alphanumerischen Anlagenkennzeichens,
- b) die Angabe der zugehörigen Vorgangsbeschreibung,

c) die Auflistung der Prüfungen in zu dokumentierenden Einzelprüfschritten und

d) die zu erfassenden Messgrößen mit Sollwerten und zulässigen Abweichungen.

(5) Im Verlauf der Prüfungen sind in die Prüfprotokoll-Formblätter folgende Informationen einzutragen:

- a) die Angabe der verwendeten Prüfgeräte mit Gerätenummer,
- b) der Stand der Konfigurations-Identifikations-Dokumentation,
- c) die Prüfergebnisse der Einzelprüfschritte,
- d) die eingestellten Werte und
- e) die Bestätigung des Prüferfolges nach Beseitigung aller Mängel durch Unterschrift der Prüfer mit Prüfdatum, bei Teilnahme des Sachverständigen) auch dessen Unterschrift.

**Hinweis:**

Durch die Eintragungen wird das Prüfprotokoll-Formblatt zum Prüfprotokoll.

## 4.2 Prüfungen des Zusammenwirkens mit den verfahrenstechnischen Systemen

### 4.2.1 Allgemeine Anforderungen

(1) Die Prüfungen des Zusammenwirkens mit den verfahrenstechnischen Systemen müssen während der verfahrenstechnischen Systeminbetriebsetzung erfolgen. Entsprechend den erreichten Betriebszuständen sind die Inbetriebsetzungsprüfungen der leittechnischen Einrichtungen im Zusammenwirken mit den verfahrenstechnischen Systemen durchzuführen. Dabei ist zu prüfen, ob die leittechnischen Einrichtungen bei den auftretenden Betriebsbedingungen den in den gültigen Unterlagen spezifizierten Anforderungen genügen.

(2) Die von der Sicherheitsleittechnik einzuleitenden Maßnahmen müssen durch verfahrenstechnische Anregung oder - wo dies eine unverhältnismäßig hohe Belastung der Anlage ergeben würde - durch Simulation der Anregung geprüft werden.

(3) Werden bei den Prüfungen Maßnahmen ausgelöst, die für die Anlage eine unverhältnismäßig hohe Belastung ergeben würden, sind in Hinblick auf das Prüfziel die Belastungen für die Anlage in Abstimmung mit der Verfahrenstechnik zu minimieren.

(4) Die Prüfungen sollen unter den Betriebsbedingungen im nichtnuklearen Betrieb (unterkritische Betriebsphasen) durchgeführt werden. Prüfungen, die den nuklearen Betrieb der Anlage voraussetzen, dürfen bei den zur Erreichung der Prüfziele erforderlichen Betriebsphasen durchgeführt werden, wenn dies sicherheitstechnisch zulässig ist.

### 4.2.2 Voraussetzungen für die Durchführung der Prüfung

(1) Die Prüfung ohne Betrieb der verfahrenstechnischen Systeme der zu prüfenden Teile der Sicherheitsleittechnik muss abgeschlossen sein. Hierzu sollen folgende Unterlagen, die den aktuellen Anlagenzustand dokumentieren, vorliegen:

- a) Übersichtspläne (z. B. Grenzsignalverarbeitungsplan, Logikplan),
- b) Funktionspläne (z. B. Verriegelungsplan),
- c) Stromlaufpläne,
- d) Messkennblätter und
- e) Liste der gültigen Einstellwerte.

(2) Die einzelnen Prüfungen des Zusammenwirkens mit den verfahrenstechnischen Systemen dürfen erst dann vorge-

nommen werden, wenn die dazu benötigten verfahrenstechnischen Systeme oder Teilsysteme funktionsfähig sind.

(3) Vor Beginn der Prüfungen des Zusammenwirkens mit den verfahrenstechnischen Systemen müssen ein Inbetriebsetzungsprogramm und Inbetriebsetzungsprüfanweisungen erstellt und mit dem Sachverständigen abgestimmt werden.

#### 4.2.3 Inbetriebsetzungsprogramm

Im Inbetriebsetzungsprogramm nach 4.1.4. sind die Prüfungen des Zusammenwirkens mit den verfahrenstechnischen Systemen aufzuführen. Dieses Inbetriebsetzungsprogramm muss die zu prüfenden Systeme oder Systemteile, die durchzuführenden Prüfungen, die zugehörigen Inbetriebsetzungsprüfanweisungen sowie die Beteiligung von Sachverständigen angeben. Dieses Inbetriebsetzungsprogramm soll mit den Inbetriebsetzungsprogrammen für die Prüfungen elektrotechnischer und verfahrenstechnischer Systeme in gemeinsamen Inbetriebsetzungsprogrammen zusammengefasst werden.

#### 4.2.4 Inbetriebsetzungsprüfanweisungen

(1) Eine Inbetriebsetzungsprüfanweisung besteht aus einer Vorgangsbeschreibung und Prüfprotokoll-Formblättern.

(2) Die Vorgangsbeschreibung muss enthalten:

- a) eine Bezeichnung einschließlich Änderungsstand, die eine Zuordnung der Vorgangsbeschreibung zum Inbetriebsetzungsprogramm sicherstellt,
- b) der Stand der Konfigurations-Identifikations-Dokumentation,
- c) eine Beschreibung des Prüfverfahrens und des Arbeitsablaufs der Prüfungsdurchführung,
- d) die Prüfbedingungen (z. B. Anlagen- und Systemzustand),
- e) die Unterlagen, die der Prüfung zugrunde liegen und
- f) die zusätzlich zur Anlageninstrumentierung zu verwendenden Prüfhilfsmittel mit Angabe der erforderlichen technischen Daten.

(3) Das Prüfprotokoll-Formblatt muss enthalten:

- a) den Prüfgegenstand mit Angabe des Einbau- oder Prüfortes und des alphanumerischen Anlagenkennzeichens,
- b) die Angabe der zugehörigen Vorgangsbeschreibung,
- c) die Auflistung der Prüfungen in zu dokumentierenden Einzelprüfschritten und
- d) die zu erfassenden Messgrößen mit Anlagenkennzeichen.

(4) Im Verlaufe der Prüfung sind in die Prüfprotokoll-Formblätter folgende Informationen einzutragen:

- a) die Angabe der zusätzlich zur Anlageninstrumentierung verwendeten Prüfgeräte mit Gerätenummer,
- b) die Prüfergebnisse der Einzelprüfschritte,
- c) die verfahrenstechnische Bewertung der Prüfergebnisse und
- d) die Bestätigung des Prüferfolges nach Beseitigung aller Mängel durch Unterschrift der Prüfer mit Prüfdatum, bei Teilnahme des Sachverständigen auch dessen Unterschrift.

Hinweis:

Durch die Eintragungen wird das Prüfprotokoll-Formblatt zum Prüfprotokoll.

#### 4.3 Anforderungen an Prüfhilfsmittel

Die Inbetriebsetzungsprüfungen sind mit den in der Inbetriebsetzungsprüfanweisung festgelegten Prüfhilfsmitteln durchzuführen. Die zusätzlich zur Anlageninstrumentierung verwendeten Prüfhilfsmittel müssen einem Wartungs- und Kalibrier-

dienst nach KTA 1401 Abschnitt 10 unterliegen. Die durchgeführte Überprüfung und der Zeitpunkt der nächsten Überprüfung müssen am Prüfhilfsmittel oder in einer das Prüfhilfsmittel begleitenden Dokumentation erkennbar sein. Die bei den Prüfungen im Testfeld oder bei den Inbetriebsetzungsprüfungen auf der Anlage verwendeten Simulatoren und Simulationsmodelle sind zu beschreiben. Die Eignung der Simulatoren und Simulationsmodelle ist nachzuweisen.

#### 4.4 Prüfer

Die Inbetriebsetzungsprüfungen sind durch das vom Antragsteller bestimmte fachkundige Personal durchzuführen. Soweit das Inbetriebsetzungsprogramm dies vorsieht, sind Sachverständige zur Prüfung hinzuzuziehen.

#### 4.5 Dokumentation

Zur Dokumentation der Inbetriebsetzungsprüfungen gehören:

- a) Inbetriebsetzungsprogramm,
- b) Inbetriebsetzungsprüfanweisungen und
- c) Inbetriebsetzungsprüfprotokolle.

Diese Unterlagen müssen während der Einsatzdauer des geprüften Teils der Sicherheitsleittechnik vom Betreiber aufbewahrt werden.

#### 4.6 Prüfungen nach Instandsetzung

Werden im Verlauf oder nach Abschluss einer Inbetriebsetzungsprüfung Instandsetzungsarbeiten durchgeführt, so sind die davon betroffenen Teilbereiche der Sicherheitsleittechnik nach den in 4.1.5 und 4.2.4 genannten Inbetriebsetzungsprüfanweisungen überlappend erneut zu prüfen. Die Prüfungen sind zu dokumentieren.

#### 4.7 Prüfungen nach Systemänderungen

##### 4.7.1 Allgemeines

Werden im Verlauf oder nach Abschluss einer Inbetriebsetzungsprüfung Änderungen der Leittechnik oder andere Änderungen mit Auswirkungen auf die Sicherheitsleittechnik als notwendig erkannt, so sind nach Durchführung der Maßnahmen und nach Änderung der Prüfunterlagen die davon betroffenen Teilbereiche der Sicherheitsleittechnik nach den in 4.1.5 und 4.2.4 genannten Inbetriebsetzungsprüfanweisungen überlappend erneut zu prüfen. Die Änderungen und der Prüfumfang sind mit dem Sachverständigen abzustimmen. Die Prüfungen sind nach 4.5 zu dokumentieren.

##### 4.7.2 Softwareänderungen

Bei digitalen softwarebasierten Sicherheitsleittechniksystemen sind die im Rahmen von Instandsetzungsarbeiten oder Systemänderungen ergänzend durchzuführenden qualitätssichernden Maßnahmen in Qualitätssicherungsanweisungen zu beschreiben. In diesen Anweisungen sind die Anforderungen und die Verfahrensschritte bei der Projektierung, Implementierung, Verifizierung und Validierung sowie bei der Dokumentation und Protokollierung von Instandsetzungsarbeiten oder Systemänderungen festzulegen.

##### 4.7.2.1 Softwareänderungen an Einrichtungen, die Leittechnikfunktionen der Kategorie A ausführen

(1) Die Änderung der Software ist zu spezifizieren. Die Prozedur zur Durchführung der Änderung soll dem Phasenmodell folgen, das dem Software-Entwicklungsprozess zugrunde liegt. Der Umfang und die Auswirkung einer Softwareänderung sind zu identifizieren. Alle Phasen des Software-

Entwicklungsprozesses sind daraufhin zu überprüfen, ob sie von der Änderung betroffen sind. Die betroffenen Phasen sind zu wiederholen.

(2) Die Änderung der Software hat so zu erfolgen, dass eine durchgängige Nachweisführung der korrekten Arbeitsweise der Software gewährleistet ist. Entwurf und Implementierung sind mit formalisierten und rechnergestützten Konstruktions- und Prüfmethoden durchzuführen. Die Änderung ist durchgängig mit rechnergestützten Werkzeugen durchzuführen.

(3) Die Ergebnisse der einzelnen Phasen der Softwareänderung sind unter Anwendung formaler Analysemethoden und zusätzlicher Tests an den Vorgaben vollständig zu verifizieren. Dazu sind an den Phasenübergängen Prüfungen vorzunehmen und die Ergebnisse zu dokumentieren.

(4) Nach Installation der geänderten Software auf den Rechnern ist das anforderungsgerechte Verhalten des Hardware- und Softwaresystems zu validieren. Wird die Validierung in mehreren Schritten durchgeführt, so sind die einzelnen Validierungsschritte überlappend durchzuführen.

(5) Durch die Organisation und Administration bei der Softwareänderung ist sicherzustellen, dass die Software nach vollständigen Entwicklungs-, Prüf-, Wartungs- und Qualitätssicherungsplänen erstellt wird. Die Unabhängigkeit zwischen Projektierung und Qualitätssicherung ist durchgehend zu gewährleisten.

(6) Die Korrektheit und Wirksamkeit der Änderung ist nachzuweisen. Hierbei ist insbesondere nachzuweisen, dass die erforderliche Funktion ausgeführt wird und keine unzulässigen Auswirkungen (Auswirkungsanalyse) durch die Änderung in den nicht geänderten Systemteilen sowie in anderen Systemen bestehen. In Abhängigkeit von Art und Umfang der Änderung darf für die Nachweisführung auch eine Testkonfiguration eingesetzt werden.

(7) Das anforderungsgerechte Verhalten des geänderten Hardware- und Softwaresystems ist zu validieren.

(8) Änderungen der Systemsoftware, Firmware oder Betriebssystemsoftware sind wie Geräteänderungen zu behandeln.

#### 4.7.2.2 Softwareänderungen an Einrichtungen, die Leittechnikfunktionen der Kategorie B ausführen

(1) Softwareänderungen sind in Übereinstimmung mit den Anforderungen nach 4.7.2.1, (1), (5), (6), (7) und (8) durchzuführen.

(2) Der Nachweis der korrekten Arbeitsweise soll mit rechnergestützten Testverfahren unterstützt werden. Art und Umfang des Nachweisverfahrens ist mit dem Sachverständigen abzustimmen.

(3) Die Softwareänderung soll mit rechnergestützten Werkzeugen erfolgen.

#### 4.7.2.3 Softwareänderungen an Einrichtungen, die Leittechnikfunktionen der Kategorie C ausführen

(1) Softwareänderungen sind zu beschreiben und die Änderungsschritte sind einzeln auszuweisen. Bei Änderungsschritten sollten Softwareentwicklungswerkzeuge eingesetzt werden.

(2) Der Abschluss der Änderungsschritte ist durch Prüfungen nachzuweisen und zu dokumentieren.

(3) Das anforderungsgerechte Verhalten des geänderten Hardware- und Softwaresystems ist in seinen sicherheitsrelevanten Funktionen zu validieren. Art und Umfang der Validie-

rungen sind mit dem Sachverständigen abzustimmen. Die Software ist nach einem Qualitätssicherungsplan zu erstellen.

## 5 Wiederkehrende Prüfungen der Sicherheitsleittechnik

### 5.1 Allgemeine Anforderungen

(1) Die A-Funktionseinrichtungen und B-Funktionseinrichtungen sind zum Nachweis ihrer vorgesehenen Funktion in festzulegenden Zeitabständen während der gesamten Nutzungsdauer der Anlage wiederkehrend zu prüfen.

(2) Auf wiederkehrende Prüfungen darf in den Teilbereichen verzichtet werden, die durch Selbstüberwachung geprüft werden. Die herangezogenen Selbstüberwachungsfunktionen sind zu beschreiben und müssen folgende Anforderungen erfüllen:

- a) Im Rahmen einer Analyse ist zu ermitteln, welche zu unterstellenden Ausfallarten durch die vorhandenen Selbstüberwachungsfunktionen aufgedeckt werden.
- b) Die Wirksamkeit der verwendeten Selbstüberwachungsfunktionen ist im Rahmen der Qualifizierung der Komponenten der leittechnischen Einrichtungen (systemimmanent) bzw. im Rahmen der Inbetriebsetzung (projektiert) zu überprüfen.
- c) Die von den Selbstüberwachungsfunktionen festgestellten Fehler sind durch Gefahrenmeldungen der Klasse I oder in der Qualität gleichwertiger Meldungen und Anzeigen zu signalisieren.

(3) Prüfungen dürfen die von Sicherheitsleittechnik der Kategorie A und B einzuleitenden Maßnahmen nicht so beeinträchtigen, dass die Wirksamkeit der Sicherheitsleittechnik unzulässig vermindert wird.

(4) Die Prüfungen sollen mittels Prüfhilfen (z. B. Prüfadapter, Prüfbuchsen) einfach und ohne Eingriff in die Verdrahtung durchführbar sein.

(5) Die erste wiederkehrende Prüfung der Sicherheitsleittechnik der Kategorie A und B ist grundsätzlich vor der ersten Kritikalität der Anlage durchzuführen. Systeme, die zum Beladen des Kerns benötigt werden, sind vor dem Beladen zu prüfen. Falls wiederkehrende Prüfungen vor der ersten Kritikalität anlagentechnisch nicht möglich sind, dürfen diese Prüfungen bis zu den Inbetriebsetzungsversuchen in der 100 %-Leistungsphase nachgeholt werden, wenn dies sicherheitstechnisch zulässig ist. Ist dies nicht zulässig, so sind für die jeweiligen Prüfungen Ersatzprüfungen durchzuführen, die im Einzelfall mit dem Sachverständigen abzustimmen sind.

(6) Teile der Inbetriebsetzungsprüfung nach Abschnitt 3 dürfen als erste wiederkehrende Prüfung gewertet werden, wenn die folgenden Kriterien erfüllt sind:

- a) Die Prüfanweisung, einschließlich der verwendeten Prüfhilfen und Prüfschritte, muss mit der Prüfanweisung der wiederkehrenden Prüfung identisch sein.
- b) Der Zeitraum seit der durchgeführten Inbetriebsetzungsprüfung darf nicht größer sein als das festgelegte Prüfintervall für die wiederkehrende Prüfung.
- c) Die Prüfanweisung nach 5.5 muss zum Zeitpunkt der Anerkennung der Inbetriebsetzungsprüfung als erste wiederkehrende Prüfung vorliegen.
- d) Es dürfen keine Montage- oder Änderungsarbeiten durchgeführt worden sein, die eine Beeinträchtigung der geprüften Sicherheitsleittechnik zur Folge gehabt haben können.

(7) Der Umfang der wiederkehrenden Prüfung für Funktionen der Kategorie C ist funktionspezifisch festzulegen.

## 5.2 Voraussetzung für die Durchführung der Prüfung

(1) Vor Beginn der wiederkehrenden Prüfungen der Sicherheitsleittechnik müssen eine Prüfliste und Prüfanweisungen erstellt und mit dem Sachverständigen abgestimmt werden.

(2) Die Anlage muss in einen Zustand gebracht werden, der eine Prüfung der Sicherheitsleittechnik in der durch die Prüfanweisung vorgegebenen Weise gestattet.

(3) Dabei ist zu beachten, dass die im Betriebshandbuch für den sicheren Reaktorbetrieb festgelegte Mindestzahl verfügbarer leittechnischer und verfahrenstechnischer Teilsysteme bei der Prüfung nicht unterschritten werden darf.

## 5.3 Prüfindervalle

(1) Die Prüfindervalle für wiederkehrende Prüfungen der Sicherheitsleittechnik sind aufgrund von Betriebserfahrungen oder Zuverlässigkeitsanalysen in Abstimmung mit dem Sachverständigen festzulegen. Anhand der Prüfindervalle sind die regelmäßigen Prüftermine und die zulässigen Abweichungen von den Prüfterminen festzulegen.

(2) Prüfungen an Systemen, die aufgrund des Anlagenzustandes nicht einsatzbereit sein müssen, dürfen ausgesetzt werden. Aufgrund dessen dürfen neue regelmäßige Prüftermine festgelegt werden. Für ausgesetzte Prüfungen ist vor oder während des Wiederanfahrens des Systems oder der Anlage eine wiederkehrende Prüfung durchzuführen.

## 5.4 Prüfliste

(1) In der Prüfliste nach 5.2 (1) sind die wiederkehrenden Prüfungen der Sicherheitsleittechnik aufzuführen. Die Prüfliste muss die zu prüfenden Systeme oder Systemteile, die durchzuführenden Prüfungen mit den jeweiligen Prüfindervallen, den Anlagenzustand, die zugehörigen Prüfanweisungen sowie die Beteiligung von Sachverständigen angeben.

Hinweis:

Anforderungen an die Prüfliste sind in KTA 1202 geregelt.

(2) Aufgrund von Prüfergebnissen und Betriebserfahrungen sind in Abstimmung mit dem Sachverständigen die Prüfliste und die Prüfanweisungen zu aktualisieren.

## 5.5 Prüfanweisungen

(1) Eine Prüfanweisung besteht aus einer Vorgangsbeschreibung und Prüfprotokoll-Formblättern.

(2) Die Vorgangsbeschreibung muss enthalten:

- eine Bezeichnung einschließlich Änderungsstand, die eine Zuordnung der Vorgangsbeschreibung zur Prüfliste sicherstellt,
- eine Beschreibung des Prüfverfahrens, in der das Prüfverfahren und der Arbeitsablauf der Prüfung festgelegt und grundsätzlich der messtechnische Prüfungsaufbau unter Verwendung einer Schaltskizze dargestellt sind (die Angaben zum Prüfungsaufbau dürfen bei einfachen Messaufbauten entfallen),
- die Prüfbedingungen oder Prüfvoraussetzungen (z. B. Anlagen- und Systemzustand) und
- die Art der zusätzlich zur Anlageninstrumentierung zu verwendenden Prüfhilfsmittel mit Angabe der erforderlichen technischen Daten.

(3) Das Prüfprotokoll-Formblatt muss enthalten:

- den Prüfgegenstand mit Angabe des Einbau- oder Prüfortes und des alphanumerischen Anlagenkennzeichens,
- die Angabe der zugehörigen Vorgangsbeschreibung,

c) die Auflistung der Prüfungen in zu dokumentierenden Einzelprüfschritten,

d) die Angabe der Simulationsmaßnahmen und

e) die zu erfassenden Messgrößen mit alphanumerischen Anlagenkennzeichen, Sollwerten und zulässigen Abweichungen.

(4) Im Verlauf der Prüfung sind in den Prüfprotokoll-Formblättern folgende Informationen zu erfassen:

- die Angabe der zusätzlich zur Anlageninstrumentierung verwendeten Prüfgeräte mit Gerätenummer,
- die Prüfergebnisse der Einzelprüfschritte,
- die vorgefundenen und neu eingestellten Werte,
- die Angabe von Mängeln und der zur Abhilfe eingeleiteten Maßnahmen,
- die Bestätigung der Schaffung und der Aufhebung des Simulationszustands,
- die Gründe bei Abweichungen von der Prüfanweisung,
- die Bewertung der Prüfergebnisse und
- die Unterschrift der Prüfer mit Prüfdatum, bei Teilnahme des Sachverständigen auch dessen Unterschrift.

Hinweis:

Durch die Eintragungen wird das Prüfprotokoll-Formblatt zum Prüfprotokoll.

## 5.6 Anforderungen an Prüfhilfsmittel

Die Prüfung ist mit den in der Prüfanweisung festgelegten Prüfhilfsmitteln durchzuführen. Die zusätzlich zur Anlageninstrumentierung verwendeten Prüfhilfsmittel müssen einem Wartungs- und Kalibrierdienst nach KTA 1401 Abschnitt 10 unterliegen. Die durchgeführte Überprüfung und der Zeitpunkt der nächsten Überprüfung müssen am Prüfhilfsmittel oder in einer das Prüfhilfsmittel begleitenden Dokumentation erkennbar sein. Durch Prüfhilfsmittel gesteuerte Prüfabläufe sind so zu gestalten, dass die vorgesehene Ausführung der Prüfabläufe im Prüfprotokoll dokumentiert wird. Es soll erkennbar sein, dass programmgesteuerte Prüfabläufe vollständig ausgeführt werden. Der Versionsstand der Prüfsoftware ist zu dokumentieren.

## 5.7 Prüfer

Die wiederkehrenden Prüfungen sind durch das vom Genehmigungsinhaber bestimmte fachkundige Personal durchzuführen. Soweit die Prüfliste dies vorsieht, sind Sachverständige zur Prüfung hinzuzuziehen.

## 5.8 Dokumentation

Zur Dokumentation der wiederkehrenden Prüfungen gehören:

- Prüfliste,
- Vorgangsbeschreibungen und
- Prüfprotokolle.

Diese Unterlagen müssen während der Einsatzdauer des geprüften Teils der Sicherheitsleittechnik vom Betreiber aufbewahrt werden.

## 5.9 Prüfungen nach Instandsetzung

Werden im Verlauf oder nach Abschluss einer wiederkehrenden Prüfung Instandsetzungsarbeiten durchgeführt, so sind die davon betroffenen Teilbereiche der Sicherheitsleittechnik nach den Prüfanweisungen der Inbetriebsetzungsprüfungen nach 4.1 und der wiederkehrenden Prüfungen überlappend erneut zu prüfen. Die Prüfungen sind nach 5.8 zu dokumentieren.

### **5.10** Prüfungen nach Freischaltungen und Simulationen

Werden Freischaltungen und Simulationen in Teilen der Sicherheitsleittechnik vorgenommen, deren Bestehenbleiben die Funktion der Sicherheitsleittechnik beeinträchtigen können, so ist der betroffene Teilbereich nach Aufhebung dieser Maßnahmen überlappend zu prüfen. Die Prüfungen sind nach 5.8 zu dokumentieren.

### **5.11** Prüfungen nach Systemänderungen

Sind Systemänderungen oder andere Änderungen mit Einfluss auf die Sicherheitsleittechnik erforderlich, so sind nach Durchführung der Maßnahmen und nach Änderung der Prüfunterlagen die davon betroffenen Teilbereiche der Sicherheitsleittechnik nach den Prüfanweisungen der Inbetriebsetzungs- und der wiederkehrenden Prüfungen überlappend erneut zu prüfen. Die Änderungen und der Prüfumfang sind mit dem Sachverständigen abzustimmen. Prüfungen sind nach 4.5 und 5.8 zu dokumentieren.

## Anhang A

### Bestimmungen, auf die in dieser Regel verwiesen wird

(Die Verweise beziehen sich nur auf die in diesem Anhang angegebene Fassung. Darin enthaltene Zitate von Bestimmungen beziehen sich jeweils auf die Fassung, die vorlag, als die verweisende Bestimmung aufgestellt oder ausgegeben wurde.)

AtG		Gesetz über die friedliche Verwendung der Kernenergie und den Schutz gegen ihre Gefahren (Atomgesetz – AtG) in der Fassung der Bekanntmachung vom 15. Juli 1985 (BGBl. I S. 1565), das durch Artikel 1 des Gesetzes vom 31. Juli 2011 (BGBl. I S. 1704) geändert worden ist
StrlSchV		Verordnung über den Schutz vor Schäden durch ionisierende Strahlen (Strahlenschutzverordnung – StrlSchV) vom 20. Juli 2001 (BGBl. I S. 1714; 2002 I S. 1459), die zuletzt durch Artikel 1 der Verordnung vom 4. Oktober 2011 (BGBl. I S. 2000) geändert worden ist
Sicherheitskriterien	(1977-10)	Sicherheitskriterien für Kernkraftwerke vom 21. Oktober 1977 (BAnz. Nr. 206 vom 3. November 1977)
Störfall-Leitlinien	(1983-10)	Leitlinien zur Beurteilung der Auslegung von Kernkraftwerken mit Druckwasserreaktoren gegen Störfälle im Sinne des § 28 Abs. 3 StrlSchV (Störfall-Leitlinien) vom 18. Oktober 1983 (Beilage zum BAnz. Nr. 245 vom 31. Dezember 1983)
RSK-Leitlinien	(1981-10)	RSK-Leitlinien für Druckwasserreaktoren; 3. Ausgabe vom 14. Oktober 1981 (Banz 1982, Nr. 69a) mit den Änderungen: in Abschn. 21.1 (BAnz 1984, Nr. 104), in Abschn. 21.2 (BAnz 1983, Nr. 106) und in Abschn. 7 (BAnz 1996, Nr. 158a) mit Berichtigung (BAnz 1996, Nr. 214)
KTA 1202	(2009-11)	Anforderungen an das Prüfhandbuch
KTA 1401	(1996-06)	Allgemeine Anforderungen an die Qualitätssicherung
KTA 1402, RE	(2011-11)	Managementsystem zur Betriebsführung von kerntechnischen Anlagen
KTA 1403	(2010-11)	Alterungsmanagement in Kernkraftwerken
KTA 1404	(2001-06)	Dokumentation beim Bau und Betrieb von Kernkraftwerken
KTA 3403	(1976-11)	Kabeldurchführungen im Reaktorsicherheitsbehälter von Kernkraftwerken
KTA 3501	(1985-06)	Reaktorschutzsystem und Überwachungseinrichtungen des Sicherheitssystems
KTA 3503	(2005-11)	Typprüfung von elektrischen Baugruppen der Sicherheitsleittechnik
KTA 3504	(2006-11)	Elektrische Antriebe des Sicherheitssystems in Kernkraftwerken
KTA 3505	(2005-11)	Typprüfung von Messwertgebern und Messumformern der Sicherheitsleittechnik
KTA 3507	(2002-06)	Werksprüfungen, Prüfungen nach Instandsetzung und Nachweis der Betriebsbewährung
KTA 3701	(1999-06)	Übergeordnete Anforderungen an die elektrische Energieversorgung in Kernkraftwerken
KTA 3702	(2000-06)	Notstromerzeugungsanlagen mit Dieselaggregaten in Kernkraftwerken
KTA 3703	(1999-06)	Notstromerzeugungsanlagen mit Batterien und Gleichrichtergeräten in Kernkraftwerken
KTA 3704	(1999-06)	Notstromanlagen mit Gleichstrom-Wechselstrom-Umformern in Kernkraftwerken
KTA 3705	(2006-11)	Schaltanlagen, Transformatoren und Verteilungsnetze zur elektrischen Energieversorgung
KTA 3904	(2007-11)	Warte, Notsteuerstelle und örtliche Leitstände in Kernkraftwerken

## Anhang B (informativ)

### Begriffe, die in dieser Regel verwendet werden

Nachstehende Begriffe sind an die RSK-Leitlinien angelehnt und werden in dieser Regel zu Grunde gelegt. Endgültig werden diese Begriffe in der überarbeiteten Fassung der KTA 3501 definiert.

#### Sicherheitsleittechnik

Die Sicherheitsleittechnik ist die Leittechnik des Sicherheitssystems und der anderen Systeme mit sicherheitstechnischer Bedeutung. Die Sicherheitsleittechnik umfasst die Leittechnik-Funktionen der Kategorien A, B und C. Sie wird durch Einrichtungen realisiert, bei denen Geräte Leittechnik-Funktionen ausführen (vgl. RSK-Leitlinien Abschnitt 7.3.1).

Hinweis:

Dazu gehören:

- a) Reaktorschutzsystem,
- b) Schutzbegrenzungen,
- c) Zustandsbegrenzungen,
- d) Sicherheitstechnisch wichtige Regel- und Steuereinrichtungen,
- e) Steuerebene für sicherheitstechnisch wichtige Antriebe,
- f) Gefahrenmeldungen der Klasse S und
- g) Gefahrenmeldungen der Klasse I.

#### Kategorisierung

Die Einrichtungen der Sicherheitsleittechnik führen Leittechnik-Funktionen unterschiedlicher sicherheitstechnischer Bedeutung aus. Entsprechend ihrer sicherheitstechnischen Bedeutung sind die Leittechnik-Funktionen in unterschiedliche Kategorien einzuordnen, für die abgestufte Sicherheitsanforderungen gelten:

##### a) Kategorie A

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

##### b) Kategorie B

Die Leittechnik-Funktionen der Kategorie B umfassen alle Funktionen, die erforderlich sind, um die Ausweitung einer Störung zu einem Störfall zu verhindern.

##### c) Kategorie C

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

(vgl. RSK-Leitlinien Abschnitt 7.3.2, wobei die Kategorien A / B / C den Kategorien 1 / 2 / 3 der RSK-Leitlinien entsprechen)

## Dokumentationsunterlage zur Regeländerung

### KTA 3506

## Systemprüfung der Sicherheitsleittechnik von Kernkraftwerken

Bisheriger Titel:

„Systemprüfung der leittechnischen Einrichtungen des Sicherheitssystems von Kernkraftwerken“

### Inhalt

- 1 Auftrag des KTA
- 2 Beteiligte Personen
- 3 Verlauf des Regeländerungsverfahrens
- 4 Berücksichtigte Unterlagen
- 5 Erläuterungen der vorgenommenen Änderungen

### 1 Auftrag des KTA

#### 1.1 Vorbemerkung

Aufgrund der nach Abschnitt 5.2 der Verfahrensordnung des KTA nach längstens 5 Jahren erforderlichen Überprüfung auf Änderungsbedürftigkeit hat der Unterausschuss ELEKTRO- UND LEITTECHNIK (UA-EL) auf seiner 58. Sitzung am 26. April 2005 über die Regel KTA 3506 beraten.

Der UA-EL stellt fest, dass die Regel zeitlich parallel zu den Arbeiten an der KTA 3501 an den aktuellen Stand von Wissenschaft und Technik angepasst werden muss. Der Anpassungsbedarf betrifft insbesondere die Systemaspekte im Zusammenhang mit den Ergänzungen zur digitalen Leittechnik in der KTA 3501.

#### 1.2 Beschlüsse

Der Kerntechnische Ausschuss fasste auf seiner 59. Sitzung am 22. November 2005 die folgenden Beschlüsse:

#### **Beschluss-Nr.: 59/8.2.3/1 vom 22.11.2005**

Der Unterausschusses ELEKTRO- UND LEITTECHNIK (UA-EL) wird beauftragt, federführend den Entwurf zur Änderung der Regel

**KTA 3506** Systemprüfung der leittechnischen Einrichtungen des Sicherheitssystems in Kernkraftwerken  
(Fassung 11/84)

mit einer Dokumentationsunterlage durch ein Arbeitsgremium erarbeiten zu lassen.

#### **Beschluss-Nr.: 59/8.2.3/2 vom 22.11.2005**

Der Unterausschusses ELEKTRO- UND LEITTECHNIK (UA-EL) wird beauftragt, den Entwurfsvorschlag zur Änderung der Regel KTA 3506 zu prüfen und eine Beschlussvorlage für den KTA zu erarbeiten.

Die Geschäftsstelle wird beauftragt, diesen Beschluss zur Regel KTA 3506 dem Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit zur Veröffentlichung im BAnz. zuzuleiten.

### 2 Beteiligte Personen

#### 2.1 Zusammensetzung des KTA-Unterausschusses ELEKTRO- und LEITTECHNIK (UA-EL)

Obmann: Dipl.-Ing. R.-D. Junge, TÜV NORD ,Hannover, bis Nov. 2010

GDir M. Hagmann; UVM-BW, Stuttgart, ab Dez. 2010

Vertreter der Hersteller und Ersteller von Atomanlagen:

Dipl.-Ing. W. Schulze	AREVA NP GmbH, Erlangen (Stellvertreter: Dr. Graf, AREVA NP GmbH , Erlangen) Dr. B. Möller, Areva NP GmbH, Erlangen, ab Dez. 2010)
Dipl.-Ing. R. Zahout	AREVA NP GmbH, Erlangen (Stellvertreter: Dipl.-Ing. L. Warnken, AREVA NP GmbH, Erlangen bis Nov.2007, Dr. P. Waber, AREVA NP GmbH, Erlangen ab Dez.2007)
Dipl.-Ing. M. Friedl	AREVA NP GmbH, Erlangen ab Dez. 2008 (Stellvertreter: Dr. Waedt, AREVA NP GmbH , Erlangen, ab Dez. 2008)

Vertreter der Betreiber von Atomanlagen:

Dipl.-Ing. K.-H. Herbers	RWE Power AG, Kernkraftwerk Emsland (Stellvertreter: Dr. Höke, E.ON Kernkraft GmbH, Hannover, bis Nov. 2007, Dr. Planitz, Vattenfall Europe Nuclear Energy GmbH, Hamburg, ab Dez. 2007)
--------------------------	--

Dipl.-Ing. J. Irlbeck	E.ON Kernkraft GmbH, Essenbach, bis Nov. 2008 (Stellvertreter: Dipl.-Ing. H. Heinrich, Kernkraftwerk Obrigheim GmbH, bis Nov. 2007, Dipl.-Ing. V. Fischer, EnBW Kraftwerke GmbH, ab Dez. 2007)
-----------------------	---

Dipl.-Ing. M. Bresler	E.ON Kernkraft GmbH, Hannover, ab Dez. 2008 (Stellvertreter: Dipl.-Ing. V. Fischer, EnBW Kraftwerke GmbH)
-----------------------	--

Vertreter des Bundes und der Länder:

Regierungsdirektor Dr. Thinnies	Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit, Bonn, bis Nov. 2006 (Stellvertreter: Oberregierungsrat P. Sperling, Bonn, BMU; Wissenschaftlicher Oberrat Dr. F. Seidel, Bundesamt für Strahlenschutz, Salzgitter)
Wissenschaftlicher Oberrat Dr. F. Seidel	Bundesamt für Strahlenschutz, Salzgitter, von Dez. 2006 - Nov.2008 (Stellvertreter: Oberregierungsrat P. Sperling, Bonn, BMU)
Regierungsdirektorin Dr. C.Wassilew	Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit, Bonn, ab Dez.2008 (Stellvertreter: Oberregierungsrat K. Weidenbrück, Bonn, BMU, ab Dez. 2008, Wissenschaftlicher Oberrat Dr. F. Seidel, Bundesamt für Strahlenschutz, Salzgitter)
Dr. A. Langenfeld	Ministerium für Soziales, Gesundheit, Familie, Jugend und Senioren des Landes Schleswig-Holstein, bis Nov. 2006 (Stellvertreter: H. Aumann, Niedersächsisches Umweltministerium, Hannover)
Wissenschaftlicher Direktor J.-H. Hagemeister	Ministerium für Justiz, Gleichstellung und Integration des Landes Schleswig-Holstein, ab Dez. 2006 (Stellvertreter: H. Aumann, Niedersächsisches Umweltministerium, Hannover)
GDir M. Hagmann	Ministerium für Umwelt, Naturschutz und Verkehr Baden-Württemberg, ab Dez. 2010

Vertreter der Gutachter und Beratungsorganisationen:

Dipl.-Ing. R.-D. Junge (Obmann)	TÜV NORD EnSys GmbH & Co. KG, Hannover, bis Nov. 2010 (Stellvertreter: Dipl.-Ing. J. Zawilak, TÜV Nord SysTec GmbH., Hamburg, bis Nov. 2007) Dipl.-Ing. J. Boenkendorf TÜV Nord SysTec GmbH., Hamburg, ab Dez. 2007,
Dipl.-Ing. A. Rottenfuß	TÜV Industrie Service GmbH, München (Stellvertreter: Dipl.-Ing. J. Zawilak, TÜV Nord SysTec GmbH., Hamburg, bis Nov. 2007, Dipl.-Ing. J. Boenkendorf TÜV Nord SysTec GmbH., Hamburg, von Dez. 2007 - Nov. 2009) Dipl.-Ing. J. Kraus, TÜV Industrie Service GmbH, München, ab Dez. 2009)
Dipl.-Ing. C. Versteegen	Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH, Köln, ab Nov. 2009 (Stellvertreterin: Dr. D. Sommer, Gesellschaft für Reaktorsicherheit (GRS) mbH, Köln, ab Dez. 2010)

Vertreter sonstiger Behörden und Stellen:

W. Fürst	(für: DGB) Gemeinschaftskernkraftwerk Grohnde GmbH, Emmerthal, bis Nov. 2008 (Stellvertreter: F.-J. Hauptmanns, (für: DGB))
T. Gerl	(für: DGB) Gemeinschaftskernkraftwerk Grohnde GmbH, Emmerthal, ab Dez. 2008 (Stellvertreter: N. Islinger, Kernkraftwerk Isar (für: DGB))
Dipl.-Ing. Schnürer	(für: DKE) Institut für Sicherheitstechnologie (ISTec) GmbH, Garching (Stellvertreter: Dipl.-Ing. G. Vogel, DKE Deutsche Kommission Elektrotechnik, Elektronik Informationstechnik im DIN und VDE, Frankfurt, Dr.-Ing. A. Lindner, (für: DKE) Institut für Sicherheitstechnologie (ISTec) GmbH, Garching)
Dipl.-Ing. D. Sonntag	Forschungszentrum Jülich GmbH

**2.2 Zusammensetzung des Arbeitsgremiums**

Dipl.-Ing. H. Averdick	EnBW Kernkraft GmbH (EnKK), Kernkraftwerk Neckarwestheim
Dipl.-Ing. H. Gradic	E.ON Kernkraft GmbH, Kernkraftwerk Unterweser GmbH
Dipl.-Ing. H. Heinsohn	Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH, Köln
Dipl.-Ing. F.-J. Kießler	AREVA NP GmbH, Offenbach
Dipl.-Ing. D. Malchers	TÜV Nord SysTec GmbH, Hamburg
Dipl.-Ing. T. Niss	E.ON Kernkraft GmbH, Hannover
Dipl.-Ing. A. Rottenfuß	TÜV Industrie Service GmbH, München
Dipl.-Ing. R. Schildheuer	TÜV Süd Energietechnik GmbH, Baden-Württemberg, Mannheim
Dipl.-Ing. R. Schmidt	Kernkraftwerk Brunsbüttel GmbH & Co. oHG
Dipl.-Ing. G. Schnürer (Obmann)	Institut für Sicherheitstechnologie (ISTec) GmbH, Garching
Dipl.-Ing. H.-J. Schwarzberg	TÜV NORD EnSys GmbH & Co. KG, Hannover

**2.3 Mitarbeiter der KTA-Geschäftsstelle**

Dr. G. Roos	KTA-Geschäftsstelle, Salzgitter, (bis Juli 2007)
Dipl.-Ing. H.-J. Schwarzberg	TÜV NORD EnSys GmbH & Co. KG, Hannover, (bis April 2009)
Dipl.-Ing. R. Piel	KTA-Geschäftsstelle, Salzgitter (seit April 2009)

**3 Verlauf des Regeländerungsverfahrens****3.1 Erstellung des Regeländerungsentwurfsvorschlages**

(1) Das Arbeitsgremium KTA 3506 erarbeitete den Regeländerungsentwurfsvorschlag in 11 Sitzungen; die Sitzungen fanden statt:

1. Sitzung am 6. Dezember 2006 bei der GRS in Garching
2. Sitzung am 20. & 21. März 2007 bei der GRS in Braunschweig
3. Sitzung am 17. Juli 2007 beim TÜV Süd in München
4. Sitzung am 28. November 2007 bei der KSG / GfS in Essen-Kupferdreh
5. Sitzung am 22. April 2008 bei der ISTec in Garching
6. Sitzung am 16. Oktober 2008 in GKN in Neckarwestheim
7. Sitzung 30. April 2009, Hochschule Zittau
8. Sitzung 24. September 2009, TÜV SÜD Mannheim
9. Sitzung 25. Februar 2010, TÜV SÜD München
10. Sitzung 28. & 29. April 2010, E.ON Kernkraft Hannover
11. Sitzung 30. Juni & 1. Juli 2010, ISTec Garching

(2) Auf der 11. Sitzung vom 30. Juni bis 1. Juli 2010 wurde der Regeländerungsentwurfsvorschlag einstimmig zur Vorlage an den Unterausschuss ELEKTRO UND LEITTECHNIK (UA-EL) verabschiedet.

(3) Der Unterausschuss ELEKTRO UND LEITTECHNIK (UA-EL) hat auf seiner 68. Sitzung am 31. August 2010 einstimmig beschlossen, den Regeländerungsentwurfsvorschlag KTA-Dok.-Nr. 3506/10/1 für den Fraktionsumlauf freizugeben.

(4) Die Regelentwurfsvorlage lag den Gruppen des KTA im Rahmen des Fraktionsumlaufs vom 15. September bis 15. Dezember 2010 zur Kommentierung vor.

(5) Im Rahmen des Fraktionsumlaufes gingen 39 Stellungnahmen ein von:

1. EnBW Kernkraft GmbH, Schreiben vom 09.10.2010
2. E.ON Kernkraft GmbH, Schreiben vom 18.11.2010
3. Rottenfußler, TÜV SÜD Industrie Service GmbH, VdTÜV, Schreiben vom 21.12.2010.

(6) Das Arbeitsgremium KTA 3506 arbeitete die eingegangenen Stellungnahmen auf seiner 12. Sitzung am 13. Januar 2011 im KKB in Brunsbüttel

ein und beschloss einstimmig die Verabschiedung des so erarbeiteten Regeländerungsentwurfsvorschlags zur Vorlage an den Unterausschuss ELEKTRO- UND LEITTECHNIK (UA-EL).

(7) Der Unterausschuss ELEKTRO- UND LEITTECHNIK (UA-EL) diskutierte die Regeländerungsentwurfsvorlage auf seiner 69. Sitzung am 22. März 2011 in Hannover und auf seiner 70. Sitzung am 15.09.2011 in Stuttgart. Er beschloss einstimmig, diese dem KTA als Regeländerungsentwurfsvorlage KTA-Dok.-Nr. 3506/11/1 vorzulegen.

(8) Der KTA hat die Regeländerungsentwurfsvorlage (Fassung September 2011) (KTA-Dok.-Nr. 3506/2011/1) auf seiner 66. Sitzung am 15.11.2011 behandelt und als Regeländerungsentwurf in der Fassung 2011-11 beschlossen. Die Bekanntmachung des BMU erfolgte im Bundesanzeiger Nr. 188 am 14.12.2011.

#### 4 Berücksichtigte Unterlagen

Neben dem im Anhang A zur KTA 3506 „Bestimmungen auf die in dieser Regel verwiesen wird“ aufgeführten Regeln wurden folgende Unterlagen bei der Regelüberarbeitung berücksichtigt:

##### 4.1 Nationale Unterlagen

- „Sicherheitskriterien für Kernkraftwerke Revision D (2009-04): Kriterien für die Leittechnik und Störfallinstrumentierung“ (Modul 5)
- BMU-Vorhaben SR 2471: Fachberatung zur Um- und Nachrüstung der Sicherheitsleittechnik in deutschen Kernkraftwerken: Zuverlässigkeitsbewertung von rechnergestützter Sicherheitsleittechnik in kerntechnischen Anlage - Digitale Leittechnik, Arbeitspunkt A.3: „Anforderungen an die Instandhaltung und Modifikation von rechnergestützten Komponenten und Teilsystemen der Sicherheitsleittechnik im Hinblick auf deutsche Belange“ (ISTec-A-899 April 2006)
- DIN EN 60987 (2010-03): Kernkraftwerke - Leittechnik für Systeme mit sicherheitstechnischer Bedeutung - Anforderungen an die Hardware-Auslegung rechnerbasierter Systeme (IEC 60987:2007)
- DIN IEC 60671 (2007-12): Kernkraftwerke - Leittechnik für Systeme mit sicherheitstechnischer Bedeutung - Prüfungen zur Sicherstellung der Funktionalität (IEC 60671:2007)
- DIN EN 60880 (2010-03): Kernkraftwerke - Leittechnik für Systeme mit sicherheitstechnischer Bedeutung - Softwareaspekte für rechnerbasierte Systeme zur Realisierung von Funktionen der Kategorie A (IEC 60880:2006)
- DIN EN 62138 (2010-03): Kernkraftwerke - Leittechnik für Systeme mit sicherheitstechnischer Bedeutung - Softwareaspekte für rechnerbasierte Systeme zur Realisierung von Funktionen der Kategorien B und C (IEC 62138:2004)
- DIN EN 61226 (2010-08) Kernkraftwerke - Leittechnik für Systeme mit sicherheitstechnischer Bedeutung - Kategorisierung leittechnischer Funktionen (IEC 61226:2009)
- DIN IEC 61513 (2002-10) Kernkraftwerke - Leittechnik für Systeme mit sicherheitstechnischer Bedeutung - Allgemeine Systemanforderungen (IEC 61513:2001)
- DIN IEC 61513/A100 (2005-02) Kernkraftwerke - Leittechnik für Systeme mit sicherheitstechnischer Bedeutung - Allgemeine Systemanforderungen - Nationaler Anhang ND (informativ): Mitgeltende Festlegungen aus anderen IEC-Normen
- DIN EN 61508-3 (2009-06): Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme -Teil 3 Anforderungen an Software (IEC 61508:2008)

##### 4.2 Internationale Unterlagen

- IAEA Safety Guide „Instrumentation and Control Systems Important to Safety in Nuclear Power Plants“, Safety Standards Series No. NS-G-1.3
- IAEA Safety Guide „Software for computer based systems“, Safety Standards Series No. NS-G-1.1
- IEEE Std 603-1998 Standard criteria for safety systems for nuclear power generating stations

## 5 Erläuterungen der vorgenommenen Änderungen

Generell wurden ersetzt:

- „Sachverständige (nach § 20 Atomgesetz)“ durch „Sachverständige“;  
der Sachverständige wurde im Abschnitt Begriffe definiert.
- „Leittechnische Einrichtungen des Sicherheitssystems“ durch „Sicherheitsleittechnik“
- „Prüfgeräte“ durch „Prüfhilfsmittel“.

Neben rein redaktionellen Änderungen wurde der Regeltext in folgenden Punkten geändert:

### Zu „Titel der Regel“

Der Titel der Regel wurde in „Systemprüfung der Sicherheitsleittechnik von Kernkraftwerken“ geändert.

Der Begriff „Sicherheitsleittechnik“ stammt aus den RSK-LL, umfasst die gesamte sicherheitsrelevante und sicherheitskritische Leittechnik und wurde unter anderem zur Harmonisierung mit den aktuellen Fassungen der KTA 3503 und der KTA 3505 eingeführt. Dieser Vorschlag zur Titeländerung wurde analog in der parallel zu überarbeitenden KTA 3501 übernommen.

Die Einführung des Begriffes Sicherheitsleittechnik ermöglicht eine Abstufung der Anforderungen, die der RSK-LL entlehnt ist, und entspricht darüber hinaus dem im IEC und EN (CENELEC) etablierten Vorgehen und insofern dem Stand von Wissenschaft und Technik.

Die Sicherheitsleittechnik umfasst alle leittechnischen Einrichtungen, die Funktionen der Kategorie A, B oder C ausführen. Diese Kategorisierung, die von der Verfahrenstechnik vorgegeben wird, schafft die Möglichkeit einer eindeutigen Abstufung der Anforderungen an die Sicherheitsleittechnik. Die hier gewählte Kategorisierung ist vergleichbar mit der Kategorisierung nach DIN EN 61226, hinterlässt aber weniger Interpretationsspielraum.

Dieser funktionale Ansatz zur Abstufung über die Kategorisierung wird die bisherigen hinsichtlich der funktionalen Bedeutung interpretationsfähigen Begriffe des Sicherheitssystems wie Zustandsbegrenzungen oder Schutzbegrenzungen ersetzen.

### Zu „Grundlagen“

#### Zu „Grundlagen“ Absatz 1

Im Abschnitt Grundlagen wurden die Schutzziele ohne Verweise auf die BMI-Sicherheitskriterien formuliert. Die Quellen sind im Anhang A aufgelistet.

Die vorhandenen Hinweise auf Regeln und Leitlinien sind aktualisiert und angepasst worden.

#### Zu „Grundlagen“ Absatz 4

Der Verweis auf die RSK-Leitlinien wurde aktualisiert.

#### Zu „Grundlagen“ Absatz 5

Die Verweise auf die KTA 3507, KTA 3503, KTA 3505 und KTA 3501 wurden aktualisiert.

Die letzten beiden Sätze des Absatzes wurden gestrichen.

Diese Sätze beziehen sich ausschließlich auf Baugruppen und Geräte, die Leittechnikfunktionen der Kategorie A ausführen. Die Änderung des Titels und die damit verbundene Erweiterung des Anwendungsbereiches auf Baugruppen und Geräte, die Leittechnikfunktionen der Kategorie A, B oder C ausführen, erfordern die Streichung.

#### Zu „Grundlagen“ Absatz 7

Die Abgrenzung zu den Schaltanlagen und elektrischen Antrieben erfolgt nicht mehr im Abschnitt 2.2 „Zu prüfende Systeme“ sondern im Abschnitt 1 „Anwendungsbereich“. Um Missverständnissen vorzubeugen wurde, wie bei allen KTA Regeln üblich, die Abgrenzung im Anwendungsbereich vorgenommen.

#### Zu „Grundlagen“ Absatz 9

Die Verweise auf die neuen Regelvorhaben KTA 1402 „Managementsysteme zur Betriebsführung von kerntechnischen Anlagen“ und KTA 1403 „Alterungsmanagement in Kernkraftwerken“ wurden ergänzt

Der letzte Satz beinhaltet allgemeingültige Informationen, die für KTA 3506 verzichtbar sind, und wurde deshalb gestrichen.

### Zu „1 Anwendungsbereich“

#### Zu „1 Anwendungsbereich“ Absatz 1

Der Anwendungsbereich wurde auf die gesamte Sicherheitsleittechnik von Kernkraftwerken erweitert. Eine Abstufung erfolgt nach Abschnitt 2.2 des ÄEV KTA 3501(Fassung 2010-06) in leittechnische Einrichtungen mit Funktionen der Kategorie A, B oder C. Der Regeltext dieses Abschnittes 2.2 (Kategorisierung) wurde in den informativen Anhang B übernommen. Auf diese Weise wird vermieden, das KTA 3506 hier eine eigenständige Kategorisierung enthält und mit dem Weißdruck der KTA 3501 wieder harmonisiert werden muss.

Mit der Erweiterung des Anwendungsbereiches auf die gesamte Sicherheitsleittechnik werden Lücken im KTA-Regelwerk geschlossen.

### Zu „1 Anwendungsbereich“ Absatz 2

Der Umfang der Systemprüfungen, auf die diese Regel angewendet werden soll, wurde um Systemprüfungen im Testfeld erweitert. Mit dieser Erweiterung und gleichzeitig möglichen Belastung der Prüfungen im Testfeld, entsprechend dem ohnehin etablierten Vorgehen, erfolgt eine Anpassung an den Stand von Wissenschaft und Technik.

Im letzten Satz wurde die Abgrenzung zu den elektrischen Systemen der Energieversorgung ergänzt und eine eindeutige Zuordnung im Sinne des Anwendungsbereiches geschaffen.

### **Zu „2 Begriffe“**

#### Zu „2 Begriffe“ (neu) Absatz 1

Der Einsatz rechnergestützter Prüfhilfsmittel erfordert die Definition der „Integrale Funktionsprüfungen“. Es wird klargestellt, welche Prüfungen in Abschnitt 3.1 (4) gemeint sind.

#### Zu „2 Begriffe“ (neu) Absatz 2

Zur Klarstellung der Einbindung des Sachverständigen nach § 20 AtG und zur besseren Lesbarkeit des Regeltextes wurde der Sachverständige an dieser Stelle definiert.

### **Zu „3 Übergeordnete Prüfanforderungen“ (alt 2)**

#### Zu „3.1 Allgemeines“ (alt 2.1) Absatz 2

Bei programmierbaren oder rechnerbasierten Systemen sind in der Regel Selbsttestroutinen mit vergleichsweise hoher Testabdeckung etabliert. Nach Ansicht des Arbeitsgremiums wurden Anforderungen an diese Selbsttests ergänzt, insbesondere wenn diese etwa im Rahmen von WKP belastet werden.

#### Zu „3.1 Allgemeines“ (alt 2.1) Absatz 3 (neu)

Die bislang fehlende Behandlung von erkannten Fehlern wurde ergänzt.

Diese Beschreibung der Vorgehensweise wurde zwar durch die Forderung des Funktionsnachweises in Absatz 2 abgedeckt, betont aber die Analyse von Auswirkung und Ursache. Es wurde nicht nur die Fehlerbeseitigung gefordert sondern auch die Recherche nach den Ursachen.

#### Zu „3.1 Allgemeines“ (alt 2.1) Absatz 4 (neu)

Die bisherigen Prüfungen der festverdrahteten Technik sind als Funktionsprüfungen der implementierten Anwendungsfunktionen realisiert. Die Selbstüberwachungsfunktionen haben demgegenüber das Ziel, die unterstellten (meist nur typischen) Hardwareausfälle zu detektieren. Die Anforderung gemäß 5.1 (2), den Nachweis der spezifizierten Funktion zu führen, kann damit nicht abdeckend erreicht werden. Deshalb sind auch für leittechnische Einrichtungen mit Selbstüberwachungsfunktionen ergänzend wiederkehrende integrale Funktionsprüfungen durchzuführen.

#### Zu „3.2 Zu prüfende Systeme“ (alt 2.1)

Im Unterabschnitt „Zu prüfende Systeme“ wurde eine Anpassung an den erweiterten Anwendungsbereich und die eingeführte Kategorisierung vorgenommen.

Die Aufzählung der Einrichtungen aus der Fassung (1984-11) bleibt als Hinweis erhalten. Die verwendeten Begriffe sind zwar etabliert, aber interpretationsfähig und deshalb umstritten. Durch die neue Kategorisierung entfallen diese interpretationsfähigen Begriffe wie z. B. Reaktorschutzsystem oder Zustandsbegrenzungen. Die Begriffe bleiben nur im Hinweis erhalten und dienen als „Brücke“ zur alten Regel.

Die Aufzählung im Hinweis wurde um den Punkt g) ergänzt, die den Prüfumfang auf Einrichtungen erweitert, die Sammelmeldungen von Gefahrenmeldungen der Klasse I auflösen.

#### Zu „3.3 Konfigurations-Management und Konfigurations-Identifikations-Dokumentation“ (neu)

Mit der Formulierung dieses Abschnittes erfolgt eine Anpassung an den Stand von Wissenschaft und Technik, die sich nicht nur auf die digitale rechnerbasierte Leittechnik bezieht. Es wurden Anforderungen an ein Konfigurations-Management und an die Konfigurations-Identifikations-Dokumentation (KID) gestellt, die sich nicht ausschließlich auf digitale rechnerbasierte Leittechniksysteme beschränken, sondern auch für die bestehende (konventionelle) Sicherheitsleittechnik im Kernkraftwerk gelten. Die Diskussionen zeigten, dass sowohl die bestehende Dokumentation als auch das Identifikationsmanagement dieser „konventionellen“ Sicherheitsleittechnik den Anforderungen von 2.3. genügt.

### **Zu „4 Inbetriebsetzungsprüfungen der Sicherheitsleittechnik“ (alt 4)**

Die Begriffe Prüfliste und Prüfanweisung sind bereits in der KTA 1202 definiert und sind speziell für wiederkehrende Prüfungen vorgesehen. Zur besseren Unterscheidbarkeit wurde diese Terminologie bei den IBS-Prüfungen nicht mehr verwendet. Die Begriffe Prüfliste, Prüfanweisung und Prüfprotokolle wurden bei IBS-Prüfungen durch Inbetriebsetzungsprogramm, Inbetriebsetzungsprüfanweisung und Inbetriebsetzungsprüfprotokoll ersetzt.

#### Zu „3.1 Prüfungen ohne Betrieb der verfahrenstechnischen Systeme“ (alt 3.1)

##### Zu „4.1.1 Allgemeine Anforderungen“ (alt 3.1.1) Absatz 1

Der ursprüngliche Absatz wurde durch den Hinweis ergänzt, der auf eine mögliche Aufteilung der Prüfungen in Prüfungen im Prüffeld und Prüfungen am endgültigen Aufstellungsort hinweist.

#### Zu „4.1.1 Allgemeine Anforderungen“ (alt 3.1.1) Absatz 2 (neu)

Bei IBS-Prüfungen ohne Betrieb der verfahrenstechnischen Systeme wurde die Möglichkeit geschaffen, Prüfungen nicht nur am endgültigen Aufstellungsort durchzuführen, sondern auch Prüfungen im Testfeld zu belasten. Eine weitere Anpassung betrifft die Möglichkeit des Einsatzes von „Simulationen“, z. B. zur Nachbildung des Anlagenverhaltens, für beide Prüfmöglichkeiten. Auf diese Weise sollen „Überraschungen“ bei der anschließenden Prüfung mit verfahrenstechnischen Systemen ausgeschlossen und darüber hinaus die Anlagenbelastung infolge IBS minimiert werden.

#### Zu „4.1.2 Sichtprüfungen“ (alt 3.1.2) Absatz 1

Neben redaktionellen Änderungen wurde die Erweiterung der Prüfungen im Testfeld berücksichtigt.

#### Zu „4.1.2 Sichtprüfungen“ (alt 3.1.2) Absatz 2

Die Aufzählung der Prüfkriterien wurde mit dem Zusatz „zum Beispiel“ erweitert.

Durch diese Aufweichung sind weitere, nicht aufgezählte Prüfkriterien möglich.

#### Zu „4.1.2 Sichtprüfungen“ (alt 3.1.1) Absatz 3

Die Sichtprüfungen wurden mit der Ergänzung „auf der Anlage“ präzisiert. Dies ist erforderlich durch die Einführung der Prüfungen im Testfeld.

#### Zu „4.1.3 Funktionsprüfungen“ (alt 3.1.3) Absatz 2 und 4 (neu)

Die Anforderungen für Funktionsprüfungen wurden auf die digitale rechnerbasierte Leittechnik ausgedehnt. Die nötigen Anpassungen wurden in den Absätzen 2 und 4 vorgenommen.

#### Zu „4.1.3 Funktionsprüfungen“ (alt 3.1.3) Absatz 2 (alt) Absatz 5 (neu)

Der ursprüngliche Absatz 2 wurde um die Belastung von Prüfungen im Testfeld und integralen Systemprüfungen ergänzt.

Zusätzlich wurde die ursprüngliche Aufzählung b) vollständig, durch Bedingungen, die die digitale rechnerbasierte Leittechnik einschließen, ersetzt.

#### Zu „4.1.4 Inbetriebsetzungsprogramm“ (alt 3.1.4) (ursprünglich: Prüfliste)

Umsetzung der neuen Terminologie, wie unter 3 beschrieben.

#### Zu „4.1.5 Inbetriebsetzungsprüfanweisung“ (alt 3.1.5) (ursprünglich: Prüfanweisungen)

Umsetzung der neuen Terminologie, wie unter 3 beschrieben.

#### Zu „4.2 Prüfungen des Zusammenwirkens mit verfahrenstechnischen Systemen“ (alt 3.2)

##### Zu „4.2.1 Allgemeine Anforderungen“ (alt 3.2.1) Absatz 4

Der in KTA 1201 (Fassung 2009-11) „Anforderungen an das Betriebshandbuch“ neu eingeführte Begriff der „Betriebsphasen“ wurde im ersten Satz in Klammern ergänzt und im zweiten Satz redaktionell eingearbeitet.

Die Einschränkung, dass IBS-Prüfungen im nuklearen Leistungsbetrieb nicht immer durchgeführt werden dürfen, wurde durch den ergänzten Nebensatz „... , wenn dies sicherheitstechnisch zulässig ist“ vorgenommen.

##### Zu „4.2.2 Voraussetzungen für die Durchführung der Prüfung“ (alt 3.2.2) Absatz 1

Es erfolgt eine Präzisierung der erforderlichen Unterlagen auf den „aktuellen“ Anlagenzustand.

Die Bedingung, dass mindestens handschriftlich revidierte Versionen vorliegen müssen, wurde fallen gelassen.

Durch die Tatsache, dass nach KTA 1404 auch elektronische Dokumente zugelassen sind, wird diese allgemeingültige Bedingung obsolet.

##### Zu „3.2.2 Voraussetzungen für die Durchführung der Prüfung“ (alt 3.2.2) Absatz 3

Umsetzung der neuen Terminologie, wie unter 3 beschrieben.

##### Zu „4.2.3 Inbetriebsetzungsprogramm“ (alt: Prüfliste) (alt 3.2.3)

Umsetzung der neuen Terminologie, wie unter 3 beschrieben.

##### Zu „4.2.4 Inbetriebsetzungsprüfanweisung“ (alt 3.2.4) (ursprünglich: Prüfanweisung)

Umsetzung der neuen Terminologie, wie unter 3 beschrieben.

#### Zu „4.3 Anforderungen an Prüfhilfsmittel“ (alt 3.3) (ursprünglich: Anforderungen an Prüfgeräte)

Bei Einsatz von digitaler rechnerbasierter Leittechnik wurde die Möglichkeit geschaffen, Prüfungen nicht nur am endgültigen Aufstellungsort durchzuführen, sondern auch Prüfungen im Testfeld zu belasten. Eine weitere Anpassung betrifft die Möglichkeit des Einsatzes von „Simulationen“, z. B. zur Nachbildung des Anlagenverhaltens, für beide Prüfmöglichkeiten. Auf diese Weise

sollen „Überraschungen“ bei der IBS Prüfung mit verfahrenstechnischen Systemen ausgeschlossen und darüber hinaus die Anlagenbelastung infolge IBS minimiert werden. Diese Anpassung an den Stand von Wissenschaft und Technik wurde an dieser Stelle vorgenommen.

Zu „4.4 Prüfer“ (alt 3.4)

Umsetzung der neuen Terminologie, wie unter 3 beschrieben.

Zu „4.5 Dokumentation“ (alt 3.5)

Umsetzung der neuen Terminologie, wie unter 3 beschrieben.

Zu „4.6 Prüfungen nach Instandsetzung“ (alt 3.6) Absatz 1

Umsetzung der neuen Terminologie, wie unter 3 beschrieben.

Zu „4.6 Prüfungen nach Instandsetzung“ (alt 3.6) Absatz 2 (neu)

Die Forderung nach einer Instandsetzungsplanung wurde entsprechen dem Stand von Wissenschaft und Technik bzw. dem auch international etabliertem Vorgehen ergänzt.

Zu „4.7 Prüfungen nach Systemänderung“ (alt 3.7)

Zu „4.7.1 Allgemeines“ (neu)

Der frühere Abschnitt Prüfungen nach Systemänderung wurde zum neuen Unterabschnitt 3.7.1 Allgemeines und redaktionell angepasst.

Zu „4.7.2 Softwareänderungen“ (neu)

Es wurden Anforderungen an die digitale rechnerbasierte Leittechnik formuliert und somit eine Anpassung an den Stand von Wissenschaft und Technik vorgenommen. Die abgestuften Anforderungen wurden entsprechend der funktionalen Kategorisierung insbesondere in Anlehnung an den Modul 5 der Sicherheitskriterien für Kernkraftwerke Revision D und den RSK LL gestellt.

**Zu „5 Wiederkehrende Prüfungen der Sicherheitsleittechnik“ (ursprünglich: „Wiederkehrende Prüfungen der leittechnischen Einrichtungen des Sicherheitssystems“) (alt 4)**

Zu „5.1 Allgemeine Anforderungen“ (alt 4.1) Absatz 1

Die neu eingeführte Kategorisierung der Sicherheitsleittechnik erfordert an dieser Stelle eine Beschränkung auf Leittechnikfunktionen der Kategorie A und B.

Zu „5.1 Allgemeine Anforderungen“ (alt 4.1) Absatz 2 (neu)

Es wurden Anforderungen an eine Selbstüberwachung gestellt, wenn diese für wiederkehrende Prüfungen belastet werden soll.

Durch den Einsatz digitaler rechnerbasierter Leittechnik, die häufig mit einer Selbstüberwachung ausgestattet ist, wurde diese Möglichkeit geschaffen.

Zu „5.1 Allgemeine Anforderungen“ (alt 4.1) Absatz 2 (alt) Absatz 3 (neu)

Die neu eingeführte Kategorisierung der Sicherheitsleittechnik erfordert an dieser Stelle eine Beschränkung auf Leittechnikfunktionen der Kategorie A und B.

Zu „5.1 Allgemeine Anforderungen“ (alt 4.1) Absatz 3(alt) Absatz 5 (neu)

Die neu eingeführte Kategorisierung der Sicherheitsleittechnik erfordert an dieser Stelle eine Beschränkung auf Leittechnikfunktionen der Kategorie A und B.

Zu „5.1 Allgemeine Anforderungen“ (alt 4.1) Absatz 7 (neu)

Durch die neu eingeführte Kategorisierung der Sicherheitsleittechnik wurde ein neuer Absatz nötig, der auf Prüfungen für Funktionen der Kategorie C eingeht. Die wiederkehrenden Prüfungen sind funktionsspezifisch festzulegen.

Zu „5.4 Prüfliste“ (alt 4.4)

Inhalt, Aufbau, Gestaltung und Erstellung der Prüfliste werden in der KTA 1202 „Anforderungen an das Prüfhandbuch“ beschrieben. Im Absatz (1) wurde deshalb der Hinweis auf diese Regel eingefügt.

Zu „5.5 Prüfanweisungen“ (alt 4.5) Absatz 2

Die Prüfbedingungen wurden bei der Aufzählung der Bestandteile der Vorgangsbeschreibung um die Prüfvoraussetzungen ergänzt.

Ein Abgleich mit Abschnitt 3.4 Prüfanweisungen in der KTA 1202 (Fassung 2009-11) ergab, dass keine Widersprüche bezüglich der Prüfanweisungen bestehen. Nur die Prüfvoraussetzungen wurden im Zusammenhang mit den Prüfbedingungen ergänzt.

Zu „5.6 Anforderungen an Prüfhilfsmittel“ (alt 4.6) (ursprünglich: Anforderungen an Prüfgeräte)

Es wurden Anforderungen an digitale rechnerbasierte Prüfhilfsmittel ergänzt. In diesem Abschnitt erfolgt eine Anpassung an die Erweiterung der Regel auf die digitale rechnerbasierte Leittechnik.

Zu „5.8 Dokumentation“ (alt 4.8)

Der Hinweis auf das Prüfhandbuch wurde ersatzlos gestrichen, da er an dieser Stelle keine nützlichen Informationen liefert.

Zu „Stichwortverzeichnis“

Das Stichwortverzeichnis wurde gelöscht.