KTA 3506

Systemprüfung der Sicherheitsleittechnik von Kernkraftwerken

Fassung: 2017-11

Frühere Fassungen dieser Regel: 1984-11 (BAnz. Nr. 40a vom 27. Februar 1985)
2012-11 (BAnz. vom 23. Januar 2013)

Inhalt

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 „Sicherheitsanforderungen an Kernkraftwerke“ (SiAnf) und den „Interpretationen zu den Sicherheitsanforderungen an Kernkraftwerke“ weiter konkretisierten Schutzziele zu erreichen.

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

(3) In dieser Regel wird vorausgesetzt, dass die konventionellen Vorschriften und Normen (z. B. Unfallverhütungsvorschriften, DIN-Normen und VDE-Bestimmungen) unter Beachtung kernkraftwerkspezifischer Sicherheitsanforderungen eingehalten werden.

(4) Basierend auf den SiAnf und deren Interpretationen werden für die leittechnischen Einrichtungen des Sicherheitssystems 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 KTA 1401, KTA 1402, KTA 1403, 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 nach KTA 3501 ausführen.

H i n w e i s :

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 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.

(5) Integrale Funktionsprüfungen können auch durch überlappende Teilprüfungen abgedeckt werden.

3.2 Zu prüfende Systeme

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

H i n w e i s :

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.

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 Jumpereinstellungen 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.

H i n w e i s :
Werksprüfungen 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.

H i n w e i s :
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 vorgenommen 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 Inbetriebsetzungs-

prüfanweisungen 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 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. 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 Validierungen 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 funktionsspezifisch 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 Prüfintervalle

(1) Die Prüfintervalle für wiederkehrende Prüfungen der Sicherheitsleittechnik sind aufgrund von Betriebserfahrungen oder Zuverlässigkeitsanalysen in Abstimmung mit dem Sachverständigen festzulegen. Anhand der Prüfintervalle 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 Prüfintervallen, 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:

a) eine Bezeichnung einschließlich Änderungsstand, die eine Zuordnung der Vorgangsbeschreibung zur Prüfliste sicherstellt,

b) 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),

c) die Prüfbedingungen oder Prüfvoraussetzungen (z. B. Anlagen- und Systemzustand) und

d) die Art der 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,

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:

a) die Angabe der zusätzlich zur Anlageninstrumentierung verwendeten Prüfgeräte mit Gerätenummer,

b) die Prüfergebnisse der Einzelprüfschritte,

c) die vorgefundenen und neu eingestellten Werte,

d) die Angabe von Mängeln und der zur Abhilfe eingeleiteten Maßnahmen,

e) die Bestätigung der Schaffung und der Aufhebung des Simulationszustands,

f) die Gründe bei Abweichungen von der Prüfanweisung,

g) die Bewertung der Prüfergebnisse und

h) 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:

a) Prüfliste,

b) Vorgangsbeschreibungen und

c) 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

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 zuletzt durch Artikel 2 Absatz 2 des Gesetzes vom 20. Juli 2017 (BGBl. I S. 2808) 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 nach Maßgabe des Artikel 10 durch Artikel 6 des Gesetzes vom 27. Januar 2017 (BGBl. I S. 114, 1222) geändert worden ist
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)
KTA 1202	(2017-11 E)	Anforderungen an das Prüfhandbuch (Entwurf)
KTA 1401	(2017-11 E)	Allgemeine Anforderungen an die Qualitätssicherung (Entwurf)
KTA 1402	(2017-11 E)	Managementsystem zur Betriebsführung von kerntechnischen Anlagen (Entwurf)
KTA 1403	(2017-11)	Alterungsmanagement in Kernkraftwerken
KTA 1404	(2013-11)	Dokumentation beim Bau und Betrieb von Kernkraftwerken
KTA 3403	(2015-11)	Kabeldurchführungen im Reaktorsicherheitsbehälter von Kernkraftwerken
KTA 3501	(2015-11)	Reaktorschutzsystem und Überwachungseinrichtungen des Sicherheitssystems
KTA 3503	(2015-11)	Typprüfung von elektrischen Baugruppen der Sicherheitsleittechnik
KTA 3504	(2015-11)	Elektrische Antriebe des Sicherheitssystems in Kernkraftwerken
KTA 3505	(2015-11)	Typprüfung von Messwertgebern und Messumformern der Sicherheitsleittechnik
KTA 3507	(2014-11)	Werksprüfungen, Prüfungen nach Instandsetzung und Nachweis der Betriebsbewährung
KTA 3701	(2014-11)	Übergeordnete Anforderungen an die elektrische Energieversorgung in Kernkraftwerken
KTA 3702	(2014-11)	Notstromerzeugungsanlagen mit Dieselaggregaten in Kernkraftwerken
KTA 3703	(2012-11)	Notstromerzeugungsanlagen mit Batterien und Gleichrichtergeräten in Kernkraftwerken
KTA 3704	(2013-11)	Notstromanlagen mit statischen und rotierenden Umformern in Kernkraftwerken
KTA 3705	(2013-11)	Schaltanlagen, Transformatoren und Verteilungsnetze zur elektrischen Energieversorgung
KTA 3904	(2017-11)	Warte, Notsteuerstelle und örtliche Leitstände in Kernkraftwerken