Interpretation I-3: Anforderungen an die Leittechnik und Störfallinstrumentierung

Inhalt

1 Geltungsbereich

Die nachfolgenden Interpretationen gelten für leittechnische Einrichtungen, die auf den Sicherheitsebenen 1 bis 4 Leittechnik-Funktionen mit sicherheitstechnischer Bedeutung ausführen.

2 Kategorisierung

Interpretation zu den Nummern 3.1 (4) und 3.7 (10) der „Sicherheitsanforderungen an Kernkraftwerke“

Entsprechend ihrer sicherheitstechnischen Bedeutung müssen Leittechnik-Funktionen, einschließlich Leittechnik-Funktionen der Störfallinstrumentierung, in unterschiedliche Kategorien eingeordnet werden, für die abgestufte Anforderungen gelten.

Kategorie A

Die Leittechnik-Funktionen der Kategorie A umfassen alle Funktionen, die erforderlich sind, um Ereignisse der Sicherheitsebene 3 zu beherrschen.

Kategorie B

Die Leittechnik-Funktionen der Kategorie B umfassen alle Funktionen, die erforderlich sind, um Ereignisse der Sicherheitsebene 2 zu beherrschen sowie das Eintreten von Ereignissen der Sicherheitsebene 3 zu vermeiden.

Kategorie C

Die Leittechnik-Funktionen der Kategorie C umfassen alle übrigen sicherheitstechnisch wichtigen Funktionen.

Nicht kategorisiert sind Leittechnik-Funktionen, die keine sicherheitstechnisch wichtigen Funktionen ausführen.

3 Auslegungsanforderungen

3.1 Leittechnische Einrichtungen einschließlich der Störfallinstrumentierung, die Leittechnik-Funktionen der Kategorien A bis C ausführen

Interpretation zu Nummer 3.7 in Verbindung mit 3.1 (1) und 3.1 (2) der „Sicherheitsanforderungen an Kernkraftwerke“

3.1 (1) Leittechnische Einrichtungen, die für die Ausführung von Leittechnik-Funktionen vorgesehen sind, die zu unterschiedlichen Kategorien gehören, müssen nach den Anforderungen an leittechnische Einrichtungen geplant, ausgelegt und betrieben werden, die sich durch die Leittechnik-Funktionen der Kategorie mit der höchsten sicherheitstechnischen Bedeutung ergeben.

3.1 (2) Es ist auf ihre Eignung geprüfte oder für den Einsatzfall und für die unterstellten Einsatzbedingungen betriebsbewährte Hardware zu verwenden. Diese Hardware soll während des Leistungsbetriebs wartungsfrei sein.

Es ist auf ihre Eignung geprüfte Software einzusetzen.

3.1 (3) Leitungen und Kabel, einschließlich Lichtwellenleiter, sind nach Redundanten getrennt und, soweit erforderlich, auch gegen Einwirkungen von innen und außen sowie aus Notstandsfällen geschützt zu verlegen.

3.1 (4) Die leittechnischen Einrichtungen müssen so ausgelegt, montiert, abgeschirmt und geschützt werden, dass eine unzulässige Beeinflussung der Signale durch anlageninterne sowie durch äußere Störquellen vermieden wird.

3.1 (5) Es müssen Maßnahmen und Einrichtungen vorhanden sein, die es ermöglichen, die Funktionsfähigkeit der leittechnischen Einrichtungen und ihr Zusammenwirken mit den aktiven und passiven Einrichtungen des Sicherheitssystems zu überprüfen und den Zustand dieser sicherheitstechnischen Einrichtungen zu überwachen.

3.1 (6) Rückmeldungen von aktiven Einrichtungen (z.B. Stellantrieben), welche den Funktionsablauf der leittechnischen Einrichtungen für Leittechnik-Funktionen der Kategorien A bis C mitbestimmen, sollen vorzugsweise aus der Prozessvariablen abgeleitet oder unmittelbar am verfahrenstechnischen Stellglied abgegriffen werden. Eine zuverlässige Kopplung zwischen dem Stellungssignalgeber und dem verfahrenstechnischen Stellglied muss gewährleistet sein.

3.1 (7) Leittechnische Einrichtungen, die Leittechnik-Funktionen der Kategorien A und B ausführen, müssen so ausgelegt und betrieben werden, dass ihre Funktionsfähigkeit unabhängig von Art und Umfang der zeitlichen Änderung ihrer Eingangssignale gewährleistet wird. Die zugehörigen Meldeanlagen müssen so ausgelegt werden, dass ein Meldeschwall ohne Verlust sicherheitsrelevanter Informationen verarbeitet wird.

3.1 (8) Die leittechnischen Einrichtungen müssen so ausgelegt werden, dass notwendige Anpassungen an regelmäßig wiederkehrende Zustände des Normalbetriebs (z.B. Streckbetrieb) einfach und zuverlässig durchführbar sind.

Interpretation zu den Nummern 3.1 (6), 3.1 (7) und 3.7 der „Sicherheitsanforderungen an Kernkraftwerke“

3.1 (9) Die leittechnischen Einrichtungen dürfen die Erfüllung der der verfahrenstechnischen Auslegung zu Grunde liegenden Anforderungen an Unabhängigkeit und Beherrschung von Fehlerkombinationen nicht unzulässig beeinträchtigen.

Interpretation zu den Nummern 3.1 (2), 3.7 (3) und 3.7 (8) der „Sicherheitsanforderungen an Kernkraftwerke“

3.1 (10) Für leittechnische Einrichtungen, die auslegungsgemäß Funktionen auch unter Störfallbedingungen ausführen, muss die Störfallfestigkeit nachgewiesen werden.

Interpretation zu Nummer 3.7 und zum Anhang 4 Nummern 4 (6) und 4 (7) der „Sicherheitsanforderungen an Kernkraftwerke“

3.1 (11) Zur Absicherung gegen Bedienungsfehler sind technische Vorkehrungen vorzugsweise vor organisatorischen Maßnahmen anzuwenden.

3.1 (12) Die leittechnischen Einrichtungen sind so auszulegen, dass die für die Beherrschung von Ereignissen und für die Durchführung von vorgeplanten Maßnahmen des anlageninternen Notfallschutzes erforderlichen Eingriffsmöglichkeiten vorhanden sind. Die Eingriffsmöglichkeiten sind so auszulegen, dass sie die Funktionsfähigkeit der leittechnischen Einrichtungen bei der Beherrschung der Ereignisse der Sicherheitsebenen 2 und 3 nicht unzulässig beeinträchtigen. Die Eingriffsmöglichkeiten sind gegen Fehlbedienung zu sichern.

3.2 Leittechnische Einrichtungen zur Ausführung von Leittechnik-Funktionen der Kategorie A

Interpretation zu Nummer 3.7 der „Sicherheitsanforderungen an Kernkraftwerke“

Interpretation zu den Nummern 3.1 (6) und insbesondere 3.7 (3) der „Sicherheitsanforderungen an Kernkraftwerke“

3.2 (1) Bei der Auslegung der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, müssen versagensauslösende Ereignisse innerhalb und außerhalb des Sicherheitssystems berücksichtigt werden.

Interpretation zu Nummer 3.7 (3) und zu Anhang 4 Nummer 4 der „Sicherheitsanforderungen an Kernkraftwerke“

3.2 (2) Veränderungen an Bereitschaftsstellungen von Einrichtungen des Sicherheitssystems dürfen nur dann vorgenommen werden, wenn entsprechende Freigabebedingungen erfüllt sind. Diese Veränderungen müssen automatisch oder durch technische Vorkehrungen bzw. organisatorische Maßnahmen wieder aufgehoben werden, wenn die Freigabebedingungen nicht mehr erfüllt sind. In dem sicherheitstechnisch geforderten Zustand müssen diese Einrichtungen gegen unzulässige Eingriffe gesichert werden.

Interpretation zu den Nummern 3.1 (2) und 3.7 (3) der „Sicherheitsanforderungen an Kernkraftwerke“

3.2 (3) Sind bei Einrichtungen des Sicherheitssystems eindeutige Bereitschaftsstellungen von Stellgliedern bei Normalbetrieb vorgeschrieben, so soll das Verlassen dieser Bereitschaftsstellung signalisiert werden. Stellglieder ohne Meldung der Bereitschaftsstellung sind gegen das Verlassen der Bereitschaftsstellung zu sichern.

Interpretation zu den Nummern 3.1 (3), 3.1 (6), 3.1 (7), 3.7 (3) und zu Anhang 4 Nummer 2 der „Sicherheitsanforderungen an Kernkraftwerke“

3.2 (4) Ein Ausfall in den leittechnischen Einrichtungen des Sicherheitssystems darf höchstens Auswirkungen auf die Funktion der betroffenen Redundante des Sicherheitssystems haben.

Die leittechnischen Einrichtungen, die für die Funktionsfähigkeit des Sicherheitssystems nach Eintritt von Ereignissen der Sicherheitsebene 3 erforderlich sind, sind so auszulegen, dass sie den jeweils ungünstigsten Umgebungs- und Störfallbedingungen standhalten, die im zugehörigen Aufstellungs- und Installationsbereich auftreten können.

Die leittechnischen Einrichtungen sind so auszulegen, dass ein fehlerhaftes Auslösen von Schutzaktionen unter Berücksichtigung der Nummer 3.2 (11) verhindert wird, wenn dies zu auslegungsüberschreitenden Anlagenzuständen führen kann.

Interpretation zu den Nummern 3.1 (2), 3.1 (3), 3.1 (12) und 3.7 (3) der „Sicherheitsanforderungen an Kernkraftwerke“

3.2 (5) Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, sind grundsätzlich selbstüberwachend auszulegen. Deren Funktionen und Eigenschaften, die von der Selbstüberwachung nicht erfasst sind, sind einer regelmäßigen und lückenlosen Überprüfung zu unterziehen. Die Prüfzyklen sind auf Grundlage von Zuverlässigkeitsbetrachtungen festzulegen. Diese Prüfungen sollen mittels Prüfhilfen an für diesen Zweck vorgesehenen Schnittstellen leicht durchführbar sein.

Prüfeingriffe und Handbetätigungen sind so festzulegen, dass notwendige Sicherheitsfunktionen weder verhindert werden noch die Zuverlässigkeit ihrer Anregung signifikant vermindert wird.

3.2 (6) Die Selbstüberwachung ist so auszulegen, dass sie die Funktion der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, nicht beeinträchtigt. Die regelmäßigen Überprüfungen sind so zu planen und durchzuführen, dass eine gleichzeitige Prüfung erforderlicher redundanter leittechnischer Einrichtungen nicht stattfindet.

Interpretation zu Nummer 3.7 (3) der „Sicherheitsanforderungen an Kernkraftwerke“

3.2 (7) Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, sollen nur für Aufgaben innerhalb des Sicherheitssystems benutzt werden. Sofern Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, auch für Leittechnik-Funktionen niedrigerer Kategorien eingesetzt werden, sind die zugehörigen leittechnischen Einrichtungen so auszulegen, dass die geforderte Zuverlässigkeit der Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, erhalten bleibt.

Interpretation zu den Nummern 3.1 (2) und 3.7 (3) der „Sicherheitsanforderungen an Kernkraftwerke“

3.2 (8) Leittechnische Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, müssen so aufgebaut werden, dass die erforderlichen Nachweise zur Qualifizierung der leittechnischen Einrichtungen des Sicherheitssystems zuverlässig möglich sind.

3.2 (9) Leittechnische Einrichtungen bestehen aus Geräten, die in drei Arten unterteilt werden können. Es gibt nichtprogrammierbare Geräte, bestehend aus diskreten, nichtprogrammierbaren Bauelementen (die Anwendungsfunktion wird durch Verdrahtung realisiert). Darüber hinaus gibt es programmierbare Geräte, bestehend aus mindestens einem diskreten programmierbaren Bauelement (die Anwendungsfunktion wird durch Verdrahtung oder durch Bauelementfunktionen realisiert). Des Weiteren gibt es rechnerbasierte Geräte, bestehend aus mindestens einem Prozessor (die Anwendungsfunktion ist im Speicher hinterlegt).

3.2 (10) Unter diversitären leittechnischen Einrichtungen versteht man leittechnische Einrichtungen, die sich in Bauart oder Wirkungsweise unterscheiden. Dissimilarität ist ein Unterbegriff der Diversität, der sich auf rechnerbasierte oder programmierbare Systeme bezieht. Als dissimilare leittechnische Einrichtungen bezeichnet man leittechnische Einrichtungen, die hinsichtlich Hardware, Software, Entwicklungswerkzeugen, Entwicklungsteams, Fertigung, Test und Instandhaltung hinreichend unähnlich oder ungleichartig zu anderen leittechnischen Einrichtungen sind, so dass ein systematischer Ausfall von den zueinander dissimilaren leittechnischen Einrichtungen nicht mehr zu unterstellen ist. Leittechnische Einrichtungen, die aus nichtprogrammierbaren Geräten bestehen, sind hinsichtlich der

Beherrschung systematischer Ausfälle als diversitär zu leittechnischen Einrichtungen, die aus programmierbaren oder rechnerbasierten Geräten bestehen, zu betrachten.

Hinweis:

Der Begriff „dissimilare leittechnische Einrichtungen“ wird eingeführt, um bei Einsatz vergleichbarer Technologien durch Bewertung unterschiedlicher Aspekte die hinreichende Unähnlichkeit zweier Systeme auszudrücken. Die Bewertung kann auch die Zulässigkeit der Gleichheit einzelner Aspekte enthalten.

Interpretation zu den Nummern 3.1 (5), 3.7 (3) und 3.7 (4), der „Sicherheitsanforderungen an Kernkraftwerke“

3.2 (11) Bei der Auslegung der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, sind Vorkehrungen gegen systematische Ausfälle der leittechnischen Einrichtungen zur Minderung der Eintrittswahrscheinlichkeit derart zu treffen, dass ein systematischer Ausfall auf der Sicherheitsebene 3 nicht mehr unterstellt werden muss.

Kann für rechnerbasierte oder programmierbare leittechnische Einrichtungen diese Nachweisführung nach dem Stand von Wissenschaft und Technik nicht erfolgen, sind Vorkehrungen derart zu treffen, dass ein systematischer Ausfall von Hardware und Software auf der Sicherheitsebene 3 beherrscht wird.

Beim Einsatz rechnerbasierter oder programmierbarer Leittechnik sind grundsätzlich diversitäre leittechnische Einrichtungen unter Beachtung der folgenden Bedingungen zu verwenden.

Es bestehen keine Vorgaben hinsichtlich des Einsatzes diversitärer Einrichtungen, wenn für die jeweils auszuführende Leittechnik-Funktion ein aktiver systematischer Ausfall sicherheitsgerichtet ist.

Beim Einsatz von rechnerbasierter oder programmierbarer Leittechnik ist für Schutzaktionen, die nicht für jeden Anlagenzustand sicherheitsgerichtet sind, in Abhängigkeit von den Auswirkungen von passiven oder aktiven systematischen Ausfällen in den leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, eine zweifache oder dreifache diversitäre Ausführung der Leittechnik einzusetzen. Eine mindestens zweifache diversitäre Ausführung ist einzusetzen,

– wenn mit den noch verfügbaren Sicherheitseinrichtungen der Störfall beherrscht wird oder

– wenn jede der beiden diversitären leittechnischen Einrichtungen für sich alleine die erforderliche Schutzaktion auslöst.

Trifft beim Einsatz von rechnerbasierter oder programmierbarer Leittechnik eine der beiden genannten Voraussetzungen für den Einsatz einer zweifach diversitären Ausführung nicht zu, ist eine dreifach diversitär ausgeführte Leittechnik einzusetzen.

Interpretation zu den Nummern 3.1 (3), 3.1 (7), 3.7 (3) und zum Anhang 4 Nummer 2 der „Sicherheitsanforderungen an Kernkraftwerke“

3.2 (12) Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, sind grundsätzlich so auszulegen, dass sie ihre Aufgaben im Anforderungsfall unter Berücksichtigung folgender Annahmen erfüllen: Es liegt

a) ein Zufallsausfall durch einen Einzelfehler,

b) und ein systematischer Ausfall (systematischer Ausfall der Hardware oder systematisches Softwareversagen); dies gilt nicht, wenn die Voraussetzung der Nummer 3.2 (11) erfüllt ist,

c) und Folgeausfälle

d) und ein Instandhaltungsfall vor.

Während eines Instandhaltungsfalls muss innerhalb einer Zeitspanne von 100 h das gleichzeitige Auftreten des systematischen Ausfalls und des Zufallsausfalls nicht unterstellt werden.

Bei rechnerbasierten und programmierbaren leittechnischen Einrichtungen mit einem ausreichend hohen Selbstüberwachungsgrad und nachgewiesenen Instandhaltungszeiten kleiner als 8 h muss gleichzeitig mit dem systematischen Ausfall das Auftreten eines Zufallsausfalls oder des Instandhaltungsfalls nicht unterstellt werden.

Hinweis:

Zum Ausfall durch Einzelfehler und Unverfügbarkeit durch Instandhaltung sind weitere Anforderungen in Anhang 4 der „Sicherheitsanforderungen an Kernkraftwerke“ festgelegt.

Interpretation zu den Nummern 3.1 (3) und 3.7 der „Sicherheitsanforderungen an Kernkraftwerke“

3.2 (13) Schutzeinrichtungen an Aggregaten und Hilfseinrichtungen sind so auszulegen, dass bei Anforderung eines Aggregats durch die leittechnischen Einrichtungen des Sicherheitssystems die Schutzeinrichtungen grundsätzlich nicht wirksam werden, es sei denn, die dadurch möglichen Folgeschäden beeinträchtigen die Sicherheit der Anlage mehr als der Ausfall des Aggregats.

Hinweis:

Schutzeinrichtungen an Aggregaten und Hilfseinrichtungen sind die Geräte (s. 3.2 (9)) des Aggregatschutzes.

Die Schutzeinrichtungen sollen so ausgelegt werden, dass der Vorrang der Leittechnik-Funktionen der Kategorie A vor den Schutzeinrichtungen sichergestellt wird.

Ist in einer Schutzeinrichtung ein Vorrang vor Leittechnik-Funktionen der Kategorie A notwendig, müssen an die Schutzeinrichtungen die Anforderungen an leittechnische Einrichtungen gestellt werden, die Kategorie A-Funktionen ausführen.

Die Anforderungen an leittechnische Einrichtungen, die Funktionen der Kategorie A ausführen, müssen an die Schutzeinrichtungen nicht gestellt werden, wenn nachgewiesen wird, dass Fehler der Schutzeinrichtung so unwahrscheinlich sind, dass eine dadurch verursachte Fehlauslösung nicht mehr unterstellt werden muss.

Interpretation zu den Nummern 3.1 (2) und 3.7 (3) der „Sicherheitsanforderungen an Kernkraftwerke“

3.2 (14) Auf der Warte und in der Notsteuerstelle sind die durch die Leittechnik-Funktionen der Kategorie A ausgelösten Schutzaktionen und Maßnahmen in dem Umfang darzustellen, der für die festgelegten Aufgaben der Warte und der Notsteuerstelle notwendig ist. Dabei sind die durch die Leittechnik-Funktionen der Kategorie A ausgelösten Schutzaktionen und Maßnahmen zusammen mit ihren Auswirkungen auf den Prozess so in der Warte und in der Notsteuerstelle darzustellen, dass eine Überprüfung des Anlagenzustandes durch das Betriebspersonal zuverlässig und rechtzeitig möglich ist.

3.3 Leittechnische Einrichtungen zur Ausführung von Leittechnik-Funktionen der Kategorie B

Interpretation zu Nummer 3.7 (2), der „Sicherheitsanforderungen an Kernkraftwerke“

Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie B ausführen, sind so auszulegen, dass sie ihre Aufgaben auch dann erfüllen, wenn im Anforderungsfall zusätzlich ein Zufallsausfall und daraus resultierende Folgeausfälle eintreten.

3.4 Anforderungen an die Störfallinstrumentierung

Interpretation zu den Nummern 3.1 (2), 3.1 (4) und 3.7 (8) der „Sicherheitsanforderungen an Kernkraftwerke“

3.4.1 Übergeordnete Kriterien für die Störfallinstrumentierung

Das Auslegungskonzept und die sicherheitstechnisch wichtigen Einzelheiten der Störfallinstrumentierung sind prüffähig zu dokumentieren.

3.4.2 Auslegung der Störfallinstrumentierung

3.4.2.1 Störfallanzeige

3.4.2.1 (1) Die Störfallanzeige ist so auszulegen, dass Daten, die vor, während und nach Eintreten eines Ereignisses der Sicherheitsebenen 3 und 4a, bei Einwirkungen von innen oder außen sowie bei Notstandsfällen für die Beurteilung der Anlagensicherheit, der Wirksamkeit des Sicherheitssystems und für die Entscheidung über Maßnahmen des anlageninternen Notfallschutzes erforderlich sind, zuverlässig und ausreichend genau angezeigt werden.

Bei Auslegung der Störfallanzeige ist zu berücksichtigen, dass die Daten, die vor, während und nach Eintreten eines Ereignisablaufs bzw. Anlagenzustands, welche zu einer erhöhten Freisetzung radioaktiver Stoffe in die Kernkraftwerksumgebung führen können (Sicherheitsebenen 4b oder 4c), für die Entscheidung über Maßnahmen des anlageninternen Notfallschutzes erforderlich sind. Sie sollen unter den anzunehmenden Umgebungsbedingungen mit der erforderlichen Genauigkeit angezeigt werden.

3.4.2.1 (2) Die Störfallübersichtsanzeige ist so auszulegen, dass die vor, während und nach Eintritt eines Ereignisses der Sicherheitsebenen 3 und 4a, bei Einwirkungen von innen oder außen sowie bei Notstandsfällen zur Beurteilung des Anlagenzustands und der radiologischen Auswirkungen auf die Umgebung wesentlichen Messgrößen erfasst werden.

3.4.2.1 (3) Es ist eine Weitbereichsanzeige für die Messgrößen vorzusehen, die die repräsentativen Ereignisabläufe und daraus abgeleiteten Anlagenzustände der Sicherheitsebenen 4b und 4c charakterisieren (siehe Interpretationen zu den „Sicherheitsanforderungen an Kernkraftwerke“, I-7: Anforderungen an den anlageninternen Notfallschutz).

3.4.2.2 Störfallaufzeichnung

3.4.2.2 (1) Die Störfallaufzeichnung ist so auszulegen, dass die Messgrößen, die vor, während und nach Eintreten

– eines Ereignisses der Sicherheitsebenen 3 und 4a, bei Einwirkungen von innen oder außen sowie bei Notstandsfällen oder

– eines Ereignisses, das zu einer erhöhten Freisetzung radioaktiver Stoffe in die

Kernkraftwerksumgebung führen kann (Sicherheitsebenen 4b oder 4c),

übersichtlich und in der richtigen zeitlichen Folge dokumentiert werden.

3.4.2.2 (2) Die Störfallaufzeichnung ist so auszulegen, dass für jede erfasste Messgröße der Störfallinstrumentierung der Zeitbezug aus den zugehörigen Dokumentationsunterlagen so genau bestimmt werden kann, dass eine zeitliche Zuordnung zu Daten aus anderen Informationsquellen möglich ist.

3.4.2.2 (3) Es ist festzulegen, welche Einrichtungen der Störfallaufzeichnung in den Betriebsphasen B bis F der Anlage in Betrieb sein müssen.

Für die Aufzeichnung und Speicherung der Störfallablaufdaten müssen zur Vorsorge gegen einen systematischen Ausfall mindestens zwei möglichst diversitäre Datenspeicher eingesetzt werden. Der Ausfall eines Datenspeichers ist anzuzeigen.

3.4.2.2 (4) Die Störfallaufzeichnungen sind gesichert aufzubewahren. Es ist sicherzustellen, dass diese gesicherten Daten weder verändert noch gelöscht werden.

3.4.2.2 (5) Die Dokumentationseinrichtungen sind übersichtlich anzuordnen sowie deutlich und eindeutig zu kennzeichnen.

3.5 Leittechnische Einrichtungen zur Ausführung von Leittechnik-Funktionen bei Notstandsfällen und auf den Sicherheitsebenen 4b oder 4c

Interpretation zu den Nummern 3.1 (10) und 3.7 der „Sicherheitsanforderungen an Kernkraftwerke“

Diese leittechnischen Einrichtungen sind so auszulegen, dass sie unter den für die jeweilige Aufgabe zu unterstellenden Umgebungsbedingungen ihre Aufgaben mit der für diese Sicherheitsebenen jeweils ausreichenden Zuverlässigkeit erfüllen. Für Maßnahmen des anlageninternen Notfallschutzes dürfen alle leittechnischen Einrichtungen eingesetzt werden, die zur Einhaltung der Schutzziele beitragen.

3.6 Anforderungsspezifikation für leittechnische Einrichtungen zur Ausführung von Leittechnik-Funktionen der Kategorien A bis C

Interpretation zu den Nummern 3.1 (2), 3.1 (4) und 3.7 der „Sicherheitsanforderungen an Kernkraftwerke“

3.6 (1) Die Anforderungen an Leittechnik-Funktionen sind in einer Anforderungsspezifikation in übersichtlicher Darstellung strukturiert zu dokumentieren.

In der Anforderungsspezifikation für die Leittechnik-Funktionen der Kategorie A, B und C sind mindestens anzugeben:

– Aufgaben,

– Kategorien der Leittechnik-Funktionen,

– Anregekriterien,

– Eingangssignale,

– Signalverarbeitung,

– Ansteuerungen der Stellglieder,

– Meldungen/Anzeigen,

– Umgebungsbedingungen,

– Anforderungen an die Datenaufzeichnung,

– Schnittstellen zu anderen Leittechnik-Funktionen,

– Reaktionszeiten und

– Schutzziele.

3.6 (2) Die Aufgaben der Leittechnik-Funktionen, die auf den Sicherheitsebenen 2, 3 und 4a, bei Einwirkungen von innen oder außen sowie bei Notstandsfällen eingesetzt werden, sind auf Basis einer Analyse der Ereignisabläufe zu ermitteln, die die in den Sicherheitsebenen 2, 3 und 4a unterstellten Ereignisse und die Einwirkungen von innen oder außen sowie die Notstandsfälle umfasst.

3.6 (3) Die Anforderungsspezifikation für die Leittechnik-Funktionen der Kategorien A und B ist so zu gestalten, dass die verfahrenstechnische Aufgabenstellung in klar abgegrenzte Teilaufgaben gegliedert wird. Diese Teilaufgaben sind in Leittechnik-Funktionen darzustellen.

Die Teilaufgaben der rechnerbasierten und programmierbaren leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, sind so auszulegen, dass die daraus abgeleiteten Leittechnik-Funktionen einen geringen Funktionsumfang haben.

Die Gesamtheit aller Leittechnik-Funktionen der Kategorien A, B und C ist übersichtlich strukturiert zu dokumentieren.

3.6 (4) Es ist nachzuweisen, dass die Einhaltung der Schutzziele mit Hilfe der erforderlichen Leittechnik-Funktionen entsprechend der Anforderungsspezifikation bei allen zu unterstellenden Ereignissen und Ereignisabläufen sichergestellt wird.

3.6 (5) Die sicherheitstechnisch relevanten Funktionen der Prozessführungs- und der Informationseinrichtungen sind in der Anforderungsspezifikation festzulegen.

3.7 Erfassung von Prozessvariablen

Interpretation zu den Nummern 3.1 (2) und 3.7 (8) der „Sicherheitsanforderungen an Kernkraftwerke“

3.7 (1) Für die unterstellten Ereignisse der Sicherheitsebenen 2 bis 4a sowie für die vorgeplanten Maßnahmen des anlageninternen Notfallschutzes (Notfallmaßnahmen) müssen die erforderlichen Prozessvariablen erfasst werden.

3.7 (2) Für jedes von den leittechnischen Einrichtungen, die Leittechnik Funktionen der Kategorie A ausführen, zu beherrschende Ereignis der Sicherheitsebene 3 müssen grundsätzlich mindestens zwei unterschiedliche Anregekriterien herangezogen werden, die aus physikalisch unterschiedlichen Prozessvariablen gebildet werden. Wenn dies technisch nicht realisierbar ist, sind andere Maßnahmen und Einrichtungen zum Erreichen hoher Zuverlässigkeit vorzusehen.

3.8 Redundanz und Unabhängigkeit

Interpretation zu den Nummern 3.1 (3), 3.1 (7) und 3.7 der „Sicherheitsanforderungen an Kernkraftwerke“

3.8 (1) Die leittechnischen Einrichtungen sind so aufzubauen, dass die in den aktiven Einrichtungen des Sicherheitssystems vorgegebene Redundanz gewahrt bleibt.

3.8 (2) Redundante leittechnische Einrichtungen, die Leittechnik-Funktionen der Kategorien A und B ausführen, sind voneinander so unabhängig auszulegen, dass ein anlageninternes versagensauslösendes Ereignis nicht zum Ausfall mehrerer Redundanten führt.

Wenn einzelne Redundanten leittechnischer Einrichtungen, die Leittechnik-Funktionen der Kategorie A ausführen, durch Notstandsfälle ausfallen, müssen die übrigen Redundanten zur Beherrschung dieses Ereignisses ausreichen.

3.8 (3) Zum Schutz gegen redundanzübergreifende versagensauslösende Ereignisse innerhalb der leittechnischen Einrichtungen und innerhalb der Anlage sollen Redundanten der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorie A oder B ausführen, räumlich getrennt angeordnet werden.

3.8 (4) Verbindungen der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorien A und B ausführen, zu nicht kategorisierten oder Datenverarbeitungs- oder Datenübertragungseinrichtungen der Kategorie C sind unter Berücksichtigung des technisch und betrieblich Notwendigen zu minimieren. Sie sind rückwirkungsfrei auszuführen.

3.8 (5) Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorien A bis C ausführen, sind voneinander so unabhängig auszulegen, dass bei versagensauslösenden Ereignissen in den Einrichtungen, die sicherheitstechnisch niederwertigere Leittechnik-Funktionen ausführen, die Leittechnik-Funktionen der sicherheitstechnisch höherwertigeren Kategorie erhalten bleiben.

3.8 (6) Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorien A bis C ausführen, sind so auszulegen, dass die Ausgangssignale von sicherheitstechnisch höherwertiger kategorisierten Leittechnik-Funktionen Priorität vor den Ausgangssignalen von sicherheitstechnisch niederwertiger kategorisierten Leittechnik-Funktionen haben.

3.9 Robustheit

Interpretation zu den Nummern 3.1 (2) und 3.7 der „Sicherheitsanforderungen an Kernkraftwerke“

3.9 (1) Für leittechnische Einrichtungen, die Funktionen der Kategorien A bis C ausführen, ist festzulegen, welche elektrischen, elektromagnetischen, thermischen, mechanischen und strahlungs- sowie feuchtigkeitsbedingten Einwirkungen beherrscht werden müssen, so dass die unterstellten Betriebs- und Störfallbedingungen zuverlässig abgedeckt werden.

3.9 (2) Die Funktionssicherheit der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorien A bis C ausführen, darf durch Bedienung und Instandhaltung nicht unzulässig beeinträchtigt werden.

3.9 (3) Die leittechnischen Einrichtungen, die für die Durchführung der im Rahmen des anlageninternen Notfallschutzes vorgesehenen Maßnahmen erforderlich sind, sind so auszulegen, dass sie durch die Folgen der zu Grunde gelegten Ereignisabläufe oder Anlagenzustände ihre erforderliche Funktionsfähigkeit nicht verlieren.

3.9 (4) Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorien A bis C ausführen, sind so auszulegen, dass Reserven gegenüber Alterungseffekten vorhanden sind.

3.9 (5) Bei der Auslegung der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorien A bis C ausführen, sind die anlagenbedingten Spannungstoleranzen zu berücksichtigen.

3.9 (6) Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorien A und B ausführen, sind fehlertolerant aufzubauen.

Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorien A und B ausführen, sollen so ausgelegt werden, dass das Ausfallverhalten definiert und sicherheitsgerichtet ist.

3.9 (7) Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorien A bis C ausführen, sind so auszulegen, dass während des Leistungsbetriebs nach Möglichkeit keine Wartungsarbeiten durchgeführt werden müssen.

3.10 Elektrische Energieversorgung der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorien A bis C ausführen

Interpretation zu Nummern 3.1 (2), 3.1 (3), 3.1 (6) und 3.7 der „Sicherheitsanforderungen an Kernkraftwerke“

3.10 (1) Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorien A und B sowie die erforderlichen Leittechnik-Funktionen der Kategorie C ausführen, müssen von unterbrechungslosen Notstromanlagen mit Energiespeicherung versorgt werden. Die Kapazität des Energiespeichers ist unter der Annahme, dass der Leistungsbedarf einer Redundante nur aus dem redundanzzugehörigen Energiespeicher gedeckt wird, so zu bemessen, dass die Versorgung mindestens 2 h aufrechterhalten wird, ohne dass die zulässige Mindestspannung unterschritten wird. Die leittechnischen Einrichtungen und deren Energieversorgung sind so auszulegen, dass nach vollständigem Spannungsausfall oder Unterschreiten der Mindestspannung die leittechnischen Einrichtungen nach Spannungswiederkehr funktionsfähig sind.

3.10 (2) Bei der Auslegung der elektrischen Energieversorgung der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorien A bis C ausführen, sind die gleichen Ausfallkombinationen zu Grunde zu legen wie bei der Auslegung der zu versorgenden leittechnischen Einrichtungen (siehe für Kategorie A in der Nummer 3.2 (12) und siehe für Kategorie B: Abschnitt 3.3).

3.10 (3) Die Auslegung der einspeisenden Erzeugungsanlagen, der Verteilernetze und der leittechnischen Einrichtungen sind so aufeinander abzustimmen, dass die für die leittechnischen Einrichtungen zu Grunde gelegten Beanspruchungen und die statischen und dynamischen Grenzwerte

der für die leittechnischen Einrichtungen spezifizierten zulässigen Versorgungsspannungen nicht überschritten werden.

3.10 (4) Ausfälle der elektrischen Energieversorgung für die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorien A bis C ausführen, sind durch Überwachungseinrichtungen zu erfassen und zu melden.

4 Qualifizierung

Interpretation zu den Nummern 3.1 (2), 3.1 (3) und 3.7 der „Sicherheitsanforderungen an Kernkraftwerke“

4.1 Qualifizierung von Hard- und Software der leittechnischen Einrichtungen für Leittechnik-Funktionen der Kategorien A bis C

4.1 (1) In allen Phasen der Entwicklung, Herstellung, Inbetriebnahme und des Betriebs der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorien A bis C ausführen, sind administrative, konstruktive und analytische Maßnahmen, einschließlich praktischer Prüfungen im Rahmen der Qualitätssicherung, durchzuführen und zu dokumentieren.

4.1 (2) Die Prüfung der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorien A bis C ausführen, hat im Fertigungs- und Montageprozess mit der Integration der Systemteile zu erfolgen. Die einzelnen Systemteile sind hinsichtlich Systemspezifikation und Ausführung darauf zu prüfen, ob die an sie gestellten leittechnischen Anforderungen erfüllt werden.

4.1 (3) Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorien A bis C ausführen, sind unter möglichst realistischen Anlagen- und Einsatzbedingungen umfassend daraufhin zu testen, dass alle zu unterstellenden Ereignisabläufe beherrscht werden.

4.1 (4) Nach Abschluss der Montage in der Anlage oder nach Änderungen an den leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorien A bis C ausführen, ist eine Inbetriebsetzungsprüfung durchzuführen.

4.1 (5) Die Informationssysteme sind gemäß ihrer sicherheitstechnischen Bedeutung zu qualifizieren.

4.2 Qualifizierung der Hardware

4.2 (1) Für leittechnische Einrichtungen, die Leittechnik-Funktionen der Kategorien A und B ausführen, ist zuverlässige, typgeprüfte oder für die unterstellten Einsatzbedingungen betriebsbewährte Hardware einzusetzen. Diese Hardware soll während des Leistungsbetriebs wartungsfrei sein.

4.2 (2) Für leittechnische Einrichtungen, die Leittechnik-Funktionen der Kategorie C ausführen, ist zuverlässige und für die unterstellten Einsatzbedingungen geeignete Hardware einzusetzen.

4.2 (3) Die anlagenbezogene Eignung ist durch den Vergleich der Eigenschaften der Hardware von leittechnischen Einrichtungen mit den für den Einsatzfall spezifizierten Kriterien nachzuweisen.

4.3 Qualifizierung der Software

4.3.1 Software für Leittechnik-Funktionen der Kategorien A bis C

4.3.1 (1) Die Software ist in verifizierbaren Schritten nach einem Phasenmodell zu entwickeln.

4.3.1 (2) Die Softwarearchitektur von leittechnischen Einrichtungen ist so zu gestalten, dass die Funktionen der Anwendersoftware und der Systemsoftware in eigenständigen Softwareeinheiten realisiert sind und die Anwendersoftware von der Systemsoftware getrennt ist.

Hinweis:

Zur Systemsoftware gehört z.B. das Betriebssystem und bei Mehrrechnersystemen die Software zur Kommunikation der Rechner.

4.3.1 (3) Die Software ist so auszulegen, dass keine unzulässigen Rückwirkungen von leittechnischen Einrichtungen, die Leittechnik-Funktionen der sicherheitstechnisch niederwertigeren Kategorie ausführen, auf die leittechnischen Einrichtungen, die Leittechnik-Funktionen der sicherheitstechnisch höherwertigeren Kategorie ausführen, auftreten.

4.3.1 (4) Die Software ist so zu gestalten, dass deren anforderungsgerechter Ablauf unabhängig von Art und Umfang der zeitlichen Änderung ihrer Eingangssignale gewährleistet ist.

4.3.2 Software für Leittechnik-Funktionen der Kategorie A

4.3.2.1 Grundsätze

4.3.2.1 (1) Die Entwicklung und Qualifizierung der Software für Leittechnik-Funktionen der Kategorie A hat so zu erfolgen, dass eine durchgängige Nachweisführung der korrekten Arbeitsweise der Software gewährleistet ist. Entwurf und Implementierung soll mit formalisierten und rechnergestützten Konstruktions- und Prüfmethoden entsprechend dem Stand von Wissenschaft und Technik durchgeführt werden.

4.3.2.1 (2) Die Software für Leittechnik-Funktionen der Kategorie A soll einfach aufgebaut sein.

4.3.2.1 (3) Der Funktionsumfang der Software für Leittechnik-Funktionen der Kategorie A soll auf das für die jeweilige Funktion notwendige Maß begrenzt werden.

4.3.2.1 (4) Die Software für Leittechnik-Funktionen der Kategorie A ist robust auszulegen. Eine Selbstüberwachung der Leittechnik-Funktionen der Kategorie A ist vorzusehen.

4.3.2.2 Qualitätssicherung

4.3.2.2 (1) Die Software ist nach einem Phasenmodell durchgängig mit rechnergestützten Werkzeugen zu erstellen.

4.3.2.2 (2) Die Software ist aus klar abgegrenzten und mit geringem Funktionsumfang versehenen Einheiten aufzubauen. Diese Softwareeinheiten sollen mit Beschränkung auf unverzichtbare Anweisungen und Schnittstellen programmiert und in eine übersichtliche Programmstruktur integriert werden.

4.3.2.2 (3) Die Ergebnisse der einzelnen Phasen der Softwareentwicklung sind unter Anwendung formaler Analysemethoden und zusätzlicher Tests an den Vorgaben vollständig zu verifizieren. Dazu sind an definierten Meilensteinen Prüfungen vorzunehmen.

4.3.2.2 (4) Nach Installation der Software auf den Rechnern soll das anforderungsgerechte Verhalten des Hardware- und Softwaresystems validiert werden. Wird die Validierung in mehreren Schritten durchgeführt, so sollen die einzelnen Validierungsschritte überlappend sein.

4.3.2.2 (5) Die Organisation und Administration der Softwareentwicklung und der Qualitätssicherung ist so zu gestalten, dass sichergestellt wird, dass die Software nach vollständigen Entwicklungs-, Prüf-, Wartungs- und Qualitätssicherungsplänen erstellt und eingesetzt wird. Die Unabhängigkeit zwischen Konstruktion und Qualitätssicherung muss durchgehend gewahrt werden. Es muss eine vollständige Entwicklungs-, Qualitätssicherungs- und Benutzerdokumentation vorhanden sein.

4.3.2.2 (6) Es sind Verfahren und Methoden anzuwenden, die die konsistenten Konfigurationen der Software sicherstellen (Konfigurationsmanagement).

4.3.2.3 Einsatz von vorgefertigter Software

4.3.2.3 (1) Der Einsatz vorgefertigter Software, sofern nicht entsprechend den Anforderungen der Abschnitte 4.3.2.1 und 4.3.2.2 ausgelegt, muss auf unverzichtbare Bestandteile beschränkt sein, wobei

Softwareänderungen vermieden werden sollen. Diese Teile sind Prüfungen und Tests zu unterziehen, die in Umfang und Tiefe den Nachweisen nach den Abschnitten 4.3.2.1 und 4.3.2.2 gleichwertig sind.

4.3.2.3 (2) Zur Bewertung der Gleichwertigkeit sollen herangezogen werden:

– Referenzen über den Hersteller der Software,

– die Entwicklungsdokumentation, Anwenderdokumentation und Qualitätssicherungsdokumentation der Software,

– die Ergebnisse unabhängiger Begutachtung (Zertifikate) der Software,

– die Betriebserfahrung der Software unter Berücksichtigung der Anwendungsprofile und

– zusätzliche Softwaretests.

4.3.3 Software für Leittechnik-Funktionen der Kategorie B

4.3.3.1 Grundsätze

4.3.3.1 (1) Für die Entwicklung und Qualifizierung der Software der Leittechnik-Funktionen der Kategorie B sind Beschreibungen und rechnergestützte Testverfahren anzuwenden, die den Nachweis der korrekten Arbeitsweise unterstützen.

4.3.3.1 (2) Die Software für Leittechnik-Funktionen der Kategorie B ist robust auszulegen. Eine Selbstüberwachung der Leittechnik-Funktionen der Kategorie B ist vorzusehen.

4.3.3.2 Qualitätssicherung

4.3.3.2 (1) Die Softwareerstellung muss nach einem Phasenmodell weitgehend mit rechnergestützten Werkzeugen erfolgen.

4.3.3.2 (2) Die Software ist aus hinsichtlich der Funktion klar abgegrenzten Einheiten aufzubauen. Diese Softwareeinheiten sollen mit Beschränkung auf unverzichtbare Anweisungen und Schnittstellen programmiert und in eine übersichtliche Programmstruktur integriert werden.

4.3.3.2 (3) Die Ergebnisse der einzelnen Phasen der Softwareentwicklung sind einer dokumentierten Prüfung zu unterziehen. Alle sicherheitsrelevanten Programmteile sind durch eine Kombination von Testverfahren zu prüfen, wobei eine vollständige Funktionsüberdeckung erreicht werden soll.

4.3.3.2 (4) Das anforderungsgerechte Verhalten des Hardware- und Softwaresystems ist zu validieren.

4.3.3.2 (5) Die Organisation und Administration der Softwareentwicklung und der Qualitätssicherung ist so zu gestalten, dass sichergestellt ist, dass die Software nach vollständigen Entwicklungs-, Prüf-, Wartungs- und Qualitätssicherungsplänen erstellt und eingesetzt wird. Die Unabhängigkeit zwischen Konstruktion und Qualitätssicherung muss durchgehend gewahrt werden. Es ist eine vollständige Entwicklungs-, Qualitätssicherungs- und Benutzerdokumentation zu erstellen.

4.3.3.2 (6) Die konsistente Konfiguration der Programme ist sicherzustellen (Konfigurationsmanagement).

4.3.3.3 Einsatz von vorgefertigter Software

4.3.3.3 (1) Der Einsatz vorgefertigter Software, sofern nicht entsprechend den Anforderungen in den Abschnitten 4.3.3.1 und 4.3.3.2 ausgelegt, muss auf unverzichtbare Bestandteile beschränkt sein, wobei Softwareänderungen vermieden werden sollen. Diese Teile sind Prüfungen und Tests zu unterziehen, die in Umfang und Tiefe den Nachweisen nach den Abschnitten 4.3.3.1 und 4.3.3.2 gleichwertig sind.

4.3.3.3 (2) Zur Bewertung der Gleichwertigkeit sollen herangezogen werden:

– Referenzen über den Hersteller der Software,

– die Entwicklungsdokumentation, Anwenderdokumentation und Qualitätssicherungsdokumentation der Software,

– die Ergebnisse unabhängiger Begutachtung (Zertifikate) der Software,

– die Betriebserfahrung der Software unter Berücksichtigung der Anwendungsprofile und

– zusätzliche Softwaretests.

4.3.4 Software für Leittechnik-Funktionen der Kategorie C

4.3.4.1 Grundsatz

Die Software für Leittechnik-Funktionen der Kategorie C ist nach dem anerkannten Stand der Technik zu qualifizieren.

4.3.4.2 Qualitätssicherung

4.3.4.2 (1) Bei der Softwareerstellung sind die Entwicklungsschritte einzeln auszuweisen. Nach Möglichkeit sind bei wesentlichen Entwicklungsschritten Software-Werkzeuge zu nutzen.

4.3.4.2 (2) Das Erreichen der Phasenziele ist durch Prüfungen nachzuweisen und zu dokumentieren.

4.3.4.2 (3) Das anforderungsgerechte Verhalten des Hardware- und Softwaresystems ist in seinen sicherheitsrelevanten Funktionen zu validieren.

4.3.4.2 (4) Die Software ist nach einem Qualitätssicherungsplan gemäß den anerkannten Regeln der Technik zu erstellen. Es ist eine vollständige Entwicklungs-, Qualitätssicherungs- und Benutzerdokumentation zu erstellen.

4.3.4.3 Einsatz von vorgefertigter Software

Eingesetzte vorgefertigte Software muss zertifiziert oder betriebsbewährt sein. Die zur Beurteilung der Einsetzbarkeit erforderlichen Eigenschaften müssen dokumentiert sein.

5 Instandhaltung und Änderungen

Interpretation zu den Nummern 3.1 (2), 3.1 (12), 3.7 und zu Anhang 4 Nummer 3 und 4 der „Sicherheitsanforderungen an Kernkraftwerke“

5 (1) Die Funktionsfähigkeit der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorien A bis C ausführen, ist während der Betriebsdauer der Anlage durch Prüfungen nachzuweisen. Diese Prüfungen müssen alle sicherheitstechnisch wichtigen Einrichtungen erfassen.

5 (2) Die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorien A bis C ausführen, sind so auszulegen, dass durch Prüfungen verursachte Veränderungen nach den Prüfungen rückgesetzt werden. Prüfungen dürfen automatisch oder manuell durchgeführt werden.

5 (3) Prüfungen an leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorien A bis C ausführen, sollen von zentralen Stellen aus überwachbar sein.

5 (4) Bei Änderungen an den leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorien A bis C ausführen, müssen mindestens gleichwertige Qualitätsstandards angewendet werden wie bei der Herstellung der leittechnischen Einrichtungen.

5 (5) Bei Änderungen an den leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorien A bis C ausführen, ist sicherzustellen, dass die geänderten Teile ihre Funktion erfüllen und mit den unveränderten Teilen anforderungsgemäß zusammenwirken.

5 (6) Änderungen der Software der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorien A bis C ausführen, sind unter Einhaltung der Qualitätsanforderungen nach Abschnitt 4 vorzunehmen. Änderungen der Software und dazu erforderliche Eingriffe in die leittechnischen Einrichtungen müssen so erfolgen, dass die Anforderungen aus den „Sicherheitsanforderungen an Kernkraftwerke“, Anhang 4 eingehalten werden. Alle Eingriffe in die Software sind zu dokumentieren.

5 (7) Änderungen von Parametrierdaten und Software der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorien A bis C ausführen, müssen so vorgenommen werden, dass sie rekonstruierbar sind.

6 Spezifische Anforderungen zur Dokumentation zu leittechnischen Einrichtungen der Kategorien A bis C einschließlich Störfallinstrumentierung

Interpretation zu den Nummern 3.1 (2) und 3.7 und zu Anhang 5 Nummer 7 der „Sicherheitsanforderungen an Kernkraftwerke“

6 (1) Die anlagenspezifische Konfiguration der Hard- und Software leittechnischer Einrichtungen, die Leittechnik-Funktionen der Kategorien A bis C ausführen, muss während ihres gesamten Lebenszyklus hinsichtlich des aktuellen Zustands und durchgeführter Änderungen dokumentiert werden.

6 (2) Die Instandhaltungsvorgänge und Eingriffe in die leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorien A bis C ausführen, sind zu dokumentieren.

6 (3) Die Betriebserfahrung aus der Instandhaltung der leittechnischen Einrichtungen, die Leittechnik-Funktionen der Kategorien A bis C ausführen, muss entsprechend der sicherheitstechnischen Bedeutung der leittechnischen Einrichtungen erfasst, dokumentiert und systematisch ausgewertet werden.