Anforderungen für die Anwendung von sicherheitsrelevanter rechnerbasierter Leittechnik in Kernkraftwerken

Hauptabteilung für die Sicherheit der Kernanlagen

zu beziehen bei:

Hauptabteilung für die Sicherheit der Kernanlagen (HSK)
CH-5232 Villigen-HSK/Schweiz

Verteiler

HSK:	Direktor, Abteilungsleiter, Sektionschefs, Anlagekoordinatoren, Sektion ELT
KSA:	Mitglieder, Experten, Sekretariat
KSR:	Präsident
BFE:	Direktor, Abteilung ARK, Sektion KE
BAG:	Abteilung Strahlenschutz
Suva:	Bereich Physik
Anlagen:	KKB, KKM, KKG, KKL, PSI, ZWILAG
Firmen:	ABB, Alstom, COLENCO

bearbeitende Sektion: ELT

Diese Richtlinie ist auch auf der HSK-Homepage http://www.hsk.ch verfügbar

	Datum	Unterschrift		Datum	Unterschrift		Datum	Unterschrift
☒	7. Apr. 2005	U. Meyer	☒	7.4.'05		☒	11.4.05	M. Schnocker

INHALT

1 Zielsetzung

Die Richtlinien der schweizerischen Behörde für die nukleare Sicherheit legen dar, wie diese ihre gesetzlichen Aufträge konkretisiert. Den Projektanten und Betreibern von Kernanlagen wird damit aufgezeigt, nach welchen Kriterien die zuständige Behörde die Gesuche beurteilt und die Aufsicht durchführt.

Die vorliegende Richtlinie hat den Zweck, auf dem Gebiet der rechnerbasierten Leittechnik das behördliche Aufsichts- und Prüfverfahren während Projektierung, Bau und Betrieb von Kernkraftwerken darzulegen. Dies erfolgt auf Basis von internationalen Standards und Richtlinien, die dem Stand von Wissenschaft und Technik entsprechen. Der Gesuchsteller bzw. Bewilligungsinhaber und seine Auftragnehmer sollen in die Lage versetzt werden, die mit dem Aufsichtsverfahren verbundenen Tätigkeiten und Termine bei ihrer Planung und Projektabwicklung zu berücksichtigen.

2 Rechtliche Grundlagen

Nach Artikel 6 Absatz 1 der Kernenergieverordnung vom 10. Dezember 2004 (KEV, SR 732.11) ist die Hauptabteilung für die Sicherheit der Kernanlagen (HSK) die Aufsichtsbehörde in Bezug auf die nukleare Sicherheit von Kernanlagen. In der KEV wird die HSK beauftragt, verschiedene Richtlinien zu erlassen. Gestützt auf ihre Aufsichtsfunktion kann die HSK weitere Richtlinien erlassen. Grundlage der vorliegenden Richtlinie bilden insbesondere die Artikel 24 Absatz 3, 25 Absatz 4, 26 Absatz 3, 27 Absatz 5, 28 Absatz 2, 40 Absatz 5 und 41 Absatz 5 der KEV. Für die Auslegung sicherheitsrelevanter rechnerbasierter Systeme gelten übergeordnet die Grundsätze nach Artikel 7, 8 und 10 des KEV.

3 Geltungsbereich

Gegenstand dieser Richtlinie sind sicherheitsrelevante Leitanlagen einschliesslich der zugehörigen Bedienelemente und Anzeigen, welche die Aufgaben Messen, Steuern, Regeln, Überwachung und Schutz realisieren. Alle Arten von sicherheitsrelevanten rechnerbasierten Leitanlagen mit deren Funktionen, Systemen und Ausrüstungen bzw. Einrichtungen (einschliesslich der speicherprogrammierbaren Steuerungen), welche die erwähnten Aufgaben erfüllen, sind darin eingeschlossen.

Diese Richtlinie wird insbesondere für die sicherheitsrelevanten rechnerbasierten Leitanlagen in Kernkraftwerken angewendet. Deren Anwendung für weitere Kernanlagen wird fallweise geregelt.

In der Richtlinie werden die Anforderungen und das Verfahren festgelegt, die beim ersten Einbau, bei Nachrüstung und Ersatz von Leitanlagen, sowie bei deren Betrieb, Instandhaltung und Änderung zu beachten sind, um jeweils den erforderlichen Sicherheitsnachweis zu erbringen.

Die Nachrüstung und der Ersatz von programmierbaren Einzelkomponenten sind nicht Gegenstand dieser Richtlinie. Das Aufsichtsverfahren für rechnerbasierte Einzelkomponenten wie z. B. Sensoren ("smart transmitters"), Aktuatoren, Linienschreiber, Schutzrelais erfolgt nach der Richtlinie HSK-R-23. Solche Komponenten sind im Aufsichtsverfahren nach der vorliegenden Richtlinie nur dann mit einbezogen, wenn sie Bestandteil des einzuführenden rechnerbasierten Systems sind (z. B. "smart transmitters“, die über das rechnerbasierte System parametriert werden).

Das Aufsichtsverfahren für sicherheitsrelevante Systeme einschliesslich Leittechnik ist in der Richtlinie HSK-R-35 festgehalten. Das Qualifikationsverfahren für Sicherheits-Ausrüstungen der rechnerbasierten leittechnischen Systeme ist in der Richtlinie HSK-R-31 festgehalten.

4 Grundsätze für die Bewertung von sicherheitsrelevanten rechnerbasierten Leitanlagen

Die Beurteilung zur Einführung und Anwendung solcher Leitanlagen erfolgen nach den folgenden Grundsätzen:

Grundsatz 1

Zur Ausführung von sicherheitsrelevanten Leittechnik-Funktionen sind rechnerbasierte leittechnische Systeme zugelassen, wenn sie zur Erfüllung dieser Funktionen geeignet sind.

Grundsatz 2

Vom Gesuchsteller ist glaubhaft und nachvollziehbar nachzuweisen, dass die Leitanlage mit seiner Hardware und Software die gestellten Sicherheitsanforderungen erfüllt.

Grundsatz 3

Von der Konzeption bis zur Inbetriebsetzung sowie während des Betriebs ist eine systematische und dokumentierte Vorgehensweise zu befolgen, welche frühzeitig zwischen dem Gesuchsteller und der HSK zu vereinbaren ist.

5 Anforderungen für die Anwendung rechnerbasierter Leitanlagen

Die Anforderungen richten sich grundsätzlich nach den Kategorien A, B oder C (siehe Anhang 3), wenn es sich um sicherheitstechnische Anforderungen an die Systemauslegung (z. B. Redundanz, diversitäre Teilsysteme, Fail-Safe-Verhalten usw.) und an die Prüftiefe (Analysen, Verifizierung, Validierung) handelt.

Wenn es sich um Anforderungen an die Qualifikation der leittechnischen Ausrüstungen und deren Eignung zur Erfüllung der geforderten Systemmerkmale (z. B. Umgebungsbedingun-

gen, Möglichkeit der Redundanztrennung, Selbstüberwachungsmöglichkeit usw.) handelt, beziehen sich die Anforderungen auf die Klassen 1, 2 oder 3 (siehe Anhang 3).

Im Folgenden sind die Anforderungen aufgeführt, die insbesondere für den Sicherheitsnachweis als wichtig erachtet werden. In den einschlägigen Normen sind weitere Angaben enthalten, die entsprechend den Kategorien und Klassen zu beachten sind.

5.1 Durch die Auslegung der Kraftwerks-Anlage bedingte Vorgaben und Randbedingungen

Die Auslegung der Kraftwerks-Anlage bildet die Grundlage für die Festlegung der Anforderungen an die Leitanlage. Diese Anforderungen werden unabhängig von der Art der einzusetzenden Leittechnik aus verfahrenstechnischer und betrieblicher Sicht analysiert und festgelegt.

Um die Anforderungen an die Leitanlage umfassend zu berücksichtigen, müssen bei neuen Systemen die im Folgenden aufgeführten Aspekte so dokumentiert sein, dass die Anforderungen an die Leitanlage darauf aufbauend und nachvollziehbar festgelegt werden können. Beim Ersatz bestehender Systeme, auch bei einem funktionsidentischen Ersatz, sollen sich diese Aspekte auf vorhandene Grundlagen abstützen. Unvollständige Grundlagen müssen identifiziert und neu erarbeitet werden. Zu diesen Grundlagen gehören die nachfolgend aufgeführten Vorgaben und Randbedingungen.

Wichtige Vorgaben aus der Kraftwerks-Anlage sind insbesondere:

- Das Defence-in-Depth-Konzept der Kraftwerks-Anlage und die Funktionsgruppen, die bei den postulierten auslösenden Ereignissen zur Erfüllung der Schutzziele zum Einsatz kommen, mit Bezeichnung der zueinander diversitären Funktionen,
- die Störfall- bzw. Sicherheitsanalysen,
- die Rolle der automatischen Funktionen und der vorgesehenen Operateuraktionen zur Beherrschung von Störungen und Störfällen,
- die Aufgabenverteilung zwischen Mensch und Leitanlage,
- die Mensch-Maschine-Schnittstellen,
- die Anlage-Informationen, die der Operateur für Handeingriffe benötigt,
- die Prinzipien des Vorrangs von automatischen und manuellen Auslösungen.

Wichtige Randbedingungen sind insbesondere:

- Die Örtlichkeiten in der Kraftwerks-Anlage mit den Umgebungsbedingungen im Normalbetrieb und im Störfall,
- die Schnittstellen zu anderen Teilen der Anlage (z. B. angesteuerte elektromechanische Komponenten, Stromversorgung),
- andere übergeordnete Dokumente des Kraftwerks, z. B. die allgemeinen Betriebs- und Instandhaltungsvorschriften,
- ein übergeordnetes kraftwerksspezifisches IT-Security-Konzept.

Aufgrund dieser Vorgaben und Randbedingungen sind für die Funktionen der Leitanlage bzw. einzelner Leitanlagen verfahrenstechnische Beschreibungen einschliesslich der erforderlichen Eingänge (Messwerte, Bedienelemente) sowie der Auslösungen und Rückmeldungen zu erstellen. Die leittechnischen Funktionen sollen nach sicherheitstechnischen Gesichtspunkten (Schutzziele, Unterschutzziele) gruppiert werden. Betriebliche leittechnische Funktionen können nach den verfahrenstechnischen Aufgaben gruppiert werden.

5.2 Anforderungen an die Leitanlage

5.2.1 Architektur der Leitanlage und Zuordnung der Leittechnik-Funktionen

Die Architektur der Leitanlage und ihrer Teilsysteme, samt den Schnittstellen (einschliesslich Datenkommunikation) zwischen den einzelnen Leitanlagen, sowie deren Zuordnung zum IT-Security-Konzept des Kraftwerkes, sind zu spezifizieren. Daraus soll der Aufbau der Leitanlage mit seinen Teilsystemen und deren Schnittstellen untereinander und nach aussen ersichtlich sein.

Die Funktionen sind gemäss der verfahrenstechnischen Beschreibung den entsprechenden Teilsystemen zuzuordnen.

Für die sicherheitsrelevanten leittechnischen Funktionen ist eine Kategorisierung nach IEC 61226 durchzuführen. Die Kategorie ist für jede leittechnische Funktion anzugeben.

Den Teilsystemen ist jeweils, entsprechend der Kategorie der zugeordneten Funktionen, die Anforderungsklasse (Anhang 3) zuzuordnen.

Die Funktionen der Kategorie A sollen so in Gruppen aufgeteilt werden, dass beim Ausfall einer Gruppe eine andere Gruppe die durch die zu betrachtenden auslösenden Ereignisse hervorgerufenen Störfälle (siehe Richtlinie HSK-R-100) beherrschen kann. Diese Aufteilung dieser Gruppen auf unabhängige Teilsysteme bildet die Grundlage für die funktionale Diversität.

Die Funktionen der Kategorien A und B verschiedener Defence-in-Depth-Ebenen sollen auf unabhängige Systeme oder Teilsysteme aufgeteilt werden.

Die Datenkommunikation soll die Vorgaben der funktionellen, elektrischen und physischen Trennung zwischen Teilsystemen erfüllen. Datenverbindungen zu niedriger klassierten Systemen dürfen im Betrieb und bei Ausfall die Sicherheit höher klassierter Systeme nicht beeinträchtigen.

Systeme und Einrichtungen, die Funktionen der Kategorie B realisieren, müssen eine den Sicherheits- bzw. den Störfallanalysen entsprechende Zuverlässigkeit, Verfügbarkeit und Unabhängigkeit aufweisen.

5.2.2 Anforderungen an die Sicherheitsüberprüfung für die Leitanlage

Nach der Festlegung der übergeordneten leittechnischen Architektur sind darauf basierend folgende Analysen durchzuführen und zu dokumentieren:

- Eine Diversitätsanalyse für die Funktionen der Kategorie A auf Basis der Störfallanalysen, um zu überprüfen, dass beim Ausfall einer Diversitätsgruppe die andere Diversitätsgruppe oder physikalisch unterschiedliche Systeme die zu betrachtenden auslösenden Ereignisse (siehe Richtlinie HSK-R-100) beherrschen können. Lücken sind zu identifizieren und Massnahmen dagegen festzulegen.

- Für die Kategorien A und B ist die übergeordnete leittechnische Architektur dahingehend zu überprüfen, ob die Unabhängigkeit der Defence-in-Depth-Ebenen (Kap. 5.2.1) gewahrt bleibt. Lücken sind zu identifizieren und Massnahmen dagegen festzulegen.

5.2.3 Planung der Einführung der Leitanlage

Zur kontrollierten Abwicklung der Tätigkeiten und zur Erfüllung der Anforderungen soll eine Gesamtplanung durchgeführt werden, welche alle betroffenen Systeme oder Teilsysteme umfasst.

Zur Gesamtplanung gehören ein Qualitätssicherungsplan (einschliesslich Verifizierungsplan und Konfigurations-Managementplan), ein Systemintegrationsplan, ein Validierungsplan, ein Installations- und Inbetriebnahmeplan, ein Schulungsprogramm und ein Instandhaltungsplan. Die einschlägigen Normen im Anhang 1 und 5 liefern dazu für die einzelnen Anforderungsklassen abgestufte Vorgaben. Die Zuordnung der Anforderungen zum abgestuften Aufsichtsverfahren ist im Kap. 6 beschrieben und im Anhang 6 ersichtlich.

5.2.4 Anforderungen zu den Phasen des Lebenszyklus der Leitanlage

Im Lebenszyklus der Leitanlage, von der Konzeption bis zur Betriebsphase, ist ein systematisches phasenweises Vorgehen zu wählen, wobei für jede Phase die Vorgaben und die Ergebnisse sowie die Tätigkeiten in der Phase klar definiert sein müssen. Nach jeder Phase, sowie bei Änderungen während der Betriebsphase sind die entsprechenden Verifizierungs- und Validierungsschritte durchzuführen.

Die allgemeinen einzelnen Phasen des Lebenszyklus der Leitanlage sind die Anforderungsspezifikation, die Systemspezifikation, die detaillierte Auslegung und Realisierung, die Systemintegration, die Validierung, die Installation und die Betriebsphase (Instandhaltung, Prüfungen, Änderungen).

Die allgemeinen Anforderungen zu jeder Phase sind den einschlägigen Normen zu entnehmen (siehe Anhänge 1, 4 und 5). Diese Anforderungen sind teilweise je nach Kategorie der Funktionen bzw. nach System-Anforderungsklasse abgestuft.

Die folgenden Angaben zu einzelnen Phasen präzisieren und ergänzen die Anforderungen.

5.2.4.1 zur Anforderungsspezifikation

Die Basis für die Anforderungsspezifikation an die Leitanlage bilden die Vorgaben gemäss Kap. 5.1, sowie 5.2.1 und 5.2.2.

Die Anforderungsspezifikation muss zudem die Forderungen betreffend räumlicher Separation, Stromversorgung, Verkabelung, EMV- (elektromagnetische Verträglichkeit) und Blitzschutzmassnahmen, Prüf- und Selbstüberwachungseinrichtungen enthalten. Die Massnahmen zum Schutz der Leitanlage (einschliesslich deren Service- und Diagnoseeinrichtungen) vor unerlaubten oder unbeabsichtigten Eingriffen sind auf Basis des IT-Security-Konzeptes des Kraftwerkes zu spezifizieren.

Im Rahmen dieser Anforderungsspezifikation ist für die einzelne Leitanlage eine Sicherheitsüberprüfung nach Anhang 9 der Richtlinie HSK-R-35 durchzuführen.

Die angewendeten Normen sind aufzuführen und Abweichungen von diesen sind zu begründen.

5.2.4.2 zur Systemspezifikation

Die Systemspezifikation legt Aufbau, Eigenschaften und Verhalten der Leitanlage auf Basis der Anforderungsspezifikation und der Angaben zum einzusetzenden Leittechnik-System in detaillierter Form fest.

Für die wiederkehrenden Prüfungen ist ein Konzept im Einklang mit den zu spezifizierenden Prüf- und Selbstüberwachungseinrichtungen zu erstellen.

Für leittechnische Systeme, die mehrere Funktionen der Kategorie A enthalten, müssen die Funktionen verschiedener Diversitätsgruppen gemäss der Diversitätsanalyse (Kap. 5.2.2) den unabhängigen Teilsystemen mit getrennten Kommunikationseinrichtungen zugeordnet werden.

Die Diversitätsanalyse und die Unabhängigkeit der Defence-in-Depth-Ebenen sind aufgrund der Systemauslegung zu verifizieren.

Für Systeme der Anforderungsklasse 1 muss eine FMEA (Fehlermöglichkeits- und Einflussanalyse) auf Systemebene durchgeführt werden, welche aufzeigt, wie der Einzelfehler und Arten von CCF (Common Cause Failure) beherrscht, und dass Fehlerausbreitungen vermieden werden. Es sollen verschiedene Fehlerarten (Zufallsfehler, CCF bzw. systematischer Fehler und Fehlerkombinationen) berücksichtigt werden.

Um für bestimmte Systeme der Anforderungsklasse 2, die Verfügbarkeitsanforderungen zu erfüllen haben (siehe Kap. 5.2.1), auf systematische Weise die Auswirkungen von Baugruppenversagen auf das Gesamtsystem zu ermitteln, kann eine FMEA auf Systemebene bezüglich Einzelversagen einzelner Baugruppen (ohne CCF und Fehlerkombinationen) angebracht sein.

5.2.4.3 zur detaillierten Auslegung und Realisierung

Die detaillierte Auslegung für die Software besteht in der Ausarbeitung der leittechnischen Funktionen (z. B. detaillierte Funktionspläne), der Erstellung der Anwender-Software, sowie der Beschaffung der System-Software.

Je nach den Merkmalen des vorgesehenen leittechnischen Systems und der bereits existierenden Software sind die Tätigkeiten zur Erstellung der Software unterschiedlich (z. B. Verwendung anwendungsorientierter formaler Programmiersprachen mit automatischer Codegenerierung, Konfigurierung bereits existierender Anwender-Software oder klassische SW-Entwickung mit allgemeinen Programmiersprachen, siehe Anhang 4).

Zur Programmierung von Leittechnik-Funktionen der Kategorie A sollen wenn immer möglich anwendungsorientierte, formale Sprachen (z. B. Funktionsblockprogrammierung) mit automatischer Codegenerierung eingesetzt werden.

Die detaillierte Auslegung für die Hardware besteht in der Ausarbeitung der Detailpläne (z.B. Kabellisten, Kabelanschlusspläne, Kabeltrassenpläne, Schrankbelegungspläne, Stromlaufpläne) sowie die Beschaffung der Hardware.

5.2.4.4 zur Systemintegration

Die Software und die Hardware werden zusammengefügt und verifiziert. Vorgaben hierzu sind in den einschlägigen Normen festgehalten (Anhang 5).

5.2.4.5 zur Validierung

Für Systeme und Einrichtungen mit Funktionen der Kategorie A muss die Validierung konform mit der IEC 60880 erfolgen. Die Unabhängigkeit der prüfenden Personen von den Personen, die das System realisiert haben, ist erforderlich.

Für Systeme und Einrichtungen mit Funktionen der Kategorien B und C soll die Validierung nach IEC 62138 erfolgen. Die Unabhängigkeit der prüfenden Personen von den Personen, die das System realisiert haben, ist nicht erforderlich, jedoch empfehlenswert.

Die Validierung von Systemen und Einrichtungen mit Funktionen der Kategorie A und B muss so weit als möglich vor deren Einbau in der Kraftwerks-Anlage erfolgen. Ergänzende Validierungsschritte sind bezüglich der Anlageschnittstellen und dem Zusammenwirken mit den bestehenden leittechnischen und den verfahrenstechnischen Komponenten bei der Inbetriebnahme durchzuführen.

Die Validierung von Systemen und Einrichtungen mit Funktionen der Kategorie C soll vor deren Einbau in der Kraftwerks-Anlage erfolgen. Wenn ein System nur zur Anzeige bzw. zur Alarmierung dient und nicht für Eingriffe in den Prozess verwendet wird, kann die Validierung teilweise nach Einbau des Systems im Betrieb erfolgen.

5.2.4.6 zur Installation

Das integrierte System wird in der Kraftwerks-Anlage installiert und angeschlossen. Vorgaben sind in den einschlägigen Normen festgehalten (Anhang 5). Die Gegebenheiten der Kraftwerks-Anlage sind zu berücksichtigen (Kap. 5.4).

5.2.4.7 zu den Änderungen nach der Installation

Änderungen können aufgrund neuer Anforderungen oder zur Behebung von Mängeln bei der Systemauslegung bzw. bei der Implementation notwendig sein. Für Änderungen ist das Vorgehen mit Berücksichtigung der spezifischen Merkmale der Leitanlage festzulegen. Die Angaben in den einschlägigen Normen sind dabei zu berücksichtigen.

Vor jeder Änderung sind die allfälligen Auswirkungen (Auslegungsgrundlagen, funktionelle Anforderungen, übergeordnete Architektur, Systemarchitektur, Hardware, Software) abzuklären. Die entsprechend notwendigen Tätigkeiten und Prüfungen sind im Voraus zu planen und schriftlich festzulegen. Alle von der Änderung betroffenen Dokumente sind nachzuführen.

5.2.5 Anforderungen an die Dokumentation

Die Anforderungsspezifikation, die Systemspezifikation, die Dokumentation zur detaillierten Auslegung und zur Integration, sowie die Dokumentation der Validierung und die Dokumentation von Änderungen müssen erstellt und verifiziert werden. Die einschlägigen Normen (Anhänge 1 und 5) liefern dazu Vorgaben.

Es muss eine Dokumentation mit der Identifikation und dem Änderungsstand jeder Hardware- und Softwarekomponente (Schränke, Baugruppenträger und Baugruppen) sowie aller Leitanlagen-Pläne (z. B. Funktionspläne, Stromlaufpläne) erstellt werden. Diese Konfigurations-Identifikations-Dokumentation muss vollständig während des ganzen Lebenszyklus des Systems, in einer für die Instandhaltung geeigneten Form, nachgeführt und auf dem aktuellen Stand gehalten werden.

5.3 Qualifikation und Eignungsüberprüfung der Leitanlage

5.3.1 Generische Qualifikation und Auslegung des leittechnischen Systems

Für Einrichtungen der Anforderungsklasse 1 soll die Qualifikation der Ausrüstungen den Vorgaben der IEC 60987 entsprechen. Eine generische Qualifikation soll nach den einschlägigen umfassenden Normen des Herstellerlandes oder eines Referenzlandes (z. B. nach KTA oder nach IEEE) durchgeführt worden sein.

Die Systemsoftware und die Anwendungs-Grundbausteine von Systemen der Anforderungsklasse 1 müssen konform mit IEC 60880 oder IEC 60880-2 erstellt worden sein. Eine generische Qualifikation soll nach den einschlägigen umfassenden Normen des Herstellerlandes oder eines Referenzlandes, im Zusammenhang mit den zugehörigen Einrichtungen, durchgeführt worden sein und soll nachvollziehbar dokumentiert sein.

Für Einrichtungen der Anforderungsklasse 2 und 3 müssen die Ausrüstungen für industrieübliche Umgebungsbedingungen und Gefahrenquellen (z. B. EMV) ausgelegt sein. Eine entsprechende Ausführung nach den Vorgaben einschlägiger Industriestandards wird vorausgesetzt.

Für die Anforderungsklasse 2 soll hierfür eine Bestätigung bzw. Dokumentation des Herstellers vorliegen. Der Hersteller soll jedoch in der Lage sein, die Nachweise vorzulegen, für welche er die Bestätigung bzw. Dokumentation abgegeben hat. Die entsprechenden Prüfungen können vom Hersteller in eigener Regie in geeigneten Prüflaboren durchgeführt werden.

Die Systemsoftware von leittechnischen Systemen der Anforderungsklasse 2 und 3 sollen nach einem qualitätsgesicherten Vorgehen entwickelt worden sein. Die Software soll die Anforderungen der IEC 62138 oder von Industriestandards, z.B. IEC 61508, erfüllen.

5.3.2 Anwendungsspezifische Eignungsüberprüfung

Die spezifischen Gegebenheiten (z. B. Aufstellungsorte, Anordnung der Baugruppen in den Leittechnikschränken) sind zu berücksichtigen.

Für die Anforderungsklasse 1 ist nachzuweisen, dass das eingesetzte Leitsystem die erforderlichen Eigenschaften aufweist, um die anwendungsspezifischen Anforderungen zu erfüllen. Die anwendungsspezifische Eignungsüberprüfung soll nachvollziehbar dokumentiert sein.

Für die Anforderungsklasse 2 ist darzulegen und zu bestätigen, dass die Auslegung des Leitsystems die anwendungsspezifischen Anforderungen abdeckt.

Für die Anforderungsklasse 1 ist nachzuweisen, dass die vorliegende generische Qualifikation den Anforderungen der Umgebungsbedingungen im Normalbetrieb und im Störfall genügt und zur Beherrschung der festgelegten Gefahrenquellen (z. B. elektromagnetische Störungen, Blitzschlag) ausreichend ist.

5.4 Installation und Inbetriebnahme in der Kraftwerks-Anlage

Die Installation, das Prüfen der Schnittstellen, das Prüfen der Ansteuerung der Komponenten, sowie die schrittweise Inbetriebnahme erfolgt nach den festgelegten übergeordneten sowie den systemspezifischen Plänen (bzw. Versuchsprogramme) und Prüfvorschriften, die bei der Planung für die Einführung einer Leitanlage festgelegt werden (5.2.3).

Die Installation und die Inbetriebnahme von Leitanlagen darf nur in einem Anlagenzustand durchgeführt werden, in welchem durch die Arbeiten der sichere Zustand der Anlage nicht beeinträchtigt wird. Allenfalls sind temporäre Massnahmen (z. B. Anzeigen, provisorische Bedienung) zu treffen.

5.5 Betrieb und Instandhaltung der Leitanlagen

5.5.1 Wiederkehrende Prüfungen

Aufgrund der Systemdokumentation und der Prüfkonzepte der Anlage ist ein Plan für die wiederkehrenden Prüfungen und die Instandhaltung, sowie die entsprechenden Vorschriften für die einzelnen Teile der Leitanlage zu erstellen.

Für Systeme und Einrichtungen mit Funktionen der Kategorie A sollen bei der Festlegung der Prüfanforderungen in den Technischen Spezifikationen die Besonderheiten der leittechnischen Architektur (z. B. gemeinsame Verarbeitungseinheiten für mehrere Funktionen) beachtet werden.

Die Funktionstüchtigkeit der Systeme und Einrichtungen der Kategorien A und B muss abdeckend und, unter Berücksichtigung der Selbstüberwachung, in festgelegter Periodizität geprüft werden.

Für Systeme und Einrichtungen mit Funktionen der Kategorie C, bei denen spezielle Anforderungen an die Verfügbarkeit bestehen (z. B. Alarmeinrichtungen, Brandmeldeanlagen, Komponentenschutzeinrichtungen), sind adäquate Kontrollen zur Funktionstüchtigkeit vorzusehen. Bei Funktionen der Kategorie C, die ständig im Eingriff sind (z. B. Regelfunktionen) und deren Fehlverhalten daher unmittelbar erkannt wird, kann auf solche Kontrollen verzichtet werden.

5.5.2 Vorgehen bei Änderungen

Für die Durchführung von Änderungen an der Leitanlage ist Kap. 5.2.4.7 zu beachten.

Vor der Durchführung von Änderungen ist zu prüfen, ob die Vorgaben aus der Kraftwerks-Anlage, die verfahrenstechnischen Beschreibungen der Leittechnik-Funktionen oder die Zuordnung der Leittechnik-Funktionen zur Architektur der Leitanlage betroffen sind. Gegebenenfalls sind die in den Kap. 5.2 angegebenen Analysen erneut durchzuführen.

Die bestehende bzw. zuletzt durchgeführte Analyse nach Anhang 9 der Richtlinie HSK-R-35 (Kap. 5.2.4.1) ist zu überprüfen und nötigenfalls zu revidieren.

Während des Betriebs der Leitanlage ist zur Durchführung, zur Prüfung und zur Dokumentation von Änderungen ein gut kontrollierbares und nachvollziehbares Vorgehen anzuwenden (qualitätsgesichertes Konfigurations- und Änderungsmanagement). Sämtliche Software-Module und Dokumentationen sind mit einzubeziehen.

Auch die gültigen Versionsstände von generisch qualifizierten leittechnischen Systemen und von validierten Systemen müssen eindeutig reproduzierbar und bezüglich deren Qualifikationsnachweise rückverfolgbar sein.

Die Installation und die Vorprüfung der geänderten Leitanlage dürfen grundsätzlich nur in einem Anlagezustand erfolgen, in dem die betroffenen Funktionen nicht betriebsbereit sein müssen. Ausnahmen müssen bezüglich Anlagesicherheit vorgängig analysiert und begründet werden.

Die Anlagen-Dokumentation und die Konfigurations-Identifikations-Dokumentation (Kap. 5.2.5) sind nachzuführen.

5.5.3 Ersatz von Komponenten

Es ist sicherzustellen, dass bei einem Austausch der für den Einbauplatz vorgesehene Hardwarekomponententyp eingesetzt wird, und dass die Komponente dem Einbauplatz entsprechend eingestellt und konfiguriert wird, z. B. Jumpereinstellung, EPROM-Version, anwendungsspezifisch einzustellende Parameter (Kalibrierparameter, Grenzwerte usw.).

6 Vorabklärungen und Aufsichtsverfahren mit einzureichender Dokumentation

Das Aufsichtsverfahren erfolgt in den vier Hierarchiestufen S1 bis S4 nach den Vorgaben der Richtlinie HSK-R-35, in denen der Sicherheitsnachweis schrittweise erbracht wird. Die spezifischen Erläuterungen zu den Hierarchiestufen sind in diesem Kapitel und im Anhang 6 beschrieben.

6.1 Vorabklärungen

Der Betreiber nimmt frühzeitig Kontakt mit der HSK auf, um je nach Umfang und sicherheitstechnischer Bedeutung des Vorhabens Ablauf und Tiefe des Aufsichtsverfahrens zu vereinbaren. Die frühzeitigen Abklärungen dienen der HSK ausserdem dazu, die notwendigen internen und allenfalls externen Ressourcen für das Aufsichtsverfahren zu planen.

Dabei sind insbesondere folgende Aspekte zu behandeln:

- Zweck, Absicht, Umfang und Art des Vorhabens, sowie grober Terminplan.

- Je nach Art, Umfang und Sicherheitsrelevanz der einzuführenden Systeme können hierzu umfangreiche Vorarbeiten notwendig sein. Der Betreiber soll erläutern, wie er die Vorgaben bzw. Anforderungen in den Kap. 5.1 und 5.2 zu erfüllen gedenkt.

  Abweichungen gegenüber diesen Anforderungen sind zu identifizieren, und es ist dafür festzulegen, wie stattdessen vorgegangen wird. Diese abweichenden Vorgehensweisen sind zudem schriftlich festzuhalten und mit der HSK abzustimmen.

Die folgenden Aspekte sind für die Funktionen der Kategorien A und B bei den Vorabklärungen zu berücksichtigen:

- Ob das Vorhaben neuartig ist, insbesondere ob voraussichtlich keine bewährten und bereits in anderen Ländern generisch qualifizierten leittechnischen Produkte zur Verfügung stehen.
- Ob es sich um eine erstmalige Aufgabenstellung oder Realisierungsart in einem schweizerischen Kernkraftwerk handelt, wie der erstmalige Einsatz einer rechnerbasierten Leittechnik für eine bestimmte sicherheitsrelevante Aufgabe (z. B. Steuerung der Anlage über Bildschirm).

6.2 Erläuterungen zu den Hierarchiestufen

Die Zuordnung der Hierarchiestufen zum Lebenszyklus der Leitanlage ist im Anhang 4 illustriert.

Die bei jeder Hierarchiestufe einzureichende Dokumentation ist, abgestuft nach Kategorien oder Anforderungsklassen, im Anhang 6 zusammengestellt.

6.2.1 Zur Hierarchiestufe S1: Konzept

Sind zum Zeitpunkt der Konzeptphase der Lieferant und das einzusetzende leittechnische System bereits bekannt, sollen die für das generische System bereits erstellten Dokumente (siehe Anhang 6) mit den Konzeptunterlagen eingereicht und die Realisierbarkeit der Anforderungen mit dem generischen System dargelegt werden. In diesem Fall kann die HSK diesen Aspekt bereits in ihre Beurteilung des Konzeptes einfliessen lassen.

6.2.2 Zur Hierarchiestufe S2: Auslegung

Es ist von Vorteil, die HSK vor einem definitiven Lieferantenentscheid zu informieren, da normalerweise die Erstellung der Systemspezifikation und die Planung der Einführung der Leitanlage vom Betreiber zusammen mit dem ausgewählten Lieferanten erfolgt.

Wegen der Komplexität der rechnerbasierten Leittechnik kann nicht ausgeschlossen werden, dass sich nach dem Entscheid für eine bestimmte Gerätefamilie und ein bestimmtes leittechnisches System Erkenntnisse ergeben, die eine Anpassung des in der Hierarchiestufe S1 bereits beurteilten Konzeptes der Leitanlage zur Folge haben. Für Leitanlagen mit Funktionen der Kategorie A sind solche Erweiterungen bzw. Änderungen der HSK zur Stellungnahme zu unterbreiten. Das Konzept ist allenfalls neu zu beurteilen.

6.2.3 Zur Hierarchiestufe S3: Ausführung

Wenn das rechnerbasierte System Funktionen mit Eingriffen in die Kraftwerks-Anlage ausführt, muss die Validierung des Systems gegenüber spezifizierten Anforderungen gemäss Kap. 5.2.4.5 so weit als möglich vor der Installation des Systems in der Kraftwerks-Anlage erfolgreich abgeschlossen sein.

Die HSK wird sich, nach vorheriger Absprache mit dem Betreiber, vor Ort über die Prüfungen und Validierungen der integrierten Leitanlage informieren.

Über allenfalls erforderliche Nach-Qualifikationen bei Systemen der Anforderungsklasse 1 wird sich die HSK, nach vorheriger Vereinbarung mit dem Betreiber, vor Ort bei der Prüfstelle informieren.

6.2.4 Zur Hierarchiestufe S4: Inbetriebnahme

Für Änderungen nach Abschluss der Validierung und während der Inbetriebnahme gelten die Anforderungen nach Kap. 5.2.4.7 und 5.5.2.

Das Aufsichtsverfahren wird nach der Inbetriebnahme (Kap. 5.4) beim Vorliegen aller Unterlagen und nach Bereinigung der offenen Punkte abgeschlossen.

Falls eine Leitanlage den nuklearen Betrieb nicht direkt betrifft, kann die HSK einer teilweisen ergänzenden Validierung während der ersten Zeit der Nutzung im Anlagebetrieb zustimmen. Der Abschluss des Aufsichtsverfahrens kann erst nach Abschluss dieser Validierung erfolgen.

Für Änderungen nach der Inbetriebnahme gelten die Anforderungen nach Kap. 5.5.2. Das Vorgehen zur Durchführung von Änderungen ist der HSK mit den Änderungsdokumenten zur Stellungnahme einzureichen. Die HSK ist über Änderungen an Systemen der Anforderungsklassen 1 und 2 im Voraus zu informieren. Dies gilt auch für Systeme der Anforderungsklasse 3, falls von den Änderungen Funktionen der Kategorie A indirekt betroffen sein könnten.

ANHANG 1

Zusammenstellung der Normen und Richtlinien

HSK-Richtlinien:

Die Richtlinie HSK-R-46/d nimmt Bezug auf folgende Richtlinien:

HSK-R-06/d:	Sicherheitstechnische Klassierung, Klassengrenzen und Bauvorschriften für Ausrüstungen in Kernkraftwerken mit Leichtwasserreaktoren
HSK-R-15/d:	Berichterstattung über den Betrieb von Kernkraftwerken
HSK-R-23/d:	Revisionen, Prüfungen, Ersatz, Reparaturen und Änderungen an elektrischen Ausrüstungen in Kernanlagen
HSK-R-30/d:	Aufsichtsverfahren beim Bau und Betrieb von Kernanlagen
HSK-R-31/d:	Aufsichtsverfahren beim Bau und dem Nachrüsten von Kernkraftwerken, 1E klassierte elektrische Ausrüstungen
HSK-R-35/d:	Aufsichtsverfahren bei Bau und Änderungen von Kernkraftwerken, Systemtechnik
HSK-R-100/d:	Nachweis ausreichender Vorsorge gegen Störfälle in Kernkraftwerken (Störfall-Richtlinie)
HSK-R-101/d:	Auslegungskriterien für Sicherheitssysteme von Kernkraftwerken mit Leichtwasserreaktoren

Internationale Regelwerke und Standards:

IEC-Standards

Der jeweils aktuelle Stand der folgenden IEC Standards ist entsprechend den Anforderungen dieser Richtlinie zu berücksichtigen:

IEC 61226	Nuclear power plants - Instrumentation and control systems important for safety - Classification
IEC 61513	Nuclear power plants - Instrumentation and control for systems important to safety - General requirements for computer-based systems
IEC 60880	Software for computers in the safety systems of nuclear power stations
IEC 60880-2	Software for computers important to safety for nuclear power plants, as a first supplement to IEC 880
IEC 62138	Nuclear power plants - Instrumentation and control - Computer-based systems important for safety - Software for I&C systems supporting category B and C functions
IEC 60987	Programmed digital computers important to safety for nuclear power stations

Gültigkeit anderer Standards:

Zur Qualifikation der leittechnischen Ausrüstungen der Anforderungsklasse 1 bzw. der 1E-klassierten leittechnischen Ausrüstungen werden als Regeln oder Standards die entsprechenden KTA-Regeln (v. a. KTA 3503) oder IEEE-Standards (v. a. IEEE-324 und IEEE-344) gegenüber dem IEC-Standard IEC 60780 (Qualification of electrical items of the safety system for nuclear power generating stations) bevorzugt.

Leittechnische Systeme und Ausrüstungen, die nach IEC-61508 (Functional Safety - Safety related systems) oder 61131 (Programmable Controllers) qualifiziert bzw. ausgelegt worden sind, müssen hinsichtlich der Eignung für die vorgesehene Anwendung im nuklearen Bereich geprüft werden. Dazu sind die Angaben in Annex D der IEC-61513 zu beachten. Für Funktionen der Kategorie A wird diese Qualifikation bzw. Auslegung allein nicht als ausreichend betrachtet. Für Funktionen der Kategorie B und C kann je nach Anwendung auf weitere Nachweise verzichtet werden, z. B. bei Prozessrechneranlagen.

Für Leittechnische Systeme und Ausrüstungen, die nach anderen Normen qualifiziert worden sind, wird ein Qualifikationsnachweis des Herstellerlandes für die gleiche oder ähnliche Anwendung verlangt (z. B. IEEE-Standards und Lizenzierung durch US-NRC).

IAEA- Safety Standards und Safety Guides:

Die folgenden Safety-Standards und Safety-Guides geben die übergeordneten Vorgaben, nach denen sicherheitsrelevante rechnerbasierte Systeme auszulegen, zu realisieren und zu betreiben sind:

NS-R-1 Safety of Nuclear Power Plants: Design
(Ersetzt 50-C-D und 50-SG-D1)

NS-G-1.1 Software for Computer Based Systems Important to Safety in Nuclear Power Plants

NS-G-1.2 Safety Assessment and Verification for Nuclear Power Plants
(Ersetzt 50-SG-D1)

NS-G-1.3 Instrumentation and Control Systems Important to Safety in Nuclear Power Plants
(Ersetzt 50-SG-D3 und 50-SG-D8)

Literaturhinweis:

/1/ IAEA-TECDOC-1066: Specification of requirements for upgrades using digital instrument and control systems

ANHANG 2

Begriffe

Anforderungsklasse

[Class of an I&C system nach IEC 61513]. Eine von drei möglichen Zuordnungen (1,2,3) sicherheitstechnisch wichtiger leittechnischer Systeme, entsprechend der Anforderung, leittechnische Funktionen unterschiedlicher Sicherheitsrelevanz zu realisieren.

Anforderungsspezifikation

Spezifikation der Anforderungen, die von der Implementierungsweise oder dem eingesetzten leittechnischen System unabhängig sind.

Ausrüstungen

[Equipment nach IEC 61513]. Ein oder mehrere Teile eines Systems. Diese bestehen aus einzelnen, definierten Grundeinheiten. In der übersetzten DIN IEC 61226 wird der Ausdruck "Einrichtung" verwendet.

Bereits existierende Software

[Pre-developed Software nach IEC 60880-2]. Im Voraus entwickelte Software. Software, welche im zu realisierenden System eingesetzt wird, aber im Voraus entwickelt, d. h. nicht ausschliesslich für das zu realisierende System erstellt wurde.

Common Cause Failure

Nach IAEA NS-G-1.3 ist "Common Cause Failure" als das "Versagen von zwei oder mehr Strukturen, Systemen oder Komponenten aufgrund eines einzelnen Ereignisses oder einer einzigen Ursache" definiert.

In der deutschen Übersetzung der IEC 61513 ist der CCF definiert als „Versagen infolge eines oder mehrerer Ereignisse, das/die ein koinzidentes Versagen in zwei oder mehreren eigenständigen Kanälen eines mehrkanaligen Systems oder in verschiedenen Systemen verursacht/verursachen, sodass es zu einem Versagen des Systems/der Systeme kommt“.

Der Begriff Systematischer Ausfall ist nach der KTA-Regel 3501 definiert als "das Versagen von Komponenten aufgrund der gleichen Ursache."

Er wird im Zusammenhang mit der Auslegung einer Leitanlage und bei der deterministischen Fehleranalyse verwendet.

In der IEC 61513 wird der Ausdruck „systematic failure“ (systematisches Versagen) verwendet. In der deutschen Übersetzung der IEC 61513 ist das „systematische Versagen“ definiert als „Versagen, das deterministisch auf eine Ursache zurückgeführt werden kann und das nur durch eine Änderung der Auslegung oder des Produktionsprozesses, der Bedienungsanleitungen, Dokumentation oder anderer relevanter Faktoren zu beheben ist“.

Defence-in-Depth

[Defence-in-Depth nach IEC 61513]. Abgestufte Massnahmen. Im Anhang A.3 der IEC 61513 sind Angaben zur Anwendung des Defence-in-Depth-Konzeptes in leittechnischen Systemen enthalten.

Leittechnische Defence-in-Depth- Stufen sind z. B. die Regelungsfunktionen, die Begrenzungsfunktionen und die Schutzfunktionen im Hinblick auf die Erfüllung eines Schutzziels. Im Weiteren zählen unabhängige leittechnische Einrichtungen für Handmassnahmen dazu.

Diversität

[Diversity nach IEC 61226]. Das Vorhandensein von zwei oder mehreren unterschiedlichen Verfahren oder Mitteln, um ein bestimmtes Ziel zu erreichen. Diversität ist besonders geeignet als Schutzmassnahme gegen Common-Cause-Fehler. Sie kann erreicht werden, indem physikalisch unterschiedliche Systeme eingesetzt werden, oder durch funktionale Diversität, bei der gleichartige Systeme ein bestimmtes Ziel über unterschiedliche Verfahren erreichen.

Einrichtungen

Siehe **Ausrüstungen**

Fehlertoleranz

Die im System eingebaute Eigenschaft, trotz dem Auftreten einer unterstellten Zahl von Fehlern in der Hardware und/oder der Software die geforderte Funktion weiter auszuführen.

FMEA

(engl.) Failure Mode and Effects Analysis.

(deutsch) Fehler Möglichkeits- und Einflussanalyse.

Durch eine systematische Methodik werden die potentiellen Fehler eines Systems, Teilsystems oder einer Baugruppe und deren Folgen analysiert. Im Zusammenhang mit dieser Richtlinie ist v. a. eine FMEA auf Systemebene gemeint.

Formale Beschreibungen

Formale Beschreibungen haben eine exakt definierte Syntax. Es sind teilweise automatische Prüfungen von Konsistenz und Übereinstimmung sowie Übersetzungen und Übertragungen möglich. Formale Beschreibungen lassen sich graphisch darstellen.

Funktion

[Funktion nach DIN IEC 61226]. Ein bestimmter Zweck oder ein Ziel, das es zu erreichen gilt, und das ohne Bezug auf die physikalische Realisierung festgelegt und beschrieben werden kann.

Die **Leittechnik-Funktion** ist derjenige Teil der Funktion, der im Leittechnik-**System** und dessen **Einrichtungen** realisiert ist.

Funktionsblockprogrammierung / Funktionsplanprogrammierung (für die Prozessverarbeitung)

Unter Funktionsblockprogrammierung wird die Erstellung von Anwendungsprogrammen mit Hilfe von vorgefertigten Bausteinen aus Bibliotheken verstanden, die zumeist eine graphische Darstellung beinhalten.

Die Funktionsblockprogammierung verwendet **formale Beschreibungen**. Mit der Verwendung von bekannten, standardisierten Symbolen aus der Verfahrenstechnik bilden die Diagramme eine anwendungsorientierte Sprache.

Die Funktionsblockprogammierung wird wegen der meist graphischen, symbolischen Darstellung auch Funktionsplan-Programmierung genannt.

Unter Bausteinen bzw. Funktionsblöcken können im Allgemeinen alle Software- bzw. Applikationselemente verstanden werden, welche vorgefertigt und geprüft in Bibliotheken zur Verfügung gestellt werden.

Graphische Programmierung (für die Prozessanzeige- und Bedienung)

Vorgefertigte, geprüfte und in Bibliotheken zur Verfügung gestellte Objekte, mit denen sich mit Hilfe der zugehörigen Werkzeuge Bildschirmanzeigen (z. B. Prozessbilder, Trendanzeigen, Protokollanzeigen) erstellen lassen.

Hardware (HW)

Physikalische Einrichtungen, bei rechnerbasierten Systemen mit programmierbaren Einheiten.

IT-Security

Physische, informationstechnische und administrative Massnahmen zum Schutz von rechnerbasierten leittechnischen und informationstechnischen Systemen gegen fehlerhafte und unbefugte Zugriffe.

Lebenszyklus der Leitanlage

Die Zeitperiode, welche mit der anlagespezifischen Konzeption beginnt und mit der Ausserbetriebnahme der Leitanlage endet. In dieser Richtlinie werden die Phasen bis und mit Betrieb betrachtet.

Leitanlage

In dieser Richtlinie wird dieser Begriff verwendet für die konkrete Implementierung eines leittechnischen Systems oder leittechnischer Einrichtungen in einer Anlage.

Die Leitanlage führt die entsprechenden anlagespezifischen leittechnischen Funktionen aus.

In den Kapiteln 5.1, 5.2.1, 5.2.2, 5.2.3 und 5.2.5 können mit dem Begriff „Leitanlage“ auch mehrere zusammenhängende und sich ergänzende Leitanlagen gemeint sein, die zusammen einen bestimmten übergeordneten Zweck erfüllen (z. B. Einhaltung der Schutzziele, Aufbereiten von Anlageinformationen, Aufbereiten von Alarmen). Diese Leitanlagen haben zusammen eine übergeordnete leittechnische Architektur [total I&C architecture nach IEC 61513] in welcher die einzelnen Leitanlagen integriert sind.

Leitsystem (leittechnisches System)

Gesamtheit aufeinander abgestimmter, zusammenarbeitender Komponenten/Geräte/ Module.

[I&C system gemäss IEC 61513]. Leittechnisches System, das sowohl leittechnische Funktionen als auch auf sich selbst bezogene Dienstleistungs- und Überwachungsfunktionen ausführt.

Obwohl dieser Begriff auch für konkrete Implementierungen gilt (z. B. in IEC 61513), wird er in dieser Richtlinie für ein generisches System ohne spezifische Implementierung verwendet.

Ein leittechnisches System ist für bestimmte Arten ähnlicher Funktionen (z. B. für Funktionen eines Reaktorschutzsystems oder einer Neutronenflussmessung) ausgelegt.

Das Leitsystem ist hersteller- und z. T. branchenspezifisch und besteht aus einer oder mehreren Gerätefamilien. Kann generisch, nicht jedoch anlagespezifisch, qualifiziert sein.

Leittechnik

[I&C Instrumentation and Control]. Die grundlegende Technik für die Aufgaben Messen, Steuern und Regeln. Wird unterschieden nach der Technologie: Elektrische und/oder elektronische und/oder programmierbare, d. h. rechnerbasierte Technologie.

Der Begriff Leittechnik ist hersteller- und systemneutral.

Leittechnische Gerätefamilie

[Equipment family gemäss IEC 61513]. Die Gerätefamilie ist ein Satz von Hardware- und Softwarekomponenten, die in einer oder mehreren Architekturen (Konfigurationen) zusammenarbeiten können.

Die Gerätefamilie ist zumeist funktionsneutral. Die Gerätefamilie kann generisch qualifiziert sein.

Leittechnik-Funktion

Siehe **Funktion**

Rechnerbasierte Leittechnik

Unter rechnerbasierter Leittechnik fallen in dieser Richtlinie alle programmierbaren Geräte, bestehend aus den Komponenten der Ausrüstung (Hardware) mit der zugehörigen Dokumentation und der SW, die zur Ausführung von Funktionen zusammenwirken.

Redundanz

Das Vorsehen von alternativen (identischen oder diversitären) Elementen oder Teilsystemen, sodass jedes die geforderte Funktion unabhängig vom Zustand der anderen ausführen kann (nach IAEA NS-G-1.3).

Schutzziele

Um den Schutz vor der ionisierenden Strahlung aus dem Betrieb von Kernkraftwerken zu gewährleisten, sind die Schutzziele

- Kontrolle der Reaktivität
- Kühlung der Brennelemente
- Einschluss radioaktiver Stoffe
- Begrenzung der Strahlenexposition

bei allen nach dem Stand der Wissenschaft und Technik in Erwägung zu ziehenden Ereignisabläufen einzuhalten.

Sicherheitsnachweis

Alle dokumentierten Massnahmen des Betreibers, gestützt auf die entsprechenden Unterlagen der Lieferanten und allenfalls bestehende Begutachtungen, um das erforderliche Sicherheitsniveau zu gewährleisten, die von der HSK beurteilt werden.

Software (SW)

Die Software ist nebst der **Hardware** der zweite wesentliche Bestandteil für die Wirksamkeit eines programmierbaren Systems und besteht aus Programmen, Prozeduren, Regeln und die gesamte zugehörige Dokumentation (nach IEC 60880).

Zur Software gehört neben dem anwendungsspezifischen Teil auch ein anwendungsunabhängiger Teil (Basissoftware, Betriebsystem, Firmware usw.).

Zur Dokumentation gehören die Spezifikationen, die Beschreibung der Software-Architektur, das in einer bestimmten Programmiersprache (Hochsprache oder Assembler) oder einer anwendungsorientierten Sprache (z. B. Funktionsblockprogrammierung, graphische Programmierung,) geschriebene Quellprogramm, Konfigurationsdaten, die Ergebnisse der Verifizierungen und Validationen, die Beschreibung der **Werkzeuge** sowie die Beschreibung der Pläne für Entwicklung und Betrieb.

Systematischer Ausfall

Siehe Common Cause Failure, CCF.

Systemspezifikation oder **Spezifikation des leittechnischen Systems**

Spezifikation des rechnerbasierten leittechnischen Systems unter Berücksichtigung der Anforderungsspezifikation und den Merkmalen der einzusetzenden Leittechnik. Entspricht dem Begriff "computer system specification" in IEC 60880 (siehe auch Anhang 4 dieser Richtlinie).

Validierung

Test und Evaluation des integrierten rechnerbasierten Systems (Hardware und Software), um die Erfüllung der Auslegungsgrundlagen (Funktionelle Anforderungen, Auslegungskriterien, Leistungsmerkmale, Schnittstellen) sicherzustellen (nach IEC 60880).

Verifizierung

Die Verifizierung ist das Vorgehen, mit welchem bestimmt wird, ob das Ergebnis jeder Phase des Entwicklungsprozesses den Anforderungen aus der vorherigen Phase entspricht.

Werkzeuge

Werkzeuge sind Software-Programme, die für die Software-Entwicklung oder zur Leitanlagen-Konfiguration und deren Dokumentation eingesetzt werden. Dazu gehören Werkzeuge zur (formalen) Spezifikation, Software-Design, Code-Generierung (Compiler), Testgeneratoren usw.

Werkzeuge sind im Allgemeinen bereits existierende Software, deren Eignung für die entsprechende Anwendung nachgewiesen sein muss.

Zudem gibt es für die Projektierung auch Software-Programme zur Erstellung der Hardware-Dokumentation, z. B. Stromlaufpläne, Kabelpläne usw.

ANHANG 3

Kategorisierung und Klassierung der Funktionen, Systeme und Ausrüstungen

<table>
<tr><th colspan="3">Systemkategorie</th><th>Klassierung der leittechnischen Ausrüstungen</th><th colspan="2">Anforderungs-klasse</th><th>Sicherheits-relevanz</th></tr>
<tr><td colspan="3">HSK-R-30 / HSK-R-35</td><td>HSK-R-06
KEV Anhang 4 Ziffer 3</td><td colspan="2">HSK-R-46</td><td>HSK-R-46</td></tr>
<tr><td colspan="3">IAEA NS-R-1
(früher IAEA 50-C-D)</td><td>IEEE 323, 344</td><td colspan="2">IEC 61513</td><td>IEC 61226</td></tr>
<tr><td rowspan="3">Sicher-heits-relevante Systeme</td><td>Sicherheits-systeme</td><td>SA</td><td>1E sicherheits-technisch klassiert (elektrisch)</td><td rowspan="3">1</td><td rowspan="2"></td><td>Kategorie A</td></tr>
<tr><td rowspan="2">Sicherheits-bezogene Systeme</td><td rowspan="2">SB</td><td rowspan="3">0E nicht sicherheits-technisch klassiert (elektrisch)</td><td rowspan="2">2</td><td>Kategorie B</td></tr>
<tr><td></td><td>3</td><td>Kategorie C</td></tr>
<tr><td colspan="3">nicht sicherheitsrelevante Systeme</td><td colspan="2">Keine Anforderungsklasse</td><td>Keine Sicherheits-relevanz</td></tr>
</table>

Erläuterungen:

- In IEC 61513 werden die Kategorien A, B und C den Anforderungsklassen 1, 2 und 3 zugeordnet. Funktionen der Kategorie A dürfen nur in Systemen der Klasse 1, Funktionen der Kategorie B nur in Systemen der Klasse 1 und 2, Funktionen der Kategorie C können in Systemen der Klassen 1, 2 und 3 implementiert werden.
- Elektrische und leittechnische Ausrüstungen für Sicherheitssysteme sind 1E-klassiert gemäss KEV Anhang 4 Ziffer 3 und der Richtlinie HSK-R-06. Diese Ausrüstungen sind entsprechend zu qualifizieren. Die Zuordnung zu den Systemkategorien entspricht derjenigen in /1/, Anhang 1.
- Ausrüstungen zu leittechnischen Systemen, welche Funktionen der Kategorie A realisieren, sind als 1E zu qualifizieren.
- Leittechnische Funktionen, Systeme und Einrichtungen, deren Ausrüstungen nach KEV Anhang 4 Ziffer 3 und der Richtlinie HSK-R-06 1E-klassiert sind, müssen die Anforderungen der Anforderungsklasse 1 erfüllen.

Typische Beispiele zu den Kategorien A, B und C

Anforderungskategorie A:

- Leittechnische Systeme und Einrichtungen zur Auslösung von Sicherheitsfunktionen:
  . Reaktorschutzsystem (Protection System)
  . Leittechnik der Steuerung der Sicherheitssysteme (Engineered Safety Features Actuation Systems, ESFAS) wie z.B. die Kernnotkühlung
- Leittechnik der Sicherheits-Hilfssysteme (Safety System Support Features) wie z.B. die Notstromversorgung
- Wichtige Anzeige-, Registrier- und Bedienelemente zur Erfüllung von geplanten Operateur-Aktionen, die in den Vorschriften vorgesehen und zur Aufrechterhaltung der Reaktorsicherheit von Bedeutung sind

Kategorie B:

- Begrenzungs- und Regelsysteme, die das Anlageverhalten wesentlich beeinflussen (z.B. Reaktorregelung, Speisewasserregelung)
- Übrige Meldungen zu Funktionen der Kategorien A und B und den zugehörigen leittechnischen Systemen
- Überwachung der radioaktiven Abgaben
- Steuerung von Brennelementhandhabungseinrichtungen

Kategorie C:

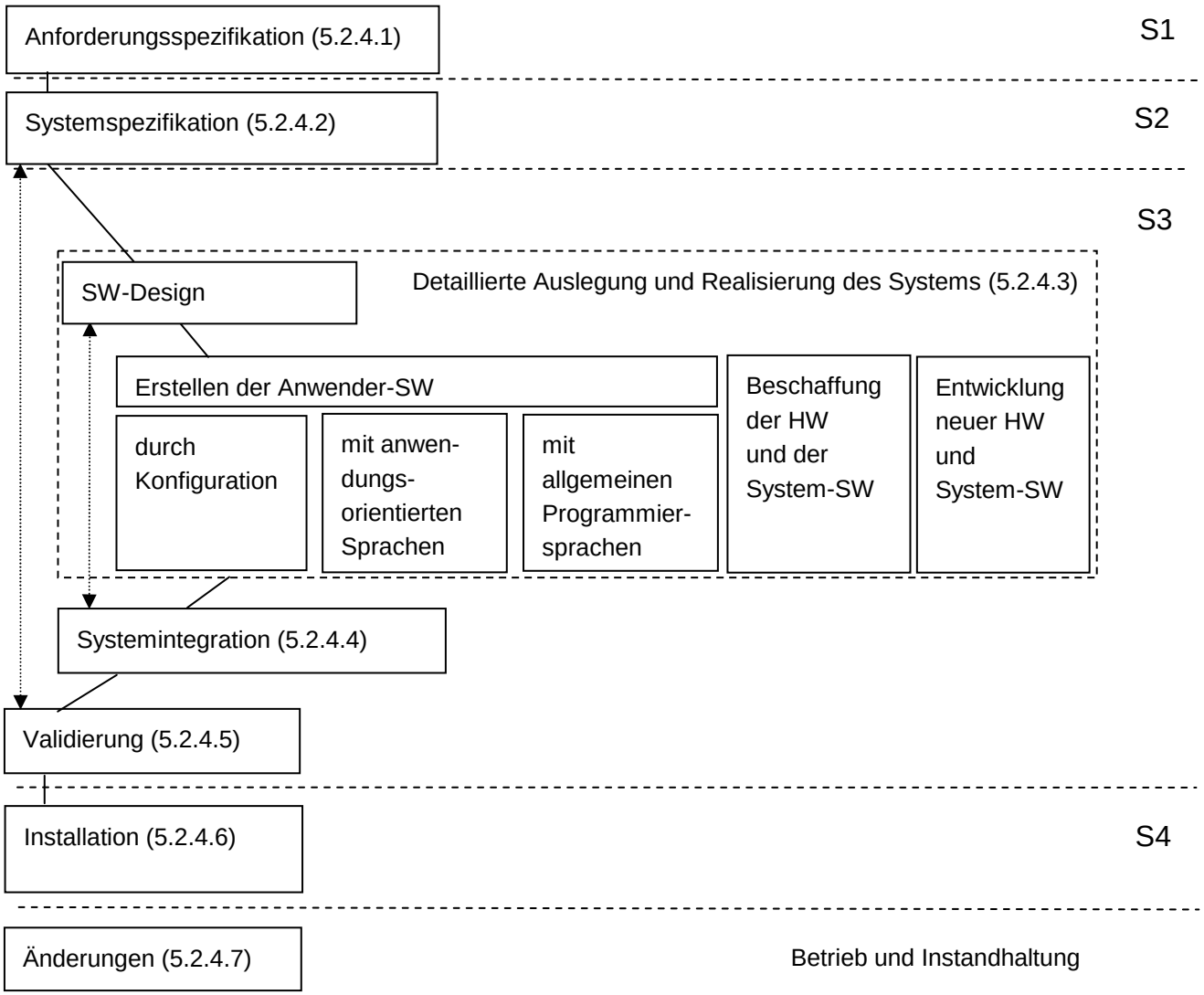
- Regelsysteme, die das Anlageverhalten mit beeinflussen
- Programmierbare Bedieneinrichtungen von Schutz- und Regelsystemen im Kommandoraum
- Datenverarbeitungssystem des Kommandoraumes (Anlage-Informationssystem, Prozessrechner), mit Funktionen wie z. B. Safety Parameter Display System (SPDS), Vorschriften auf Computer, Computerisierte Alarmsysteme, Störfallaufzeichnungssysteme
- Übrige sicherheitsbezogene Meldungen
- Kernüberwachungssysteme, Kernberechnungssysteme
- Brandmeldeanlagen
- Erdbebeninstrumentierung
- Zutrittskontrollsysteme
- Kommunikationsmittel, die zum Einsatz bei Störfällen und Unfällen vorgesehen sind
- Warn- und Lautsprecheranlagen

ANHANG 4

Lebenszyklus der Leitanlage

Die Darstellung des Lebenszyklus der Leitanlage entspricht derjenigen in IEC 61513, ergänzt mit Angaben aus IEC 60880, IEC 62138 und IEC 60987. Die Detailquerverweise auf diese IEC-Normen sind aus Anhang 5 ersichtlich.

In Klammern wird auf die Kapitel dieser HSK-Richtlinie verwiesen. Die Bezeichnungen S1 bis S4 zeigen die Zuordnung des Lebenszyklus zu den Hierarchiestufen der Richtlinie HSK-R-35.



ANHANG 5

Bezug der Anforderungen zu den einschlägigen Normen

Im Folgenden sind wichtige Anforderungen dieser Richtlinie aufgeführt. Die Referenzen zu den Normen beziehen sich auf die folgenden Revisionen: IEC 61513: 2001-03; IEC 60880: 1986; IEC 60880-2: 2000-12; IEC 62138: 2004-01; IEC 60987: 1989; IEC 61226: 1993.

Zur Anforderungsspezifikation sind als Hinweis einige wesentliche Merkmale der Leittechnik-Systeme mit den entsprechenden Stellen in den Normen aufgeführt. Diese Angaben zu den geforderten Merkmalen sind jedoch nicht vollständig. In den Normen sind weitere Anforderungen enthalten, die entsprechend den Anforderungs-Kategorien und Klassen zu beachten sind.

Kapitel	**Anforderung**	**Kat/Kl**			**Norm / Richtlinie**
5.1	Anforderungen aus der Kraftwerks-Anlage	A	B	C	IEC 61513, 5.1
5.1.1	Verfahrenstechnische Vorgaben und Randbedingungen	A	B	C	IEC 61513, 5.1.1, 5.1.2 und 5.1.3
	Verfahrenstechnische Beschreibung der Funktionen	A	B	C	IEC 61513, 5.2
5.2	Anforderungen an die Leitanlage	A	B	C	IEC 61513, 5.3 bis 5.5
5.2.1	Architektur der Leitanlage und Zuordnung der Leittechnik-Funktionen	A	B	C	IEC 61513, 5.3.1 und 5.3.2
	Trennung und Unabhängigkeit der Datenkommunikation	A	B	C	IEC 61615,5.3.1.3
	Funktionskategorisierung	A	B	C	IEC 61226
	Zuordnung der Systeme zu Anforderungsklassen 1, 2 oder 3	A	B	C	IEC 61513, 5.3.1.1
5.2.2	Anforderungen an die Sicherheitsüberprüfung für die Leitanlage	A	B	C	IEC 61513, 5.3.3
	Diversitätsanalyse, Common-Cause-Fehler	A			IEC 61513, 5.3.1.5, 5.3.3.1
	Überprüfung der Unabhängigkeit der Defence-in-Depth-Ebenen	A	B		[1])
5.2.3	Planung der Einführung der Leitanlage	A	B	C	IEC 61513, 5.4
		1	2	3	IEC 61513, 6.2
		A			IEC 60880
		A			IEC 60987
5.2.4	Anforderungen zu den Phasen des Lebenszyklus der Leitanlage	1	2	3	IEC 61513, 6.1
		A			IEC 60880, IEC 60880-2
			B	C	IEC 62138, (IEC 61508)
5.2.4.1	Anforderungsspezifikation	1	2	3	IEC 61513, 6.1.1

[1]) Die einschlägigen IEC-Normen enthalten keine direkten Angaben zur Umsetzung des Defence-in-Depth-Konzeptes für Leitanlagen. Generell sind die Forderungen in IAEA-NS-R-1, Kap. 5.69 und NS-G-1.1, Kap. 5.22 angegeben. Indirekt kann allerdings aus IEC 61513, Kap. 5.3.1.5 entnommen werden, dass analysiert werden soll, ob ein CCF zwischen verschiedenen Defence-in-Depth-Ebenen möglich ist.

Kapitel	Anforderung	Kat/Kl			Norm / Richtlinie
		A			IEC 60880
			B		IEC 62138, 6.3
				C	IEC 62138, 5.3
	Sicherheitsüberprüfung nach HSK-R-35, Anhang 9	A	B	C	HSK-R-35, Anhang 9
	Einzelfehlerkriterium	A	B		IEC 61226, 8.2.2
		1			IEC 61513, 6.1.1.2.1d
	Redundanz, Verfügbarkeit, Fehlertoleranz	1	2	3	IEC 61513, 6.1.1.2.1b
	Verhinderung der Fehlerausbreitung zu Systemen höherer Sicherheitsrelevanz	1	2	3	IEC 61513, 6.1.1.2.1c
	Verhinderung der Fehlerausbreitung zwischen Redundanzen von Systemen der Anforderungsklasse 1	1			IEC 61513, 6.1.1.2.1c
	Deterministisches Verhalten	1	2	3	IEC 61513, 6.1.1.2.2
	Hochwertiges deterministisches Verhalten	1 A			IEC 61513, 6.1.1.2.2c IEC 60880
	Angemessene Reaktion auf alle Zustände		2		IEC 61513, 6.1.1.2.2d/e
	Selbstüberwachung und Fehlertoleranz	1	2	3	IEC 61513, 6.1.1.2.3
	Selbstüberwachung konform mit IEC 60880 und IEC 60987	A			IEC 60880 IEC 60987
	Einrichtungen zur Prüfung	1	2	3	IEC 61513, 6.1.1.2.4
	Anlagesicherheit während Prüfungen gewährleistet	1			IEC 61513, 6.1.1.2.4d
5.2.4.2	Systemspezifikation	1	2	3	IEC 61513, 6.1.2
5.2.4.3	Detaillierte Auslegung und Realisierung	1	2	3	IEC 61513, 6.1.3
	Software	A			IEC 60880, IEC 60880-2
			B		IEC 62138,6.2, 6.4,6.5
				C	IEC 62138, 5.2, 5.4,5.5
	Hardware	A			IEC 60987, 5
5.2.4.4	Systemintegration	1			IEC 61513, 6.1.4
	Software	A			IEC 60880,
			B		IEC 62138,6.6
				C	IEC 62138,5.6
	Hardware	A			IEC 60987, 6
5.2.4.5	Validierung	1	2	3	IEC 61513, 6.1.5
	Software	A			IEC 60880
			B		IEC 62138,6.7
				C	IEC 62138,5.7
	Hardware	A			IEC 60987, 6 und 9

Kapitel	Anforderung	Kat/Kl			Norm / Richtlinie
5.2.4.6	Installation	1	2	3	IEC 61513, 6.1.6
	Software	A			IEC 60880
			B		IEC 62138,6.8
				C	IEC 62138,5.8
	Hardware	1			(IEC 60987, 8) IEC 60987, 9
5.2.4.7	Änderungen nach der Installation	1	2	3	IEC 61513, 6.1.7
	Software	A			(IEC 60880)
			B		IEC 62138,6.9,6.10
				C	IEC 62138,5.9,5.10
	Hardware	1			IEC 60987, 10
		1			IEC 60987, 11
5.2.5	Anforderungen an die Dokumentation	1	2	3	IEC 61513, 6.3
	Software	1			IEC 60880
	Hardware	1			IEC 60987
5.3	Qualifikation und Eignungsprüfung der Leitanlage	1	2	3	IEC 61513, 6.4
	Software	1			IEC 60880-2
			2	3	IEC 62138, (IEC 61508)
		A			IEC 60880-2
			B	C	IEC 62138
	Hardware	1			KTA 3503 IEEE 323, IEEE 344
			2	3	IEC 61508
5.4	Installation und Inbetriebnahme in der Kraftwerks-Anlage	1	2	3	IEC 61513, 7
	Software	A			IEC 60880
			B		IEC 62138,6.8
				C	IEC 62138,5.8
	Hardware	A			IEC 60987, 12
5.5	Betrieb und Instandhaltung der Leitanlagen	1	2	3	IEC 61513, 8
	Software	A			IEC 60880
			B		IEC 62138,6.9,6.10
				C	IEC 62138,5.9,5.10
	Hardware	A			IEC 60987, 10 und 12

Erläuterungen:

Kat/Kl: Kategorie (A, B oder C) oder System-Anforderungsklasse (1, 2 oder 3), siehe Anhang 3

ANHANG 6

Angaben zur einzureichenden Dokumentation

Die einzureichende Dokumentation basiert auf den Vorgaben der KEV Anhang 4 Ziffern 1 und 2. Es sind grundsätzlich die Unterlagen gemäss Richtlinie HSK-R-35 Anhang 3, einzureichen. Die Zuordnung der Systemkategorien SA und SB nach Richtlinie HSK-R-35 zu den Kategorien A, B und C nach IEC 61226 ist im vorstehenden Anhang 3 beschrieben.

Die folgenden Angaben sind als Präzisierungen und Ergänzungen bezüglich rechnerbasierter leittechnischer Systeme zu betrachten.

Hierarchiestufe	**Kapitel**	**Kat/ Kl**		
Frühzeitige Abklärungen				
Zweck, Absicht, Umfang und Art des Vorhabens	6.1	A	B	C
Grober Terminplan	6.1	A	B	C
Darlegung des Vorgehens zur Erfüllung der Kap. 5.1 und 5.2 dieser Richtlinie	6.1	A	B	C
Identifikation abweichender Vorgehensweisen	6.1	A	B	C
S1 Konzept				
Zusammenstellung und Darlegung der Vorgaben und der Randbedingungen	5.1.1	A	B	C
Verfahrenstechnische Beschreibung der Funktionen	5.1, 5.1.1	A	B	C
Architektur der Leitanlage und Zuordnung der Leittechnik-Funktionen zu den Teilsystemen	5.2.1	A	B	C
Zuordnung der Teilsysteme zum übergeordneten IT-Security-Konzept des Kraftwerkes	5.1.1, 5.2.1	A	B	C
Kategorisierungsanalyse der Leittechnik-Funktionen nach IEC 61226, und Angabe der Anforderungsklasse der Teilsysteme nach IEC 61513	5.2.1	A	B	C
Ergebnisse der Diversitätsanalyse	5.2.2	A		
Ergebnisse der Unabhängigkeit der Defence-in-Depth-Ebenen	5.2.2	A	B	
Planung für die Einführung der Leitanlage: Qualitätssicherungsplan einschliesslich Verifizierungsplan und Konfigurations-Managementplan, Systemintegrationsplan, Validierungsplan, Installations- und Inbetriebnahmeplan, Schulungsprogramm, Instandhaltungsplan	5.2.3	A	B	C
ev. Information über den Lieferanten und Dokumentation zum einzusetzenden leittechnischen System	6.2.1	A	B	
Anforderungsspezifikation	5.2.4.1	A	B	C
Sicherheitsüberprüfung nach Richtlinie HSK-R-35, Anhang 9	5.2.4.1	A	B	C
Anforderungen an die IT-Security der Leitanlage	5.2.4.1	A	B	C

Hierarchiestufe	**Kapitel**	**Kat/ Kl**		
S2 Auslegung				
Information über den Lieferanten und Dokumentation zum einzusetzenden leittechnischen System	6.2.2	A	B	
Systemspezifikation der Leitanlage mit übergeordneten Funktionsplänen	5.2.4.2	1	2	3
FMEA	5.2.4.2	1		
Deterministische Betrachtung bzgl. Fehlertoleranz/Fehlerauswirkungen	5.2.4.2		2	3
Ergebnisse der Verifikation der Diversitätsanalyse und der Unabhängigkeit der Defence-in-Depth-Ebenen	5.2.4.2	1	2	3
Nachweise zur generischen Qualifikation	5.3.1	1		
Belege zur Auslegung (z. B. EMV, Umgebungsbedingungen)	5.3.1		2	3
Nachweise zur anwendungsspezifischen Qualifikation	5.3.2	1		
Darlegungen zur anwendungsspezifischen Qualifikation	5.3.2		2	
Netzwerkplan zur Leitanlage bzw. den Leitanlagen (Darlegung der Kommunikationsverbindungen zwischen den Teilsystemen)	5.2.4.2	1	2	3
Verkabelungskonzept	5.2.4.2	1	2	
Spezifikationen zur räumlichen Separation, der Stromversorgung, Verkabelung, EMV- und Blitzschutzmassnahmen, der IT-Security, der Prüf- und Selbstüberwachungseinrichtungen	5.2.4.2	1	2	
Konzept der wiederkehrenden Prüfungen für die Leitanlage	5.2.4.2, 5.5.1	1		
S3 Ausführung				
Detailpläne (z. B. Kabellisten, Kabelanschlusspläne, Kabeltrassenpläne, Schrankbelegungspläne, Stromlaufpläne)	5.2.4.3	1	2	
Detaillierte Funktionspläne	5.2.4.3	A	B	
Verifikation der Korrektheit der Detailauslegung gegenüber der Anforderungsspezifikation bzgl. Funktionalität und Leistung	5.2.4.3	1	2	3
Dokumentation zur Systemintegration	5.2.4.4, 5.2.5	1	2	3
Konfigurations-Identifikations-Dokumentation	5.2.5	1	2	
Dokumentation der Ergebnisse der Systemvalidierung	5.2.4.5	1	2	3
Nachweise bzw. Unterlagen zur Nachqualifikation (falls zutreffend)	6.2.3	1		
S4 Inbetriebnahme				
Detaillierter Installationsplan, Angaben zur Gewährleistung der Anlagesicherheit, detaillierte Inbetriebsetzungspläne (bzw. Versuchsprogramme) und Prüfvorschriften	5.2.3, 5.4, 6.2.4, 5.2.4.6	1	2	3
Prüfergebnisse der Inbetriebnahme	5.4, 6.2.4	1	2	3
Vorschriften für wiederkehrende Prüfungen und für die Instandhaltung	5.5.1	1		
Weisung für die Durchführung von Änderungen	5.2.4.7, 5.5.2	1	2	3

Hierarchiestufe	**Kapitel**	**Kat/ Kl**		
Betrieb				
Ergebnisse der Validierung während des Betriebs	6.2.4			C
Vorgehen zur Durchführung von Änderungen an der Leitanlage	5.2.4.7	A	B	C
Analyse, Spezifikation und schriftliche Festlegung der Vorgehensweise für Änderungen für Systeme der Anforderungsklassen 1 und 2	5.5.2, 5.2.4.7	A	B	
Sicherheitsüberprüfung nach Richtlinie R-35, Anhang 9 bei Änderungen	5.5.2	A	B	C
Analyse, Spezifikation und schriftliche Festlegung der Vorgehensweise für Änderungen für Systeme der Anforderungsklasse 3, falls Funktionen der Kategorien A indirekt betroffen sein könnten.	5.5, 5.5.2, 5.2.4.7			C

Erläuterungen: Kat/Kl: Kategorie oder Anforderungsklasse gemäss Anhang 3 dieser Richtlinie (HSK-R-46).