Aufstellung von Kriterien und Kenngrößen zur deterministischen Prüfung der Eignung von Redesign-Komponenten für den Einsatz in der Sicherheitsleittechnik von Kernkraftwerken

GRS - 395

Gesellschaft für Anlagen-
und Reaktorsicherheit
(GRS) gGmbH

Aufstellung von Kriterien und Kenngrößen zur deterministischen Prüfung der Eignung von Redesign-Komponenten für den Einsatz in der Sicherheitsleittechnik von Kernkraftwerken

Robert Arians
Simone Arnold
Falk Lindner
Hervé Mbonjo
Claudia Quester
Dagmar Sommer

April 2017

Anhang auf beiliegender CD-ROM

Anmerkung:

Das diesem Bericht zugrunde liegende FE-Vorhaben 3611R01355 wurde im Auftrag des Bundesministeriums für Umwelt, Naturschutz, Bau und Reaktorsicherheit (BMUB) durchgeführt.

Die Verantwortung für den Inhalt dieser Veröffentlichung liegt beim Auftragnehmer.

Der Bericht gibt die Auffassung und Meinung des Auftragnehmers wieder und muss nicht mit der Meinung des Auftraggebers übereinstimmen.

GRS - 395
ISBN 978-3-944161-76-1

Hinweis

Im März 2016 wurde unter dieser Berichtsnummer aufgrund eines redaktionellen Versehens eine andere als die tatsächlich zur Veröffentlichung vorgesehene Berichtsfassung veröffentlicht. Dieser Bericht gibt die finale Berichtsfassung wieder.

Deskriptoren

Digitale Leittechnik, Diversitätsmerkmale, Ersatzbaugruppen, Lebenszyklus, Leittechniksystem, programmierbare und rechnerbasierte Komponenten, Redesign, Sicherheitsleittechnik, softwarebasierte Leittechnik

Kurzfassung

Diversität ist ein Auslegungsprinzip das zum Ziel hat, die Wahrscheinlichkeit eines gemeinsam verursachten Ausfalls von leittechnischen Systemen und ihren Komponenten zu verringern und ihre Zuverlässigkeit zu erhöhen. Im Verlauf dieses Projekts wurde eine Matrix der Diversitätsmerkmale entwickelt, die bei der Beurteilung der Diversität von programmierbaren und rechnerbasierten leittechnischen Komponenten und Systemen als Grundlage eingesetzt werden kann. Diese Matrix enthält Diversitätsmerkmale, die anhand des Lebenszyklus eines leittechnischen Systems und seiner Komponenten strukturiert sind, und zeigt deren Anwendbarkeit auf die technischen Komponenten und zusätzlichen Elemente eines generischen Leittechniksystems.

Abstract

Diversity is one of the key concepts in the challenge to improve the robustness of digital instrumentation and control (I&C) systems important to safety against common cause failures. In the cause of this project, a diversity matrix was established that can be used as a basis in the assessment of the diversity of digital I&C systems or their components. The matrix comprises diversity criteria which are structured according to the life cycle of I&C systems and their components, and shows their applicability to the technical components and additional items of a generic digital I&C system.

Inhaltsverzeichnis

1 Einleitung, Aufgabenstellung und Zielsetzung

Die leittechnischen Einrichtungen in deutschen Kernkraftwerken sind seit einigen Jahren Gegenstand umfangreicher Modernisierungsmaßnahmen. Ursachen für die Durchführung der Modernisierungsmaßnahmen sind eine erschwerte Ersatzteilbeschaffung bei den bisher eingesetzten konventionellen leittechnischen Einrichtungen, Kompatibilitätsprobleme der alten Leittechnik mit neuen maschinenbautechnischen Komponenten und die Möglichkeit, durch die Einführung programmierbarer oder rechnerbasierter leittechnischer Einrichtungen Prozessoptimierungen vornehmen zu können. Eine Alternative zur weitgehenden Umrüstung auf programmierbare oder rechnerbasierte leittechnische Komponenten bietet der Einsatz von sogenannten Redesign-Komponenten (im weiteren Dokument als Ersatzbaugruppen bezeichnet, siehe Abschnitt 2.1). Darunter werden im Rahmen des Vorhabens Neu- oder Nachbauten verstanden, die kompatibel zu den in Analogtechnik ausgeführten Originalen sind und den gleichen Anforderungen genügen müssen. Die Ersatzbaugruppen sind jedoch aus moderner, ggf. auch mittels programmierbarer oder rechnerbasierter Elektronik gefertigt und werden ihrem Zweck entsprechend neu entworfen.

Das Reaktorschutzsystem ist bislang in allen deutschen Leistungsreaktoren in konventioneller, „festverdrahteter“ Leittechnik (Analogtechnik) aufgebaut. Im Zuge des forcierten Ausstiegs aus der Kernenergie bis 2022 sind entgegen ursprünglicher Planungen keine Umrüstungen des Reaktorschutzsystems auf programmierbare oder rechnerbasierte Leittechnik mehr zu erwarten. Im Rahmen der Restlaufzeit der Kernkraftwerke ist jedoch mit kontinuierlicher Ersatzteilbeschaffung und Austausch an den leittechnischen Einrichtungen auch durch Ersatzbaugruppen zu rechnen. Diese Komponenten kommen nicht nur für das Reaktorschutzsystem, sondern auch für andere Teilsysteme des Sicherheitssystems und weitere Systeme etwa der Sicherheitsebene 2 in Frage. Da eine Vielzahl der hierbei betroffenen leittechnischen Funktionen auch bei langfristigem Nichtleistungsbetrieb und deutlich über den Abschaltzeitpunkt der Kernkraftwerke hinaus während der Stilllegung und dem Rückbau benötigt werden, haben solche Austauschmaßnahmen noch für einen langen Zeitraum eine sehr hohe sicherheitstechnische Bedeutung.

Die in der Leittechnik eingesetzten Baugruppen und Bauteile werden stetig weiterentwickelt und dem Stand der Technik angepasst. Dies führt dazu, dass die in der Sicher-

heitsleittechnik der Kernkraftwerke bislang eingesetzten Original-Baugruppen und Bauteile nach und nach nicht mehr hergestellt werden. Um den bestehenden Bedarf zu decken, bieten mittlerweile mehrere Firmen Ersatzbaugruppen an.

Bislang gibt es noch keine umfassenden und systematischen Informationen dazu, welche Typen von Baugruppen und Bauteilen in welchen Systemen ausgetauscht werden, welche Technologien dabei im Einzelnen zum Einsatz kommen und wie der Austausch realisiert wird. Darüber hinaus gibt es noch keine Bewertungskriterien und Kenngrößen speziell für den Einsatz von Ersatzbaugruppen in der Sicherheitsleittechnik von Kernkraftwerken, insbesondere für Ersatzbaugruppen, in denen softwarebasierte Technik verbaut wird. Bislang wird bei der Beurteilung der Komponenten auf das vorhandene Regelwerk zurückgegriffen. Doch gerade für die programmierbaren oder rechnerbasierten Anteile in Ersatzbaugruppen sollte z. B. nach einer notwendigen Diversität gefragt werden, um etwa dem Potential systematischer Ausfälle zu begegnen, oder nach speziellen Merkmalen, die für Zuverlässigkeitsaussagen dieser Komponenten genutzt werden könnten.

Die Zielstellung des Vorhabens ist deshalb, Anforderungen für den Einsatz von Ersatzbaugruppen in der Sicherheitsleittechnik von Kernkraftwerken zu entwickeln und nach Kriterien und Kenngrößen zu suchen, um Ersatzbaugruppen zu bewerten. Dabei sollen im Rahmen eines Unterauftrags an das ISTec auch Anforderungen an die Typprüfungen einbezogen werden. Dabei sollen spezifische Vorgehensweisen, die bei der Prüfung von Ersatzbaugruppen mit programmierbaren oder rechnerbasierten Bauteilen anzuwenden sind, bewertet und Typprüf-Anforderungen an Ersatzbaugruppen abgeleitet werden. In einem weiteren Arbeitspaket soll das ISTec im Unterauftrag die Machbarkeit einer Ausdehnung der beim ISTec angewandten Komplexitätsmessung auf Ersatzbaugruppen mit programmierbaren oder rechnerbasierten Bauteilen untersuchen.

In den Vorhaben 3610R01361 „Entwicklung und Einsatz von Analysemethoden zur Beurteilung softwarebasierter leittechnischer Einrichtungen in deutschen Kernkraftwerken“ /GRS15a/ und 3611R01620 „Sicherheitstechnische Analyse zum Einsatz und Betrieb elektrotechnischer Einrichtungen in deutschen Kernkraftwerken, Überwachung und Schutz gegen sicherheitstechnisch bedeutsame Einwirkungen aus dem Verbundnetz sowie anderen äußeren Quellen“ /GRS15b/ wurde die Betriebserfahrung mit programmierbaren oder rechnerbasierten Einrichtungen unterhalb der Meldeschwelle erfasst und analysiert. Ergebnisse dieser Projekte werden zur Definition von Diversitätsmerkmalen ebenfalls mit einbezogen.

Die erarbeiteten Ergebnisse und Zwischenergebnisse wurden im Rahmen einer Veröffentlichung beim International Automation Congress 2014 im Oktober 2014 in Budapest präsentiert und dem interessierten Fachpublikum zugänglich gemacht /GRS14b/. Die gewonnenen Erkenntnisse erweitern die Kompetenz der GRS z. B. für sicherheitstechnische Bewertungen. Außerdem werden die Erkenntnisse aus diesem Vorhaben im Rahmen von Stellungnahmen, in Arbeitsgremien und Fachausschüssen verwendet und besitzen daher auch einen hohen generischen Wert. Die GRS ist im RSK Ausschuss Elektrische Einrichtungen vertreten. Darüber hinaus war sie u. a. in den Arbeitsgremien zur Überarbeitung der KTA Regeln 3501 (zurzeit im Gründruck) /KTA14b/, 3503 /KTA13/ und 3507 /KTA14a/ beteiligt.

Im Rahmen des Vorhabens wurden fünf verschiedene Arbeitspunkte aufgestellt, von denen drei von der GRS bearbeitet wurden. Die übrigen zwei Arbeitspunkte wurden unabhängig von den Arbeiten der GRS von der TÜV Rheinland ISTec GmbH betrachtet. Der Arbeitsbericht der TÜV Rheinland ISTec GmbH /IST14/ wird gemeinsam mit diesem Bericht dem Auftraggeber zur Verfügung gestellt.

Die für die GRS relevanten Arbeitspakete sind in den folgenden Abschnitten beschrieben.

1.1 Arbeitspaket 1: Aufarbeitung des für das Vorhaben relevanten Standes von Wissenschaft und Technik

Der für die Bearbeitung des Vorhabens relevante Stand von Wissenschaft und Technik wird in diesem Arbeitspaket systematisch aufbereitet. Dazu sind insbesondere folgende Fragen zu beantworten:

- Welche bislang in analoger Technik ausgeführten Typen von Baugruppen aber auch anderer Komponenten werden durch Ersatzbaugruppen (analog oder digital) ersetzt?
- Welche Typen von Ersatzbaugruppen (Steckerkompatibilität, Funktionskompatibilität, Programmierbarkeit für verschiedene Funktionen) werden realisiert?
- Welche Technologie (FPGA, ASICs etc.) kommt bei Ersatzbaugruppen zum Einsatz?

- Wie werden die Ersatzbaugruppen qualifiziert?
- In welchen deutschen Anlagen werden in welchen Systemen Ersatzbaugruppen eingesetzt?
- Gibt es bereits Betriebserfahrung mit diesen Ersatzbaugruppen?

Die Ermittlung und Aufbereitung des Standes von Wissenschaft und Technik bezieht sich u. a. auf:

- Bisherige Arbeiten (Methoden, Daten, Vorgehensweisen und Ergebnisse) der GRS auch im Rahmen der Vorhaben 3610R01361 /GRS15a/, RS1180 /GRS10/
- Feststellung des nationalen und internationalen Standes von Wissenschaft und Technik für die Erarbeitung von Anforderungen an Ersatzbaugruppen und die Ermittlung von Diversitätsmerkmalen
- Wichtige Untersuchungen und Ergebnisse anderer Stellen, beispielsweise NUREG-0800 /NUR07/, NUREG-6680 /NUR00/, NUREG-7007 /NUR10/, NUREG-6303 /NUR94/
- Sichtung der aktuellen, relevanten Informationssysteme
- Ergebnisse aktueller Beratungen in einschlägigen nationalen und internationalen Gremien, z. B. RSK AG ERL
- Besuch von internationalen Fachtagungen, wie der Eurosafe und beispielsweise IAEA- bzw. OECD-Meetings

Der ermittelte, für das Vorhaben relevante Stand von Wissenschaft und Technik wird zusammen mit den weiteren Vorhabensergebnissen zum Abschluss des Vorhabens in einem Bericht aufbereitet, dokumentiert und veröffentlicht.

1.2 Arbeitspaket 2: Entwicklung von Anforderungen für den Einsatz von Ersatzbaugruppen in der Sicherheitsleittechnik

In diesem Arbeitspunkt sollen Anforderungen an Ersatzbaugruppen entwickelt werden, die für einen Einsatz in der Sicherheitsleittechnik von Kernkraftwerken vorgesehen sind,

und es sollen Bewertungskriterien für diese Baugruppen erarbeitet werden. Wesentliche Aspekte hierbei sind:

- Erarbeitung von Anforderungen an den Einsatz speziell von Ersatzbaugruppen in der Sicherheitsleittechnik von Kernkraftwerken
- Betrachtung der vorhandenen Betriebserfahrung und des Aufbaus speziell von Ersatzbaugruppen (soweit Unterlagen zugänglich sind)
- Durchführung einer FMEA für beispielhafte Ersatzbaugruppen (soweit Unterlagen zugänglich sind)
- Überprüfung, ob für Ersatzbaugruppen generell ein CCF unterstellt werden muss
- Ausarbeitung von Bedingungen, unter denen für Ersatzbaugruppen Diversität gefordert werden muss bzw. verzichtbar ist.

1.3 Arbeitspaket 3: Definition von Diversitätsmerkmalen und Erarbeitung Kriterien und Kenngrößen

Aufbauend auf dem zweiten Arbeitspaket sollen Diversitätsmerkmale von programmierbaren oder rechnerbasierten Komponenten und Baugruppen ermittelt und definiert werden. Es wird zu beurteilen sein, welche dieser Diversitätsmerkmale im Einzelfall besonders relevant sind, um Baugruppen in diversitären Systemen einzusetzen.

Dazu sollen insbesondere aus allen möglichen Diversitätsmerkmalen diejenigen ausgewählt werden, die für die Zuverlässigkeit relevant sind. Für jedes dieser Diversitätsmerkmale werden anschließend mögliche Merkmalseigenschaften bestimmt, d. h. es wird ermittelt, in welchen Ausprägungen das Merkmal vorliegen kann.

Zur Ermittlung und Definition der Diversitätsmerkmale und Merkmalseigenschaften werden die in den Arbeitspaketen 1 und 2 (siehe Kapitel 4) gewonnenen Ergebnisse herangezogen sowie die Erkenntnisse der US N.R.C. /NUR94/, /NUR00/, /NUR07/, /NUR10/) berücksichtigt und die Ergebnisse aus den vorangehenden Projekten RS1180 /GRS10/ und 3610R01361 /GRS15a/ der GRS mit einbezogen.

Anhand der definierten Diversitätsmerkmale wird erarbeitet, inwieweit aufgrund dieser Merkmale eine Aussage über die Diversität von programmierbaren oder softwarebasierten Systemen getroffen werden kann. Hierzu sind folgende Arbeitsschritte vorgesehen:

- Auswahl einer beispielhaften Ersatzbaugruppe
- Selektion der auf die gewählte Baugruppe zutreffenden Diversitätsmerkmale und Merkmalseigenschaften
- Bewertung der Diversitätsmerkmale bezüglich ihrer Relevanz für die Baugruppe, insbesondere soll ermittelt werden, bezüglich welcher Merkmale das Vorliegen von Diversität unverzichtbar ist
- Bewertung, welche Kombination von Merkmalseigenschaften eine Minimalanforderung für die Diversität der Baugruppe darstellt
- Erarbeitung von Kriterien und Kenngrößen für den Einsatz von Ersatzbaugruppen

2 Begriffe

2.1 Begriffe Redesign, Design und Ersatzbaugruppe

Gespräche mit Betreibern, Behörden und Herstellern zeigen, dass der Begriff Redesign nicht eindeutig verwendet wird und unterschiedliche Definitionen benutzt werden.

Der BMUB versteht unter dem Begriff Redesign die Nachentwicklung und den Nachbau von ausgewählten Leittechnik-Komponenten als kostengünstige Alternative zum Austausch von Leittechnik-Teilsystemen /RSK12/. Danach ist als Redesign die pin- und funktionskompatible Neuentwicklung einer nicht mehr lieferbaren Baugruppe zu verstehen, die in einem vorgegebenen System anstelle des Originalteils eingesetzt werden kann. Eine weitere Unterteilung je nach Reichweite der Neufertigung wird von Seiten des BMUB in drei Gruppen vorgenommen, wobei der Gruppe 1 Kopien bestehender Baugruppen zugeordnet werden, die Gruppe 2 Komponenten auf Basis moderner programmierbarer Bausteine beschreibt und die Komponenten der Gruppe 3 im Gegensatz dazu statt programmierbarer Bausteine moderne analoge Bauteile beinhalten.

Im Gegensatz zu der Definition des BMUB verwendet der VGB Powertech e.V. folgende Begriffsdefinition /VGB11/:

Den Begriff Redesign verwendet der VGB Powertech e.V., wenn ein Ersatz für ein Gerät entwickelt werden muss, welches nicht mehr reparierbar ist, beziehungsweise wenn es für das Gerät keinen Ersatz am Markt gibt. Der Begriff Redesign wird dabei im Unterschied zu der Gruppierung im Beratungsauftrag des BMUB für eine funktions-, Pin- und steckkompatible Substitution mit ggf. veränderter Aufbautechnik verwendet, während der Begriff Design für eine Substitution mit darüber hinaus auch veränderten technischen Daten oder Veränderungen in der Funktionalität verwendet wird.

Unter Design versteht der VGB Powertech e.V., wenn durch eine Geräteabkündigung die am Markt vorhandenen Ersatzgeräte nicht mehr kompatibel beschaffbar sind und für den Einsatz ein neues Gerät entwickelt und qualifiziert werden muss. Dieser Fall trat laut VGB Powertech e.V. in einem Fall auf, nämlich bei der Entwicklung einer Vierleiterbox für den Ersatz von Vierleiter-Messumformern durch Zweileiter-Messumformer /VGB11/.

Darüber hinaus unterscheidet die RSK nach Vorgabe des BMUB zwischen drei verschiedenen Gruppen unter den Design/Redesign-Produkten /RSK12/.

Die **Gruppe 1** sind 1:1 Nachbauten bestehender Baugruppen und Komponenten (Kopien). Dabei wird ein Nachbau erzeugt, der sich in seinen elektrischen Anschlussgrößen, dem Funktionsumfang, dem Stromlaufplan, dem (Platinen-)Layout und den physischen Abmessungen nicht oder nur unwesentlich vom Original unterscheidet.

In **Gruppe 2** lassen sich Baugruppen und Komponenten einordnen, die auf Basis moderner programmierbarer Bausteine so nachgefertigt werden, dass zwar die elektrischen Anschlussgrößen, der Funktionsumfang und die physischen Abmessungen sowie die Pin-Kompatibilität zu den Originalen gegeben ist, Stromlaufplan, Platinenlayout und das Entwurfskonzept sind aber aufgrund der eingesetzten Technologie zum Original grundlegend verschieden.

Der **Gruppe 3** können solche Baugruppen und Komponenten zugeordnet werden, die hinsichtlich elektrischer Anschlussgrößen, des Funktionsumfangs und der physischen Abmessungen kompatibel sowie pinkompatibel sind, statt programmierbarer Bausteine aber ausschließlich moderne Analogbauteile auf weiterentwickelten Platinen verwenden.

In Gesprächen mit mehreren Betreibern stellte sich heraus, dass in der Praxis von Betreibern Definitionen des Begriffes Redesign verwendet werden, die von der VGB-Definition abweichen. Teilweise wird der Begriff Redesign nur dann verwendet, wenn die neue Baugruppe von einem anderen Hersteller gefertigt wird und von Herstellerseite eine Abkündigung für die ursprüngliche Baugruppe vorliegt. Nimmt der Hersteller der ursprünglichen Baugruppe eine Änderung vor, wird von einer Variante oder einem Upgrade gesprochen. Ein Betreiber nannte auch die Abweichung von der ursprünglichen Herstellerspezifikation als Merkmal einer Redesign-Baugruppe. Werden zusätzliche Funktionen auf der neuen Baugruppe realisiert oder die Funktionen mehrerer Baugruppen auf einer Baugruppe vereint, wird eher von Design als von Redesign gesprochen. Laut Betreiberauskunft tritt in der Praxis der Fall, dass ein Redesign-Bauelement pinkompatibel ist, fast nicht auf. In fast allen Fällen müssen Verdrahtungsänderungen vorgenommen werden beziehungsweise Kodierbrücken gesteckt werden.

Weitere im Zusammenhang mit dem Nachbau von Baugruppen wichtige Begriffe finden sich in der KTA 3507. Dort wird von Original-Bauelementen im Unterschied zu Äquivalenz-Bauelementen gesprochen. In Anhang C der KTA 3507 werden Bauelemente in die Klassen K-I bis K-IV kategorisiert /KTA14a/. Die dort verwendete Kategorisierung ist in Tabelle 2.1 dargestellt.

Tab. 2.1 Kategorisierung von Bauelementen in KTA 3507, Anhang C /KTA14a/

Klasse	Bezeichnung	Definition
K-I	Original/Äquivalenz	Original-/Äquivalenz-Bauelemente werden vom Hersteller der Komponente in der Stückliste benannt. Die Verifikation der Eignung des Bauelements erfolgt im Rahmen des Qualitätsmanagementsystems des Herstellers durch dessen Werkssachverständigen. Die Validation der Eignung des Original-/Äquivalenz-Bauelements hinsichtlich des spezifischen Einsatzzwecks erfolgt im Rahmen der Typprüfung der Komponente.
K-II	gleicher Typ wie Original/Äquivalenz, jedoch anderer Bauelementhersteller	Wie K-I, jedoch ein anderer Hersteller des Bauelementes Die Verifikation und Validation der Eignung des Bauelements erfolgt im Rahmen des Qualitätsmanagementsystems durch den Werkssachverständigen nach KTA 3507 und wird durch die Werksprüfbescheinigung der Komponente bestätigt. Der Einsatz des Bauelements ist einer typprüfenden Stelle mitzuteilen.
K-III	anderer Bauelementtyp mit gleichwertigen Eigenschaften	Die Typbezeichnung kann von dem Stücklisteneintrag nach K-I abweichen. Die technischen Daten des Bauelements sind aber gleichwertig zum Original-bzw. Äquivalenzbauelement (K-I) insbesondere hinsichtlich folgender Kriterien: elektrische Daten Geometrie Funktionsprinzip Aufbau/Technologie Material Übertragungsverhalten Durch den Einsatz dieses K-III-Bauelements ergeben sich keine Auswirkungen auf die technischen Daten und Eigenschaften des Gerätes. Die Verifikation und Validation der Eignung des Bauelements erfolgt im Rahmen des Qualitätsmanagementsystems durch den Werkssachverständigen nach KTA 3507 und wird durch die Werksprüfbescheinigung bestätigt. Die Vorgehensweise zur Validation der Eignung des Bauelements ist einer typprüfenden Stelle anzuzeigen.
K-IV	anderer Bauelementtyp, andere Eigenschaften	Die Typbezeichnung und die technischen Daten des Bauelements weichen von denen des Stücklisteneintrags ab. Die Verifikation der Eignung des Bauelements erfolgt im Rahmen des Qualitätsmanagementsystems durch den Werkssachverständigen nach KTA 3507 und wird durch die Werksprüfbescheinigung bestätigt. Die Validation der Eignung des Bauelements hinsichtlich des spezifischen Einsatzzwecks erfolgt im Rahmen einer Typprüfung bzw. einer ergänzenden Typprüfung des Gerätes.

In diesem Vorhaben sollen die Probleme betrachtet werden, die entstehen können, wenn eine längerfristig eingesetzte Baugruppe durch eine modifizierte Baugruppe ersetzt wird, ohne dass ein komplettes System erneuert wird. Für die Analyse der GRS ist es daher nicht von Bedeutung, aus welchem Grund eine Baugruppe ersetzt wird. Es spielt keine Rolle, ob die neue Baugruppe vom selben Hersteller produziert wird, oder ob eine Geräteabkündigung vorliegt. Da der Begriff Redesign von verschiedenen Organisationen bereits definiert und verwendet wurde, aber keine einheitliche Definition vorliegt, wird in diesem Bericht nicht von Redesign-Baugruppen sondern allgemein von Ersatzbaugruppen gesprochen.

Unter Ersatzbaugruppen versteht die GRS jegliche Baugruppen, die durch Modifizierung bisher eingesetzter Baugruppen entstehen und diese ersetzen bzw. ersetzen sollen, unabhängig davon, ob es sich um Nachbauten oder Nachfolgemodelle handelt.

2.2 Begriff softwarebasierte Leittechnik

Des Weiteren wird vom VGB Powertech e.V. der Begriff softwarebasierte Technik verwendet. Dieser Begriff ist nach Ansicht der GRS nicht eindeutig, da unter softwarebasierter Technik sowohl im herkömmlichen Sinne programmierbare Technologien (solche, die einen Prozessor besitzen) als auch nutzerprogrammierbare Hardware (PLDs wie FPGA und ASICs) verstanden werden können. Nach Ansicht des VGB Powertech e.V. werden PLDs nicht zu softwarebasierter Technik gezählt, da sie nur einmalig bei ihrer Herstellung programmiert werden, zum Beispiel durch Setzen der so genannten Look-Up-Table, und danach in der Regel nicht mehr verändert werden. Nichtdestotrotz ist es möglich auch später noch die Programmierung gezielt zu verändern /TÜV10/. Daher zählt die GRS auch PLDs zu den softwarebasierten Komponenten. Diese Tatsache sorgt immer wieder für Diskussionen. Um solche zu vermeiden, vermeidet die GRS den Begriff „softwarebasiert“ und verwendet in Anlehnung an die KTA 3501 /KTA14b/ sowie die Interpretationen zu den Sicherheitsanforderungen an Kernkraftwerke /BMU13/ die Begriffe „nicht programmierbare“, „programmierbare“ und „rechnerbasierte leittechnische Einrichtungen“.

2.3 Weitere Begriffe und Abkürzungen

Im Folgenden wird ein Überblick über weitere, im Dokument verwendete Begriffe und Abkürzungen in tabellarischer Form gegeben.

Tab. 2.2 Übersicht über die im Bericht verwendeten Begriffe und Abkürzungen

Begriff oder Abkürzung	Erläuterung
ASIC	Ein ASIC (application-specific integrated circuit) ist eine elektronische Schaltung, die als integrierter Schaltkreis realisiert wurde. Im Normalfall wird ein ASIC bei der Herstellung einmalig programmiert. Eine nachträgliche Manipulation ist daher schwierig, wenngleich nicht ausgeschlossen. Ein ASIC wird kundenspezifisch produziert.
CCF	Bei einem Common Cause Failure (gemeinsam verursachter Ausfall) handelt es sich um die gleichzeitige Nichtverfügbarkeit von zwei oder mehreren Strukturen, Systemen oder Komponenten infolge eines einzelnen spezifischen Ereignisses oder Grundes.
Configware	Modifizierbare Datei zur Konfiguration rekonfigurierbarer Bauelemente wie z. B. FPGAs.
cPLD	Unter cPLD (complex Programmable Logic Device) versteht man eine Weiterentwicklung von universellen PAL (Programmable Array Logic). Hier werden mehrere universelle PAL zu einer Blockstruktur zusammengefasst und über eine programmierbare Verbindungsmatrix verbunden.
Dissimilarität	Eigenschaft eines Geräts hinsichtlich Hardware, Software, Entwicklungswerkzeugen, Entwicklungsteams, Fertigung, Test und Instandhaltung hinreichend unähnlich bzw. ungleichartig zu anderen Geräten zu sein. Anmerkung 1: Die Dissimilarität stellt damit eine Untermenge der Diversität dar. Anmerkung 2: Ziel ist es, unabhängige Systeme oder Teilsysteme (unabhängige leittechnische Systeme) so aufzubauen, dass deren sicherheitstechnisch unverzichtbare Funktionen auch beim postulierten systematischen Versagen von einem der unabhängigen Systeme oder Teilsysteme erhalten bleiben. Dazu muss die Dissimilarität in den zur Fehlerbeherrschung wichtigen Eigenschaften aufgezeigt werden. /VDI11/
Diversität	Vorhandensein von zwei oder mehr redundanten Systemen oder Komponenten, um eine bestimmte Funktion durchzuführen, wobei die verschiedenen Systeme oder Komponenten derartig unterschiedliche Eigenschaften haben, dass die Möglichkeit von Versagen aufgrund gemeinsamer Ursache verringert wird. /DIN13/

Begriff oder Abkürzung	Erläuterung
Ersatzbaugruppe	Jegliche in irgendeiner Art modifizierte Baugruppe, die als Ersatz für eine eingesetzte Baugruppe verwendet wird. /DIN10a/
Failure Mode	Ein Failure Mode (Fehlzustand) bezeichnet den Zustand einer Einheit, in dem sie unfähig ist, eine geforderte Funktion zu erfüllen, wobei die durch Wartung oder andere geplante Handlungen bzw. durch das Fehlen äußerer Mittel verursachte Funktionsunfähigkeit ausgeschlossen ist. Ein Fehlzustand ist oft das Ergebnis eines Ausfalls der Einheit selbst, er kann aber auch ohne vorherigen Ausfall vorhanden sein. /DIN06/
Firmware	Von Herstellerseite in die Hardware fest eingebaute Datei (read-only Software), welche durch den Anwender nicht oder nur mit speziellen Mitteln rekonfigurierbar ist und definierte gerätespezifische Funktionen erbringt.
FPGA	Ein FPGA (Field Programmable Gate Array) ist ein integrierter Schaltkreis, in den eine logische Schaltung, üblicherweise über eine look-up-table, programmiert werden kann. FPGA weisen im Allgemeinen eine einfache Struktur auf und besitzen keinen Mikroprozessor. Die Programmierung kann auf einem steckbaren Speicher, z. B. EEPROM gespeichert werden. Durch Änderung der Einträge in der look-up-table kann die Programmierung des FPGA geändert werden.
FMEA	Die Fehlzustandsart- und -auswirkungsanalyse (Failure mode and effects analysis, FMEA) ist ein systematisches Vorgehen bei der Analyse eines Systems, um mögliche Fehlzustandsarten, ihre Ursachen und ihre Auswirkungen auf das Systemverhalten zu ermitteln. /DIN06/
Funktionale Diversität	Anwendung der Diversität auf der Funktionsebene (z. B. Ableitung eines Abschaltkriteriums sowohl aus Druck- als auch Temperaturgrenzwerten). /DIN10a/
PLD	Ein PLD (Programmable Logic Device) ist ein einfacher über eine Matrix programmierbarer Schaltkreis, einige der ersten PLD wurden unter dem Firmennamen PAL (Programmable Array Logic) bekannt.
Runtime Environment	Programm, welches die Anwendungssoftware, die nicht direkt im Betriebssystem lauffähig ist, ausführbar macht.

Begriff oder Abkürzung	Erläuterung
Systemsoftware	Für ein bestimmtes Rechnersystem erstellte Software, um Entwicklung, Betrieb und Modifikation des Systems und der zugehörigen Programme zu erleichtern. Die Systemsoftware schließt das Betriebssystem, d. h. die Software zur Verwaltung der Systemressourcen (z. B. Arbeitsspeicher, Festplatten) des Rechnersystems, ein. Das Betriebssystem dient als Schnittstelle zwischen den Hardwarekomponenten des Rechnersystems bzw. deren Firmware und der Anwendungssoftware.
Zuverlässigkeit	Wahrscheinlichkeit, dass ein Gerät, System oder eine Einrichtung seine beabsichtigte Funktion für eine spezifizierte Zeit unter festgelegten Betriebsbedingungen zufriedenstellend ausführt. Anmerkung: Die Zuverlässigkeit eines rechnerbasierten Systems umfasst die Zuverlässigkeit seiner Hardware, die üblicherweise quantifiziert ist, und die Zuverlässigkeit seiner Software, die üblicherweise ein qualitatives Maß darstellt, weil es im Allgemeinen keine anerkannten Mittel für eine Quantifizierung gibt./DIN10a/

3 Aufbereitung des für das Vorhaben relevanten Standes von Wissenschaft und Technik

Im Gegensatz zum Reaktorschutzsystem wird in vielen betrieblichen leittechnischen Einrichtungen bereits programmierbare und rechnerbasierte Technik eingesetzt. Es ist zu erwarten, dass zumindest für die sicherheitstechnisch wichtigen Funktionen, die auch bei langfristigem Nichtleistungsbetrieb, sowie während Stilllegung und Rückbau noch benötigt werden, mit einer kontinuierlichen Erneuerung der vorhandenen leittechnischen Einrichtungen und mit verstärktem Einsatz von Ersatzbaugruppen zu rechnen ist. Eine intensive Befassung mit diesen Ersatzbaugruppen, insbesondere jenen, auf denen programmierbare oder rechnerbasierte Bauelemente zum Einsatz kommen (Digitaltechnik wie ASIC, FPGA, etc.), ist erforderlich. Im Folgenden wird der derzeitige Stand von Wissenschaft und Technik ermittelt und beschrieben. Dazu werden folgende Fragen beantwortet:

- Welche bislang in analoger Technik ausgeführten Typen von Baugruppen aber auch andere Komponenten werden durch Ersatzbaugruppen (analog oder digital) ersetzt?
- Welche Typen von Ersatzbaugruppen (Steckerkompatibilität, Funktionskompatibilität, Programmierbarkeit für verschiedene Funktionen) werden realisiert?
- Welche Technologie (FPGA, ASICs, etc.) kommt bei Ersatzbaugruppen zum Einsatz?
- Wie werden die Ersatzbaugruppen qualifiziert?
- In welchen deutschen Anlagen werden in welchen Systemen Ersatzbaugruppen eingesetzt?
- Gibt es bereits Betriebserfahrung mit Ersatzbaugruppen?

3.1 Welche bislang in analoger Technik ausgeführten Typen von Baugruppen aber auch andere Komponenten werden durch Ersatzbaugruppen (analog oder digital) ersetzt?

Auf Veranlassung der RSK wurden vom VGB Powertech e. V. Untersuchungen zur Ersatzbeschaffung von technischen Einrichtungen der E- und Leittechnik in Kernkraftwerken durchgeführt. Dabei wurde insbesondere die Beschaffung von Ersatzbaugruppen[1] in technischen Einrichtungen untersucht. An der Untersuchung waren insbesondere die EnBW Kernkraft GmbH (EnKK) und die VENE GmbH beteiligt. Substitutionen durch Ersatzbaugruppen sind nach Angabe des VGB Powertech e.V. bislang für Baugruppen aus den Gerätesystemen Geamatik, DM, Teleperm B, Simatic P sowie für Siemens Sonderbaugruppen durchgeführt worden und in den Gerätekategorien E1 und E2 gemäß den Definitionen der RSK-Leitlinien für Druckwasserreaktoren /RSK96/ eingesetzt. Die genauen Einsatzorte der ersetzten Baugruppen sind der GRS nicht bekannt. Die genannten Gerätekategorien beinhalten somit Geräte, die Leittechnikfunktionen auf verschiedenen Sicherheitsebenen /BMU12/, also auch in sicherheitsrelevanten Anlagenteilen, ausführen. Die vorliegenden Betriebserfahrungen sind laut VGB Powertech e.V. uneingeschränkt positiv. So sind laut VGB Powertech e.V. in allen Fällen die Ausfallraten der Substitutionen geringer als die Ausfallraten der ersetzten Baugruppen. /VGB11/

Ein Hersteller bietet nach Auskunft des VGB Powertech e.V. Ersatzbaugruppen mit PLD-Technik (Programmable Logic Devices) an. Nach Auskunft des VGB Powertech e.V. werden die Produkte dieses Herstellers nicht in sicherheitsrelevanten Einrichtungen in Kernkraftwerken eingesetzt. /VGB11/

In Tabelle 3.1 sind die in den vom VGB Powertech e.V. betrachteten Anlagen eingesetzten Ersatzbaugruppen aufgelistet. Darüber hinaus ist das Datum angegeben, an dem die Originaltypen durch den Ersatzbaugruppen-Typ ausgetauscht wurden. /VGB11/

In Tabelle 3.2 sind die eingesetzten Ersatzbaugruppen in die Kategorisierung der RSK (Beschreibung siehe Abschnitt 2.1) eingeordnet. Alle eingesetzten Baugruppen in vom VGB Powertech e.V. betrachteten Anlagen gehören der Gruppe 3 an. Darüber hinaus ist der Typ der eingesetzten Bauelemente angegeben, wobei nach den Typen, diskrete

[1] In /VGB11/ wird der Begriff Redesign verwendet.

Bauelemente, betriebsbewährte diskrete Bauelemente und Hybridbauweise unterschieden werden. /VGB11/

Diskrete Bauelemente bedeutet, dass ein Bauelement nur eine Funktionalität beinhaltet.

Hybridbauweise bedeutet, dass eine kompaktere Bauweise gegenüber einer Bestückung nur mit diskreten Bauelementen verwendet wird. Zum Teil werden Funktionalitäten mehrerer Baugruppen auf der Ersatzbaugruppe zusammengefasst. Je nachdem müssen dann auch Verdrahtungsänderungen vorgenommen werden. Bei der Hybridbauweise handelt es sich um industriebewährte Technik. Ein Beispiel für Hybridbauweise ist: drei Zeitbaugruppen (XPH80, XPH81, XPH82) wurden auf einer Baugruppe (ZV600) zusammengefasst.

Tab. 3.1 Übersicht der durch Ersatzbaugruppen ausgetauschten Komponenten (aus /VGB11/)

System	Originaltyp	Ersatzbaugruppen-Typ	Austausch erfolgt in/ist geplant in:
Geamatik	XPH101 (Zeitglied)	BDT-42-01-01	1992
	XPG70 (UND/ODER Glied)	XPG70T	1990
	XPH80 (Zeitglied)	ZV600	2005 bis 2007 in unterschiedlichen Mengen
	XPH81 (Zeitglied)		
	XPH82 (Zeitglied)		
DM	C74111-A1068-B5 (Relais Baugruppe)	RBG2008	2010
	C74111-A1068-B6 (Relais Baugruppe)		
	C71458-A1279-A1 (Relais Baugruppe)		2011
	C71458-A1279-A11 (Relais Baugruppe)		
Teleperm B	M4200-R4110 (Trennverstärker)	TUI2000	Baugruppe wurde nicht eingesetzt
	M4335-A2 (Signalumformer I/U U/U)	BDT-044-361	1998

System	Originaltyp	Ersatzbaugruppen-Typ	Austausch erfolgt in/ist geplant in:
Simatik P	ARB-1AA (Vorrangbaugruppe)	GKN1-EL10-E22A	1984 und 1988
	ARB-1AB (Vorrangbaugruppe)		
Siemens Sonderbaugruppen	V796-25032-300-000 (Relaisbaugruppe)	ER26	2000 bis 2001 in unterschiedlichen Mengen
Keine Systemzuordnung möglich	Kein Vorgängertyp	Vierleiterbox (Design Vorgang)	2000
DM	RG11	GWM4132	2012
Teleperm C8000	M74003-A8320	AMV01	2012
	M74003-A8334		
Teleperm C	M74003-A9143	SIU	2012

Tab. 3.2 Einordnung der ersetzten Ersatzbaugruppen in die in Abschnitt 2.1 definierten Gruppen (aus /VGB11/)

Ersatzbaugruppen-Typ	Einordnung in Gruppe
BDT-42-01-01	Gruppe 3, betriebsbewährte diskrete Bauelemente
XPG70T	Gruppe 3, betriebsbewährte diskrete Bauelemente
ZV600	Gruppe 3, Hybridbauweise
RBG2008	Gruppe 3, betriebsbewährte Bauelemente
TUI2000	Gruppe 3, Hybridbauweise
BDT-044-361	Gruppe 3, betriebsbewährte diskrete Bauelemente
GKN1-EL10-E22A	Gruppe 3, betriebsbewährte diskrete Bauelemente
ER26	Gruppe 3, betriebsbewährte diskrete Bauelemente
Vierleiterbox (Design Vorgang)	Gruppe 3, betriebsbewährte diskrete Bauelemente
GWM4132	Gruppe 3, betriebsbewährte diskrete Bauelemente
AMV01	Gruppe 3, betriebsbewährte diskrete Bauelemente
M74003-A9143 Ersatz	Gruppe 3, betriebsbewährte diskrete Bauelemente

3.2 Welche Typen von Ersatzbaugruppen (Steckerkompatibilität, Funktionskompatibilität, Programmierbarkeit für verschiedene Funktionen) werden realisiert?

In Tabelle 3.3 sind die Eigenschaften Funktionalität, Pin-Kompatibilität, Funktionsidentität und Umgebungskompatibilität der laut VGB Powertech e.V. eingesetzten Ersatzbaugruppen[2] dargestellt. /VGB11/

Funktionalität
Identische Funktionalität bedeutet, dass die Ersatzbaugruppe exakt die gleichen Funktionen ausführen kann wie die Originalbaugruppe. Kann die Ersatzbaugruppe zusätzliche Funktionen ausführen, spricht man nicht mehr von einer identischen Funktionalität.

Nach /VGB11/ hat der größte Teil der Ersatzbaugruppen die gleiche Funktionalität wie die Originalbaugruppen. In zwei Fällen wurden die betrachteten Baugruppen um einen zusätzlichen Überspannungsschutz erweitert.

Pin-Kompatibilität
Pin-Kompatibilität bedeutet, dass die Ersatzbaugruppe dieselben Pinbelegungen und Steckerverbindungen aufweist wie die Originalbaugruppe.

Nach /VGB11/ kann ein Teil der Ersatzbaugruppen ohne Änderungen verwendet werden. In drei Fällen mussten Verdrahtungsänderungen durchgeführt werden, in einem Fall mussten Kodierbrücken gesteckt werden.

Funktionsidentität
Funktionsidentität bedeutet, dass die Funktionen der Ersatzbaugruppe in zur Originalbaugruppe identischer Weise ausgeführt werden (gleiche Umsetzung der Funktionen).

Nach /VGB11/ trifft dies für einen Großteil der Ersatzbaugruppen zu. Nicht funktionsidentische Baugruppen haben nachfolgend beschriebene Unterschiede im Vergleich zu ihren Originalbaugruppen. In einem Fall wurden die Funktionen mehrerer Originalbaugruppen zu einer Baugruppe zusammengefasst und die Ersatzbaugruppe überstreicht

[2] In /VGB11/ wird der Begriff Redesign verwendet.

die Zeitbereiche der drei Originalbaugruppen. In einem anderen Fall besitzt die Ersatzbaugruppe zusätzliche Funktionen. Des Weiteren findet sich eine Ersatzbaugruppe, bei der im Unterschied zur Originalbaugruppe die Ausgänge nicht potentialfrei sind.

Umgebungskompatibilität

Umgebungskompatibilität bedeutet, dass die Ersatzbaugruppe in den gleichen Umgebungsbedingungen (Feuchte, Spannung, Temperatur, EMV, Schwingfestigkeit usw.) wie die Originalbaugruppe eingesetzt werden kann.

Nach /VGB11/ ist die Umgebungskompatibilität bei allen Ersatzbaugruppen gegeben.

Tab. 3.3 Übersicht über die Eigenschaften der laut VGB Powertech e.V. verwendeten Ersatzbaugruppen (aus VGB11/)

Originaltyp	Ersatzbau-gruppen Typ	Funktionalität	Pin-Kompatibel	Funktionsidentisch	Umgebungs-kompatibilität
XPH101	BDT-42-01-01	erweitert um zusätzlichen Überspannungsschutz	nein, die Baugruppe XPH101 war mit Lötanschlüssen versehen und auf der Schrankrückseite in der Verdrahtung eingebaut.	Ja	ja
XPG70	XPG70T	identisch	ja	Ja	
XPH80	ZV600		ja, es müssen aber, je nach Originalbaugruppe, Verdrahtungsänderungen durchgeführt werden.	abweichend, die ZV600 überstreicht die Zeitbereiche der drei Originalbaugruppen	
XPH81					
XPH82					
C74111-A1068-B5	RBG2008		ja	ja	
C74111-A1068-B6					
C71458-A1279-A1					
C71458-A1279-A11					
M4200-R4110	TUI2000		ja		

Originaltyp	Ersatzbau-gruppen Typ	Funktionalität	Pin-Kompatibel	Funktionsidentisch	Umgebungs-kompatibilität
M4335-A2	BDT-044-361	erweitert um zusätzlichen Überspannungsschutz			
ARB-1AA	GKN1-EL10-E22A	identisch	ja		
ARB-1AB					
V796-25032-300-000	ER26	identisch			
Kein Originaltyp	Vierleiterbox		ja, es müssen Verdrahtungsänderungen durchgeführt werden.	nein, Ausgänge sind nicht potenzialfrei	
V796-25032-300-000	ER26		ja	ja	
RG11	Keine Bezeichnung		ja, es müssen aber, je nach Originalbaugruppe entsprechend Kodierbrücken gesteckt werden	abweichend, es sollen z. B. zusätzliche Funktionen wie, Radizierung, Einschaltverzögerungen, 2/4-Leiterbetrieb enthalten sein	
M74003-A8320	AMV01				
M74003-A8334			ja	Ja	
M74003-A9143	Keine Bezeichnung				

3.3 Welche Technologie (FPGA, ASICs etc.) kommt bei Ersatzbaugruppen zum Einsatz?

Die eingesetzten Ersatzbaugruppen[3] gehören nach Auskunft des VGB Powertech e.V alle zu Gruppe 3 (siehe Abschnitt 2.1), beinhalten also keinerlei programmierbare oder rechnerbasierte Technik. /VGB11/

Der VGB Powertech e.V. betont, dass beim Einsatz von industriebewährten technischen Einrichtungen (z. B. Schaltanlageneinschub) der Einsatz von Software oder Firmware nicht ausgeschlossen werden kann. Diese Komponenten müssen nach anerkannten Regelwerken (Methoden der Softwaretechnik) qualifiziert sein. /VGB11/

3.4 Wie werden die Ersatzbaugruppen qualifiziert?

Die Reparaturmaßnahmen für leittechnische Einrichtungen von deutschen Kernkraftwerken werden von zertifizierten Werkstätten ausgeführt. Zur Erhaltung des zugrunde liegenden qualitativen Niveaus haben diese Werkstätten ein abgestuftes Qualifizierungssystem definiert und die zugehörigen Qualifizierungsverfahren werden von den von den Aufsichtsbehörden zugezogenen Sachverständigen nach §20 AtG bewertet.

Der Designprozess für eine Ersatzbaugruppe[4] gemäß VGB-Richtlinie Nr. RL005/A erfolgt nach den Vorgaben des geltenden kerntechnische Regelwerkes in folgenden Schritten /VGB11/, /VGB11b/:

1. **Erstellung einer Bedarfsbeschreibung**.
   Zunächst wird spezifiziert, wieso eine Ersatzbaugruppe aus technischen Gründen notwendig ist. Es wird festgelegt, wie hoch der Bedarf an der Ersatzbaugruppe ist und ob es erforderliche Neuerungen gibt.

2. **Erstellung der Anforderungsspezifikation**
   Die Anforderungsspezifikation wird erstellt, dabei werden technische Anforderungen, räumliche Anforderungen, Störfallanforderungen und die Sicherheitskategorie getrennt spezifiziert. Hierzu werden die technischen Unterlagen der zu ersetzenden

[3] In /VGB11/ wird der Begriff Redesign verwendet.

[4] In /VGB11b/ als Redesign bzw. Designprozess bezeichnet.

technischen Einrichtung und deren technische Systemdaten zugrunde gelegt. Darüber hinaus werden die jeweils ungünstigsten betrieblichen Umgebungsbedingungen spezifiziert, in denen die Ersatzbaugruppe eingesetzt werden soll. Die Störfallanforderungen, beispielsweise bezüglich der Versorgungsspannungsbereiche, der mechanischen Beanspruchungen, der elektromagnetischen Verträglichkeit, der Temperatur, Feuchte, Druck, Strahlung und mehr, sind im KTA Regelwerk festgelegt /KTA13/.

Zum Schluss wird die Sicherheitskategorie der Ersatzbaugruppe entsprechend der Sicherheitsanforderungen für Kernkraftwerke /BMU12/ und den Interpretationen zu den Sicherheitsanforderungen für Kernkraftwerke /BMU13/ beziehungsweise nach DIN EN Norm 61226 „Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Kategorisierung leittechnischer Funktionen“ /DIN10e/ festgelegt. Die Einordnung in eine Sicherheitskategorie bestimmt den anzuwendenden Prüfumfang und die Prüftiefe der Qualifizierung.

3. **Erstellung eines Lastenheftes**

   Die spezifizierten Anforderungen werden in einem so genannten Lastenheft zusammengefasst. Das Lastenheft dient dem Hersteller als Grundlage für den Designprozess der Ersatzbaugruppe.

4. **Auswahl eines Auftragnehmers**

   Der Auftragnehmer muss grundsätzlich nach KTA qualifiziert sein. Der VGB Powertech e.V. erwähnt die Möglichkeit, dass falls der Auftraggeber nicht nach KTA qualifiziert ist, es trotzdem möglich ist, diesen Auftragnehmer zu beauftragen. In einem solchen Fall müssen Ersatzmaßnahmen im Lastenheft festgelegt werden /VGB11/. Dies muss unter Absprache mit der Behörde von statten gehen. Laut VGB Powertech e.V. sind anerkannte Regelwerke zur Fertigung von Elektronikbaugruppen (z. B. IPC*-A-610) zu berücksichtigen.

5. **Erstellung Pflichtenheft durch Auftragnehmer**

   Auf der Basis des Lastenheftes erstellt der Auftragnehmer dann ein Pflichtenheft. Dieses wir dann zur Prüfung an den VGB-Arbeitskreis GQ E+L übergeben.

6. **Fertigung und Vorprüfung der Prototypserie**

   Auf der Basis des freigegebenen Pflichtenheftes wird die Nullserie entwickelt, gefertigt und die erforderlichen Geräteunterlagen werden erzeugt. Durch eine Vorprüfung der Nullserie wird sichergestellt, dass vom Entwickler die Vorgaben der Anforderungsspezifikation sowie des Lasten- und Pflichtenheftes umgesetzt werden.

7. **Durchführung der Erstqualifizierung**

Die einzelnen Schritte der Erstqualifizierung werden nach dem VGB-Prozessbild „Vorgehensweise bei der Qualifizierung“ am Serienprodukt durchgeführt /VDI11/. Diese Schritte beinhalten:

a) Festlegung der erforderlichen Prüfart und Prüflingsbeschaffung durch den Arbeitskreis Gerätequalifizierung E- und Leittechnik in KKW des VGB Powertech e.V.

b) Auftrag zur Erstqualifikation an einen §20 Sachverständigen (§20 AtG) durch den Arbeitskreis Gerätequalifizierung E- und Leittechnik in KKW des VGB Powertech e.V.

c) Abstimmung des Prüfplans und der Prüfspezifikation zwischen dem Arbeitskreis Gerätequalifizierung E- und Leittechnik in KKW des VGB Powertech e.V. und dem Sachverständigen in einem ersten Gespräch

d) Einreichung von Prüfplan, Prüfspezifikation und Geräteunterlagen an den Sachverständigen durch den Arbeitskreis Gerätequalifizierung E- und Leittechnik in KKW des VGB Powertech e.V.

e) Prüfung von Prüfplan, Prüfspezifikation und Geräteunterlagen durch den Sachverständigen

f) Prüfdurchführung gemäß Prüfspezifikation und Prüfplan durch den Arbeitskreis Gerätequalifizierung E- und Leittechnik in KKW des VGB Powertech e.V. und den Sachverständigen

g) Zusammenstellung der Prüfdokumentation durch den Arbeitskreis Gerätequalifizierung E- und Leittechnik in KKW des VGB Powertech e.V.

h) Erstellung der Prüfnachweisblätter und Übergabe an den Arbeitskreis Gerätequalifizierung E- und Leittechnik in KKW des VGB Powertech e.V. durch den Sachverständigen

i) Zusammenstellung der Nachweisdokumentation und Eintrag in das VGB-Informationssystem durch den Arbeitskreis Gerätequalifizierung E- und Leittechnik in KKW des VGB Powertech e.V.

3.5 In welchen deutschen Anlagen werden in welchen Ersatzbaugruppen eingesetzt?

Laut /VGB11/ sind in vom VGB Powertech e.V. betrachteten Anlagen Ersatzbaugruppen[5] eingesetzt. Der GRS ist dabei nicht bekannt, wie die eingesetzten Ersatzbaugruppen auf die einzelnen Anlagen verteilt sind.

3.6 Gibt es bereits Betriebserfahrung mit Ersatzbaugruppen?

Die vorliegenden Betriebserfahrungen mit den eingesetzten Ersatzbaugruppen[5] sind laut VGB Powertech e.V. positiv. So seien in allen Fällen die Ausfallraten der Substitutionen geringer als die Ausfallraten der ersetzten Baugruppen bewertet. Insgesamt liegen laut VGB Powertech e.V. genügend Betriebserfahrungen mit Ersatzbaugruppen vor und wie die Ausfallstatistiken zeigen, sind die Ersatzbaugruppen in der Regel zuverlässiger als die Originalbaugruppen /VGB11/. Die Ausfallraten der Ersatzbaugruppen sind laut /VGB11/ deutlich kleiner als die der Originalbaugruppen. Die Grundlage für diese Ausfallraten wurde allerdings nicht von der GRS geprüft und kann daher nicht bewertet werden.

3.6.1 Auswertung nationaler und internationaler Betriebserfahrung

Eine Auswertung der Ereignisdatenbanken, wie beispielsweise der GRS eigenen VERA, der internationalen IRS Datenbank der IAEA oder der amerikanischen ADAMS hinsichtlich Ereignissen, an denen Ersatzbaugruppen beteiligt waren, erweist sich als schwierig, da im allgemeinen nicht bekannt ist, ob die ausgefallene Baugruppe eine Ersatzbaugruppe ist oder nicht. Dennoch wurde in diesen Quellen nach Fällen gesucht, die aufgrund des Einsatzes einer Ersatzbaugruppe aufgetreten sind oder bei denen Ersatzbaugruppen beteiligt waren. Darüber hinaus wurde nach Ereignissen gesucht, bei denen der Einsatz von Ersatzbaugruppen zwar nicht ereignisauslösend war, aus denen sich aber weitere Erkenntnisse zum Einsatz von Ersatzbaugruppen ergaben. Zusätzlich zu den oben genannten Quellen wurden auch der GRS-A-Bericht 3395 zur „Auswertung von Ereignissen aufgrund nicht funktionsgleicher Ersatzbetriebsmittel in sicherheitstechnisch

[5] In /VGB11/ wird der Begriff Redesign verwendet.

wichtigen Einrichtungen“ sowie Weiterleitungsnachrichten zu ausgewählten Ereignissen bei der Recherche herangezogen.

Im Folgenden werden Ereignisse beschrieben, an denen Ersatzbaugruppen beteiligt waren.

3.6.1.1 Reaktorschnellabschaltung aufgrund eines Fehlsignals

Im Rahmen des Anfahrens nach der Revision wurde eine wiederkehrende Prüfung durchgeführt. Während dieser trat ein Fehlsignal auf und führte zur Reaktorschnellabschaltung.

In der vorangegangenen Revision war ein Austausch von Messumformern auf einen Nachfolgetyp vorgenommen worden. Nachdem Messumformer des Vorläufertyps wieder installiert wurden, traten die Fehlsignale nicht mehr auf. Die wiederkehrende Prüfung des Einspeisesystems konnte ordnungsgemäß abgearbeitet werden. Der aufgetretene Effekt kann entweder durch Änderung der Masse (Länge der Wirkdruckleitung) oder durch Änderung der Feder (Messbereich des Messumformers) erklärt werden. Das Verschiebevolumen des Nachfolgetyps ist kleiner als das des Vorläufertyps. Das bedeutet, dass damit die Feder in dem vorliegenden Feder/Masse-System verändert wurde und dadurch die Resonanzfrequenz der Messstelle (Messumformer plus Wirkdruckleitung) in die Nähe der prozessbedingten Anregefrequenz verschoben wurde. Die jetzt auftretenden Differenzdruckimpulse erzeugten am Messumformer ein entsprechendes Ausgangssignal.

Ursache für den Ausfall ist ein Fehler des Herstellers bei der Umstellung des Vorläufertyps auf einen Nachfolgetyp. Beim Design des Nachfolgetypen wurden nicht alle Eigenschaften betrachtet, so dass er den Vorläufertyp nicht gleichwertig ersetzt.

3.6.1.2 Nichtzuschalten des Entregungsschalters eines Notstromdieselaggregates bei wiederkehrender Prüfung

Im Rahmen der wiederkehrenden Prüfung des Notstromsignals nach Prüfhandbuch für ein Notstromdieselaggregat schaltete sich der Entregungsschalter nicht automatisch zu. Demzufolge blieben der Dieselgenerator unentregt und die durch das Notstromsignal

abgeschalteten Notstromschienen dieser Redundanz spannungslos. Das Notstromaggregat wurde von Hand abgeschaltet und die Notstromschienen durch Zuschaltung der Netzschalter wieder unter Spannung gesetzt. Der Entregungsschalter des Notstromaggregates ist normalerweise immer zugeschaltet; er wird lediglich jeweils vor einer Notstromprüfung prüfvorbereitend von Hand ausgeschaltet, um zu kontrollieren, dass er vom Notstromsignal einen "Ein"-Befehl erhält. Nach Beendigung der Prüfung bleibt der Schalter eingeschaltet.

Während der vorherigen Revision waren an insgesamt sechs Leistungsschaltern die "Rückhaltefedern" gegen neue, verstärkte Federn ausgetauscht worden. Vier dieser Schalter sind als Entregungsschalter für die Notstromgeneratoren eingesetzt. Nach dem Austausch der Federn traten bisher zwei Fälle von Einschaltversagen auf.

Der Hersteller hatte empfohlen, die Rückstellfedern im Erregerschalter auszutauschen. Der Hersteller lieferte aber ungeeignete Federn, da zwischenzeitlich eine Designänderung der Erregerschalter stattgefunden hatte. Der Einsatz dieser neuen Federn ist jedoch nur für Schalter des geänderten Typs geeignet, da diese auch mit neuen Stützklinken ausgerüstet und diese auf neue verstärkte Rückholfedern abgestimmt worden waren.

3.6.1.3 Nichtöffnen einer Armatur bei einer WKP

Bei einer wiederkehrenden Prüfung wurde festgestellt, dass eine Armatur nicht ordnungsgemäß öffnete. Die Fehlfunktion resultierte aus dem Ansprechen des Drehmomentschalters. Anschließend ging die Armatur über Laufzeitüberschreitung in Störung. Nach Quittieren am Wartenbaustein ließ sich die Armatur von Hand öffnen. Wirkleistungsmessungen ergaben eine geringfügige Überhöhung gegenüber dem eingestellten Drehmomentabschaltwert über eine Dauer von etwa 100 ms.

Der Fehler konnte durch den Rücktausch der Vorrang-Baugruppen an den betroffenen Armaturen gegen Vorgänger-Vorrang-Baugruppen behoben werden.

Die modifizierte Baugruppenkombination mit der neuen Vorrang-Baugruppe überbrückt die Drehmomentabschaltung für die Dauer von 200 ms lediglich mit Beginn des AUF-Signals. Bei der Ursachenklärung wurde festgestellt, dass bei der Auslegung dieser Baugruppen nicht berücksichtigt wurde, dass eine Spannungslosigkeit die erforderliche kurzzeitige Drehmomentüberbrückung wirkungslos machen kann. Kann die Armatur erst

nach Spannungswiederkehr öffnen, ist diese Überbrückungszeit abgelaufen. Eine Drehmomentüberhöhung beim anschließenden Anlaufen führt dann unverzögert zum Abbruch des Öffnungsvorgangs.

3.6.1.4 Nicht spezifikationsgerechte Funktion von Messumformer-Versorgungsbaugruppen

Im Rahmen der Kontrolle von Sicherungen in Reaktorschutzschränken wurde die Versorgungsspannung für jeweils eine Redundanz abgeschaltet. Dabei wurde auch eine Messumformer-Versorgungsbaugruppe für die Messung der Frequenz auf einer Notstromschiene spannungslos. Nach Ende der Kontrollen und dem ordnungsgemäßen Wiederzuschalten der Schrank-Stromversorgung blieb der Messumformer weiterhin unbemerkt spannungslos, da die Messumformer-Versorgungsbaugruppe keine Ausgangsspannung lieferte. Bei der Fortsetzung der Kontrollen in der zweiten Redundanz kam es folgerichtig zur 2v3-Auslösung mit ordnungsgemäßem Start des zugehörigen Notstromdiesels.

Die Untersuchung der Messumformer-Versorgungsbaugruppe durch den Baugruppenhersteller ergab folgenden Sachverhalt: Der Fehler tritt reproduzierbar auf, wenn die Versorgungsspannung beim Einschaltvorgang, z. B. durch Kontaktprellen, kurzzeitig wieder abgeschaltet ist. Auch bei anderen untersuchten Baugruppen aus dem betroffenen Fertigungszeitraum konnte das beschriebene Fehlverhalten festgestellt werden. Die betroffenen Baugruppen sind alle mit einem integrierten Schaltkreis (IC) eines bestimmten Herstellers bestückt. Dieser Schaltkreis wird von verschiedenen Herstellern gefertigt, wobei das Fehlverhalten der Baugruppe nach einem Wechsel des ICs gegen einen gleichen Typ eines anderen Herstellers nicht mehr herbeigeführt werden konnte. Eine genaue Ursachenanalyse ergab, dass das IC des genannten Herstellers hinsichtlich der erlaubten Eingangsspannung an einem Eingang nicht der Spezifikation genügt und sich zudem durch eine geringere erlaubte Eingangsspannung von denen anderer Hersteller unterscheidet. Daraus resultiert letztendlich, dass sich abhängig von den vorhandenen Randbedingungen während des Wiederzuschaltens der Spannungsversorgung nach einer vorhergehenden Abschaltung Betriebszustände einstellen können, für die dieses spezielle IC nicht geeignet ist und die in der Folge zum „Nichtanlaufen“ der Messumformer-Versorgungsbaugruppe führen.

3.6.1.5 Fehlerhafte sekundärseitige Lastabsenkung und nicht erfolgter Stabeinwurf

Bei dem im Folgenden beschriebenen Ereignis waren Ersatzbaugruppen zwar am Ereignis beteiligt, jedoch lag die Ereignisursache in der fehlerhaften Projektierung der Ersatzbaugruppe. Damit ist das Ereignis ein Beispiel dafür, dass sich durch relevante Änderungen an Baugruppen, wie beispielsweise die Umrüstung auf programmierbare und rechnerbasierte Baugruppen, Fehler ergeben können.

Während des Streckbetriebs sollte zur Instandsetzung einer gestörten Ionisationskammer der Neutronenfluss-Instrumentierung der betroffene Gliederzug der Kernaußeninstrumentierung gezogen werden. Hierfür wurden in der digitalen Leittechnik der Begrenzungseinrichtungen Simulierungen vorgenommen. Dadurch entstand eine Störung in einer Betriebsbegrenzung, die u. a. zur schnellen Absenkung der Generatorleistung führte und gleichzeitig den Einwurf und das Fahren der Steuerstäbe durch die Begrenzungseinrichtungen blockierte. Die betroffene „Reaktor-Leistungs-Begrenzung“ wurde von festverdrahteter auf digitale Leittechnik umgerüstet. Bei der Projektierung der neuen Leittechnik wurde nicht berücksichtigt, dass die vier Ionisationskammern des Leistungsbereichs eines Gliederzuges der Neutronenfluss-Kernaußeninstrumentierung für Instandsetzungsmaßnahmen gemeinsam gezogen werden. Aufgrund der realisierten Schaltungslogik mussten durch drei fehlerhafte Signale aus einem Gliederzug zwangsläufig die beim Ereignis aufgetretenen Fehlfunktionen der Begrenzungseinrichtungen entstehen.

3.6.1.6 Nicht spezifikationsgerechte Ersatzteile für Anlassluftschläuche an Notstromdieseln

Im Rahmen der Wartung eines Notstromdiesels wurde festgestellt, dass der neu einzusetzende Anlassluftschlauch relativ weich ist. Eine daraufhin durchgeführte Überprüfung der Referenznummer ergab, dass ein Einsatz mit Druckschläuchen einer anderen Referenznummer gefordert ist.

Eine Bestellung von Ersatzteilen für die Notstromdiesel erfolgt durch den Betreiber nur über den Hersteller. Genutzt wird dabei der vom Hersteller für das jeweilige Aggregat zur Verfügung gestellte Bestellkatalog. In diesem war für die spezifikationsgerechten Druckschläuche eine seit Jahren unveränderte Referenznummer genannt. Unter dieser

Nummer wurden früher die richtigen Druckschläuche geliefert. Die Referenznummer für Druckschläuche wurde jedoch beim Hersteller geändert, ohne dass dies Berücksichtigung in den Katalogen fand. Die alte Referenznummer bezog sich nun auf Druckschläuche, deren Spezifikation von der geforderten Spezifikation hinsichtlich Dauerbetriebsdruck, Prüf- und Berstdruck abwich. Bezüglich der Abmessungen unterscheiden sich die beiden Druckschläuche nicht. Eine Überprüfung weiterer Notstromdiesel ergab, dass dort bereits seit der letzten Wartung – vor einem bzw. vier Jahren – nicht spezifikationsgerechte Ersatzteile im Einsatz waren.

3.6.1.7 Fehlöffnen von Schaltern an einer 400-V-Notstromschiene bei einer wiederkehrenden Prüfung und Anzugsversagen von Hilfsschützen

Im Rahmen einer WKP kam es kurz nach dem Wiederzuschalten des Einspeiseschalters sowie kurz nach der automatischen Umschaltung zum Fehlöffnen dreier Schalter, wodurch eine 400-V-Notstromschiene spannungslos wurde. Bei der Ursachenklärung für das Fehlöffnen dieser drei Schalter wurde das Fehlen der Signalisierung der Überstromauslösung festgestellt. Im Rahmen der Ursachenklärung wurde erkannt, dass bei Anregung des magnetischen Kurzschlussauslösers ein Hilfsschütz nicht anzieht. Die Funktion dieses Hilfsschützes ist, im Falle der Überstromauslösung eine entsprechende Signalisierung zur Weiterverarbeitung in der Leittechnik abzusetzen sowie durch eine Verriegelung auf der Funktionsgruppenebene eine Wiedereinschaltung des Leistungsschalters zu verhindern.

Die Ursache für das Ansprechversagen der Hilfsschütze wurde bei Prüfungen der Leistungsschalter auf dem Prüfstand ermittelt. Die zeitliche Länge des durch die Kurzschlussauslösung erzeugten Spannungsimpulses zur Schaltung des Hilfsschützes reichte nicht aus, um das Hilfsschütz zu schalten und in Selbsthaltung zu bringen. Die Hilfsschütze waren vorbeugend im Rahmen des Alterungsmanagements ausgetauscht worden. Die Schütze vom Vorgängertyp schalteten mit den kurzen Spannungsimpulsen ordnungsgemäß, die neuen Schütze haben eine längere Schaltzeit und benötigen deshalb länger dauernde Spannungsimpulse. Der neue Typ war vom Hersteller als Ersatztyp für das alte Schütz benannt worden. Das Hilfsschütz ist nicht Bestandteil des Schalters, sondern ist im Schaltschrank eingebaut.

3.6.1.8 Temporäre Störung von elektronischen Baugruppen

Es trat eine Störung in der schrankinternen Buskommunikation (Rückwandbus) eines Leittechnikschranks auf, die zu einem vollständigen Ausfall der Regelungs- und Überwachungsfunktionen im betroffenen Schrank führte. In dem Schrank sind ausschließlich betriebliche Leittechnikfunktionen realisiert. Nach Rücksprache mit dem Hersteller wurde die Störung durch Neustart der Buskommunikation des betroffenen Leittechnikschranks behoben. Anschließend standen die betrieblichen Leittechnikfunktionen des Schrankes wieder zur Verfügung. Die in Zusammenarbeit mit dem Hersteller durchgeführte Störungsanalyse ergab, dass die Störung von Leittechnik-Baugruppen mit bestimmten Hardwareversionen ausgelöst worden war. Die Baugruppen dieser Hardwareversionen waren nach Aussage des Herstellers mit neuen Kommunikationsbausteinen in FPGA- statt ASIC- Technologie bestückt. Die Technologieumstellung war erforderlich, weil die Bausteine in ASIC-Technologie vom Bausteinhersteller nicht mehr ausgeliefert werden. Der für die ASIC-Chips vorhandene Programmcode wurde bei der Umstellung auf FPGA-Chips übernommen, musste aber in einzelnen Bereichen angepasst werden. Kommunikationsbausteine sind generell sowohl auf den zentralen Prozessorbaugruppen als auch auf den analogen und digitalen Ein- und Ausgabebaugruppen des Leittechniksystems vorhanden. Die fehlerbehafteten Leittechnik-Baugruppen waren im Zuge von vier Änderungsanzeigen in das bereits bestehende Leittechniksystem eingebaut worden. Aus der Betriebserfahrung in nichtkerntechnischen Anlagen war dem Hersteller bekannt, dass es in sehr wenigen Einzelfällen zu Störungen in der Buskommunikation gekommen ist. Erste Analysen des Herstellers hatten dann ergeben, dass die Ausfälle ausschließlich im Zusammenhang mit den neuen Kommunikationsbausteinen in FPGA-Technologie aufgetreten sind. Dem Betreiber lagen diese Informationen zum Zeitpunkt des Ereigniseintritts nicht vor. Als Ursache für die Störung in der schrankinternen Buskommunikation wurde vom Hersteller ein fehlerhaftes Dauersenden eines Kommunikationsbausteins ermittelt. Das Dauersenden eines Kommunikationsbausteins hatte die Unterbrechung der Buskommunikation zwischen den Leittechnikbaugruppen des betroffenen Schrankes zur Folge. Als wahrscheinliche Ursache für das Dauersenden der Kommunikationsbausteine wurde vom Hersteller ein systematischer Fehler in der Firmware angenommen. Die exakte Ursache ist unbekannt. Auch im Rahmen umfangreicher Labortests und Simulationen des Herstellers ließ sich der Fehler nicht reproduzieren. Der Hersteller folgert daraus, dass nur bestimmte, sehr seltene Konstellationen im System zum Fehlverhalten des Kommunikationsbausteins in FPGA-Technologie führen können.

3.6.1.9 Funktionsstörungen an Einschüben von Armaturen und Abweichungen vom spezifizierten Zustand an Einschüben von Armaturen

Im Rahmen einer wiederkehrenden Prüfung eines Notstromdieselaggregats wurden die zugeordneten Notstromschienen gestaffelt wieder zugeschaltet. Bei der Zuschaltung einer 380-V-Notstromschiene fielen die Steuerköpfe der Schalteinschübe zur Versorgung der Stellantriebe einiger Armaturen. Die Einschübe der betroffenen Stellantriebe wurden im Rahmen eines Änderungsantrages umgebaut. Dabei wurden die alten Steuerköpfe in den Einschüben belassen. Zur Versorgung der neuen elektronischen Wendelastrelais sowie der Wirkleistungsmessmodule waren Schaltnetzteile erforderlich. Es waren 0,65-A-Schaltnetzteile vorgesehen, die über die 1-A-Sicherung der alten Steuerköpfe abgesichert wurden, obwohl in den Schaltnetzteilen eine interne Sicherung vorhanden ist. Der Umbau erfolgte redundanzweise über mehrere Revisionen.

Ein Jahr vor dem Ereignis wurden die 0,65-A-Schaltnetzteile vom Hersteller abgekündigt. Dem Zulieferer wurde versichert, dass die 1-A-Schaltnetzteile vergleichbare Eigenschaften haben und an Stelle der 0,65-A-Schaltnetzteile verwendet werden können. Daher kam es zur Lieferung einer gemischten Charge von Schaltnetzteilen (0,65 und 1 A) und folglich zum Einbau der 1-A-Schaltnetzteile. Diese Informationen lagen dem Betreiber aber zum Ereigniszeitpunkt nicht vor. Die Auslösung der Steuerköpfe ist auf eine erhöhte Stromaufnahme der 1-A-Schaltnetzteile bei Spannungszuschaltung zurückzuführen. In Kombination der verwendeten 1-A-Automaten in den alten Steuerköpfen, deren Auslösecharakteristik in einer statischen Bandbreite liegt, und einer erhöhten (zulässigen) Schienenspannung U>12 kV der betroffenen Notstromschiene kam es zur Auslösung.

3.6.1.10 Auffälligkeit an Vorsteuermagneten in der FSA Station sowie Fehlöffnen von Vorsteuerventilen im Frischdampfleitungssystem

Verschiedene Betreiber meldeten jeweils ein Ereignis mit Fehlöffnen von Magnetvorsteuerventilen in den Frischdampf-Sicherheits-Absperrarmaturen-Stationen (FSA-Stationen). Nachfolgend sind die Sachverhalte zu den jeweiligen Ereignismeldungen dargestellt:

Auffälligkeit an Vorsteuermagneten in der FSA Station

In einem Strang der FSA-Stationen wurden während einer Revision 12 Vorsteuermagnete getauscht, die im Ruhestromprinzip (RSP) betrieben werden. Bei den eingebauten RSP-Vorsteuermagneten gab es keine Auffälligkeiten. In der Revision im darauf folgenden Jahr wurden in einem anderen Strang der FSA-Stationen 14 nach dem Arbeitsstromprinzip arbeitende Magnete (ASP-Magnete) und 12 nach dem Ruhestromprinzip arbeitende Vorsteuermagnete (RSP-Magnete) getauscht. Von den RSP-Magneten wurden zwei Magnete auffällig: Diese lösten aufgrund erhöhter Stromaufnahme nach fünf bzw. 36 Betriebsstunden die vorgeschalteten Sicherungen aus. Die Anlage befand sich zum Zeitpunkt der Störung im Anfahrbetrieb, im Zustand unterkritisch heiß. Die GRS geht davon aus, dass der Ausfall der Magnete zum Fehlöffnen der zugehörigen Vorsteuerventile führte.

Als kurzfristige Maßnahmen wurden die zwei defekten RSP-Magnete und vorsorglich die zehn weiteren eingebauten RSP-Magnete durch geprüfte/betriebsbewährte RSP-Magnete aus dem Ersatzteillager ausgetauscht. Im Anschluss an den Austausch der Magnete wurde durch Funktionsprüfungen die Funktionsfähigkeit der Magnete nachgewiesen. Einer der beiden auffälligen RSP-Magnete wurde vom Betreiber untersucht. Der andere auffällige RSP-Magnet und die zehn weiteren RSP-Magnete der fehlerbehafteten Charge wurden dem Hersteller zur Untersuchung zwecks Ursachenklärung geschickt.

Fehlöffnen von Vorsteuerventilen im Frischdampfleitungssystem

Im Zuge von Instandhaltungstätigkeiten während einer Revision öffnete ein Vorsteuerventil der Absperrarmatur vor dem Frischdampf-Sicherheitsventil (FD-AVSIV) in einem Strang fehlerhaft. Einige Tage später öffnete ein Vorsteuerventil des Frischdampf-Sicherheitsventils (FD-SIV) in einem anderen Strang fehlerhaft. Die Vorsteuerventile werden von Magneten betätigt, die nach dem Ruhestromprinzip (RSP) betrieben werden. Die Magneten der beiden fehlöffnenden Vorsteuerventile lösten jeweils aufgrund erhöhter Stromaufnahme die zugeordneten Sicherungsautomaten aus. Die auffällig gewordenen, nach Meinung des Betreibers neu qualifizierten Magnete wurden in der Revision im Rahmen des Alterungsmanagements eingebaut.

Als kurzfristige Maßnahmen wurden die betroffenen Vorsteuerstränge abgesperrt, die beiden defekten Magnete gegen lagerhaltige betriebsbewährte Magnete gleichen Typs

getauscht und die Funktionsfähigkeit der betroffenen Vorsteuerventile nach dem Austausch der Magnete nachgewiesen. Die beiden auffälligen Magnete der fehlerbehafteten Charge wurden dem Hersteller zur Untersuchung zwecks Ursachenklärung geschickt.

Fehlöffnen von Vorsteuerventilen im Frischdampfleitungssystem

Während einer Revision öffnete ein Vorsteuerventil der Absperrarmatur vor dem Frischdampfsicherheitsventil in einem Strang fehlerhaft. Einige Monate später öffnete ein Vorsteuerventil des Frischdampfsicherheitsventils (FD-SIV) in einem anderen Strang fehlerhaft. Die Anlage befand sich zum Zeitpunkt des Ereignisses im Leistungsbetrieb. Die betreffenden Vorsteuerventile werden von Magnetspulen im Ruhestromprinzip (RSP-Magnete) betätigt. Die RSP-Magnete der beiden auffälligen Vorsteuerventile lösten aufgrund erhöhter Stromaufnahme die zugeordneten Sicherungsautomaten aus. Bei den beiden auffälligen RSP-Magneten handelt es sich nach Meinung des Betreibers um neu qualifizierte Magnete. Weitere RSP-Magnete aus der Liefercharge blieben bisher unauffällig.

Als kurzfristige Maßnahmen wurden die betreffenden Vorsteuerstränge abgesperrt und die defekten RSP-Magnete getauscht. Der defekte RSP-Magnet am Vorsteuerventil der Absperrarmatur vor dem Frischdampfsicherheitsventil wurde durch einen anderen aus dem gleichen Produktionsjahr ersetzt. Der ausgefallene RSP-Magnet am Vorsteuerventil des Frischdampfsicherheitsventils wurde durch einen betriebsbewährten Magneten aus einer älteren Liefercharge ersetzt. Im Anschluss an den Austausch der beiden auffälligen Magnete wurde die Funktionsfähigkeit der Vorsteuerventile nachgewiesen. Zudem wurden vorsorglich Stromaufnahmemessungen an allen vergleichbaren RSP-Magneten in den FSA-Stationen durchgeführt. Die Stromaufnahmemessungen haben keine Auffälligkeiten gezeigt. Die beiden auffälligen RSP-Magnete der fehlerbehafteten Charge wurden dem Hersteller zur Untersuchung übergeben.

Ereignisursache

Die ausgefallenen Magnete wurden zwischenzeitlich vom Hersteller untersucht. Die Schadensbilder der ausgefallenen Magnete sind weitgehend miteinander vergleichbar. Die nachfolgenden Ausführungen zu dem Fehlermechanismus beziehen sich auf die der GRS vorliegenden Informationen. Bei der Untersuchung der ausgefallenen Magnete wurde festgestellt, dass die Magnete einen örtlich gleichen Masseschluss zwischen Spu-

lenwicklung und Spulengehäuse aufweisen. Zudem wurden klare Verformungen im oberen Bereich der Spulen beobachtet. Außerdem wurden folgende Änderungen in der Spulenfertigung der Magnete aus den betroffenen Produktionsjahren gegenüber der spezifizierten und nach KTA 3504 /KTA06/ qualifizierten Serie festgestellt:

- Die Wickelgeometrie wurde geändert,
- die Anzahl der Bandagen wurde erhöht,
- die Anzahl der Beilagen wurde erhöht,
- das Tränkverfahren der Spule wurde geändert,
- der Tränklack wurde geändert und
- der Abstand zwischen der Spulenwicklung und dem Spulengehäuse wurde verringert (2 mm statt 3 mm).

Laut dem Hersteller ist der Ausfall der Magnete auf einen Masseschluss zurückzuführen. Wie bereits dargestellt, führte der Masseschluss zu erhöhter Stromaufnahme der Spulen. Die zugeordneten Sicherungsautomaten lösten aus. Die Magnete wurden stromlos und die Vorsteuerventile öffneten. Dieser Masseschluss entstand durch eine Drahtverschiebung einer Kupferwindung, wodurch es zu einem direkten Kontakt mit dem Gehäuse kam. Bei seinen Untersuchungen kommt der Hersteller zu dem Schluss, dass die Verwendung des Vergussmaterials Sylgard 170 in Verbindung mit dem zu weichen Tränklack Damisol den Masseschluss verursacht hat. Durchgeführte Versuche und Untersuchungen beim Hersteller haben gezeigt, dass das verwendete Vergussmaterial Sylgard 170 bei der ersten Erwärmung bis zur Einsatztemperatur der Magnete sich maximal verformt bzw. eine sehr hohe Volumenausdehnung erfährt. Diese hohe Erstverformung ermöglicht es bei Verwendung von zu weichem Tränklack (Damisol) einen Spulendraht aus dem Verbund zu lösen. Nach den der GRS vorliegenden Informationen ist davon auszugehen, dass die Änderungen bei der Fertigung der Spulen der Magnete in Verbindung mit den thermischen Einwirkungen (Ruhestrom) auf die Spulen zu den Ausfällen der Magnete geführt haben.

3.6.1.11 Fehlfunktion von sicherheitstechnisch wichtigen Relais

Bei dem im Folgenden beschriebenen Ereignis waren Ersatzbaugruppen zwar am Ereignis beteiligt, jedoch war die Ersatzbaugruppe nicht ursächlich für das Ereignis. Allerdings ist das Ereignis ein weiteres Beispiel dafür, dass relevante Änderungen an Baugruppen, wie beispielsweise der Einsatz von programmierbaren und rechnerbasierten Bauelementen auf den Baugruppen, teilweise auch erfolgen, ohne dass sich dies in einer Änderung der Bezeichnung niederschlägt und insbesondere auch ohne dass der Betreiber der Anlage von der Änderung in Kenntnis gesetzt wird.

Bei periodischen Prüfungen wurden zwei ähnliche Fehlfunktionen von Relais entdeckt. Es kam zu zeitlichen Verzögerungen bei der Anregung der Relais von bis zu einigen Minuten.

Aufgrund der sich ähnelnden Fehlfunktion wurde sowohl von Seiten des Betreibers als auch von Seiten des Herstellers der Relais ein CCF vermutet. Da die aufgetretene Fehlfunktion der Relais zu einer Verzögerung beim automatischen Start der Notstromdieselgeneratoren oder sogar zum Startversagen führen kann, wurden die fehlerhaften Relais in den beiden betroffenen Dieselgeneratoren ausgetauscht. Zusätzlich wurde mit dem Austausch der Relais in den verbliebenen sechs Dieselgeneratoren begonnen. Dies wurde aber nicht zu Ende geführt, da die Anlage vom Hersteller die Information erhielt, dass auch die im Lager befindlichen Relais aus der vom Fehler betroffenen Charge stammen. Bereits früher hatte der Hersteller vorübergehende Qualitätsmängel in der Produktion der Relais festgestellt, wodurch sich das Risiko einer Fehlfunktion für die betroffenen Relaistypen erhöht hatte. Nach Identifikation der Qualitätsmängel wurden diese beseitigt und die Produktion der Relais mit einer reparierten Fertigungsstraße weitergeführt. Die Information über die Qualitätsmängel wurde nicht an die Anlage weitergegeben, weshalb in allen acht Dieselgeneratoren Relais, die im fraglichen Zeitraum gefertigt worden waren, eingebaut wurden. Zusätzlich stellte sich heraus, dass die aus einem lokalen Lager gelieferten und eingebauten Relais aus derselben Charge stammten wie die ursprünglich verbauten. Nach Ergebnissen einer vom Hersteller durchgeführten Untersuchung wurde die Fehlfunktion der Relais vom Luftspalt zwischen der Spule und dem Kern und der Beschichtung des Kerns verursacht. Nach Herstellerangaben war dabei entweder der Luftspalt zu schmal oder die Beschichtung zu dick, wodurch sich die Reibung der bewegten Teile erhöhte. Es wurden neue Relais in allen Dieselgeneratoren der Anlage eingebaut. Im Zuge der Untersuchung der fehlerhaften Relais stellte sich heraus, dass die betroffenen Relais ebenso wie die neu

gelieferten Relais programmierbare Technik in Form eines Mikroprozessors mit eingebetteter Software zur Steuerung der Spule der Relais enthielten. Daher war die Qualifizierung der Relais nicht mehr gültig. Die Information darüber, dass die Relais nun rechnerbasierte Technik enthielten, war nicht an den Betreiber weitergegeben worden. Allerdings wurde hier kein ursächlicher Zusammenhang zwischen der rechnerbasierten Technik und der Fehlfunktion der Relais festgestellt.

Die Relais mit rechnerbasierter Technik wurden vom Betreiber gegen diversitäre, qualifizierte Relais mit nicht programmierbarer Technik ausgetauscht.

4 Anforderungen für den Einsatz von Ersatzbaugruppen

Im Rahmen des Projektes 3611 R01355 „Aufstellung von Kriterien und Kenngrößen zur deterministischen Prüfung der Eignung von Redesign-Komponenten für den Einsatz in der Sicherheitsleittechnik von Kernkraftwerken“ wurden verschiedene nationale und internationale Normen sowie weitere relevante Dokumente hinsichtlich Anforderungen an Ersatzbaugruppen und ihren Einsatz ausgewertet.

In den folgenden Abschnitten werden diese Normen und Regelwerke kurz inhaltlich dargestellt.

4.1 Ausgewertete Normen und Dokumente

Aus dem nationalen Regelwerk wurden die KTA 3501 /KTA14b/, KTA 3503 /KTA13/ und die KTA 3507 /KTA14a/ ausgewertet. Die KTA 3501 „Reaktorschutzsystem und Überwachungseinrichtungen des Sicherheitssystems“ enthält Anforderungen an Aufbau, Ausführung, Gerätequalität, Einbau und Prüfung von Einrichtungen der Sicherheitsleittechnik, die in Kernkraftwerken leittechnische Funktionen der Kategorien A und B ausführen. Sie enthält eine Zusammenstellung von Auslegungskriterien, Anforderungen an die Qualität und Qualitätssicherung und Anforderungen an die Funktionsweise der oben genannten Einrichtungen. Die KTA 3503 „Typprüfung von elektrischen Baugruppen der Sicherheitsleittechnik“ beschreibt die bei einer Typprüfung von elektrischen Baugruppen der Sicherheitsleittechnik, die leittechnische Funktionen der Kategorien A und B realisieren, anzuwendenden theoretischen und praktischen Prüfungen. Außerdem werden Anforderungen an die Prüfdokumentation gestellt. Die KTA 3507 „Werksprüfungen, Prüfungen nach Instandsetzung und Nachweis der Betriebsbewährung der Baugruppen und Geräte der Leittechnik des Sicherheitssystems“ stellt Anforderungen an die Planung, Durchführung und Dokumentation von Werksprüfungen, Prüfungen nach Instandsetzung und an den Nachweis der Betriebsbewährung für Baugruppen und Geräte der Sicherheitsleittechnik, die leittechnische Funktionen der Kategorien A und B ausführen, auf.

Des Weiteren wurde der Bericht GRS-A-3550 zum Reaktorsicherheitsforschungs-Vorhaben RS1180 „Weiterentwicklung und Erprobung von Methoden und Werkzeugen für probabilistische Sicherheitsanalysen“ /GRS10/ berücksichtigt. In diesem Vorhaben soll-

ten Methoden und Werkzeuge für die Durchführung von probabilistischen Sicherheitsanalysen weiterentwickelt und nutzbar gemacht werden. Dabei wurde ein neues Konzept zur Modellierung programmierbarer und rechnerbasierter Sicherheitsleittechnik entwickelt.

Von den internationalen Normen und Richtlinien wurde eine Reihe von DIN EN-Normen ausgewertet:

- Die DIN IEC 61513 „Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Allgemeine Systemanforderungen“ /DIN13/ beschäftigt sich mit allgemeinen Anforderungen an die leittechnischen Einrichtungen, die in Kernkraftwerken für die Durchführung sicherheitstechnisch wichtiger Funktionen verwendet werden. Dabei stehen die Gesamtarchitektur der Leittechnik und der Zusammenhang mit den Anforderungen an die einzelnen sicherheitstechnisch wichtigen Systeme im Vordergrund.

- Darauf aufbauend enthält die DIN EN 60987 „Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Anforderungen an die Hardwareauslegung rechnerbasierter Systeme“ /DIN10c/ generische Anforderungen an die Hardware-Auslegung von rechnerbasierten Systemen für sicherheitstechnisch wichtige Einrichtungen.

- Die DIN EN 60880 „Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Softwareaspekte für rechnerbasierte Systeme zur Realisierung von Funktionen der Kategorie A“ /DIN10a/ deckt gemeinsam mit der DIN EN 62138 „Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Softwareaspekte für rechnerbasierte Systeme zur Realisierung von Funktionen der Kategorie B oder C“ /DIN10b/ Anforderungen an die Software rechnerbasierter Systeme ab, wobei sich die DIN EN 60880 auf rechnerbasierte Systeme zur Realisierung von leittechnischen Funktionen der Kategorie A bezieht und die DIN EN 62138 die Kategorien B und C umfasst.

- Die DIN EN 62340 „Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Anforderungen zur Beherrschung von Versagen aufgrund gemeinsamer Ursache“ /DIN10d/ ergänzt die vorgenannten Normen um Anforderungen zur Beherrschung und Vermeidung von Ausfällen leittechnischer Einrichtungen aufgrund gemeinsamer Ursache.

- Die VDI/VDE 3528 „Anforderungen an Serienprodukte und für deren Einsatz in der Sicherheitsleittechnik in Kernkraftwerken“ /VDI11/ gibt weitere Empfehlungen zu den

erforderlichen Eigenschaften von Komponenten, die in sicherheitstechnisch wichtigen leittechnischen Einrichtungen eingesetzt werden. Hierzu zählen grundsätzliche Anforderungen an Serienprodukte mit hochintegrierten Bauelementen bzw. mit eingebundener Software.

Außerdem wurde eine Reihe von IEEE Standards ausgewertet. Der Standard IEEE 603 „IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations“ /IEE09/ beinhaltet die minimalen Anforderungen an die Funktionalität und das Design von Leittechniksystemen, die zur Durchführung sicherheitstechnisch wichtiger Funktionen in Kernkraftwerken verwendet werden. Es werden z. B. Kriterien zu den Themen Einzelfehler, Qualität, Unabhängigkeit, Reparatur, menschliche Faktoren und Zuverlässigkeit aufgestellt. Außerdem werden Anforderungen an Design und Funktionalität von Messwertaufnahme und an die Ausgabe von Steuerbefehlen sowie deren Ausführung aufgestellt. Der Standard IEEE 7-4.3.2 „IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations“ /IEE10/ erweitert die im Standard IEEE 603 aufgestellten Kriterien und Anforderungen auf den Gebrauch von rechnerbasierten Systemen zur Durchführung sicherheitstechnisch wichtiger Funktionen. Der Standard IEEE 1633 „IEEE Recommended Practice on Software Reliability“ /IEE08/ beschreibt diverse Modelle zur Bestimmung der Zuverlässigkeit von Software, außerdem wird deren Anwendbarkeit in verschiedenen Situationen bewertet.

Aus dem US-Regelwerk wurden vier NUREG Dokumente ausgewertet. Die US Normen NUREG 6303 „Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems“ /NUR94/ und NUREG 7007 „Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems” /NUR10/ beschäftigen sich mit Methoden zur Durchführung von defense-in-depth Analysen des Reaktorschutzsystems. Hier finden sich zahlreiche Bemerkungen zum Einsatz und zur Bewertung von Diversität von Systemen. Der NUREG 0800 „Guidance for evaluation of diversity and defense-in-depth in digital computer-based instrumentation and control systems“ /NUR07/ beschreibt, wie die NRC vorgeht, um den Safety Analysis Report von kerntechnischen Anlagen zu bewerten. Zur Unterstützung der Bewertung von computerbasierten Reaktorschutzsystemen hat die US NRC ein Computerprogramm entwickelt, welches im NUREG 6680 „Review templates for computer-based reactor protection systems“ /NUR00/ beschrieben wird.

Der ebenfalls ausgewertete Safety Guide NS-G-1.3 „Instrumentation and Control Systems Important to Safety in Nuclear Power Plants“ /IAE12/ der IAEA gibt allgemeine

Richtlinien zu Design und Einsatz von Leittechniksystemen, die in Kernkraftwerken sicherheitstechnisch wichtige Funktionen durchführen. Dabei werden z. B. Richtlinien bezüglich der Zuverlässigkeit des Designs, den Fehlermöglichkeiten, dem Mensch-Maschine-Interface und Test und Wartbarkeit aufgestellt.

Darüber hinaus wurde der Bericht “Operating Experience Insights on Common-Cause Failures in Digital Instrumentation and Control Systems” /EPR08/ des EPRI betrachtet. In diesem Bericht wurde die Betriebserfahrung von Kernkraftwerken in den USA bezüglich Systemausfälle bzw. potentieller Ausfälle von softwarebasierten Systemen hinsichtlich ihrer Ausfallursachen ausgewertet.

4.2 Allgemeine relevante Anforderungen an Ersatzbaugruppen aus dem nationalen und internationales Regelwerk

Im betrachteten nationalen und internationalen Regelwerk finden sich kaum Anforderungen speziell zu Ersatzbaugruppen. Im nationalen Regelwerk sind Anforderungen an Ersatzbaugruppen in den derzeitigen Fassungen der KTA 3501 (Gründruck) /KTA14b/ und der KTA 3503 /KTA13/ zu finden. Die KTA 3501 enthält Anforderungen bezüglich des Eignungsnachweises und der Auslegung neu entwickelter oder modifizierter Geräte für die Ausführung von A-Funktions-Einrichtungen. In der KTA 3503 und der KTA 3507 werden Anforderungen an Äquivalenzbauelemente formuliert. Die Dokumente RS1180 /GRS10/, EPRI 1016731 /ERP08/, IAEA NS-G-1.3 /IAE12/, IEEE Std 1633-2008 /IEE08/, IEEE Std 603-2009 /IEE09/, IEEE Std 7-4.3.2-2010 /IEE10/ sowie die NUREG 6303 /NUR94/ und 7007 /NUR10/ enthalten keine konkreten Anforderungen zur Thematik Ersatzbaugruppen

4.2.1 KTA 3501, „Reaktorschutzsystem und Überwachungseinrichtungen des Sicherheitssystems“

In der KTA 3501 /KTA14b/ werden in Abschnitt 5.1.1.2 bezüglich des Eignungsnachweises für neu entwickelte oder modifizierte Geräte für die Ausführung von A-Funktions-Einrichtungen folgende Anforderungen aufgestellt:

- Nachweis der Fertigungs- und Designqualität von leittechnischen Baugruppen, Geräten und Systemteilen.

- Erforderliche Qualität von Fertigung und Design muss mindestens Stufe B nach DIN EN 61192-1 genügen.
- Es ist eine Typprüfung abzulegen.

In Abschnitt 5.1.1.3 werden Anforderungen an die Auslegung neu entwickelter oder modifizierter Geräte für die Ausführung von A-Funktions-Einrichtungen aufgestellt. Es werden folgende Anforderungen genannt:

- Einfaches, übersichtliches und zweckentsprechendes Schaltungskonzept
- Verwendung von bewährten, zuverlässigen Bauteilen und Schaltungen, Beachtung von Betriebserfahrungen
- Prüfung der Gerätefunktionen muss ohne Eingriff in die Verdrahtung möglich sein
- Auslegung gegen Umgebungseinflüsse
- Bezüglich statischer und dynamischer Eigenschaften muss den Anforderungen der A-Funktionen genügt werden (Stabilität, Genauigkeit, Nutz-Störsignalverhältnis, Drift, Hysterese, Zeitverhalten, Reproduzierbarkeit)

Für Geräte zur Ausführung von B-Funktions-Einrichtungen sind in den Abschnitten 5.2.1.2 und 5.2.1.3 nahezu identische Anforderungen aufgestellt. Lediglich die Anforderung nach einem einfachen, übersichtlichen und zweckentsprechendem Schaltungskonzept ist hier nicht genannt.

4.2.2 KTA 3503 „Typprüfung von elektrischen Baugruppen der Sicherheitsleittechnik“

In der KTA 3503 /KTA13/ werden in Abschnitt 4.2.6 „Hardwareunterlagen“ Äquivalenzbauelemente angesprochen. Dort sind folgende Forderungen aufgestellt:

- Sind Bestückungsvarianten durch den Einsatz von Äquivalenzbauelementen bei der Fertigung vorgesehen, sind diese in der Stückliste zu spezifizieren und in der Typprüfung zu berücksichtigen. Bei entsprechender Gleichwertigkeit der eingesetzten Bauelemente kann eine theoretische Betrachtung der Äquivalenzen ausreichen. /KTA13/

In Abschnitt 4.3.2 „Ausfallratenbestimmung für die Hardware der Baugruppe aufgrund von Betriebserfahrung“ wird auf die Ermittlung von Ausfallraten neuentwickelter oder modifizierter Baugruppen eingegangen. Zur Ausfallratenermittlung neuentwickelter oder modifizierter Baugruppen sind laut KTA 3503 Ausfallraten vergleichbarer Baugruppen oder Funktionseinheiten zu verwenden, wenn bestimmte Bedingungen erreicht wurden (ausreichende Anzahl an Betriebsstunden, ausreichende Anzahl verwendeter Baugruppen und vergleichbare Betriebsbedingungen). Laut KTA 3503 /KTA13/ müssen Baugruppen oder Funktionseinheiten mindestens in folgenden Aspekten vergleichbar sein:

a) elektrische Bauelemente,

b) Konstruktionselemente,

c) Firmware,

d) Datei zum Programmieren der Bauelemente (z. B. bei FPGA, CPLD, ASIC),

e) Auslegungsgrundsätze und

f) Umgebungsbedingungen.

4.3 Anforderungen an die Diversität

Im betrachteten nationalen und internationalen Regelwerk finden sich eine Reihe von Anforderungen an die Diversität von programmierbaren und rechnerbasierten Baugruppen, Komponenten oder Systemen. Diese werden in den folgenden Abschnitten beschrieben.

4.3.1 KTA 3501 „Reaktorschutzsystem und Überwachungseinrichtungen des Sicherheitssystems“

Die KTA 3501 /KTA14b/ enthält in Abschnitt 4.1.3.1 folgende grundsätzliche Forderung nach Diversität für leittechnische Einrichtungen, die Funktionen der Kategorie A ausführen:

- Bei der Auslegung von A-Funktions-Einrichtungen sind die Potentiale für und die Auswirkungen von systematischem Versagen der leittechnischen Einrichtungen auf die Störfallabläufe unter Berücksichtigung der verfahrenstechnischen Vorgaben zu

analysieren. Es sind Vorkehrungen gegen systematisches Versagen zur Minderung von dessen Eintrittswahrscheinlichkeit derart zu treffen, dass es zum Nachweis der Störfallbeherrschung nicht mehr unterstellt werden muss.
Kann eine Nachweisführung nach [der o. g. Anforderung] nach dem Stand von Wissenschaft und Technik nicht erfolgen, sind Vorkehrungen derart zu treffen, dass ein systematisches Versagen von Hardware und Software der A-Funktions-Einrichtungen durch diversitäre oder dissimilare leittechnische Einrichtungen mit gleichen Qualitätsanforderungen beherrscht wird. Diversitätsgrad und Struktur sind dabei derart zu wählen, dass das systematische Versagen mit den damit verbundenen Auswirkungen die Störfallbeherrschung durch die verbleibenden diversitären Einrichtungen nicht unzulässig beeinflusst.

In der KTA 3501 /KTA14b/ wird damit auch der Begriff „dissimilare leittechnische Einrichtungen“ eingeführt. Dieser Begriff soll bei Einsatz vergleichbarer Technologien durch die Bewertung unterschiedlicher Aspekte die hinreichende Unähnlichkeit der Systeme ausdrücken. Die hierbei zu bewertenden Aspekte sind:

- Hardware
- Software
- Entwicklungswerkzeuge
- Entwicklungsteams
- Fertigung
- Test
- Instandhaltung

Anforderungen an die Auslegung neu entwickelter oder modifizierter Geräte

- Es sollen bewährte und zuverlässige Bauteile und Schaltungen vorgesehen werden, Betriebserfahrungen sind zu beachten.

Zuverlässigkeit und Qualitätsprüfung

- Es sind Angaben über die Zuverlässigkeit der Gerätetypen zu machen, zum Beispiel durch statistische Methoden, Ausfalleffektanalysen, Grenzbelastungsprüfungen oder durch Auswertung von Betriebserfahrungen.

4.3.2 KTA 3503 „Typprüfung von elektrischen Baugruppen der Sicherheitsleittechnik“

In der KTA 3503 /KTA13/ sind keine Kriterien zur Bewertung von Diversität in softwarebasierten Systemen vorhanden.

In Abschnitt 4.3 „Ermittlung der Zuverlässigkeitsangaben“ findet sich unter anderem folgende Anforderung:

- Die Verfahren zur Ermittlung der Zuverlässigkeitsangaben der Hard- und Softwarekomponenten sind anzugeben.
  Hinweis: Über die Verfahren zur quantitativen Zuverlässigkeitsermittlung von Software liegen zurzeit in der Fachwelt keine anerkannten Methoden vor. Deshalb muss der Nachweis der Softwarezuverlässigkeit bei der Typprüfung qualitativ geführt werden. /KTA13/

4.3.3 KTA 3507 „Werksprüfungen, Prüfungen nach Instandsetzung und Nachweis der Betriebsbewährung der Baugruppen und Geräte der Leittechnik des Sicherheitssystems“

In der KTA 3507 /KTA14a/ sind keine Kriterien zur Bewertung von Diversität in softwarebasierten Systemen vorhanden.

4.3.4 Bericht zum Vorhaben RS1180 „Weiterentwicklung und Erprobung von Methoden und Werkzeugen für probabilistische Sicherheitsanalysen“

Im Abschlussbericht /GRS10/ „Entwicklung eines aktualisierten Ansatzes zur Berücksichtigung softwarebasierter Sicherheitsleittechnik in der PSA“ des Reaktorsicherheitsvorhabens RS1180 wird darauf hingewiesen, dass der Einsatz diversitärer (dissimilarer) Sicherheitsleittechnik unter Verwendung diversitärer (dissimilarer) Hard- und Software gegenwärtig bei nationalen und internationalen Gutachterorganisationen als eine wegweisende Lösung zur Beherrschung gemeinsam verursachter Ausfälle betrachtet wird. Ein gleichzeitiges Versagen mehrerer, zueinander diversitärer (dissimilarer) Einrichtungen aufgrund einer gemeinsamen Ursache wird dabei durch den Einsatz möglichst unähnlicher redundanter Einrichtungen verhindert.

Es wird darauf hingewiesen, dass sowohl in der deterministischen als auch in der probabilistischen Sicherheitsbewertung die Einführung von Diversität (Dissimilarität) zu berücksichtigen ist. Dazu ist laut /GRS10/ zukünftig ein Bewertungsschema für den Diversitätsgrad der Hard- und Software zu entwickeln, in dem die relevanten Faktoren bzw. Merkmale für die Bewertung der Diversität (Dissimilarität) und deren Beitrag hinsichtlich der Beherrschung eines gemeinsam verursachten Ausfalls enthalten sind.

Die Bestimmung der Zuverlässigkeit der Hardware softwarebasierter Leittechnik kann konventionell auf der Grundlage der empirisch gewonnenen Ausfallhäufigkeiten (Ausfallraten) erfolgen, deren Ausfälle dann im Fehlerbaummodell des zu analysierenden Systems berücksichtigt werden. Für die Bestimmung der Ausfallarten der Hardware ist prinzipiell die Methode der Fehlerart- und Effektanalyse (FMEA) geeignet. Für die probabilistische Bewertung der Software existieren bisher keine anerkannten Methoden.

Die wesentlichen Modelle zur Bewertung der Software-Zuverlässigkeit stammen aus einer Phase, die vom Beginn der 70er Jahre bis in die 80er Jahre reicht. In diesem Zeitraum wurde intensiv an dieser Problematik gearbeitet. In der Folge hat sich hinsichtlich der Software-Zuverlässigkeit das Interesse der Industrie vermehrt auf die konstruktive Seite verlagert (fortschrittliche Software-Entwicklungsumgebungen, Standards und Methoden zur Qualitätssicherung der Software), während Software-Zuverlässigkeitsmodelle praktisch nicht mehr weiter entwickelt wurden.

In der Fachliteratur und auf Fachveranstaltungen (u. a. SAFECOMP, PSAM 09, PSAM 10) wurden moderne Verfahren zum Thema Risikobewertung und Risikomanagement in verschiedenen Industriezweigen unter den Aspekten Sicherheit, Sicherung und Zuverlässigkeit vorgestellt und diskutiert. Es ist deutlich geworden, dass in naher Zukunft keine etablierte Methode zur quantitativen Zuverlässigkeitsbewertung von softwarebasierten Einrichtungen zu erwarten ist.

4.3.5 NUREG 6303 „Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems“

Im NUREG 6303 /NUR94/ wurde von der US NRC eine Methode entwickelt, um Möglichkeiten von gemeinsam verursachten Ausfällen in rechnerbasierten Reaktorschutzsystemen aufzudecken. Als wichtigstes Mittel gegen gemeinsam verursachte Ausfälle wird hier Diversität genannt. In diesem Zusammenhang werden verschiedene

Attribute definiert, die bezüglich ihrer Diversität untersucht werden können. Diese Attribute sind

- Diversität im Design
- Diversität der Geräte
- Funktionale Diversität
- Diversität des Personals
- Diversität der Signale
- Diversität der Software

Zur Beurteilung der Diversität eines Systems soll nach NUREG 6303 /NUR94/ das Leittechniksystem in Blöcke unterteilt werden, die dann hinsichtlich der verschiedene Diversitätsattribute untersucht werden. Unter einem Block wird hierbei die kleinste Teilmenge von Bauelementen und Software verstanden, bei dem angenommen werden kann, dass ein interner Fehler (inklusive Softwarefehler) in diesem Block nicht zu anderen Komponenten und Software weiterpropagiert. Beispiele für Blöcke sind Computer, LAN, Multiplexer und PLCs.

4.3.6 NUREG 7007 „Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems"

Der NUREG 7007 /NUR10/ ist eine Weiterentwicklung des NUREG 6303 /NUR94/. Im NUREG 7007 werden Strategien entwickelt, um gegen das Potential von gemeinsam verursachten Ausfällen von computerbasierten Reaktorschutzsystemen auszulegen. Als Grundlage für diese Strategien dienen hierzu die im NUREG 6303 /NUR94/ entwickelten Diversitätsattribute. Die Attribute haben sich leicht verändert, sie sind im NUREG 7007

- Design
- Baugruppen/Komponenten Hersteller
- Informationsverarbeitungssysteme
- Funktional
- Lebenszyklus

- Logik
- Signale
- Andere Diversitätsbetrachtungen

Im NUREG 7007 werden drei verschiedene Strategien genannt, die unterschiedliche Grade an Diversität beschreiben.

Strategie A bezieht sich auf die Verwendung von fundamental diversitären Technologien. Betrachtet werden hier Hersteller der Komponenten, Verarbeitungsgeräte, funktionale Diversität, Diversität im Lebenszyklus und in der Logik.

Strategie B bezieht sich auf die Verwendung von deutlich unterschiedlichen Technologien. Diese können aber zum Beispiel auch unterschiedliche digitale Technologien sein.

Strategie C bezieht sich auf die Verwendung von konstruktiven Variationen einer Technologie.

Darüber hinaus werden im NUREG 7007 die in NUREG 6303 entwickelten Attribute näher betrachtet. Es werden Ansätze für Diversitätsausprägungen der verschiedenen Attribute genannt (Beispiel Attribut Design: Ansätze sind hier verschiedene Technologien, unterschiedlicher Zugang bei gleicher Technologie, verschiedene Architekturen einer Technologie).

Darüber hinaus wird untersucht, wie Diversität in nichtnuklearen Industrien als Mittel gegen gemeinsam verursachte Ausfälle eingesetzt wird und wie sich die Strategien A,B und C dort wiederfinden. Eine solche Untersuchung wird auch für die nukleare Industrie international durchgeführt.

4.3.7 EPRI Bericht 1016731 „Operating Experience Insight on Common-Cause Failures in Digital Instrumentation and Control Systems“

Der EPRI Bericht 1016731 /EPR08/ „Operating Experience Insight on Common-Cause Failures in Digital Instrumentation and Control Systems“ wurde unter anderem aus dem Grund verfasst, Erkenntnisse aus der Betriebserfahrung von U.S. Kernkraftwerken zur Verbesserung von Diversitätsbewertungen und zur Verbesserung des Schutzes der

Kernkraftwerke gegen gemeinsam verursachte Ausfälle aufgrund von Fehlern in digitalen Leittechniksystemen zu nutzen. Dabei wurde unter anderem betrachtet, welche Arten von Diversität einen effektiven Schutz digitaler Leittechniksysteme gegen systematische Fehler bieten.

Es wurden 27 Ereignisse gefunden, bei denen es zu Fehlern in mehreren Redundanzen des Sicherheitssystems kam. Die meisten dieser Fehler (18 von 27) resultierten in Effekten in Teilsystemen oder Kanälen, wobei die Sicherheitsfunktionen weiterhin ausgeführt werden konnten. Dies wird auf das Vorhandensein von funktionaler Diversität oder Signal-Diversität zurückgeführt. /EPR08/

In dem Bericht /EPR08/ wurde das folgende Ereignis beschrieben. In einem Kernkraftwerk kam es im Jahr 1991 aufgrund eines Blitzschlags zur Abschaltung des Generators und zu einer Absenkung der Reaktorleistung. Nach etwa 35 Sekunden erfolgte eine Reaktorschnellabschaltung aufgrund eines zu geringen Abstandes zum Filmsieden (DNB-Verhältnis zu gering). Nach dem Ereignis durchgeführte Untersuchungen haben ergeben, dass die Reaktorschnellabschaltung um 16 Sekunden verzögert erfolgt ist. Der Grund dafür war, dass im Steuerstabfahrrechner eine Funktion zur Detektion einer Reaktorleistungsabsenkung einprogrammiert wurde, indem der Einfall einiger Steuerstabgruppen erkannt wird. Wird eine Reaktorleistungsabsenkung erkannt, führt dies dazu, dass die Position dieser Steuerstäbe für 16 Sekunden ignoriert wird, um eine unnötige Reaktorschnellabschaltung zu verhindern. In dem vorliegenden Ereignis kam es zu einem unerwünschten Einfahren von Steuerstäben nach dem erfolgreichen Absenken der Reaktorleistung, weshalb der Steuerstabfahrrechner eine zweite Reaktorleistungsabsenkung vermutete und somit eine zweite Verzögerung von 16 Sekunden einleitete. Nachdem die Verzögerungszeit abgelaufen war, erkannte die Kernüberwachung eine Abweichung der Steuerstäbe von der vorgesehenen Position, woraufhin aufgrund des geringen Abstandes zum Filmsieden die Reaktorschnellabschaltung erfolgte.

Laut /EPR08/ war das oben beschriebene Ereignis ein systematischer Fehler in einem Teilsystem des Reaktorschutzsystems. Es hatte aber nur einen geringen Einfluss auf das Sicherheitssystem, da diversitär vorhandene Schnellabschaltsignale nicht betroffen waren. Durch das Ereignis wurde laut /EPR08/ aufgezeigt, dass ein Fehler in einem Teilsystem nicht zu einem Ausfall des gesamten Reaktorschutzsystems führen muss, wenn das Reaktorschutzsystem über eine ausreichende Diversität verfügt, z. B. in Form von unterschiedlichen Anregekriterien die eine Schnellabschaltung auslösen können.

Das Ereignis hat aber laut /EPR08/ auch aufgezeigt, dass einige Diversitätsmerkmale wie z. B. die Plattform-Diversität nicht in allen Situationen effektiv sind. Wären bei dem beschriebenen Ereignis diversitäre Systemplattformen in redundanten Reaktorschutzteilen verwendet worden, hätte dies auf dieses Ereignis laut /EPR08/ keinen Einfluss gehabt, da der Fehler im Systemdesign lag. Eine diversitäre Systemplattform mit der gleichen Logik hätte somit den gleichen Fehler verursacht.

4.3.8 IAEA NS-G-1.3 „Instrumentation and Control Systems Important to Safety in Nuclear Power Plants“

Im IAEA Safety Guide NS-G-1.3 „Instrumentation and Control Systems Important to Safety in Nuclear Power Plants“ /IAE12/ wird Diversität als ein Prinzip beschrieben, bei dem

- verschiedene Parameter überwacht sowie
- verschiedene Technologien,
- verschiedene Logiken oder Algorithmen oder
- verschiedene Möglichkeiten zur Ansteuerung

genutzt werden, um mit unterschiedlicher Art und Weise ein Ereignis zu detektieren und darauf zu reagieren.

Es werden verschiedene Arten von Diversität erwähnt:

- Menschliche Diversität
- Design-Diversität
- Software-Diversität
- Funktionale Diversität
- Signal-Diversität
- Diversität der Ausrüstung
- Diversität des Systems

Typischerweise sollen laut /IAE12/ verschiedene Arten von Diversität in einem System vorliegen. Als besonders wirksam werden die funktionale Diversität und die Signal-Diversität angesehen. Funktionale Diversität wird in /IAE12/ beschrieben als das Vorhandensein mehrerer Systeme, welche unterschiedliche physikalische Funktionen bereitstellen, die überlappend auf die Sicherheit wirken. Signal-Diversität wird als Überwachung unterschiedlicher Parameter beschrieben, welche Schutzmaßnahmen auslösen können.

In jeder Anwendung muss laut /IAE12/ darauf geachtet werden, dass tatsächlich Diversität im verwendeten Design erreicht wird und über die gesamte Laufzeit des Kraftwerks erhalten bleibt. Der Designer muss das Design untersuchen, um die Möglichkeit von Gemeinsamkeiten in Teilen, die eigentlich diversitär sein sollen, auszuschließen. Dazu gehören z. B. Werkstoffe, Bauteile, Fertigungsverfahren, Software oder Arbeitsprinzipien.

Die Diversität der Ausrüstung oder der zugehörigen Software des Leittechniksystems wie beispielsweise des Betriebssystems sollte laut /IAE12/ auch auf die Bauteile der Ausrüstung ausgeweitet werden. Beispielsweise könnten verschiedene Hersteller den gleichen Prozessor oder das gleiche Betriebssystem nutzen, wodurch die potenzielle Möglichkeit für Fehler gemeinsamer Ursache gegeben wird.

Im Hinblick auf Software-Diversität reicht es laut /IAE12/ nicht aus, wenn verschiedene Softwareversionen mit den gleichen Anforderungsspezifikationen an die Software entwickelt werden. Dadurch bestünde die Möglichkeit, dass unabhängig voneinander entwickelte Programmversionen gemeinsame Fehler besitzen. Zusätzlich genutzte Arten von Diversität wie funktionale Diversität oder Signal-Diversität werden laut /IAE12/ als wirksamste Möglichkeit gesehen, dieses Problem zu lösen.

Zuverlässigkeit ist ein wichtiges Merkmal sicherheitstechnisch wichtiger Systeme. Die Anforderungen an das Design fordern für alle Strukturen, Systeme und Komponenten sicherheitstechnisch wichtiger Systeme, dass diese so aufgebaut sind, dass ihre Güte und Zuverlässigkeit ihrer Klassifikation entsprechen. Insbesondere sind zuverlässige, sicherheitstechnisch wichtige Leittechniksysteme notwendig, um unzulässigen Anforderungen an die Unversehrtheit physikalischer Barrieren vorzubeugen und um die Zuverlässigkeit der technischen Schutzsysteme zu sichern.

Um sicherzustellen, dass die Anforderungen an die Zuverlässigkeit des Designs für sicherheitstechnisch wichtige Leittechniksysteme eingehalten werden, sollte typischerweise eine angemessene Kombination probabilistischer und deterministischer Merkmale zum Einsatz kommen. Für hardwarebezogene Systemfehler sollten typischerweise quantitative Zuverlässigkeitszahlen bereitgestellt werden. Beim Design sicherheitstechnisch wichtiger Leittechniksysteme sollten Eigenschaften wie die Toleranz gegen Zufallsfehler, die Toleranz gegen gemeinsam verursachte Ausfälle, ausfallsicheres Design, die Unabhängigkeit von Ausrüstung und Systemen, die Verwendung von Ausrüstung hoher Qualität, die Testbarkeit und die Instandhaltbarkeit als zweckmäßig erachtet werden.

Umso besser die Zuverlässigkeit einzelner Komponenten eines Leittechniksystems ist, umso besser ist die Zuverlässigkeit des gesamten Systems. Es gibt allerdings praktische Grenzen für die Zuverlässigkeit einzelner Komponenten. Die Zuverlässigkeit wird durch den Einsatz von Diversität erhöht. Zum Beispiel ist es möglich, die Reaktorleistung mit mehreren Kanälen aufzuzeichnen oder durch diversitäre Mittel wie die Messung des Neutronenflusses oder der Temperatur und über Durchflussmessungen oder Druckmessungen. Die Nutzung redundanter Messungen schützt vor Zufallsfehlern. Die Nutzung von Diversität schützt vor Fehlern gemeinsamer Ursache.

Die für jedes System benötigte Zuverlässigkeit hängt von der Bedeutung der Systemfunktionen für die Sicherheit des Kernkraftwerks ab und sollte typischerweise während des Designs spezifiziert werden. Je wichtiger das Leittechniksystem für die Sicherheit ist, desto höher sollte die Zuverlässigkeit des Systems sein. Eine Herangehensweise zur Spezifizierung der geforderten Zuverlässigkeit ist, numerische Zuverlässigkeitszahlen zu verwenden. Eine andere Herangehensweise ist, deterministische Designmerkmale auf der Basis von ingenieurmäßiger Bewertung zu spezifizieren. In den meisten Fällen wird eine Kombination aus probabilistischen und deterministischen Methoden verwendet.

Sicherheitssysteme sollten dem Einzelfehlerkriterium genügen und das Potential für gemeinsam verursachte Ausfälle sollte bei der Auslegung berücksichtigt werden. Beim Design von Sicherheitssystemen sollten die potentiellen Ursachen für Fehler sorgfältig identifiziert und untersucht werden um festzulegen, wo die Anwendung des Diversitätsprinzips sinnvoll ist.

Wo der Nachweis der Zuverlässigkeit des Systems nicht erbracht werden kann, sollte zusätzlicher Konservatismus eingesetzt werden, beispielsweise wenn die Zuverlässigkeit eines mehrfach redundanten Systems durch Faktoren wie gemeinsam verursachte Ausfälle oder Unsicherheiten im Design begrenzt wird. Spezifische Schwierigkeiten können beispielsweise bei dem Nachweis der Zuverlässigkeit von rechnerbasierten Systemen auftreten. Diversität ist eine Möglichkeit, um Konservatismus zu integrieren um die Schwierigkeiten beim Zuverlässigkeitsnachweis zu kompensieren.

Anforderungen wie Redundanz, Diversität, der Einsatz von bewährter Ausrüstung, Testbarkeit, durchgehende Überwachung und Instandhaltbarkeit werden angewendet um einen zusätzlichen Anstieg der Zuverlässigkeit über das zum Erreichen des Einzelfehlerkriteriums notwendige Maß zu erzielen.

In der Bewertung der Zuverlässigkeit von digitalen Leittechniksystemen sollten die Effekte von möglichen Hardware- und Software-Fehlern sowie die Designmerkmale zu Verhinderung oder Limitierung von deren Auswirkungen berücksichtigt werden. Bei den Hardware-Fehlern sollten sowohl Fehler von Teilen des Rechners als auch von Teilen der Kommunikationssysteme berücksichtigt werden. Sowohl permanente als auch flüchtige Fehler sollten berücksichtigt werden.

Software-Fehler sind durch Fehler im Design verursachte systematische Fehler, weswegen diese nicht das Verhalten zufälliger Fehler aufweisen, welches in der Hardware-Zuverlässigkeitsanalyse angenommen wird. Als Folge daraus können unterschiedliche Methoden notwendig sein, um die durch Hardware und Software eingeführte Unzuverlässigkeit bewerten zu können. Zum Beispiel kann die Zuverlässigkeit von rechnerbasierten Systemen auf Basis einer qualitativen Auswertung demonstriert werden, bei der die Komplexität des Designs, die Qualität von Verifikation, Validation und dem Test des Entwicklungsprozesses über einen weiten Bereich von Eingangsbedingungen sowie die Betriebserfahrung berücksichtigt werden.

4.3.9 IEEE Std 1633-2008 „IEEE Recommended Practice on Software Reliability“

Im IEEE Standard 1633-2008 „IEEE Recommended Practice on Software Reliability“ /IEE08/ wird funktionale Diversität diskutiert. Als Bespiel für funktionale Diversität wird

die Überwachung von sowohl Temperatur als auch Druck bei der Dampferzeugung genannt, wobei weder Druck noch Temperatur die Sicherheitskriterien überschreiten dürfen. Eine weitere Möglichkeit wäre die Nutzung von zwei zueinander diversitären Rechenprogrammen, aber laut /IEE08/ wird der Einsatz von funktionaler Diversität dieser Lösung vorgezogen. Der Grund dafür ist, dass die Unabhängigkeit von zwei diversitären Funktionen einfacher nachzuweisen ist als die Unabhängigkeit von zwei Rechenprogrammen.

Es bestehen mindestens zwei signifikante Unterschiede zwischen der Zuverlässigkeit von Hardware und Software. Der erste Unterschied besteht darin, dass Software nicht altert oder verschleißt. Der zweite Unterschied besteht darin, dass die Softwarebeschreibungen innerhalb der Speicher der Computer zugänglich sind, wodurch jede beliebige Zeile Programmcode einen Fehler enthalten kann, welcher nach Ausführung imstande ist, eine Fehlfunktion zu verursachen.

4.3.10 IEEE Std 603-2009 „IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations“

Der IEEE Standard 603-2009 „IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations“ /IEE09/ enthält keine Anforderungen zum Thema Diversität.

4.3.11 IEEE Std 7-4.3.2-2010 „IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations“

Im IEEE Standard 7-4.3.2-2010 „IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations“ /IEE10/ wird ausgesagt, dass ein gemeinsam verursachter Ausfall mehrerer digitaler Komponenten nicht unterstellt werden muss, wenn eine hinreichende Diversität zwischen diesen Komponenten vorliegt. Für Verfahren und Richtlinien um eine hinreichende Diversität zwischen digitalen Komponenten zu erreichen, wird in /IEE10/ auf NUREG 6303 verwiesen.

In /IEE10/ werden folgende Hinweise bezüglich Diversität gegeben:

- Die Diversität der Ausrüstung oder der Systemsoftware wie beispielsweise des Betriebssystems sollte sich bis auf die einzelnen Komponenten der Ausrüstung erstrecken, um sicher zu gehen, dass tatsächlich Diversität erreicht wird. Als Beispiel wird

angeführt, dass verschiedene Hersteller den gleichen Prozessor oder das gleiche Betriebssystem nutzen könnten, wodurch gemeinsam verursachte Fehler auftreten könnten.

- Bezüglich Software-Diversität deutet die Betriebserfahrung darauf hin, dass keine Diversität erreicht wird, wenn mehrere Softwareversionen verwendet werden, die mit den gleichen Anforderungsspezifikationen an die Software entwickelt wurden.

Um eventuell vorhandene Schwachstellen in Sicherheitssystemen bezüglich der Möglichkeit gemeinsam verursachter Ausfälle zu verhindern, sollen laut /IEE10/ Back-up-Systeme genutzt werden, um eine diversitäre Möglichkeit zur Ausführung der Sicherheitsfunktion bereitzustellen. Diese diversitäre Einrichtung

- soll nicht der gleichen Schwachstelle unterliegen,
- soll entweder die gleiche Funktion oder eine andere Funktion, welche aber den Ereignisverlauf entschärft, ausführen,
- kann im nicht sicherheitsrelevanten Teil der Ausrüstung eingebaut sein, muss dann aber eine ausreichende Güte besitzen,
- kann automatisch oder manuell oder durch eine Kombination von beidem ausgelöst werden,
- soll von Energiequellen versorgt werden, die auch während eines Ereignisses, für welches die Einrichtung vorgesehen ist, verfügbar sind (z. B. während und nach dem Ausfall der externen Spannungsversorgung),
- soll in den Umgebungsbedingungen, die während des Ereignisses, für welches die Einrichtung vorgesehen ist, herrschen, betrieben werden können.

Diversitäre manuelle Maßnahmen können laut /IEE10/ als Back-up für aufgrund eines gemeinsam verursachten Ausfalls ausgefallene automatische Sicherheitsfunktionen genutzt werden. Voraussetzung dafür ist, dass die manuelle Maßnahme zuverlässig ausgeführt werden kann. Der Operator sollte dazu für die benötigte Handlung ausreichende Anzeigen und Bedienelemente auf der Warte haben, welche diversitär zu denen sind, die bei dem gemeinsam verursachten Ausfall ausgefallen sind.

Laut /IEE10/ können auch diversitäre automatische Maßnahmen als Back-up für durch einen gemeinsam verursachten Ausfall ausgefallene Sicherheitsfunktionen dienen.

Dazu sollen diese automatischen Maßnahmen durch eine Einrichtung bereitgestellt werden, die nicht durch den gleichen gemeinsam verursachten Ausfall betroffen ist. Die Einrichtung kann sowohl programmierbar oder rechnerbasiert als auch nicht programmierbar sein. Um die Ausführung der automatischen diversitären Maßnahmen verfolgen zu können, sollen entsprechende Anzeigen dazu auf der Warte verfügbar sein. Die Einrichtung für die diversitären automatischen Maßnahmen soll so ausgelegt sein, dass die Möglichkeit einer ungewollten Auslösung und die Belastung für das Sicherheitssystem begrenzt werden. Außerdem soll die Einrichtung für die diversitären automatischen Maßnahmen so ausgelegt sein, dass die Anregung erst nach Überschreitung der Anregebedingungen für das Sicherheitssystem erfolgt. Die Auslegung der automatischen diversitären Maßnahmen muss so erfolgen, dass der Anlagenzustand innerhalb der durch die Regulierungsbehörde vorgegebenen Grenzen gehalten werden kann. Des Weiteren müssen die automatischen diversitären Maßnahmen von ausreichender Qualität sein.

Wenn Zuverlässigkeitsziele aufgestellt werden, sollte der Nachweis, dass diese Ziele erreicht werden, auch die Software berücksichtigen. Die Methode zur Bestimmung der Zuverlässigkeit kann Kombinationen von Analysen, Betriebserfahrung oder Prüfungen berücksichtigen.

4.3.12 DIN-Normen

Hinsichtlich der Anforderungen an leittechnische Systeme in Kernkraftwerken in Bezug auf Diversität, Zuverlässigkeit und CCF sind eine Reihe von DIN-Normen relevant:

- DIN 60880 „Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Softwareaspekte für rechnerbasierte Systeme zur Realisierung von Funktionen der Kategorie A“. /DIN10a/
- DIN 61513 „Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Allgemeine Systemanforderungen“ /DIN13/, sowie
- DIN 62340 „Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Anforderungen zur Beherrschung von Versagen aufgrund gemeinsamer Ursache“ /DIN10d/

Die in den genannten Normen enthaltenen Aussagen und Anforderungen werden thematisch sortiert im Folgenden zusammengefasst.

Ursachen von Softwarefehlern

DIN 61513 „Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Allgemeine Systemanforderungen“ /DIN13/:

- *„Softwareversagen: Systemversagen infolge der Aktivierung eines Auslegungsfehlers in einer Softwarekomponente“* /DIN13/
- *„Jedes Softwareversagen hat seine Ursache in Auslegungsfehlern, weil Software sich nicht abnützt oder von physikalischen Ausfällen abhängt. Die Aktivierung von Auslegungsfehlern der Software während des Betriebs erfolgt zufällig, daher tritt auch Softwareversagen zufällig ein.“* /DIN13/

DIN 60880 „Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Softwareaspekte für rechnerbasierte Systeme zur Realisierung von Funktionen der Kategorie A“ /DIN10a/:

- „*Der grundlegende Ansatz für das Treffen von Maßnahmen gegen Softwarefehler ergibt sich aus der Überlegung, dass jeder Softwarefehler so lange im betroffenen System oder Kanal verbleibt, bis er erkannt und berichtigt ist, und dass jeder Softwarefehler vor der Berichtigung ein Versagen aufgrund einer den fehlerhaften Programmteil ansprechenden Signaltrajektorie verursachen kann. Wenn der Fehler in zwei oder mehr Systemen oder Kanälen, die unterschiedliche Maßnahmenstufen gegen die Auswirkungen desselben anzunehmenden Versagen auslösenden Ereignisses realisieren, enthalten ist, und diese den spezifischen Signaltrajektorien innerhalb eines kritischen Zeitintervalls ausgesetzt werden, können beide (oder alle) Systeme oder Kanäle versagen, d. h. es tritt ein CCF ein.“* /DIN10a/
- *„Die Möglichkeit eines durch Softwarefehler verursachten CCF unterschiedlicher Systeme oder unterschiedlicher Kanäle eines Systems besteht, wenn gleiche Software oder gleiche Software-Module verwendet werden. Potentielle Quellen latenter Fehler sind Auslegungsfehler aufgrund der Anforderungs-Spezifikation für das leittechnische System, die Architektur, Algorithmen, Entwicklungsverfahren, Werkzeuge, Realisierungsverfahren oder die Wartung. Anforderungen, die nicht richtig verstanden oder korrekt umgesetzt werden, können Ursache für Fehler in der Software-Spezifikation sein, die das Risiko von CCF bei einem Ansprechen des so entstandenen Softwarefehlers erhöhen. Mängel in der Software können durch fehlerhafte, unvollständige, ungeeignete oder missverstandene Software-Anforderungen und -Spezifikationen verursacht werden. Auslegungsfehler, die zu Softwarefehlern*

führen, können in verschiedene Programme eingebracht werden, und zwar infolge üblicher gleicher Praxis bei Schulung, Organisation, Denkprozessen und Auslegungsansätzen. Andere mögliche Ursachen von CCF können durch die Verbindung von Systemen mit anderen Systemen entstehen, in denen Software geringerer Qualität verwendet wird.“ /DIN10a/

Software-CCF

DIN 62340 „Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Anforderungen zur Beherrschung von Versagen aufgrund gemeinsamer Ursache“ /DIN10d/:

- „*Da es nicht möglich ist, die Fehlerfreiheit für ein einzelnes leittechnisches System vollständig nachzuweisen, können daher im Prinzip auch das Bestehen von latenten Fehlern und von entsprechenden Auslösemechanismen nicht* ausgeschlossen *werden. Folglich kann auch das Auftreten von CCF für ein einzelnes leittechnisches System nicht ausgeschlossen werden.*“ /DIN10d/

- „*Die Reduktion der Wahrscheinlichkeit eines koinzidenten Fehlers für unabhängige leittechnische Systeme auf einen vernachlässigbaren Wert macht es notwendig, dass die Systeme mit verschiedenen Signaltrajektorien betrieben werden und hinreichend gegen physikalische Gefahren geschützt sind. Unterschiedliche Signaltrajektorien können durch die Anwendung von Diversität (z. B. Gerätediversität oder funktionale Diversität) sichergestellt werden.*“ /DIN10d/

  DIN 60880 „Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Softwareaspekte für rechnerbasierte Systeme zur Realisierung von Funktionen der Kategorie A“ /DIN10a/:

- „*Änderungsmaßnahmen für Software haben das Potential, CCF zu* verursachen*. Die bei der Änderung von Software oder Daten verwendeten Verfahren sollten sicherstellen, dass solche Fehler nicht eingeschleppt werden.*“ /DIN10a/

- „*Wenn in* mehreren *Systemen dieselben Softwaremodule verwendet werden, sind diese zu identifizieren und die Zuverlässigkeit solcher gemeinsamer Module muss sichergestellt werden.*“ /DIN10a/

Zuverlässigkeit

DIN 61513 „Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Allgemeine Systemanforderungen“ /DIN13/:

- „*Die* Zuverlässigkeit *eines rechnerbasierten Systems umfasst die Zuverlässigkeit seiner Hardware, die gewöhnlich qualifiziert wird, und die Zuverlässigkeit seiner Software, die gewöhnlich ein qualitatives Maß darstellt, weil es keine allgemein anerkannten Mittel für die Qualifizierung der Softwarezuverlässigkeit gibt.*“ /DIN13/

- „*Es muss nachgewiesen werden, dass die Zuverlässigkeit der durch das System ausgeführten Anwendungsfunktionen angemessen ist.*“ /DIN13/

- „*Die Ermittlung des Anteils möglicher Softwareauslegungsfehler an der* Zuverlässigkeit *der Funktion sollte auf einer qualitativen Abschätzung beruhen, bei der die Komplexität der Auslegung, die Qualität des Entwicklungsvorgangs und der Rückfluss an Betriebserfahrung berücksichtigt werden. Die Abschätzung sollte auf einem zuvor vereinbarten Verfahren beruhen und sollte dem Nachweis dienen, dass die Softwarequalität der Zielzuverlässigkeit entspricht.*“ /DIN13/

- „*Das Potential von Servicefunktionen für das System, die* Anwendungsfunktionen *zu beeinträchtigen, muss mit einer Strenge analysiert werden, die der Bedeutung der Anwendungsfunktion für die Sicherheit entspricht.*“ /DIN13/

- „*Für Systeme der Klasse 1* [Anm.: entspricht leittechnischen Einrichtungen, die Funktionen der Kategorie A ausführen] *muss in der Zuverlässigkeitsanalyse auch die Eignung der Prüfeinrichtungen für das System* […] *untersucht werden.*“ /DIN13/

- „*Aus der Zuverlässigkeitsanalyse des Systems können sich ergänzende Anforderungen an die detaillierte Auslegung und die Systemarchitektur ergeben, z. B. an den Redundanzgrad oder gar die Wahl der gesamten leittechnischen Architektur.*“ /DIN13/

DIN 60880 „Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Softwareaspekte für rechnerbasierte Systeme zur Realisierung von Funktionen der Kategorie A“ /DIN10a/:

- „*Erreichen der geforderten Software-Zuverlässigkeit: Die in Kernkraftwerken für sicherheitstechnische Zwecke verwendete Software, die oft nur in Notfällen erforderlich ist, muss vor* Verwendung *im Betrieb vollständig validiert und qualifiziert werden. Um die geforderte hohe Zuverlässigkeit zu erreichen, muss während des gesamten Lebenszyklus von den grundsätzlichen Anforderungen über die verschiedenen Entwicklungsphasen bis zu den Verifizierungs- und Validierungs-Prozeduren für Betrieb und Wartung große Sorgfalt aufgewendet werden.*“ /DIN10a/

Diversität

DIN 61513 „Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Allgemeine Systemanforderungen“ /DIN13/:

- „*Bei der Auslegung der* leittechnischen *Architektur sollte das Prinzip der Diversität verwendet werden, wenn für eine Sicherheitsgruppe hohe Zuverlässigkeit verlangt wird und daher Quelle und Auswirkungen von CCF zu berücksichtigen sind.*“ /DIN13/
- „*Wenn Diversität verwendet wird, um die Vorsorge gegen CCF zu unterstützen, sollte die* Auslegung *eine Analyse der Wirksamkeit diversitärer Merkmale mit einschließen, die für eine Minimierung des CCF-Potentials in Anspruch genommen werden.*“ /DIN13/

DIN 60880 „Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Softwareaspekte für rechnerbasierte Systeme zur Realisierung von Funktionen der Kategorie A“ /DIN10a/:

- „*Eine Möglichkeit zur* Erhöhung *der Zuverlässigkeit von Systemen und zur Verringerung des Potentials bestimmter CCF ist die Verwendung der Diversität.*“ /DIN10a/
- „Der Grad der Verbesserung *durch Vorkehrungen gegen CCF und die durch Diversität erreichbare* Steigerung *der Zuverlässigkeit kann nicht quantifiziert werden. Es ist eine Beurteilung erforderlich, die von der durch die Software erreichbaren, qualitativen Zuverlässigkeit ausgeht.*“ /DIN10a/
- „*Zur Realisierung von Diversität sollten unabhängige Systeme mit funktionaler Diversität verwendet werden. Wenn funktionale Diversität nicht geeignet oder nicht möglich ist, sollte die Verwendung von diversitären Systemen, diversitären Software-Merkmalen und diversitären Auslegungsansätzen in Betracht gezogen werden.*“ /DIN10a/
- „*Wenn funktionale oder Software*-Diversität *verwendet wird, bietet die Verschiedenheit der Versionen* [Anm.: Software-Version: jeweilige Ausgabe eines Software-Produkts, die durch Änderung oder Korrektur eines vorhergehenden Software-Produkts erstellt wurde /DIN10a/] *einen erhöhten Schutz gegen CCF durch Software.*“ /DIN10a/
- „*Nachteile von Diversität können sein:*
  - *insgesamt größere Komplexität;*

- *erhöhtes Risiko von unbeabsichtigter Auslösung;*
- *komplexere Spezifikationen und Entwicklung;*
- *Überwachung von zwei Zulieferern;*
- *Probleme bei Wartung und Änderung, z. B. darf die Diversität durch eine Änderung nicht verloren gehen;*
- *umfangreichere Dokumentation;*
- *höherer Raum- und Versorgungsbedarf, höhere Anforderungen an die Umgebungsüberwachung;*
- *die Kosten für mehrere Versionen der Software können deren kommerzielles Potential schwächen, mit Ausnahme ihrer Anwendung als Testmethode;*
- *jede neue Version kann von geringerer Qualität als die vorher erstellten Versionen sein.“ /DIN10a/*

Funktionale Diversität

DIN 62340 „Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Anforderungen zur Beherrschung von Versagen aufgrund gemeinsamer Ursache“ /DIN10d/:

- „*Die Anwendung* funktionaler *Diversität stellt die einzige Möglichkeit dar, einen Schutz gegen postulierte latente funktionale Fehler in der Anforderungsspezifikation zu bieten. Die Zuordnung von diversitären Funktionen zu unabhängigen leittechnischen Systemen kann gleichzeitig als ein Mittel benutzt werden, um unterschiedliche Signaltrajektorien beim Betrieb der leittechnischen Systeme zu erreichen.*“ /DIN10d/
- „*Die Wirksamkeit* des *Einsatzes funktionaler Diversität bei der Realisierung leittechnischer Systeme ist unabhängig von der verwendeten Technologie der Leittechnik.*“ /DIN10d/

5 FMEA von generischen Baugruppen

Im Folgenden werden die Ergebnisse der für drei generische Baugruppen durchgeführten Fehlzustandsart- und -auswirkungsanalyse (Failure Mode and Effects Analysis, FMEA) dargestellt. In Abschnitt 5.1 wird erläutert, warum die Vorgehensweise zur Durchführung der FMEA entgegen der ursprünglichen Planung geändert wurde. Anschließend werden in Abschnitt 5.2 die drei Arten von Baugruppen (nichtprogrammierbar, programmierbar, rechnerbasiert), für die jeweils generisch eine FMEA durchgeführt wurde sowie die jeweiligen Ergebnisse der Fehlzustandsart- und -auswirkungsanalysen vorgestellt.

5.1 Änderung der Vorgehensweise

In der ursprünglichen Planung für dieses Arbeitspaket war es vorgesehen, eine FMEA für eine beispielhafte Ersatzbaugruppe (soweit Unterlagen zugänglich sind) durchzuführen. Dadurch sollte beispielhaft überprüft werden, ob für Ersatzbaugruppen generell bestimmte Fehlerarten und Fehlereffekte zu unterstellen sind. Diese beispielhafte Vorgehensweise kann aber nur einen sehr geringen Teil der auf dem Markt befindlichen Baugruppen abdecken. Sinnvoll ist es aber im Rahmen dieses Vorhabens ein möglichst breites Spektrum an möglichen Baugruppen abzudecken. Daher wurde in Absprache mit dem Auftraggeber beschlossen, das ursprünglich geplante Vorgehen zu ändern und generische Baugruppentypen zu untersuchen. Im Folgenden werden die FMEAs von folgenden drei generischen Baugruppen diskutiert:

- nichtprogrammierbare Baugruppe (wie z. B. Geamatic, Iskamtic B)
- programmierbare Baugruppe (wie z. B. Symphony, Step 5, Step 7)
- rechnerbasierte Baugruppe (wie z. B. T2000, TXS, Spinline)

5.2 FMEA

„*Die Fehlzustandsart- und -auswirkungsanalyse (Failure Mode and Effects Analysis, FMEA) ist eine Methode zur Analyse der Zuverlässigkeit und der Auswirkungen von Ausfällen eines Systems. Im Rahmen der Qualifizierung von Systemen, die leittechnische Funktionen der Kategorie A ausführen, kann solch eine Methode angewendet werden, um Werte für die Zuverlässigkeit zu erhalten, es sei denn es ist genügend Betriebserfahrung vorhanden.*“ /DIN10c/

„*Ausfälle mit gemeinsamer Ursache können durch eine FMEA qualitativ analysiert werden, aber die Fähigkeit der FMEA, diese vollständig zu analysieren, ist begrenzt. Dennoch ist die FMEA ein Verfahren, alle Ausfallarten und die zugehörigen Ursachen sukzessiv zu untersuchen und zusätzlich alle wiederkehrenden Prüfungen, vorbeugende Instandhaltungsmaßnahmen usw. festzulegen. Sie ermöglicht eine Untersuchung aller Ursachen, die mögliche Ausfälle mit gemeinsamer Ursache hervorrufen können.*“ /DIN06/

5.2.1 Vorgehensweise

Grundsätzlich können die Baugruppen bzw. Komponenten leittechnischer Einrichtungen gemäß KTA 3501 /KTA14b/ oder den Interpretationen zu den Sicherheitsanforderungen an Kernkraftwerke /BMU13/ in drei Arten eingeteilt werden:

- **Nichtprogrammierbare Baugruppen**, die aus diskreten Bauelementen aufgebaut sind, einschließlich Baugruppen, die zwar programmierbare Bauelemente enthalten, deren Programmierung aber im Herstellungsprozess vorgenommen wird und anschließend nicht mehr verändert werden kann. Diese Gruppe umfasst also Baugruppen sehr unterschiedlicher Komplexität von festverdrahteten Logikgattern bis hin zu einfachen ASICs ohne integrierten Mikroprozessor, deren Programmierung beim Kunden nicht mehr veränderbar ist.

- **Programmierbare Baugruppen**, die zumindest ein diskretes, programmierbares Bauelement enthalten und die nach dem Herstellungsprozess konfigurierbar sind und rekonfigurierbar bleiben. Diese Gruppe umfasst also ebenfalls Baugruppen unterschiedlicher Komplexität von PLAs (programmierbare logische Anordnungen) über CPLDs (complex programmable logic devices) bis hin zu FPGAs (field programmable gate arrays), die sogar während des Betriebs ganz oder teilweise neu programmiert werden können.

- **Rechnerbasierte Baugruppen**, die zumindest einen Prozessor enthalten. Auch diese Gruppe umfasst Baugruppen sehr unterschiedlicher Komplexität von einfachen Mikrocontrollern über Mikroprozessoren bis hin zu Multi-Core Prozessoren. ASICs und FPGAs, welche Mikroprozessoren enthalten, werden ebenfalls dieser Baugruppenart zugeordnet.

Für diese drei Arten von Baugruppen werden im Folgenden beispielhaft Fehlermöglichkeiten und deren Auswirkungen untersucht. Hierzu wird für jede der drei Arten eine

FMEA an einer vereinfachten, allgemein dargestellten Beispielbaugruppe durchgeführt. Diese Beispielbaugruppen werden jeweils stellvertretend für eine Vielzahl unterschiedlicher Realisierungen einer Art untersucht.

5.2.2 Nichtprogrammierbare Baugruppen

Nichtprogrammierbare Baugruppen bestehen im Allgemeinen aus einer Eingabe- sowie einer Ausgabe-Einheit, einer nichtprogrammierbaren Verarbeitungslogik und einer Stromversorgung.

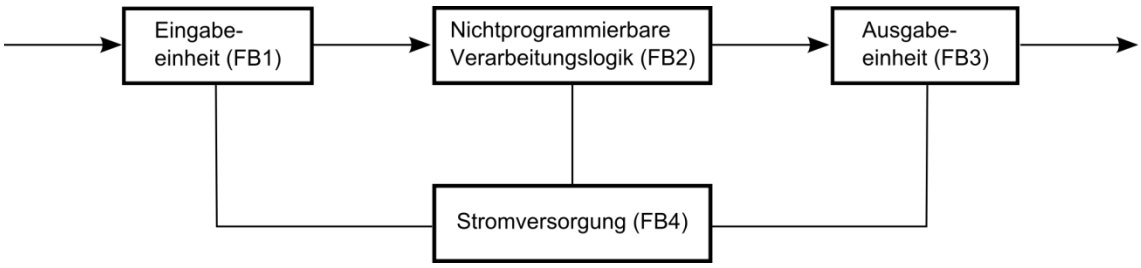

Abb. 5.1 Schematische Darstellung einer nichtprogrammierbaren Baugruppe (NB)

Die Funktionsblöcke „Eingabeeinheit“, „Ausgabeeinheit“ und „Stromversorgung“ sind prinzipiell in allen drei eingeführten Arten von Baugruppen enthalten. Der grundlegende Unterschied in den drei Arten von Baugruppen stellt die Verarbeitungslogik dar. Bei den nichtprogrammierbaren Baugruppen ist dies eine „Nichtprogrammierbare Verarbeitungslogik“.

Der Funktionsblock „Nichtprogrammierbare Verarbeitungslogik“ (siehe Abbildung 5.1) kann dabei unterschiedlich komplex aufgebaut sein. Je nach Komplexität kann der Funktionsblock beispielsweise folgende Elemente enthalten:

- Diskrete Bauelemente wie Kondensatoren oder Widerstände
- Integrierte Schaltkreise
- Halbleiterbauelemente wie Transistoren oder CMOS-Bauelemente
- Anwendungsspezifische integrierte Schaltkreise (ASICs) ohne Prozessor
- Operationsverstärker
- Digital-Analog-Wandler

- Flipflops

Nichtprogrammierbare Baugruppen erhalten ihre endgültige Konfiguration immer vor Auslieferung an den Kunden. Diese Konfiguration ist anschließend nicht mehr veränderbar. Somit ist eine nichtprogrammierbare Baugruppe auf die vorgesehene Aufgabe beschränkt.

In ihrer Komplexität können sich nichtprogrammierbare Baugruppen stark unterscheiden. Baugruppen für einfache oder häufig verwendete Aufgaben sind überwiegend als Standardprodukte verfügbar. Typische, im Kernkraftwerk eingesetzte Beispiele sind hierbei beispielsweise die Baulinien Iskamatic, Geamatic und Contronic. Für komplexere Aufgaben wird auf anwendungsspezifische Baugruppen wie ASICs zurückgegriffen. Dies ist in der Regel mit einem größeren Kosten- und Entwicklungsaufwand verbunden.

Die nachfolgende Tabelle 5.1 zeigt die FMEA für die in Abbildung 5.1 dargestellte, generische nichtprogrammierbare Baugruppe.

Tab. 5.1 FMEA für generische nichtprogrammierbare Baugruppe

Nummer Funktionsblock	Beschreibung Funktionsblock	Nummer Ausfallart	Untergruppe Funktionsblock	Funktion	Ausfallart	Auswirkungen auf Funktionsblock	Auswirkungen auf Baugruppe
NB_FB1	Eingabeeinheit	NB_FB1_EE_FM1	Eingang Eingabeeinheit	Eingangssignal der Eingabeeinheit	Unterbrechung/Kurzschluss	Fehlerhaftes Eingangssignal der Eingabeeinheit	Fehlerhaftes Ausgangssignal der Baugruppe
NB_FB1	Eingabeeinheit	NB_FB1_ESE_FM1	Eingang Stromversorgung Eingabeeinheit	Stromversorgung der Eingabeeinheit	Unterbrechung/Kurzschluss	Keine Stromversorgung der Eingabeeinheit	Fehlerhaftes Ausgangssignal der Baugruppe
NB_FB1	Eingabeeinheit	NB_FB1_E_FM1	Eingabeeinheit	Erfassung und Aufbereitung der Eingangssignale	Fehlerhafte Eingabeeinheit	Fehlerhaftes Ausgangssignal der Eingabeeinheit	Fehlerhaftes Ausgangssignal der Baugruppe
NB_FB1	Eingabeeinheit	NB_FB1_AE_FM1	Ausgang Eingabeeinheit	Ausgangssignal der Eingabeeinheit	Unterbrechung/Kurzschluss	Fehlerhaftes Ausgangssignal der Eingabeeinheit	Fehlerhaftes Ausgangssignal der Baugruppe
NB_FB2	Nichtprogrammierbare Verarbeitungslogik	NB_FB2_EV_FM1	Eingang Verarbeitungslogik	Eingangssignal der Verarbeitungslogik	Unterbrechung/Kurzschluss	Fehlerhaftes Eingangssignal der Verarbeitungslogik	Fehlerhaftes Ausgangssignal der Baugruppe
NB_FB2	Nichtprogrammierbare Verarbeitungslogik	NB_FB2_ESV_FM1	Eingang Stromversorgung Verarbeitungslogik	Stromversorgung der Verarbeitungslogik	Unterbrechung/Kurzschluss	Keine Stromversorgung der Verarbeitungslogik	Fehlerhaftes Ausgangssignal der Baugruppe
NB_FB2	Nichtprogrammierbare Verarbeitungslogik	NB_FB2_V_FM1	Nichtprogrammierbare Verarbeitungslogik	Signalverarbeitung	Fehlerhafte Signalverarbeitung	Fehlerhaftes Ausgangssignal der Verarbeitungslogik	Fehlerhaftes Ausgangssignal der Baugruppe
NB_FB2	Nichtprogrammierbare Verarbeitungslogik	NB_FB2_AV_FM1	Ausgang Verarbeitungslogik	Ausgangssignal der Verarbeitungslogik	Unterbrechung/Kurzschluss	Fehlerhaftes Ausgangssignal der Verarbeitungslogik	Fehlerhaftes Ausgangssignal der Baugruppe

Nummer Funktionsblock	Beschreibung Funktionsblock	Nummer Ausfallart	Untergruppe Funktionsblock	Funktion	Ausfallart	Auswirkungen auf Funktionsblock	Auswirkungen auf Baugruppe
NB_FB3	Ausgabeeinheit	NB_FB3_EA_FM1	Eingang Ausgabeeinheit	Eingangssignal der Ausgabeeinheit	Unterbrechung/Kurzschluss	Fehlerhaftes Eingangssignal der Ausgabeeinheit	Fehlerhaftes Ausgangssignal der Baugruppe
NB_FB3	Ausgabeeinheit	NB_FB3_ESA_FM1	Eingang Stromversorgung Ausgabeeinheit	Stromversorgung der Ausgabeeinheit	Unterbrechung/Kurzschluss	Keine Stromversorgung der Ausgabeeinheit	Fehlerhaftes Ausgangssignal der Baugruppe
NB_FB3	Ausgabeeinheit	NB_FB3_A_FM1	Ausgabeeinheit	Aufbereitung der Ausgangssignale	Fehlerhafte Ausgabeeinheit	Fehlerhaftes Ausgangssignal der Ausgabeeinheit	Fehlerhaftes Ausgangssignal der Baugruppe
NB_FB3	Ausgabeeinheit	NB_FB3_AA_FM1	Ausgang Ausgabeeinheit	Ausgangssignal der Ausgabeeinheit	Unterbrechung/Kurzschluss	Fehlerhaftes Ausgangssignal der Ausgabeeinheit	Fehlerhaftes Ausgangssignal der Baugruppe
NB_FB4	Stromversorgung	NB_FB4_ASE_FM1	Ausgang Stromversorgung Eingabeeinheit	Stromversorgung der Eingabeeinheit	Unterbrechung/Kurzschluss	Keine Stromversorgung der Eingabeeinheit	Fehlerhaftes Ausgangssignal der Baugruppe
NB_FB4	Stromversorgung	NB_FB4_ASV_FM1	Ausgang Stromversorgung Verarbeitungslogik	Stromversorgung der Verarbeitungslogik	Unterbrechung/Kurzschluss	Keine Stromversorgung der Verarbeitungslogik	Fehlerhaftes Ausgangssignal der Baugruppe
NB_FB4	Stromversorgung	NB_FB4_ASA_FM1	Ausgang Stromversorgung Ausgabeeinheit	Stromversorgung der Ausgabeeinheit	Unterbrechung/Kurzschluss	Keine Stromversorgung der Ausgabeeinheit	Fehlerhaftes Ausgangssignal der Baugruppe
NB_FB4	Stromversorgung	NB_FB4_S_FM1	Stromversorgung	Stromversorgung	Fehlerhafte Stromversorgung	Keine Stromversorgung der Baugruppe	Fehlerhaftes Ausgangssignal der Baugruppe

Die FMEA der generischen nichtprogrammierbaren Baugruppe in Tabelle 5.1 zeigt, dass jeder Fehler in einem der Funktionsblöcke der nichtprogrammierbaren Baugruppe zu einem fehlerhaften Ausgangssignal der Baugruppe führt. Da die FMEA an einer generischen Baugruppe durchgeführt wurde, können die tatsächlichen Failure Modes hier nicht aufgezeigt werden. Wie oben bereits beschrieben, stellt die Verarbeitungslogik den grundlegenden Unterschied zwischen den drei Arten von Baugruppen dar. Aus diesem Grund wird ein Fehler in der nichtprogrammierbaren Verarbeitungslogik (in der FMEA farbig markiert) detaillierter untersucht. Dazu wird auf Abschnitt 5.2.5 verwiesen, wo mögliche Failure Modes für die Elemente, die in der nichtprogrammierbaren Verarbeitungslogik enthaltenen sein können, dargestellt sind.

5.2.3 Programmierbare Baugruppen

Programmierbare Baugruppen wie PLDs (Programmable logic devices) und FPGAs (Field programmable gate arrays) bestehen im Allgemeinen neben einer Stromversorgung und einer Eingabe- sowie einer Ausgabeeinheit aus einer programmierbaren Verarbeitungslogik und A/D- bzw. D/A-Wandlern.

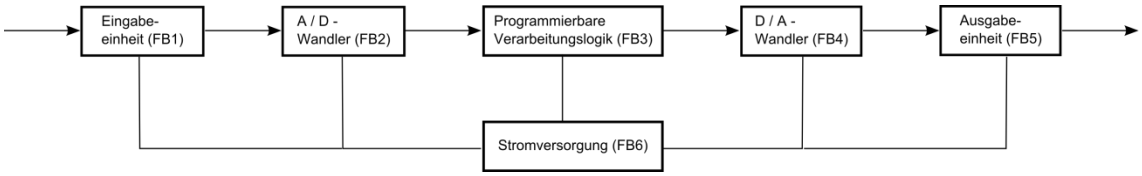

Abb. 5.2 Schematische Darstellung einer programmierbaren Baugruppe (PB)

Wie bereits bei den nichtprogrammierbaren Baugruppen erwähnt wurde, stellt die Verarbeitungslogik den grundlegenden Unterschied in den drei Arten von Baugruppen dar. In den programmierbaren Baugruppen sind zwar im Gegensatz zu den nichtprogrammierbaren Baugruppen zwingend A/D- und D/A-Wandler vorhanden, aber diese können auch in den nichtprogrammierbaren Baugruppen vorkommen und stellen deshalb keinen grundlegenden Unterschied dar. Bei den programmierbaren Baugruppen ist die Verarbeitungslogik eine „Programmierbare Verarbeitungslogik“.

Der Funktionsblock „Programmierbare Verarbeitungslogik“ (siehe Abbildung 5.2) kann dabei unterschiedlich komplex aufgebaut sein. Grundsätzlich kann der Funktionsblock auch die bei den nichtprogrammierbaren Baugruppen genannten Elemente enthalten. Zusätzlich können sie je nach Komplexität beispielsweise folgende Elemente enthalten:

- UND-Arrays
- ODER-Arrays
- Lookup-Tabellen
- RAM
- SRAM
- Register
- Taktgeneratoren
- Speicher wie z. B. ROM, EPROM, Flash

Im Gegensatz zu nichtprogrammierbaren Baugruppen haben programmierbare Baugruppen zum Zeitpunkt der Fertigung noch keine festgelegte Konfiguration, d. h. es muss noch nicht feststehen, für welche Aufgabe die Baugruppe eingesetzt werden soll. Programmierbare Baugruppen können ihre Konfiguration daher auch erst vor Ort, nach Auslieferung an den Kunden erhalten. Eine programmierbare Baugruppe ist im Wesentlichen ein Halbleiterbauelement, das programmierbare logische Komponenten (logische Blöcke) und programmierbare Verbindungen enthält. Mittels einer Hardwarebeschreibungssprache (HDL – hardware description language) lassen sich die programmierbaren logischen Blöcke so programmieren, dass sie beispielsweise die Funktionalität von Logikgattern oder mathematische Funktionen nachbilden. Die Funktion wird implementiert, indem Konfigurationsdaten zu den gewünschten Schaltungsstrukturen an den Baustein übertragen werden. Die Festlegung der Funktion durch diese Konfigurationsdaten ermöglicht die Verwendung baugleicher programmierbarer Baugruppen für unterschiedliche Aufgaben. Im Vergleich zu anwendungsspezifischen nichtprogrammierbaren Baugruppen kann so insbesondere bei kleinen Stückzahlen der Entwicklungs- und Kostenaufwand reduziert werden.

Die nachfolgende Tabelle 5.2 zeigt die FMEA für die in Abbildung 5.2 dargestellte, generische programmierbare Baugruppe.

Tab. 5.2 FMEA für generische programmierbare Baugruppe

Nummer Funktionsblock	Beschreibung Funktionsblock	Nummer Ausfallart	Untergruppe Funktionsblock	Funktion	Ausfallart	Auswirkungen auf Funktionsblock	Auswirkungen auf Baugruppe
PB_FB1	Eingabeeinheit	PB_FB1_EE_FM1	Eingang Eingabeeinheit	Eingangssignal der Eingabeeinheit	Unterbrechung/Kurzschluss	Fehlerhaftes Eingangssignal der Eingabeeinheit	Fehlerhaftes Ausgangssignal der Baugruppe
PB_FB1	Eingabeeinheit	PB_FB1_ESE_FM1	Eingang Stromversorgung Eingabeeinheit	Stromversorgung der Eingabeeinheit	Unterbrechung/Kurzschluss	Keine Stromversorgung der Eingabeeinheit	Fehlerhaftes Ausgangssignal der Baugruppe
PB_FB1	Eingabeeinheit	PB_FB1_E_FM1	Eingabeeinheit	Erfassung und Aufbereitung der Eingangssignale	Fehlerhafte Eingabeeinheit	Fehlerhaftes Ausgangssignal der Eingabeeinheit	Fehlerhaftes Ausgangssignal der Baugruppe
PB_FB1	Eingabeeinheit	PB_FB1_AE_FM1	Ausgang Eingabeeinheit	Ausgangssignal der Eingabeeinheit	Unterbrechung/Kurzschluss	Fehlerhaftes Ausgangssignal der Eingabeeinheit	Fehlerhaftes Ausgangssignal der Baugruppe
PB_FB2	A/D-Wandler	PB_FB2_EAD_FM1	Eingang A/D-Wandler	Eingangssignal des A/D-Wandlers	Unterbrechung/Kurzschluss	Fehlerhaftes Eingangssignal des A/D-Wandlers	Fehlerhaftes Ausgangssignal der Baugruppe
PB_FB2	A/D-Wandler	PB_FB2_ESAD_FM1	Eingang Stromversorgung A/D-Wandler	Stromversorgung des A/D-Wandlers	Unterbrechung/Kurzschluss	Keine Stromversorgung des A/D-Wandlers	Fehlerhaftes Ausgangssignal der Baugruppe
PB_FB2	A/D-Wandler	PB_FB2_AD_FM1	A/D-Wandler	Wandlung analoger Signale in digitale Signale	Fehlerhafter A/D-Wandler	Fehlerhaftes Ausgangssignal des A/D-Wandlers	Fehlerhaftes Ausgangssignal der Baugruppe
PB_FB2	A/D-Wandler	PB_FB2_AAD_FM1	Ausgang A/D-Wandler	Ausgangssignal des A/D-Wandlers	Unterbrechung/Kurzschluss	Fehlerhaftes Ausgangssignal der A/D-Wandlers	Fehlerhaftes Ausgangssignal der Baugruppe

Nummer Funktionsblock	Beschreibung Funktionsblock	Nummer Ausfallart	Untergruppe Funktionsblock	Funktion	Ausfallart	Auswirkungen auf Funktionsblock	Auswirkungen auf Baugruppe
PB_FB3	Programmierbare Verarbeitungslogik	PB_FB3_EV_FM1	Eingang Verarbeitungslogik	Eingangssignal der Verarbeitungslogik	Unterbrechung/Kurzschluss	Fehlerhaftes Eingangssignal der Verarbeitungslogik	Fehlerhaftes Ausgangssignal der Baugruppe
PB_FB3	Programmierbare Verarbeitungslogik	PB_FB3_ESV_FM1	Eingang Stromversorgung Verarbeitungslogik	Stromversorgung der Verarbeitungslogik	Unterbrechung/Kurzschluss	Keine Stromversorgung der Verarbeitungslogik	Fehlerhaftes Ausgangssignal der Baugruppe
PB_FB3	Programmierbare Verarbeitungslogik	PB_FB3_V_FM1	Programmierbare Verarbeitungslogik	Signalverarbeitung	Fehlerhafte Signalverarbeitung	Fehlerhaftes Ausgangssignal der Verarbeitungslogik	Fehlerhaftes Ausgangssignal der Baugruppe
PB_FB3	Programmierbare Verarbeitungslogik	PB_FB3_AV_FM1	Ausgang Verarbeitungslogik	Ausgangssignal der Verarbeitungslogik	Unterbrechung/Kurzschluss	Fehlerhaftes Ausgangssignal der Verarbeitungslogik	Fehlerhaftes Ausgangssignal der Baugruppe
PB_FB4	D/A-Wandler	PB_FB4_EDA_FM1	Eingang D/A-Wandler	Eingangssignal des D/A-Wandlers	Unterbrechung/Kurzschluss	Fehlerhaftes Eingangssignal des D/A-Wandlers	Fehlerhaftes Ausgangssignal der Baugruppe
PB_FB4	D/A-Wandler	PB_FB4_ESDA_FM1	Eingang Stromversorgung D/A-Wandler	Stromversorgung des D/A-Wandlers	Unterbrechung/Kurzschluss	Keine Stromversorgung des D/A-Wandlers	Fehlerhaftes Ausgangssignal der Baugruppe
PB_FB4	D/A-Wandler	PB_FB4_DA_FM1	D/A-Wandler	Wandlung digitaler Signale in analoge Signale	Fehlerhafter D/A-Wandler	Fehlerhaftes Ausgangssignal des D/A-Wandlers	Fehlerhaftes Ausgangssignal der Baugruppe
PB_FB4	D/A-Wandler	PB_FB4_ADA_FM1	Ausgang D/A-Wandler	Ausgangssignal des D/A-Wandlers	Unterbrechung/Kurzschluss	Fehlerhaftes Ausgangssignal der D/A-Wandlers	Fehlerhaftes Ausgangssignal der Baugruppe
PB_FB5	Ausgabeeinheit	PB_FB5_EA_FM1	Eingang Ausgabeeinheit	Eingangssignal der Ausgabeeinheit	Unterbrechung/Kurzschluss	Fehlerhaftes Eingangssignal der Ausgabeeinheit	Fehlerhaftes Ausgangssignal der Baugruppe

Nummer Funktionsblock	Beschreibung Funktionsblock	Nummer Ausfallart	Untergruppe Funktionsblock	Funktion	Ausfallart	Auswirkungen auf Funktionsblock	Auswirkungen auf Baugruppe
PB_FB5	Ausgabeeinheit	PB_FB5_ESA_FM1	Eingang Stromversorgung Ausgabeeinheit	Stromversorgung der Ausgabeeinheit	Unterbrechung/Kurzschluss	Keine Stromversorgung der Ausgabeeinheit	Fehlerhaftes Ausgangssignal der Baugruppe
PB_FB5	Ausgabeeinheit	PB_FB5_A_FM1	Ausgabeeinheit	Aufbereitung der Ausgangssignale	Fehlerhafte Ausgabeeinheit	Fehlerhaftes Ausgangssignal der Ausgabeeinheit	Fehlerhaftes Ausgangssignal der Baugruppe
PB_FB5	Ausgabeeinheit	PB_FB5_AA_FM1	Ausgang Ausgabeeinheit	Ausgangssignal der Ausgabeeinheit	Unterbrechung/Kurzschluss	Fehlerhaftes Ausgangssignal der Ausgabeeinheit	Fehlerhaftes Ausgangssignal der Baugruppe
PB_FB6	Stromversorgung	PB_FB6_ASE_FM1	Ausgang Stromversorgung Eingabeeinheit	Stromversorgung der Eingabeeinheit	Unterbrechung/Kurzschluss	Keine Stromversorgung der Eingabeeinheit	Fehlerhaftes Ausgangssignal der Baugruppe
PB_FB6	Stromversorgung	PB_FB6_ASAD_FM1	Ausgang Stromversorgung A/D-Wandler	Stromversorgung des A/D-Wandlers	Unterbrechung/Kurzschluss	Keine Stromversorgung des A/D-Wandlers	Fehlerhaftes Ausgangssignal der Baugruppe
PB_FB6	Stromversorgung	PB_FB6_ASV_FM1	Ausgang Stromversorgung Verarbeitungslogik	Stromversorgung der Verarbeitungslogik	Unterbrechung/Kurzschluss	Keine Stromversorgung der Verarbeitungslogik	Fehlerhaftes Ausgangssignal der Baugruppe
PB_FB6	Stromversorgung	PB_FB6_ASA_FM1	Ausgang Stromversorgung Ausgabeeinheit	Stromversorgung der Ausgabeeinheit	Unterbrechung/Kurzschluss	Keine Stromversorgung der Ausgabeeinheit	Fehlerhaftes Ausgangssignal der Baugruppe
PB_FB6	Stromversorgung	PB_FB6_ASDA_FM1	Ausgang Stromversorgung D/A-Wandler	Stromversorgung des D/A-Wandlers	Unterbrechung/Kurzschluss	Keine Stromversorgung des D/A-Wandlers	Fehlerhaftes Ausgangssignal der Baugruppe
PB_FB6	Stromversorgung	PB_FB6_S_FM1	Stromversorgung	Stromversorgung	Fehlerhafte Stromversorgung	Keine Stromversorgung der Baugruppe	Fehlerhaftes Ausgangssignal der Baugruppe

Die FMEA der generischen programmierbaren Baugruppe in Tabelle 5.2 zeigt, dass jeder Fehler in einem der Funktionsblöcke der programmierbaren Baugruppe zu einem fehlerhaften Ausgangssignal der Baugruppe führt. Wie bereits für die nichtprogrammierbare Baugruppe beschrieben, werden auch die für einen Fehler in der programmierbaren Verarbeitungslogik (in der FMEA farbig markiert) möglichen Failure Modes in Abschnitt 5.2.5 gesondert dargestellt. Da in der programmierbaren Verarbeitungslogik neben den auch in der nichtprogrammierbaren Verarbeitungslogik enthaltenen Elementen zusätzlich noch andere Elemente enthalten sein können (siehe obige Beschreibung), ergeben sich für die programmierbare Verarbeitungslogik im Vergleich zur nichtprogrammierbaren Verarbeitungslogik mehr mögliche Failure Modes.

5.2.3.1 FPGA

Zu den prominentesten Beispielen für programmierbare Baugruppen zählt das Field Programmable Gate Array (FPGA). Der nachfolgende Text zu FPGAs basiert vorwiegend auf den Quellen /ZEI06a/, /ZEI06b/, /WAN98/, /RAN11/ und /BAT11/.

Ein FPGA ist ein programmierbarer elektronischer Baustein zum Aufbau digitaler, logischer Schaltungen. Ein FPGA besteht im Wesentlichen aus einzelnen Logikblöcken, die in einer regelmäßigen Struktur (engl.: Array) angeordnet sind, Eingangs- und Ausgangsblöcken (I/O-Blöcke) und einem Netzwerk von Verbindungen zwischen diesen Blöcken[6] (siehe Abbildung 5.3).

Die an der Peripherie des FPGA-Bausteins angeordneten Eingangs- und Ausgangsblöcke (I/O-Blöcke) dienen dem Anschluss des FPGA-Bausteins an die Platine, auf der er montiert ist. Das Verbindungsnetzwerk zwischen den Logikblöcken besteht in der Regel aus Leitungen und Schaltboxen. Die Funktionen der einzelnen Logikblöcke und die Verbindungen zwischen diesen werden abhängig von der vorgesehenen Aufgabe der zu realisierenden logischen Schaltung im Anwendungsfeld, d. h. vom Anwender, programmiert. Die Programmierung erfolgt durch Verknüpfen der in den Logikblöcken realisierten Logikfunktionen über das Verbindungsnetzwerk. Dies geschieht durch Programmierung der Schaltzustände der Schaltboxen.

[6] Zusätzlich kann ein FPGA auch weitere Funktionsblöcke (RAM, PLLs oder Signalverarbeitung) enthalten.

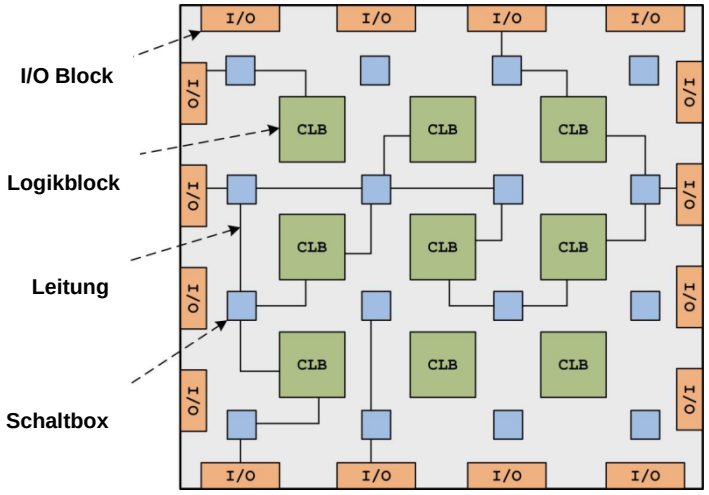

Abb. 5.3 Aufbau eines FPGA-Bausteins /VAL14/

Die Schaltboxen werden in der Regel als „Speicherzellen“ realisiert, deren Zustände („0“ oder „1“) die Schaltzustände der Schaltboxen („offen“ oder „geschlossen“) und folglich das Programm, d. h. die realisierte logische Schaltung, auf dem FPGA-Baustein bestimmen. Die Programmierung des FPGAs erfolgt durch Konfiguration der Zustände der Speicherzellen („Einschreiben“ der Zustände der Speicherzellen) in den FPGA-Baustein.

Zur Programmierung eines FPGAs gibt es drei Technologien, die sich in der technischen Realisierung der „Speicherzellen“ unterscheiden:

- Die SRAM-Technologie verwendet Static Random Access Memory-Speicherzellen. Das FPGA-Programm wird in SRAM-Speicherzellen abgelegt. Der Speicherinhalt kann gelöscht und neu geschrieben werden, wodurch SRAM-basierte FPGAs mehrmals programmiert werden können. Der Speicherinhalt ist bei SRAM-Speicherzellen flüchtig, d. h. bei Unterbrechung der Stromversorgung wird der Speicherinhalt gelöscht. Aus diesem Grund müssen SRAM-basierte FPGAs nach Unterbrechung der Stromversorgung erneut konfiguriert werden.

- Bei der Flash-EEPROM Technologie werden Electrically Erasable Programmable Read-Only Memory-Speicherzellen verwendet. Das FPGA-Programm wird in Flash-EEPROM-Speicherzellen abgelegt. Der Speicherinhalt kann wie bei SRAM basierten FPGAs gelöscht und neu geschrieben werden, wodurch flashbasierte FPGAs mehrmals programmiert werden können. Der Speicherinhalt ist – im Gegensatz zu SRAM – bei der EEPROM-Technologie nicht flüchtig, d. h. bei Unterbrechung der Stromversorgung bleibt der Speicherinhalt und folglich die Konfiguration des FPGAs erhalten.

- In der Antifuse-Technologie wird der Schaltzustand der Schaltboxen und folglich der Zustand der Speicherzellen (das FPGA-Programm) durch Erzeugen einer elektrisch leitenden Verbindung zwischen vorher voneinander elektrisch isolierten Verbindungsleitungen realisiert. Ein nicht flüchtiger und nicht mehr veränderbarer Speicher entsteht, d. h. Antifuse-FPGA sind nur einmal programmierbar.

Die verwendete Technologie für die technische Realisierung der Schaltboxen-„Speicherzellen“ hat kaum Einfluss auf die Gestaltung der logischen Funktionen auf dem FPGA-Baustein. Die Unterschiede zwischen den drei Technologien sind im Wesentlichen durch die physikalischen Eigenschaften der realisierten FPGA-Bausteine bestimmt. Zu den physikalischen Eigenschaften zählen beispielweise die Datensicherheit (Schutz gegen unerlaubte Zugriffe) der FPGA-Bausteine sowie die Robustheit bzw. die Störanfälligkeit der FPGA-Bausteine. In /ACT03/ wird aufgeführt, dass SRAM-basierte FPGAs eine deutlich höhere strahlungsinduzierte Störfanfälligkeit im Vergleich zu Flash- und Antifuse-FPGAs aufweisen. In Bezug auf die Erfüllung einer hohen Datensicherheit werden in /ACT03/ Antifuse-FPGAs als geeignet angesehen, denn sie bieten technologiebedingt (nicht flüchtiger Speicher, nur einmal programmierbar) einen hohen Schutz gegen unerlaubte Zugriffe.

Ein weiterer Unterschied zwischen den verwendeten Technologien liegt in den für die technische Realisierung der Schaltboxen-„Speicherzellen“ erforderlichen Ressourcen. Ein SRAM-basierter FPGA erfordert mehrere Transistoren, ein flashbasierter nur einen Transistor. Flashbasierte-FPGAs eignen sich daher insbesondere für Anwendungen mit dem Erfordernis niedrigen Leistungsverbrauchs des FPGA-Bausteins. Die Antifuse-Technologie erfordert die wenigsten Ressourcen, die Herstellung von Antifuse-FPGAs ist jedoch komplexer als die von SRAM-basierten und flashbasierten FPGAs. Die Herstellung von SRAM-FPGAs erfolgt nach einem Standardverfahren, ähnlich der herkömmlichen Chip-Herstellung. Die hohe Integrationsdichte der SRAM-Technologie im Vergleich zu der Flash- und der Antifuse-Technologie resultiert in einer hohen Kapazität von SRAM-FPGAs gegenüber Flash-FPGAs und Antifuse-FPGAs. Die meisten eingesetzten FPGAs sind SRAM-basiert.

Ein zusammenfassender Vergleich dieser drei Technologien ist in der Tabelle 5.3 enthalten.

Tab. 5.3 Vergleich der FPGA-Technologien

	SRAM	Flash	Antifuse
Kapazität (Anzahl der Logikblöcke)	Hoch	Mittel	Niedrig
Reprogrammier-bar	Ja	Ja	Nein
Störanfälligkeit	Hoch	Mittel	Niedrig
Flüchtigkeit	Ja	Nein	Nein
Anwendungsfeld	Alle	Niedrige Leistung	Sicherheitskritisch
Hersteller	Xilinx	Altera, Microsemi (früher Actel), Lattice	Microsemi

5.2.4 Rechnerbasierte Baugruppen

Rechnerbasierte Baugruppen wie Mikro-Controller, Mikroprozessoren oder FPGAs mit CPU besitzen im Unterschied zu programmierbaren Baugruppen in der Regel einen Prozessor, mit dem die programmierbaren Elemente kommunizieren:

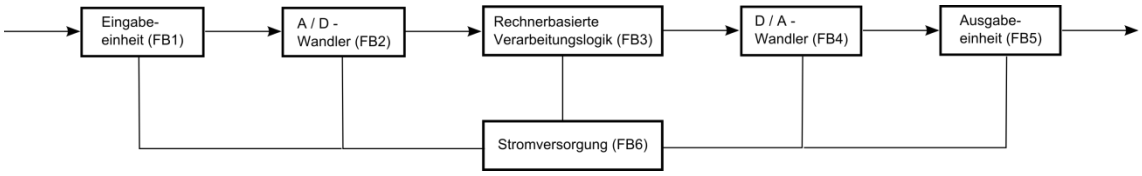

Abb. 5.4 Schematische Darstellung einer rechnerbasierten Baugruppe (RB)

Wie bereits bei den nichtprogrammierbaren und programmierbaren Baugruppen erwähnt wurde, stellt die Verarbeitungslogik den grundlegenden Unterschied in den drei Arten von Baugruppen dar. Bei den rechnerbasierten Baugruppen ist die Verarbeitungslogik eine „Rechnerbasierte Verarbeitungslogik“.

Der Funktionsblock „Rechnerbasierte Verarbeitungslogik“ (siehe Abbildung 5.4) kann dabei unterschiedlich komplex aufgebaut sein. Grundsätzlich kann der Funktionsblock auch die bei den nichtprogrammierbaren und programmierbaren Baugruppen genannten Elemente enthalten. Zusätzlich können sie je nach Komplexität beispielsweise folgende Elemente enthalten:

- Prozessor (Mikroprozessor, CPU)
- Serielle Schnittstellen
- Watchdog

Eine rechnerbasierte Baugruppe kann hinsichtlich ihrer Funktion auch vor Ort vergleichsweise einfach umprogrammiert werden. Die mit rechnerbasierten Baugruppen realisierbare Logik kann dabei deutlich komplexer sein als bei programmierbaren Baugruppen. Beispielsweise lassen sich auch mehrere Anwendungsfunktionen auf einer Baugruppe zusammenfassen ohne die damit verbundene Menge an Hardwarebauelementen wesentlich zu erhöhen.

Die nachfolgende Tabelle 5.4 zeigt die FMEA für die in Abbildung 5.4 dargestellte, generische rechnerbasierte Baugruppe.

Tab. 5.4 FMEA für generische rechnerbasierte Baugruppe

Nummer Funktionsblock	Beschreibung Funktionsblock	Nummer Ausfallart	Untergruppe Funktionsblock	Funktion	Ausfallart	Auswirkungen auf Funktionsblock	Auswirkungen auf Baugruppe
RB_FB1	Eingabeeinheit	RB_FB1_EE_FM1	Eingang Eingabeeinheit	Eingangssignal der Eingabeeinheit	Unterbrechung/Kurzschluss	Fehlerhaftes Eingangssignal der Eingabeeinheit	Fehlerhaftes Ausgangssignal der Baugruppe
RB_FB1	Eingabeeinheit	RB_FB1_ESE_FM1	Eingang Stromversorgung Eingabeeinheit	Stromversorgung der Eingabeeinheit	Unterbrechung/Kurzschluss	Keine Stromversorgung der Eingabeeinheit	Fehlerhaftes Ausgangssignal der Baugruppe
RB_FB1	Eingabeeinheit	RB_FB1_E_FM1	Eingabeeinheit	Erfassung und Aufbereitung der Eingangssignale	Fehlerhafte Eingabeeinheit	Fehlerhaftes Ausgangssignal der Eingabeeinheit	Fehlerhaftes Ausgangssignal der Baugruppe
RB_FB1	Eingabeeinheit	RB_FB1_AE_FM1	Ausgang Eingabeeinheit	Ausgangssignal der Eingabeeinheit	Unterbrechung/Kurzschluss	Fehlerhaftes Ausgangssignal der Eingabeeinheit	Fehlerhaftes Ausgangssignal der Baugruppe
RB_FB2	A/D -Wandler	RB_FB2_EAD_FM1	Eingang A/D-Wandler	Eingangssignal des A/D-Wandlers	Unterbrechung/Kurzschluss	Fehlerhaftes Eingangssignal des A/D-Wandlers	Fehlerhaftes Ausgangssignal der Baugruppe
RB_FB2	A/D -Wandler	RB_FB2_ESAD_FM1	Eingang Stromversorgung A/D-Wandler	Stromversorgung des A/D-Wandlers	Unterbrechung/Kurzschluss	Keine Stromversorgung des A/D-Wandlers	Fehlerhaftes Ausgangssignal der Baugruppe
RB_FB2	A/D -Wandler	RB_FB2_AD_FM1	A/D-Wandler	Wandlung analoger Signale in digitale Signale	Fehlerhafter A/D-Wandler	Fehlerhaftes Ausgangssignal des A/D-Wandlers	Fehlerhaftes Ausgangssignal der Baugruppe
RB_FB2	A/D -Wandler	RB_FB2_AAD_FM1	Ausgang A/D-Wandler	Ausgangssignal des A/D-Wandlers	Unterbrechung/Kurzschluss	Fehlerhaftes Ausgangssignal der A/D-Wandlers	Fehlerhaftes Ausgangssignal der Baugruppe

Nummer Funktionsblock	Beschreibung Funktionsblock	Nummer Ausfallart	Untergruppe Funktionsblock	Funktion	Ausfallart	Auswirkungen auf Funktionsblock	Auswirkungen auf Baugruppe
RB_FB3	Rechnerbasierte Verarbeitungslogik	RB_FB3_EV_FM1	Eingang Verarbeitungslogik	Eingangssignal der Verarbeitungslogik	Unterbrechung/Kurzschluss	Fehlerhaftes Eingangssignal der Verarbeitungslogik	Fehlerhaftes Ausgangssignal der Baugruppe
RB_FB3	Rechnerbasierte Verarbeitungslogik	RB_FB3_ESV_FM1	Eingang Stromversorgung Verarbeitungslogik	Stromversorgung der Verarbeitungslogik	Unterbrechung/Kurzschluss	Keine Stromversorgung der Verarbeitungslogik	Fehlerhaftes Ausgangssignal der Baugruppe
RB_FB3	Rechnerbasierte Verarbeitungslogik	RB_FB3_V_FM1	Rechnerbasierte Verarbeitungslogik	Signalverarbeitung	Fehlerhafte Signalverarbeitung	Fehlerhaftes Ausgangssignal der Verarbeitungslogik	Fehlerhaftes Ausgangssignal der Baugruppe
RB_FB3	Rechnerbasierte Verarbeitungslogik	RB_FB3_AV_FM1	Ausgang Verarbeitungslogik	Ausgangssignal der Verarbeitungslogik	Unterbrechung/Kurzschluss	Fehlerhaftes Ausgangssignal der Verarbeitungslogik	Fehlerhaftes Ausgangssignal der Baugruppe
RB_FB4	D/A -Wandler	RB_FB4_EDA_FM1	Eingang D/A-Wandler	Eingangssignal des D/A-Wandlers	Unterbrechung/Kurzschluss	Fehlerhaftes Eingangssignal des D/A-Wandlers	Fehlerhaftes Ausgangssignal der Baugruppe
RB_FB4	D/A -Wandler	RB_FB4_ESDA_FM1	Eingang Stromversorgung D/A-Wandler	Stromversorgung des D/A-Wandlers	Unterbrechung/Kurzschluss	Keine Stromversorgung des D/A-Wandlers	Fehlerhaftes Ausgangssignal der Baugruppe
RB_FB4	D/A -Wandler	RB_FB4_DA_FM1	D/A-Wandler	Wandlung digitaler Signale in analoge Signale	Fehlerhafter D/A-Wandler	Fehlerhaftes Ausgangssignal des D/A-Wandlers	Fehlerhaftes Ausgangssignal der Baugruppe
RB_FB4	D/A -Wandler	RB_FB4_ADA_FM1	Ausgang D/A-Wandler	Ausgangssignal des D/A-Wandlers	Unterbrechung/Kurzschluss	Fehlerhaftes Ausgangssignal der D/A-Wandlers	Fehlerhaftes Ausgangssignal der Baugruppe
RB_FB5	Ausgabeeinheit	RB_FB5_EA_FM1	Eingang Ausgabeeinheit	Eingangssignal der Ausgabeeinheit	Unterbrechung/Kurzschluss	Fehlerhaftes Eingangssignal der Ausgabeeinheit	Fehlerhaftes Ausgangssignal der Baugruppe

Nummer Funktionsblock	Beschreibung Funktionsblock	Nummer Ausfallart	Untergruppe Funktionsblock	Funktion	Ausfallart	Auswirkungen auf Funktionsblock	Auswirkungen auf Baugruppe
RB_FB5	Ausgabeeinheit	RB_FB5_ESA_FM1	Eingang Stromversorgung Ausgabeeinheit	Stromversorgung der Ausgabeeinheit	Unterbrechung/Kurzschluss	Keine Stromversorgung der Ausgabeeinheit	Fehlerhaftes Ausgangssignal der Baugruppe
RB_FB5	Ausgabeeinheit	RB_FB5_A_FM1	Ausgabeeinheit	Aufbereitung der Ausgangssignale	Fehlerhafte Ausgabeeinheit	Fehlerhaftes Ausgangssignal der Ausgabeeinheit	Fehlerhaftes Ausgangssignal der Baugruppe
RB_FB5	Ausgabeeinheit	RB_FB5_AA_FM1	Ausgang Ausgabeeinheit	Ausgangssignal der Ausgabeeinheit	Unterbrechung/Kurzschluss	Fehlerhaftes Ausgangssignal der Ausgabeeinheit	Fehlerhaftes Ausgangssignal der Baugruppe
RB_FB6	Stromversorgung	RB_FB6_ASE_FM1	Ausgang Stromversorgung Eingabeeinheit	Stromversorgung der Eingabeeinheit	Unterbrechung/Kurzschluss	Keine Stromversorgung der Eingabeeinheit	Fehlerhaftes Ausgangssignal der Baugruppe
RB_FB6	Stromversorgung	RB_FB6_ASAD_FM1	Ausgang Stromversorgung A/D-Wandler	Stromversorgung des A/D-Wandlers	Unterbrechung/Kurzschluss	Keine Stromversorgung des A/D-Wandlers	Fehlerhaftes Ausgangssignal der Baugruppe
RB_FB6	Stromversorgung	RB_FB6_ASV_FM1	Ausgang Stromversorgung Verarbeitungslogik	Stromversorgung der Verarbeitungslogik	Unterbrechung/Kurzschluss	Keine Stromversorgung der Verarbeitungslogik	Fehlerhaftes Ausgangssignal der Baugruppe
RB_FB6	Stromversorgung	RB_FB6_ASA_FM1	Ausgang Stromversorgung Ausgabeeinheit	Stromversorgung der Ausgabeeinheit	Unterbrechung/Kurzschluss	Keine Stromversorgung der Ausgabeeinheit	Fehlerhaftes Ausgangssignal der Baugruppe
RB_FB6	Stromversorgung	RB_FB6_ASDA_FM1	Ausgang Stromversorgung D/A-Wandler	Stromversorgung des D/A-Wandlers	Unterbrechung/Kurzschluss	Keine Stromversorgung des D/A-Wandlers	Fehlerhaftes Ausgangssignal der Baugruppe
RB_FB6	Stromversorgung	RB_FB6_S_FM1	Stromversorgung	Stromversorgung	Fehlerhafte Stromversorgung	Keine Stromversorgung der Baugruppe	Fehlerhaftes Ausgangssignal der Baugruppe

Die FMEA der generischen rechnerbasierten Baugruppe in Tabelle 5.4 zeigt, dass jeder Fehler in einer der Funktionsblöcke der rechnerbasierten Baugruppe zu einem fehlerhaften Ausgangssignal der Baugruppe führt. Wie bereits für die nichtprogrammierbare und programmierbare Baugruppe beschrieben, werden auch die für einen Fehler in der rechnerbasierten Verarbeitungslogik (in der FMEA farbig markiert) möglichen Failure Modes in Abschnitt 5.2.5 gesondert dargestellt. Da in der rechnerbasierten Verarbeitungslogik neben den auch in den nichtprogrammierbaren und programmierbaren Verarbeitungslogiken enthaltenen Elementen noch andere Elemente enthalten sein können (siehe obige Beschreibung), ergeben sich für die rechnerbasierte Verarbeitungslogik im Vergleich zu den nichtprogrammierbaren und programmierbaren Verarbeitungslogiken mehr mögliche Failure Modes.

5.2.5 Mögliche Failure Modes

In den nachfolgenden Tabellen mit möglichen Failure Modes werden ausschließlich Failure Modes für die jeweiligen Verarbeitungslogiken (nichtprogrammierbare Verarbeitungslogik, programmierbare Verarbeitungslogik, rechnerbasierte Verarbeitungslogik) dargestellt, da diese den grundlegenden Unterschied zwischen den drei Arten von Baugruppen darstellen. Da bei den für die drei Arten von Baugruppen durchgeführten FMEAs generische Baugruppen betrachtet werden, können keine konkreten Failure Modes angegeben werden, da keine konkreten Elemente, die in den Verarbeitungslogiken der Baugruppen enthalten sind, angegeben werden können. In den jeweiligen Abschnitten zu den drei Arten von Baugruppentypen werden aber Elemente genannt, die in den jeweiligen Verarbeitungslogiken enthalten sein können. Dabei wird darauf hingewiesen, dass es Elemente gibt, die in allen drei Arten von Baugruppen enthalten sind. Darüber hinaus gibt es noch Elemente, die nur in den programmierbaren und rechnerbasierten Baugruppen aber nicht in den nichtprogrammierbaren Baugruppen enthalten sind. Für die rechnerbasierten Baugruppen gibt es darüber hinaus noch Elemente, die nur in diesen Baugruppen aber nicht in den nichtprogrammierbaren und programmierbaren Baugruppen enthalten sind. Im Folgenden werden mögliche Failure Modes für die in den Abschnitten 5.2.2 bis 5.2.4 genannten Elemente, die in den jeweiligen Verarbeitungslogiken enthalten sein können, dargestellt.

5.2.5.1 Übergreifende Failure Modes für alle Beispielbaugruppen

In Tabelle 5.5 werden Failure Modes dargestellt, die in allen drei untersuchten Arten von Baugruppen (nichtprogrammierbar, programmierbar, rechnerbasiert) vorkommen können, da die entsprechenden Elemente in allen drei Verarbeitungslogiken enthalten sein können.

Tab. 5.5 Mögliche Failure Modes für alle Beispielbaugruppen

Element der Verarbeitungslogik	Mögliche Failure Modes
Kondensatoren	Elektrolytverlust
	Erhöhter Leckstrom
	Kapazitätsänderung
	Kurzschluss
	Unterbrechung
Widerstände	Kurzschluss
	Unterbrechung
	Widerstandsänderung
Spulen	Kurzschluss
	Unterbrechung
	Windungsschluss
Transformatoren	Kurzschluss
	Unterbrechung
	Windungsschluss
Halbleiter-Bauelemente	Erhöhter Leckstrom
	Instabiler Betrieb
	Kurzschluss
	Lötfehler
	Mangelnde Spannungsfestigkeit

Element der Verarbeitungslogik	Mögliche Failure Modes
Halbleiter-Bauelemente	Unterbrechung
	Verschiebung der Schwellenspannung
	Widerstandsschwankungen
Integrierte Schaltkreise	Erhöhter Leckstrom
	Kurzschluss
	Unterbrechung
Lötverbindungen	Kontaktfehler
	Unterbrechung
Schalter	Kurzschluss
	Leckstrom
	Unstabil
	Unterbrechung
Kabel	Unterbrechung
Relais	Ermüdung Feder
	Kontakt öffnet nicht
	Kontakt schließt nicht
	Kurzschluss Spule
	Unterbrechung Spule
	Windungsschluss Spule
Operationsverstärker	Ausgang dauerhaft auf „max“
	Ausgang dauerhaft auf „min“
	Kurzschluss zwischen Eingang und Ausgang
	Kurzschluss zwischen positiver und negativer Versorgungsspannung

Element der Verarbeitungslogik	Mögliche Failure Modes
A/D-Wandler	Alle Bits des A/D-Wandlers bleiben bei „0“ oder „1“ stecken
A/D-Wandler	Zufälliger Bit-Fehler des A/D-Wandlers
	Taktgenerator liefert falschen/keinen Takt
	Fehlerhafter Komparator
D/A-Wandler	Alle analogen Signale des D/A-Wandlers fehlerhaft „max“
	Alle analogen Signale des D/A-Wandlers fehlerhaft „min“
	Fehlerhafter Komparator
	Taktgenerator liefert falschen/keinen Takt
Flipflops	Durchlauf einer Änderung am Eingang ohne Laufzeiten zu beachten (race-through), vor allem bei Master-Slave-Flipflops
	Fehler aufgrund von degradiertem Taktsignal (clock slope)
	Fehlerhafte Ausgangssignale aufgrund von Störungen in der Spannungsversorgung (power supply noise)
	Verlust der gespeicherten Daten aufgrund von Leckströmen (dynamic node discharge)
	Zu langsame Reaktionszeit um Änderung am Eingang zu detektieren
Ein-/Ausgabebaugruppen mit analogen Ausgängen	Aufhängen/Absturz
	Driftendes Ausgangssignal
	Fehlerhaftes Ausgangssignal (fehlerhaft auf „MAX“)
	Fehlerhaftes Ausgangssignal (fehlerhaft auf „MIN“)

Element der Verarbeitungslogik	Mögliche Failure Modes
	Fehlerhaftes Ausgangssignal (außerhalb des zulässigen Bereichs)
	Verzögertes Ausgangssignal
Ein-/Ausgabebaugruppen mit analogen Ausgängen	Zufälliges Ausgangssignal (z. B. fluktuierend zwischen MIN und MAX)
ASICs ohne Prozessor	Defekter Transistor
	Erhöhter Leckstrom
	Kurzschluss
	Unterbrechung

5.2.5.2 Zusätzliche mögliche Failure Modes für FGPA-basierte Baugruppen

Der nachfolgende Text und die Abbildungen zu Failure Modes für FPGA-basierte Baugruppen basieren vorwiegend auf der Quelle /QUI08/.

Mehrere Forschungsprojekte zur Untersuchung des Einflusses der Weltraumstrahlung auf FPGAs insbesondere auf SRAM-FPGAs wurden durchgeführt. Zwei strahlungsinduzierte Fehlermodes wurden in SRAM-FPGAs identifiziert:

- Single Event Upsets (SEUs): Eine beliebige Speicherzelle des FPGAs ändert ihren Zustand (Bitzustandswechsel)
- Single Event Functional Interrupts (SEFIs): Ein Konfigurationsbit des FPGAs ändert seinen Zustand, d. h. ein Bitzustandswechsel („bit flip“) findet in einer Speicherzelle zur Konfiguration des FPGAs statt

Ein „bit flip“ auf einem SRAM-FPGA kann die Funktionalität des FPGAs wie nachfolgend erläutert beeinflussen.

- Routingfehler in Schaltboxen (siehe Abbildung 5.5):
  In Schaltboxen werden Verknüpfungen zwischen logischen Funktionen durch Vorgabe des Speicherzustandes der Schaltbox-Speicherzellen realisiert. Ein Bitzustandswechsel („bit flip“) in der Speicherzelle der Schaltbox (d. h. der Speicherzustand wechselt von „0“ auf „1“ oder umgekehrt) führt zu einem Verbindungsfehler

(Routingfehler) zwischen den Logik-blöcken (CLBs), d. h. zu fehlerhaften Verknüpfungen der logischen Funktionen. Ein Routingfehler kann zu Fehlfunktionen des FPGAs führen.

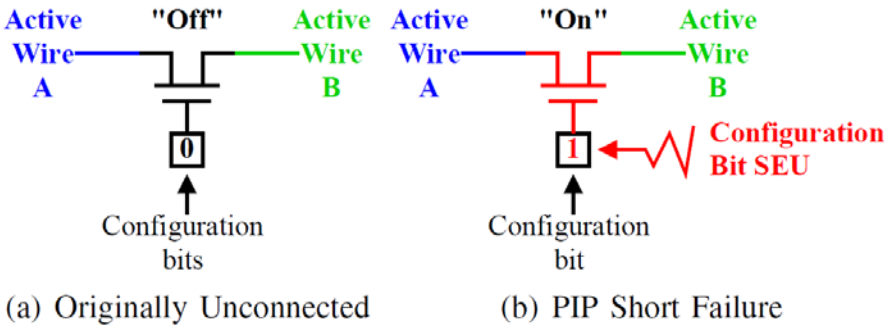

Abb. 5.5 Beispiel Routingfehler in Schaltboxen /QUI08/

- Routingfehler in Logikblöcken (CLBs) (siehe Abbildung 5.6):
  Ein Routingnetzwerk besteht aus Multiplexern (MUX) zur Weiterleitung der Logik innerhalb der CLBs und zu den externen Elementen. Ein Routingfehler entsteht beim Bitzustandswechsel in Konfigurationsbits des Multiplexers. Ein Bitzustandswechsel führt zum Fehler in der MUX-Auswahl. Ein Routingfehler kann zu Fehlfunktionen des FPGAs führen.

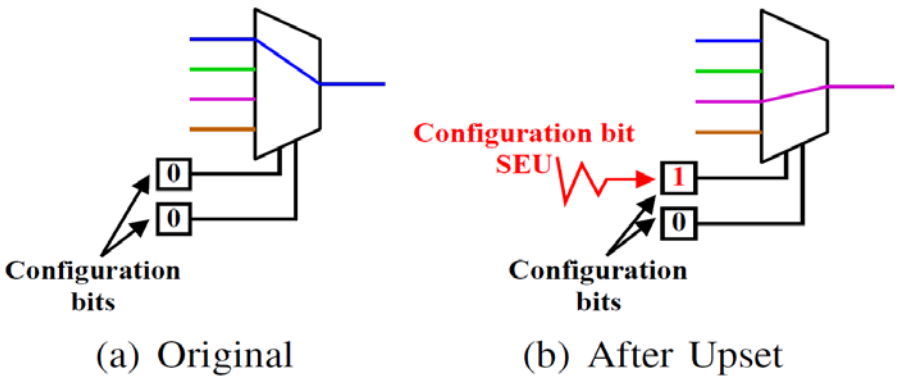

Abb. 5.6 Routingfehler in CLBs /QUI08/

- Logikfehler (siehe Abbildung 5.7):
  Die logischen Funktionen des FPGAs sind in Wertetabellen (sogenannte Look Up Tables (LUT)) in den Logikblöcken gespeichert. Ein Logikfehler entsteht bei Bitzustandswechsel in LUTs. Ein Bitzustandswechsel führt zur Änderung eines Wertes der LUT. Dies kann zu Ausgabefehlern führen.

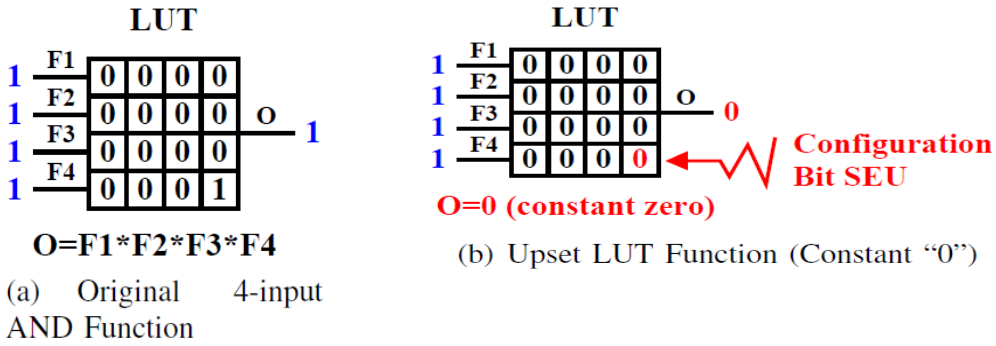

Abb. 5.7 Logikfehler in der LUT /QUI08/

- Fehler in den Kontrollelementen des FPGAs:
  Kontrollelemente des FPGAs sind i. d. R. Speicherelemente zur Konfiguration des FPGAs (Schnittstellen-Konfiguration Pins, Ein- und Ausgabe Pins), Logik-Controller für Testzwecke und Fehlersuche und Reset-Controller. Ein Bitzustandswechsel in den Kontrollelementen führt zur Änderung der Konfiguration des FPGAs, d. h. zur Änderung des FPGA-Programms. Ein Bitzustandswechsel in den Kontrollelementen kann zum Verlust der Funktionalität des FPGAs führen.

- Fehler in den Anwenderdaten:
  Ein Bitzustandswechsel in den Speicherzellen für Anwenderdaten kann zu Eingabefehlern und demzufolge zur Fehlfunktion des FPGAs führen.

- Programmierfehler:
  Der Entwicklungsprozess von FPGAs ist überwiegend softwarebasiert. Der Entwicklungsprozess erfolgt mit proprietären Softwaretools der Hersteller. Die Qualifizierung und Validierung der proprietären Softwaretools gestaltet sich schwierig. Fehler in den Softwaretools können zu Fehlern in den FPGAs führen. Die Komplexität des FPGA-Designs kann zu Programmierfehlern des FPGAs führen, d. h. der programmierte Bitstrom zur Konfiguration des FPGAs kann fehlerhaft sein.

5.2.5.3 Zusätzliche mögliche Failure Modes für programmierbare und rechnerbasierte Baugruppen

Wie in den Abschnitten 5.2.2, 5.2.3 und 5.2.4 beschrieben, können in den Verarbeitungslogiken der programmierbaren und rechnerbasierten Baugruppen neben den Elementen, die in der Verarbeitungslogik der nichtprogrammierbaren Baugruppen (und damit in den

Verarbeitungslogiken aller drei betrachteten Arten von Baugruppen) enthalten sein können, zusätzlich weitere Elemente enthalten sein. Daraus ergeben sich für die programmierbaren und rechnerbasierten Bauelemente neben den in Tabelle 5.5 dargestellten Failure Modes weitere Failure Modes, die nur in den Verarbeitungslogiken dieser beiden Arten von Baugruppen, aber nicht in der Verarbeitungslogik der nichtprogrammierbaren Baugruppen vorkommen können. Diese zusätzlichen Failure Modes sind in der nachfolgenden Tabelle 5.6 dargestellt.

Tab. 5.6 Zusätzliche mögliche Failure Modes für programmierbare und rechnerbasierte Baugruppen

Element der Verarbeitungslogik	Mögliche Failure Modes
Multiplexer	Verlust aller Signale vom Multiplexer
	Verlust eines Signals vom Multiplexer
Demultiplexer	Alle analogen Ausgangssignale fehlerhaft
	Ein analoges Ausgangssignal fehlerhaft
RAM/SRAM	Ausfall des RAM/SRAM
	Falscher Speicherinhalt
Taktgenerator	Falscher Takt
	Kein Takt
ROM, EPROM, EEPROM, Flash	Drift der injizierten Elektronen durch den Isolator, daher Ladungsverlust und Ausgang wird zu „0“
	Einfang von Elektronen im Gate-Oxid während des Überschreibens (EEPROM), nach etlichen Zyklen kann daher nicht mehr zwischen „0“ und „1“ unterschieden werden und der Ausgang ist immer „1“
Prozessor (Mikroprozessor, CPU)	Prozessor funktioniert scheinbar fehlerfrei, sendet aber ein fehlerhaftes Ausgangssignal
	Stopp bei Aktualisierung des Ausgangssignals
Mikrocontroller	Interner Fehler

Element der Verarbeitungslogik	Mögliche Failure Modes
	On-Board Speicherfehler
Watchdog	Fehlerhaftes Reset-Signal an Prozessor
	Fehlerhafter Timer
	Softwarefehler
Ein-/Ausgabebaugruppen mit digitalen Ausgängen	Aufhängen/Absturz
	Ausgangssignal bleibt auf gegenwärtigem Wert hängen („Einfrieren“)
	Fehlerhaftes Ausgangssignal (fehlerhaft „1“)
	Fehlerhaftes Ausgangssignal (fehlerhaft „0“)
	Verzögertes Ausgangssignal
	Zufälliges Ausgangssignal
Softwarefehler	Aufhängen/Absturz (z. B. durch Stecken-bleiben in Endlosschleife, Teilen durch Null, illegaler Speicherzugriff, Zugriff auf ungültige Daten)
	Fehlerhaftes Ausgangssignal (fehlerhaft „1“)
	Fehlerhaftes Ausgangssignal (fehlerhaft „0“)
	Ausgangssignal bleibt auf gegenwärtigem Wert hängen („Einfrieren“)
	Verzögertes Ausgangssignal
	Zufälliges Ausgangssignal
Baugruppen zur Datenverarbeitung	Aufhängen/Absturz
	Falsches Ausgangssignal
	Verzögertes Ausgangssignal
Baugruppen zur Datenverarbeitung	Zufälliges Ausgangssignal
Kommunikationsbezogene Fehlermodes digitaler Systeme	Verfälschtes Telegramm (gekipptes Bit aufgrund von elektromagnetischen Einkopplungen, Prozessorfehlern, Speicherfehlern, Interferenzen)

Element der Verarbeitungslogik	Mögliche Failure Modes
	Ungewollte Telegrammwiederholung
	Falsche Reihenfolge von Telegrammen
	Telegrammverlust
	Inakzeptable Verzögerung (Nachricht erreicht Empfänger außerhalb eines definierten Zeitfensters)
	Insertion (Einfügen nicht erwünschter Daten in das Telegramm)
	Maskerade (Telegramm mit richtiger Struktur um als valide anerkannt zu werden, aber tatsächlich handelt es sich um ein „falsches“ Telegramm)
	Falsche Adressierung (Telegramm wird an für dieses Telegramm nicht vorgesehenen Teilnehmer geschickt)
	Broadcast Sturm (Überflutung des Netzwerks mit Nachrichten)
	Babbling Idiot (Netzwerkteilnehmer, der zu beliebigen Zeitpunkten Daten sendet, dadurch extreme Belegung des Übertragungsmediums bis hin zum vollständigen Zusammenbruch der Kommunikation; im Prinzip wie Broadcast Sturm, aber nur ein Verursacher)
Kommunikationsbezogene Fehlermodes digitaler Systeme	Inkonsistenz (byzantinischer Fehler) (Netzwerkteilnehmer erhält Werte von zwei redundanten Quellen, diese Werte unterscheiden sich; daraufhin weiß Teilnehmer nicht, welche Information wahr ist und es entsteht Konfusion, welche sich weiter ausbreiten kann; kann Kommunikation über das gesamte redundante System zum Erliegen bringen)

Element der Verarbeitungslogik	Mögliche Failure Modes
	Exzessives Jittern (zeitlich variable Verzögerung von Ausgangswerten in verschiedenen Abfragezyklen, d. h. der berechnete Wert wird in verschiedenen Abgabezyklen zu verschiedenen Zeiten ausgegeben)
	Kollision (zwei oder mehr Teilnehmer senden gleichzeitig Daten über das Übertragungsmedium, dabei Überlagerung der Daten und Verfälschung der Originaldaten aufgrund von Interferenzen)

Wie in Tabelle 5.6 zu sehen ist, ergeben sich bei der Verwendung von programmierbaren oder rechnerbasierten Baugruppen eine deutlich höhere Anzahl an möglichen Failure Modes, die zum Ausfall der Baugruppen führen können. Das Ausfallverhalten einer Baugruppe und die dabei möglichen Failure Modes hängen also entscheidend davon ab, ob diese Baugruppe nicht programmierbar ist oder ob sie Softwarebestandteile enthält, d. h. entweder auf einer programmierbaren oder einer rechnerbasierten Verarbeitungslogik basiert. Vor allem bei Baugruppen mit Softwarebestandteilen ist es nicht möglich, die Fehlerfreiheit der Baugruppe durch Test oder Analyse zu zeigen, da die Software aufgrund ihrer Komplexität nicht vollständig geprüft werden kann. Mögliche Fehler in der Software sind normalerweise latent vorhanden. Ein systematisches Versagen der Baugruppe aufgrund eines gemeinsam verursachten Ausfalls (common cause failure, CCF) der Software kann durch Ereignisse ausgelöst werden, die so komplex sind, dass die Fehler in der Testphase nur sehr schwer aufzufinden sind. Damit ein systematisches Versagen aufgrund eines CCF nicht mehr zu unterstellen ist, muss eine hinreichende Diversität von Hard- und Software sichergestellt werden. Aus diesem Grund werden in Kapitel 6 Diversitätsmerkmale definiert, mittels derer die Diversität von Baugruppen oder Systemen bewertet werden kann. Hierzu werden zunächst die Bestandteile eines generischen leittechnischen Systems definiert, wobei zwischen nicht programmierbaren, programmierbaren und rechnerbasierten Baugruppen sowie zwischen Komponenten mit und ohne Softwarebestandteilen unterschieden wird. Anschließend werden die erarbeiteten Diversitätsmerkmale mittels einer Matrix mit den definierten Bestandteilen eines generischen Leittechniksystems in Bezug gesetzt.

6 Definition von Diversitätsmerkmalen und Erarbeitung Kriterien und Kenngrößen

Die FMEA hat gezeigt, dass bei der Verwendung von programmierbaren oder rechnerbasierten Baugruppen eine deutlich höhere Zahl an Failure Modes, die zum Ausfall der Baugruppe führen können, möglich ist. Daher ist es für die Erarbeitung von Diversitätsmerkmalen wichtig, zwischen Komponenten mit und ohne Softwarebestandteilen zu unterscheiden. Dies wurde bei der Erarbeitung von Diversitätsmerkmalen ebenso zugrunde gelegt wie die Erkenntnisse aus den nationalen und internationalen Normen und Regelwerken zu Diversitätsmerkmalen.

6.1 Vorgehensweise zur Erstellung einer Matrix der Diversitätsmerkmale

Die Recherchen in nationalen und internationalen Normen und Regelwerken zu Diversitätsmerkmalen haben ergeben, dass die Herangehensweise bei der Beurteilung der Diversität sehr unterschiedlich ist. In einigen Normen und Regelwerken finden sich lediglich grob strukturierte Aufzählungen von Merkmalen, aber keine weiteren Aussagen zu möglichen Merkmalsausprägungen oder zur Anwendung dieser Merkmale (siehe beispielsweise /DIN10a/).

Andererseits gibt es einen Ansatz der U. S. NRC, der als Anwendungsbezug für die aufgelisteten Diversitätsmerkmale noch Abstufungen von „nicht erfüllt“, über „teilweise erfüllt“ bis hin zu „vollständig erfüllt“ einführt und für diese Abstufungen Punkte vergibt, die sich zu einer Gesamtpunktzahl addieren, welche laut /NUR10/ eine Aussage zum Erfüllungsgrad der Diversität geben soll.

Die GRS hält diese Vorgehensweisen für nicht zielführend. Nach Ansicht der GRS ist eine Auflistung von Diversitätsmerkmalen ohne weitere Erklärung aufgrund des fehlenden Anwendungsbezugs nicht ausreichend. Die von der U. S. NRC vorgeschlagene Einführung eines Punktesystems zur Bewertung der Diversität ist nach Einschätzung der GRS aufgrund der zu starken Verallgemeinerung nicht sinnvoll. Beide Herangehensweisen sind daher als Unterstützung in atomrechtlichen Genehmigungs- und Aufsichtsverfahren aus Sicht der GRS nicht geeignet.

Nach Einschätzung der GRS gibt es bei der Beurteilung der Diversität zwei wesentliche Punkte:

- Betrachtung relevanter Aspekte des Lebenszyklus von der Formulierung der Anforderungen über Entwicklung und Herstellung bis hin zu Betrieb und Instandhaltung
- Herstellung des Anwendungsbezugs über flexible Anwendbarkeit auf einzelne Baugruppen, verschiedene Redundanzen eines Leittechniksystems oder ganze Leittechniksysteme

Um diese beiden Punkte zu erfüllen, wurde von der GRS zunächst eine generische Darstellung eines Leittechniksystems erarbeitet. Dabei wurden sowohl die für die Ausführung der Leittechnik-Funktionen wichtigen Bestandteile des Leittechniksystems berücksichtigt als auch weitere technische Aspekte des Leittechniksystems, die nicht direkt für die Ausführung der Leittechnik-Funktionen verantwortlich sind (siehe Abschnitt 6.2). Im nächsten Schritt wurden Diversitätsmerkmale erarbeitet und definiert, welche die für die Beurteilung der Diversität relevanten Aspekte des Lebenszyklus dieses generischen Leittechniksystems abdecken. Da nicht alle Diversitätsmerkmale auf jeden Teil einer Baugruppe oder eines Leittechniksystems anzuwenden sind, wurde von der GRS eine Matrix erstellt, welche die Bestandteile des generischen Leittechniksystems mit den Diversitätsmerkmalen verknüpft (siehe Abschnitt 6.3). Diese Matrix ist fallspezifisch anwendbar, Anwendungsbeispiele werden in Abschnitt 6.4 gegeben. Durch die Bewertung der Diversität einer Einrichtung oder eines Systems mittels der Diversitätsmerkmale in der Matrix der Diversitätsmerkmale soll erreicht werden, dass ein systematisches Versagen aufgrund gemeinsam verursachter Ausfälle (common cause failure, CCF) nicht mehr unterstellt werden muss.

Die Matrix kann nicht nur speziell auf Ersatzbaugruppen angewandt werden, sondern generell auf Baugruppen, Komponenten, Teilsysteme und Systeme deren Diversität geprüft werden soll. Je nach Art und Umfang der zu beurteilenden leittechnischen Einrichtung findet entweder die komplette Matrix der Diversitätsmerkmale Anwendung oder ein Auszug der relevanten Zeilen und Spalten der Matrix der Diversitätsmerkmale. Anwendungsbeispiele werden in Abschnitt 6.4.1 beschrieben.

6.2 Definition der typischen Bestandteile eines Leittechniksystems

Bei der Erarbeitung der generischen Darstellung eines Leittechniksystems wurden zum einen die direkt mit der Ausführung der Leittechnik-Funktion verbundenen Ebenen betrachtet:

- Eingabe (siehe Abschnitt 6.2.1)
- Verarbeitung (siehe Abschnitt 6.2.2)
- Ausgabe (siehe Abschnitt 6.2.3)

Zusätzlich wurden auch folgende technische Aspekte mit betrachtet, die zwar nicht direkt zum Signalpfad der Leittechnik-Funktion gehören, aber für deren Ausführung unverzichtbar sind:

- Stromversorgung (siehe Abschnitt 6.2.4)
- Schutzeinrichtungen (siehe Abschnitt 6.2.5)
- Kommunikation (siehe Abschnitt 6.2.6)
- Zugriffsmöglichkeiten (siehe Abschnitt 6.2.7)

Auch die Funktionsweise des Gesamtsystems wird betrachtet (siehe Abschnitt 6.2.8).

Die Arbeiten im zweiten Arbeitspaket, vor allem die Ergebnisse der beispielhaft durchgeführten FMEA, haben gezeigt, dass das Ausfallverhalten einer Baugruppe und die dabei möglichen Failure Modes entscheidend davon abhängen, ob diese Baugruppe nicht programmierbar ist oder ob sie Softwarebestandteile, d. h. entweder programmierbare oder rechnerbasierte Bestandteile, enthält. Daher werden Komponenten mit und Komponenten ohne Softwarebestandteile in allen oben genannten Bereichen getrennt betrachtet.

6.2.1 Eingabe

Die Eingabeebene des von der GRS definierten generischen Leittechniksystems umfasst alle Komponenten, die für die Erfassung und Eingabe von Messwerten und Daten zur Ausführung der Leittechnik-Funktion verantwortlich sind. Dabei werden für die hier erstellte Matrix der Diversitätsmerkmale folgende Bestandteile eingeführt und definiert:

Sonden

Unter Sonden wird die zur Messung der Anlagenparameter (physikalisch messbare Größe, z. B. Druck, Temperatur) eingesetzte Hardware verstanden.

Messumformer ohne Softwarebestandteile

Ein Messumformer ohne Softwarebestandteile ist ein Gerät ohne Softwarebestandteile, welches zur Umformung der mittels Sonden gemessenen Anlagenparameter in elektrische Eingangssignale für die Verarbeitungsebene eingesetzt wird.

Messumformer mit Softwarebestandteilen

Ein Messumformer mit Softwarebestandteilen ist ein Gerät mit Softwarebestandteilen, welches zur Umformung der mittels Sonden gemessenen Anlagenparameter in elektrische Eingangssignale für die Verarbeitungsebene eingesetzt wird.

Bedienelemente ohne Softwarebestandteile

Bedienelemente ohne Softwarebestandteile sind Vorrichtungen ohne Softwarebestandteile, welche eine manuelle Bedienung oder Konfiguration einer Komponente oder eines Systems durch den Operateur ermöglichen (z. B. Schalter, Potentiometer etc.).

Bedienelemente mit Softwarebestandteilen

Bedienelemente mit Softwarebestandteilen sind Vorrichtungen mit Softwarebestandteilen, welche eine manuelle Bedienung oder Konfiguration einer Komponente oder eines Systems durch den Operateur ermöglichen (z. B. Eingabedisplays, Touchscreens etc.).

6.2.2 Verarbeitung

Die Verarbeitungsebene des von der GRS definierten generischen Leittechniksystems umfasst alle Komponenten, die eingesetzt werden, um die von der Eingabeebene des Leittechniksystems zur Verfügung gestellten Daten zu verarbeiten. Dies schließt beispielsweise die Grenzwertbildung, logische Operationen, den Signalvergleich und die Berechnung der Ausgangssignale für die Ausgabeebene ein. Zusätzlich werden Baugruppen für die Priorisierung der Ausgangssignale hier mit betrachtet. Für die hier erstellte Matrix der Diversitätsmerkmale werden auf der Verarbeitungsebene folgende Typen von Baugruppen und Komponenten unterschieden und wie folgt definiert:

Nicht programmierbare Baugruppen ohne Softwarebestandteile

Nichtprogrammierbare Baugruppen ohne Softwarebestandteile sind aus diskreten Bauelementen aufgebaute Baugruppen, die keine programmierbaren Bauelemente enthalten. Sie enthalten beispielsweise festverdrahtete Logikgatter.

Nicht programmierbare Baugruppen mit Softwarebestandteilen

Nichtprogrammierbare Baugruppen mit Softwarebestandteilen sind Baugruppen, die zusätzlich zu den diskreten Bauelementen auch Bauelemente enthalten, deren softwarebasierte Konfigurierung im Herstellungsprozess vorgenommen wird und anschließend nicht mehr verändert werden kann (beispielsweise vom Anwender nicht veränderliche Firmware). Diese Baugruppen enthalten beispielsweise einfache ASICs ohne integrierten Mikroprozessor, deren Programmierung beim Kunden nicht mehr veränderbar ist.

Programmierbare Baugruppen

Programmierbare Baugruppen sind Baugruppen, die mindestens ein diskretes, programmierbares Bauelement enthalten. Die softwarebasierte Konfigurierung der Baugruppen bleibt nach dem Herstellungsprozess veränderbar. Diese Gruppe umfasst also Baugruppen unterschiedlicher Komplexität, wie z. B. CPLDs (complex programmable logic devices) oder FPGAs (field programmable gate arrays).

Rechnerbasierte Baugruppen

Rechnerbasierte Baugruppen sind Baugruppen, die einen oder mehrere Prozessoren enthalten. Sowohl Konfiguration als auch Funktion der Baugruppe werden durch die Ausführung von Software in einem Betriebssystem realisiert. Auch diese Gruppe umfasst Baugruppen sehr unterschiedlicher Komplexität von einfachen Mikrocontrollern über Mikroprozessoren bis hin zu Multi-Core Prozessoren. ASICs und FPGAs, welche Mikroprozessoren enthalten, werden ebenfalls dieser Baugruppenart zugeordnet.

Rechner

Unter Rechner sind mit dem Leittechniksystem dauerhaft oder zeitweise verbundene, eigenständige Rechneranlagen zu verstehen, die für die Ausführung von Leittechnik-Funktionen relevant sind, wie beispielsweise Steuerstabfahrrechner etc.

6.2.3 Ausgabe

Die Ausgabe- und Anregeebene des von der GRS definierten generischen Leittechniksystems umfasst alle Komponenten, die für die Umformung der elektrischen Signale aus der Verarbeitungsebene und für die Ansteuerung der verfahrenstechnischen Komponenten genutzt werden. Die Aktuatoren werden ebenfalls mit betrachtet. Dabei werden für die hier erstellte Matrix der Diversitätsmerkmale folgende Bestandteile eingeführt und definiert:

Koppelebene ohne Softwarebestandteile

Unter der Koppelebene ohne Softwarebestandteile sind Geräte ohne Softwarebestandteile zu verstehen, welche die Ausgangssignale aus der Verarbeitungsebene umformen, um die Ansteuerung der Aktuatoren zu ermöglichen (z. B. Relais oder Schütze ohne Softwarebestandteile).

Koppelebene mit Softwarebestandteilen

Unter der Koppelebene mit Softwarebestandteilen sind Gerät mit Softwarebestandteilen zu verstehen, welche die Ausgangssignale aus der Verarbeitungsebene umformen, um die Ansteuerung der Aktuatoren zu ermöglichen (z. B. Relais mit softwarebasierter Ansteuerung der Relaisspule).

Aktuatoren

Aktuatoren sind Komponenten, welche zur Beeinflussung der Anlagenparameter eingesetzte werden, wie beispielsweise Ventile, Schieber, Pumpen, Motoren etc.

Anzeigen (einschließlich Meldeeinrichtungen) ohne Softwarebestandteile

Anzeigen ohne Softwarebestandteile sind Vorrichtungen ohne Softwarebestandteile, welche zur Signalisierung von Informationen (z. B. Messwerte) genutzt werden (z. B. Zeigerelemente, Siebensegmentanzeigen, Schreiber etc.).

Anzeigen (einschließlich Meldeeinrichtungen) mit Softwarebestandteilen

Anzeigen mit Softwarebestandteilen sind Vorrichtungen mit Softwarebestandteilen, welche zur Signalisierung von Informationen (z. B. Messwerte) genutzt werden (z. B. Displays, Monitore, Melderechner etc.).

6.2.4 Stromversorgung

Die Stromversorgung des von der GRS definierten generischen Leittechniksystems umfasst alle für die Stromversorgung wichtigen Komponenten. Dabei werden für die hier erstellte Matrix der Diversitätsmerkmale folgende Bestandteile eingeführt und definiert:

Kabel und Leitungen

Zu dieser Gruppe gehören Kabel und Leitungen, welche zur Stromversorgung einer Baugruppe eingesetzt werden. Zur Kommunikation eingesetzte Kabel und Leitungen fallen in die Gruppe Kommunikation und sind hier nicht gemeint.

Einrichtungen der Stromversorgung ohne Softwarebestandteile

Unter dieser Gruppe sind Einrichtungen der Stromversorgung zusammengefasst, die keine Softwarebestandteile enthalten. Darunter fallen beispielsweise Batterien, Gleichrichter, Wechselrichter, Transformatoren, Dieselgeneratoren etc.

Einrichtungen der Stromversorgung mit Softwarebestandteilen

Unter dieser Gruppe sind Einrichtungen der Stromversorgung zusammengefasst, die Softwarebestandteile enthalten. Darunter fallen Gleich- oder Wechselrichter mit Softwarebestandteilen (z. B. softwaregesteuerter pulsweitenmodulierter Gleichrichter).

6.2.5 Schutzeinrichtungen

Die Schutzeinrichtungen des von der GRS definierten generischen Leittechniksystems umfassen sowohl Schutzeinrichtungen für einzelne Komponenten als auch Einrichtungen des Block-, Turbinen-, Generatorschutzes etc. Dabei werden für die hier erstellte Matrix der Diversitätsmerkmale folgende Einrichtungen eingeführt und definiert:

Aggregateschutz ohne Softwarebestandteile

Unter dieser Gruppe versteht man eine Schutzeinrichtung ohne Softwarebestandteile, die ein einzelnes Aggregat überwacht und vor Beschädigung schützt, wie z. B. Buchholzschutz, Öldrucküberwachung oder Überdrehzahlüberwachung ohne Softwarebestandteile.

Aggregateschutz mit Softwarebestandteilen

Unter dieser Gruppe versteht man eine Schutzeinrichtung mit Softwarebestandteilen, die ein einzelnes Aggregat überwacht und vor Beschädigung schützt, wie z. B. Buchholzschutz, Öldrucküberwachung oder Überdrehzahlüberwachung mit Softwarebestandteilen.

Sonstige Schutzeinrichtungen ohne Softwarebestandteile

Unter dieser Gruppe versteht man Schutzeinrichtungen des Blockschutzes, Generatorschutzes, Turbinenschutzes etc. ohne Softwarebestandteile, welche Fehler erkennen und deren weitere Ausbreitung unterbinden. Zu dieser Gruppe gehören beispielsweise Differentialschutz, Unterfrequenzschutz, Schieflastschutz, Distanzschutz, etc. ohne Softwarebestandteile.

Sonstige Schutzeinrichtungen mit Softwarebestandteilen

Unter dieser Gruppe versteht man Schutzeinrichtungen des Blockschutzes, Generatorschutzes, Turbinenschutzes etc. mit Softwarebestandteilen, welche Fehler erkennen und deren weitere Ausbreitung unterbinden. Zu dieser Gruppe gehören beispielsweise Differentialschutz, Unterfrequenzschutz, Schieflastschutz, Distanzschutz, etc. mit Softwarebestandteilen.

6.2.6 Kommunikation

Die Kommunikation des von der GRS definierten generischen Leittechniksystems umfasst alle hard- und softwaretechnischen Komponenten sowie Protokolle, die am Datenfluss des Leittechniksystems beteiligt sind. Dabei werden für die hier erstellte Matrix der Diversitätsmerkmale folgende Bestandteile eingeführt und definiert:

Hardwaresysteme zur Realisierung des Datenflusses

Unter dieser Gruppe ist die gesamte, entlang des Signalpfades von der Sonde bis zum Aktuator verwendete, Hardware zur Realisierung des Datenflusses zusammengefasst. Dazu gehören beispielsweise Kupferleitungen oder Glasfaserkabel ebenso wie die Hardware von Ethernet und Bussystemen etc. einschließlich der Schnittstellen.

Protokolle

Unter Protokollen versteht man Vereinbarungen zum Ablauf der Kommunikation innerhalb eines Datennetzes, wie z. B. TCP/IP, Fieldbus Data Link, DP-Protokoll etc.

Signalwandler ohne Softwarebestandteile

Signalwandler ohne Softwarebestandteile werden zur Konvertierung von Signalen zu deren weiterer Verarbeitung genutzt. Ein Beispiel für einen solchen Signalwandler ohne Softwarebestandteile ist ein AD-Wandler, der beispielsweise dazu dienen kann, ein analoges Spannungssignal in ein Binärsignal zu wandeln.

Signalwandler mit Softwarebestandteilen

Signalwandler mit Softwarebestandteilen werden zur Konvertierung von Signalen oder Datenpaketen zu deren weiterer Verarbeitung genutzt. Ein Beispiel für einen solchen Signalwandler mit Softwarebestandteilen ist ein Gateway, welches beispielsweise zwei auf unterschiedlichen Netzwerkprotokollen operierende Datennetze verbindet und dabei die Konvertierung der Daten vornimmt.

6.2.7 Zugriffsmöglichkeiten

Die Zugriffsmöglichkeiten auf das von der GRS definierte generische Leittechniksystem umfassen sowohl die prinzipiellen Möglichkeiten, auf das System zuzugreifen als auch die technischen Umsetzungen administrativer Zugriffsregeln. Dabei werden für die hier erstellte Matrix der Diversitätsmerkmale folgende Bestandteile eingeführt und definiert:

Zugriffsmöglichkeiten ohne Softwarebestandteile
Unter Zugriffsmöglichkeiten ohne Softwarebestandteile sind hardwaretechnische Möglichkeiten zusammengefasst, um vor Ort oder per Fernzugriff auf ein System zuzugreifen. Hierzu zählen beispielsweise Schlüsselschalter, Kodiereinrichtung etc.

Zugriffsmöglichkeiten mit Softwarebestandteilen (einschließlich Servicerechner)
Unter Zugriffsmöglichkeiten mit Softwarebestandteilen sind hard- und softwaretechnische Möglichkeiten zusammengefasst, um vor Ort oder per Fernzugriff auf ein System zuzugreifen. Hierzu zählt beispielsweise der Anschluss eines Servicerechners, USB-Sticks etc.

Hardwaretechnische Umsetzung administrativer Zugriffsregeln
Unter dieser Gruppe versteht man organisatorische und administrative Festlegungen, die den Zugriff (vor Ort oder per Fernzugriff) auf ein System betreffen und hardwaretechnisch umgesetzt sind, wie z. B. Schlüsselwesen etc.

Softwaretechnische Umsetzung administrativer Zugriffsregeln
Unter dieser Gruppe versteht man organisatorische und administrative Festlegungen, die den Zugriff (vor Ort oder per Fernzugriff) auf ein System betreffen und softwaretechnisch umgesetzt sind, wie z. B. Rechtevergabe an Nutzer durch Systemadministrator etc.

6.2.8 Funktionsweise des Gesamtsystems

Zusätzlich zu den in den vorangegangenen Abschnitten definierten Bestandteilen des generischen Leittechniksystems ist es für die Diversitätsbetrachtung von leittechnischen Systemen notwendig, neben den Einzelbestandteilen auch die Funktionsweise des Gesamtsystems zu betrachten.

6.3 Definition von Diversitätsmerkmalen

Ausgehend von den Ergebnissen der Auswertung von nationalen und internationalen Normen und Regelwerken zur Diversität (siehe Kapitel 4) wurden Diversitätsmerkmale von Komponenten und Baugruppen erarbeitet und definiert. Die von der GRS definierten Diversitätsmerkmale decken dabei die für die Beurteilung der Diversität relevanten Aspekte des Lebenszyklus eines generischen Leittechniksystems von Herstellung und Entwicklung über Systemaufbau und Technologie bis hin zu Betrieb und Instandhaltung sowie das daran beteilige Personal ab.

Sie lassen sich folgenden Gruppen zuordnen:

- Herstellung und Entwicklung
  - Design
  - Softwareerstellung
  - Entwicklung und Fertigung der Hardware
  - Tests
- Systemaufbau und Technologie
  - Eingesetzte Software
  - Eingesetzte Hardware
  - Logik
  - Ankopplung an die Verfahrenstechnik
- Betrieb und Instandhaltung
  - Hard- und Softwaremanagement
  - Tests und Prüfungen
- Beteiligtes Personal
  - Personal bei Herstellung und Entwicklung
  - Personal bei Betrieb und Instandhaltung

Die Diversitätsmerkmale, die sich diesen Gruppen zuordnen lassen, werden in den folgenden Abschnitten näher beschrieben. Darüber hinaus wird beschrieben, unter welchen Bedingungen Diversität in den Diversitätsmerkmalen vorliegt.

Als Verknüpfung zwischen den erarbeiteten Diversitätsmerkmalen und den Bestandteilen des in Abschnitt 6.2 eingeführten generischen Leittechniksystems wurde eine Matrix der Diversitätsmerkmale erstellt. Diese Matrix ist sowohl für ganze Leittechniksysteme als auch redundante Stränge eines Leittechniksystems oder für einzelne Baugruppen oder Komponenten einsetzbar. Sie gibt Aufschluss darüber, welche Diversitätsmerkmale für das Vorliegen von Diversität in einem bestimmten Bestandteil eines Leittechniksystems relevant sind. Dies wird durch Kreuze in der Matrix angezeigt.

Wird beispielsweise im Rahmen eines atomrechtlichen Genehmigungs- und Aufsichtsverfahrens der Einsatz von diversitären Sonden in einem leittechnischen System gefordert, sind alle in der Zeile „Sonden“ der Matrix mit Kreuzen gekennzeichneten Diversitätsmerkmale für die Beurteilung der Diversität relevant. Diversität der Sonden liegt im Rahmen der betrachteten Merkmale dann vor, wenn in allen so gekennzeichneten Diversitätsmerkmalen Diversität vorliegt. In Fällen, in denen nicht in allen Diversitätsmerkmalen Diversität vorliegt, verschafft die Anwendung der Matrix der Diversitätsmerkmale einen Überblick über erfüllte und nicht erfüllte Diversitätsmerkmale. Dies zeigt mögliche Schwächen der zu beurteilenden Sonden im Hinblick auf CCF auf, gibt gleichzeitig aber auch Hinweise auf Verbesserungsmöglichkeiten bei der Diversität der Sonden. Es muss von der zuständigen Aufsichts- und Genehmigungsbehörde dann von Fall zu Fall entschieden werden, ob die Untermenge der erfüllten Diversitätsmerkmale für den vorliegenden Anwendungszweck der Sonden ausreichend ist. Darüber hinaus kann es in der Praxis durchaus vorkommen, dass es schwierig zu beurteilen ist, ob ein Diversitätsmerkmal erfüllt ist oder nicht, oder dass die Frage nach der Erfüllung mit einem „teilweise“ beantwortet wird. Auch in diesen Fällen muss von der zuständigen Aufsichts- und Genehmigungsbehörde entschieden werden, wie mit diesen Merkmalen umzugehen ist.

Generell ist zu beachten, dass es sich bei dem hier beschriebenen System um ein generisches Leittechniksystem handelt, und dass sich die definierten Diversitätsmerkmale auf dieses generische Leittechniksystem beziehen. Daher können die Details eines konkreten Leittechniksystems oder auch die zeitlichen Abläufe in der Praxis, beispielsweise bei der Vorgehensweise im Entwicklungsprozess, von dem hier zugrunde gelegten Lebenszyklus abweichen. Im Allgemeinen lässt sich die Matrix dennoch anwenden. Bei Erarbeitung der generischen Darstellung eines Leittechniksystems (siehe Abschnitt 6.2)

wurde ebenso wie bei der Definition der Diversitätsmerkmale (siehe Abschnitt 6.3) darauf geachtet, ein breites Spektrum an konkreten leittechnischen Systemen, Redundanzen von leittechnischen Systemen und Komponenten abzudecken. Daher ist zu erwarten, dass in der Praxis nur ein Teil der beschriebenen Bestandteile eines Leittechniksystems für das konkret betrachtete System oder die konkret betrachtete Komponente eine Rolle spielen. Ebenso ist es denkbar, dass nicht alle Diversitätsmerkmale auf das zu bewertende System zutreffen. In diesen Fällen fallen die nicht relevanten Zeilen und Spalten der Matrix der Diversitätsmerkmale weg.

In Tabelle 6.1 ist die Matrix der Diversitätsmerkmale vollständig dargestellt. Dies dient lediglich der groben Übersicht. In den folgenden Abschnitten werden jeweils Auszüge aus der Matrix der Diversitätsmerkmale dargestellt und näher beschrieben. Hierbei ist zu beachten, dass diese Matrizen die Bestandteile eines generischen Leittechniksystems als Zeilen und die Diversitätsmerkmale in den Spalten enthalten.

Tab. 6.1 Übersicht über die Matrix der Diversitätsmerkmale

		Diversitätsmerkmale																																															
		Beteiligtes Personal								Betrieb und Instandhaltung						Systemaufbau und Technologie																Herstellung und Entwicklung																	
		Personal bei Betrieb und Instandhaltung			Personal bei Herstellung und Entwicklung					Tests und Prüfungen				Hard- / Software-Management		Ankopplung an die Verfahrenstechnik				Logik				Eingesetzte Hardware				Eingesetzte Software				Tests		Entwicklung und Fertigung der Hardware						Softwareerstellung								Design	
Bestandteile eines generischen Leittechniksystems		Teams für die Durchführung von Wartung und Instandhaltung	Teams für die Durchführung von WKPs und anderen Prüfungen des LT-Systems nach Inbetriebnahme	Inbetriebnahmeteams	Validierungsteams	Implementierungsteams	Entwicklungs- / Designteams	Management des Entwicklungs- und Herstellungsprozesses	Teams zur Formulierung der Anforderungen	Instandhaltungszeitpunkte	Werkzeuge und Hilfsmittel bei der Instandhaltung	WKPs und andere Prüfungen des LT-Systems nach Inbetriebnahme	Tests bei Inbetriebnahme	Patchmanagement	Versionsmanagement	Mechanismen zur Einhaltung eines Schutzziels	Auslösemechanismus der Schutzaktion	Anregekriterien	Messprinzip	Überwachungsmethoden	Vorrangschaltung	Verarbeitungslogik	Verarbeitungsalgorithmus	Datenspeicherung	Rechnerarchitektur	Bauteile und Komponenten	Art der Baugruppen	Datenstrukturen	Programmstrukturen	System- und Anwendersoftware	Softwarearchitektur	Test bei Qualifizierung	Tests bei Fertigung / Entwicklung	Ort der Fertigung	Fertigungsprozess	Zulieferer	Hersteller einschließlich Unterauftragnehmer	Genutzte Software	Hardwareentwicklungsverfahren	Vorgefertigte Software	Hersteller einschließlich Unterauftragnehmer	Unterstützende Bibliotheken	Programmiersprachen	Softwarewerkzeuge	Programmierverfahren	Verfahren zur Softwareerstellung	System- und Anwendersoftware	Entwurfsspezifikationen	Anforderungsformulierungen
Eingabe	Sonden	X	X	X	X	X	X	X	X	X	X	X	X		X				X							X						X	X	X	X	X	X	X	X									X	X
	Messumformer ohne Softwarebestandteile	X	X	X	X	X	X	X	X	X	X	X	X		X					X		X	X			X	X					X	X	X	X	X	X	X	X									X	X
	Messumformer mit Softwarebestandteilen	X	X	X	X	X	X	X	X	X	X	X	X	X	X					X		X	X	X	X	X		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	Bedienelemente ohne Softwarebestandteile	X	X	X	X	X	X	X	X	X	X	X	X		X					X		X	X			X	X					X	X	X	X	X	X	X	X									X	X
	Bedienelemente mit Softwarebestandteilen	X	X	X	X	X	X	X	X	X	X	X	X	X	X					X		X	X	X	X	X		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Verarbeitung	nicht programmierbare Baugruppen ohne Softwarebestandteile	X	X	X	X	X	X	X	X	X	X	X	X		X					X	X	X	X			X	X					X	X	X	X	X	X	X	X									X	X
	nicht programmierbare Baugruppen mit Softwarebestandteilen (ggf. vom Anwender nicht veränderliche Firmware)	X	X	X	X	X	X	X	X	X	X	X	X	X	X					X	X	X	X			X		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	programmierbare Baugruppen	X	X	X	X	X	X	X	X	X	X	X	X	X	X					X	X	X	X	X		X		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	rechnerbasierte Baugruppen	X	X	X	X	X	X	X	X	X	X	X	X	X	X					X	X	X	X	X	X	X		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	Rechner	X	X	X	X	X	X	X	X	X	X	X	X	X	X					X	X	X	X	X	X	X		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Ausgabe	Koppelebene ohne Softwarebestandteile	X	X	X	X	X	X	X	X	X	X	X	X		X		X			X		X	X			X	X					X	X	X	X	X	X	X	X									X	X
	Koppelebene mit Softwarebestandteilen	X	X	X	X	X	X	X	X	X	X	X	X	X	X		X			X		X	X	X	X	X		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	Aktuatoren	X	X	X	X	X	X	X	X	X	X	X	X		X		X									X						X	X	X	X	X	X	X	X									X	X
	Anzeigen (einschließlich Meldeeinrichtungen) ohne Softwarebestandteile	X	X	X	X	X	X	X	X	X	X	X	X		X					X		X	X			X	X					X	X	X	X	X	X	X	X									X	X
	Anzeigen (einschließlich Meldeeinrichtungen) mit Softwarebestandteilen	X	X	X	X	X	X	X	X	X	X	X	X	X	X					X		X	X	X	X	X		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Stromversorgung	Kabel / Leitungen	X	X	X	X	X	X	X	X	X	X	X	X		X					X						X						X	X	X	X	X	X	X	X									X	X
	Einrichtungen der Stromversorgung (Gleich- und Wechselrichter, Batterien, Generatoren etc.) ohne Softwarebestandteile	X	X	X	X	X	X	X	X	X	X	X	X		X					X		X	X			X	X					X	X	X	X	X	X	X	X									X	X
	Einrichtungen der Stromversorgung mit Softwarebestandteilen	X	X	X	X	X	X	X	X	X	X	X	X	X	X					X		X	X	X	X	X		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Schutzeinrichtungen	Aggregateschutz ohne Softwarebestandteile	X	X	X	X	X	X	X	X	X	X	X	X		X		X		X	X	X	X	X			X	X					X	X	X	X	X	X	X	X									X	X
	Aggregateschutz mit Softwarebestandteilen	X	X	X	X	X	X	X	X	X	X	X	X	X	X		X		X	X	X	X	X	X	X	X		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	Sonstige Schutzeinrichtungen ohne Softwarebestandteile	X	X	X	X	X	X	X	X	X	X	X	X		X		X		X	X	X	X	X			X	X					X	X	X	X	X	X	X	X									X	X
	Sonstige Schutzeinrichtungen mit Softwarebestandteilen	X	X	X	X	X	X	X	X	X	X	X	X	X	X		X		X	X	X	X	X	X	X	X		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Kommunikation	Hardwaresysteme zur Realisierung des Datenflusses	X	X	X	X	X	X	X	X	X	X	X	X		X					X						X						X	X	X	X	X	X	X	X									X	X
	Protokoll		X	X	X	X	X	X	X			X	X	X	X					X	X	X	X					X	X	X	X	X	X							X	X	X	X	X	X	X	X	X	X
	Signalwandler ohne Softwarebestandteile (AD-Wandler etc.)	X	X	X	X	X	X	X	X	X	X	X	X		X					X		X	X			X	X					X	X	X	X	X	X	X	X									X	X
	Signalwandler mit Softwarebestandteilen (Gateways etc.)	X	X	X	X	X	X	X	X	X	X	X	X	X	X					X		X	X	X	X	X		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Zugriffsmöglichkeiten	Zugriffsmöglichkeiten ohne Softwarebestandteile	X	X	X	X	X	X	X	X	X	X	X	X		X					X	X	X	X			X	X					X	X	X	X	X	X	X	X									X	X
	Zugriffsmöglichkeiten mit Softwarebestandteilen (einschließlich Servicerechner)	X	X	X	X	X	X	X	X	X	X	X	X	X	X					X	X	X	X	X	X	X		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	Hardwaretechnische Umsetzung administrativer Zugriffsregeln	X	X	X	X	X	X	X	X	X	X	X	X		X					X		X	X			X	X					X	X	X	X	X	X	X	X									X	X
	Softwaretechnische Umsetzung administrativer Zugriffsregeln		X	X	X	X	X	X	X			X	X	X	X					X		X	X					X	X	X	X	X	X															X	X
Funktionsweise des Gesamtsystems			X	X	X	X	X	X	X			X	X			X	X	X				X	X																									X	X

6.3.1 Herstellung und Entwicklung

Im Bereich „Herstellung und Entwicklung“ muss bewertet werden, ob Entwicklung und Herstellung der zu prüfenden Leittechniksysteme, Teilsysteme oder Komponenten derartig unabhängig durchgeführt wurden, dass ein CCF nicht unterstellt werden muss. Dazu muss bewertet werden, ob in den im Folgenden aufgeführten Diversitätsmerkmalen Diversität vorliegt.

6.3.1.1 Design

Im Bereich des Designs (siehe auch Tabelle 6.2) werden folgende Diversitätsmerkmale betrachtet:

Anforderungsformulierungen
In den Anforderungsformulierungen werden die Anforderungen an die Baugruppe oder Komponente bzw. das Teilsystem oder System durch den Auftraggeber schriftlich formuliert. Für das Vorliegen von Diversität in diesem Merkmal muss der Designprozess auf Grundlage unterschiedlicher, unabhängig voneinander erarbeiteter Anforderungsformulierungen erfolgen.

Entwurfsspezifikationen
In den Entwurfsspezifikationen erfolgt die Umsetzung der Anforderungsformulierungen in unterschiedliche Spezifikationen zum Entwurf der Baugruppe oder Komponente bzw. des Teilsystems oder Systems auf Auftragnehmerseite. Für das Vorliegen von Diversität in diesem Merkmal muss der Designprozess auf Grundlage unterschiedlicher, unabhängig voneinander erarbeiteter Entwurfsspezifikationen erfolgen.

Tab. 6.2 Design – Matrix der Diversitätsmerkmale

		Anforderungsformulierungen	Entwurfsspezifikationen
Eingabe	Sonden	X	X
	Messumformer ohne Softwarebestandteile	X	X
	Messumformer mit Softwarebestandteilen	X	X
	Bedienelemente ohne Softwarebestandteile	X	X
	Bedienelemente mit Softwarebestandteilen	X	X
Verarbeitung	Nicht programmierbare Baugruppen ohne Softwarebestandteile	X	X
	Nicht programmierbare Baugruppen mit Softwarebestandteilen	X	X
	Programmierbare Baugruppen	X	X
	Rechnerbasierte Baugruppen	X	X
	Rechner	X	X
Ausgabe	Koppelebene ohne Softwarebestandteile	X	X
	Koppelebene mit Softwarebestandteilen	X	X
	Aktuatoren	X	X
	Anzeigen (einschl. Meldeeinrichtungen) ohne Softwarebestandteile	X	X
	Anzeigen (einschl. Meldeeinrichtungen) mit Softwarebestandteilen	X	X
Stromver-sorgung	Kabel/Leitungen	X	X
	Einrichtungen der Stromversorgung ohne Softwarebestandteile	X	X
	Einrichtungen der Stromversorgung mit Softwarebestandteilen	X	X
Schutzeinrich-tungen	Aggregateschutz ohne Softwarebestandteile	X	X
	Aggregateschutz mit Softwarebestandteilen	X	X
	Sonstige Schutzeinrichtungen ohne Softwarebestandteile	X	X
	Sonstige Schutzeinrichtungen mit Softwarebestandteilen	X	X
Kommu-nika-tion	Hardwaresysteme zur Realisierung des Datenflusses	X	X
	Protokoll	X	X
	Signalwandler ohne Softwarebestandteile	X	X
	Signalwandler mit Softwarebestandteilen	X	X
Zugriffsmög-lichkeiten	Zugriffsmöglichkeiten ohne Softwarebestandteile	X	X
	Zugriffsmöglichkeiten mit Softwarebestandteilen	X	X
	Hardwaretechnische Umsetzung administrativer Zugriffsregeln	X	X
	Softwaretechnische Umsetzung administrativer Zugriffsregeln	X	X
	Funktionsweise des Gesamtsystems	X	X

Anforderungsformulierungen und Entwurfsspezifikationen sind sehr grundlegend für den Design- und Entwicklungsprozess von Baugruppen, Komponenten und Systemen. Daher spielen Anforderungsformulierungen und Entwurfsspezifikationen bei der Beurteilung der Diversität immer eine wichtige Rolle, unabhängig davon, ob einzelne Baugruppen oder ganze leittechnische Systeme betrachtet werden. Daher sind diese beiden Diversitätsmerkmale bei allen Bestandteilen des in Abschnitt 6.2 eingeführten generischen Leittechniksystems mit Kreuzen gekennzeichnet.

6.3.1.2 Softwareerstellung

Im Bereich der Softwareerstellung (siehe auch Tabelle 6.3) werden folgende Diversitätsmerkmale betrachtet:

System- und Anwendungssoftware
System- und Anwendungssoftware schließt Betriebssysteme, systemnahe Software sowie den Teil der Software eines leittechnischen Systems ein, durch den Anwendungsfunktionen realisiert werden, wobei hier diejenige System- und Anwendungssoftware gemeint ist, die bei der Softwareerstellung zum Einsatz kommt. Für das Vorliegen von Diversität in diesem Merkmal muss beim Herstellungsprozess der Software grundlegend unterschiedliche Systemsoftware (z. B. Windows, UNIX etc.) sowie verschiedenartige Anwendungssoftware zum Einsatz kommen.

Vorgehensmodell oder Verfahren zur Softwareentwicklung
Ein Vorgehensmodell oder Verfahren zur Softwareentwicklung organisiert den Prozess der Softwareerstellung. Für das Vorliegen von Diversität in diesem Merkmal muss der Prozess der Softwareerstellung mit unterschiedlichen Verfahren erfolgen (z. B. V-Modell, Scrum, etc.).

Programmierverfahren
Ein Programmierverfahren ist das planmäßige Vorgehen zur Erzeugung von Anwendungsprogrammen. Für das Vorliegen von Diversität in diesem Merkmal müssen bei der Softwareerstellung verschiedenartige Programmierverfahren (z. B. maschinelle oder nichtmaschinelle Programmierverfahren) eingesetzt werden.

Softwarewerkzeuge
Softwarewerkzeuge sind Programme, die dazu dienen, den Softwareentwickler bei der Erstellung von Software zu unterstützen. Für das Vorliegen von Diversität in diesem

Merkmal dürfen bei der Softwareerstellung nur unterschiedliche Softwarewerkzeuge (z. B. Compiler, Codegeneratoren, Versionskontrollsysteme, etc.) zum Einsatz kommen.

Programmiersprachen

Eine Programmiersprache ist eine formale Sprache, die zur Kommunikation mit einer Maschine oder einem Rechner dient. Sie dient der Formulierung von Datenstrukturen und Algorithmen, die von einem Rechner ausgeführt werden können. Für das Vorliegen von Diversität in diesem Merkmal müssen bei der Softwareerstellung grundlegend unterschiedliche Programmiersprachen (z. B. objektorientiert oder nicht objektorientiert, anwendungsorientierte oder allgemeine Sprachen) verwendet werden.

Unterstützende Bibliotheken

Unter unterstützenden Bibliotheken wird eine systemeigene Sammlung von Software-Elementen verstanden, die mittels einer Referenzierung in andere Programme miteinbezogen werden können. Für das Vorliegen von Diversität in diesem Merkmal müssen sich im Zuge des Einsatzes unterschiedlicher Programmiersprachen auch alle bei der Softwareerstellung eingesetzten unterstützenden Bibliotheken unterscheiden.

Hersteller einschließlich Unterauftragnehmer

Hier wird neben dem Hersteller einer Software auch jeder von diesem beauftragte Unterauftragnehmer betrachtet. Für das Vorliegen von Diversität in diesem Merkmal muss die gesamte Erstellung der Software bei unterschiedlichen Herstellern erfolgen. Sofern eine Auslagerung der Codeerstellung an Unterauftragnehmer erfolgt, müssen voneinander unabhängige Firmen beauftragt werden.

Vorgefertigte Software

Vorgefertigte Software ist als kommerzielles oder gesetzlich geschütztes Produkt verfügbar, wobei sie für den Einsatz in einem rechnerbasierten System vorgesehen ist. Sofern vorgefertigte Softwarebestandteile verwendet werden, muss für das Vorliegen von Diversität in diesem Merkmal über den gesamten Prozess der Softwareerstellung hinweg die vorgefertigte Software von unterschiedlichen Herstellern bezogen werden. Insbesondere muss auch die vorgefertigte Software alle zutreffenden Diversitätsmerkmale erfüllen.

Tab. 6.3 Softwareerstellung – Matrix der Diversitätsmerkmale

		System- und Anwendungssoftware	Vorgehensmodell	Programmierverfahren	Softwarewerkzeuge	Programmiersprachen	Unterstützende Bibliotheken	Hersteller mit Unterauftragnehmer	Vorgefertigte Software
Eingabe	Sonden								
	Messumformer ohne Softwarebestandteile								
	Messumformer mit Softwarebestandteilen	X	X	X	X	X	X	X	X
	Bedienelemente ohne Softwarebestandteile								
	Bedienelemente mit Softwarebestandteilen	X	X	X	X	X	X	X	X
Verarbeitung	Nicht programmierbare Baugruppen ohne Softwarebestandteile								
	Nicht programmierbare Baugruppen mit Softwarebestandteilen	X	X	X	X	X	X	X	X
	Programmierbare Baugruppen	X	X	X	X	X	X	X	X
	Rechnerbasierte Baugruppen	X	X	X	X	X	X	X	X
	Rechner	X	X	X	X	X	X	X	X
Ausgabe	Koppelebene ohne Softwarebestandteile								
	Koppelebene mit Softwarebestandteilen	X	X	X	X	X	X	X	X
	Aktuatoren								
	Anzeigen (einschl. Meldeeinrichtungen) ohne Softwarebestandteile								
	Anzeigen (einschl. Meldeeinrichtungen) mit Softwarebestandteilen	X	X	X	X	X	X	X	X
Stromver-sorgung	Kabel/Leitungen								
	Einrichtungen der Stromversorgung ohne Softwarebestandteile								
	Einrichtungen der Stromversorgung mit Softwarebestandteilen	X	X	X	X	X	X	X	X
Schutzeinrich-tungen	Aggregateschutz ohne Softwarebestandteile								
	Aggregateschutz mit Softwarebestandteilen	X	X	X	X	X	X	X	X
	Sonstige Schutzeinrichtungen ohne Softwarebestandteile								
	Sonstige Schutzeinrichtungen mit Softwarebestandteilen	X	X	X	X	X	X	X	X
Kommu-nika-tion	Hardwaresysteme zur Realisierung des Datenflusses								
	Protokoll	X	X	X	X	X	X	X	X
	Signalwandler ohne Softwarebestandteile								
	Signalwandler mit Softwarebestandteilen	X	X	X	X	X	X	X	X
Zugriffsmög-lichkeiten	Zugriffsmöglichkeiten ohne Softwarebestandteile								
	Zugriffsmöglichkeiten mit Softwarebestandteilen	X	X	X	X	X	X	X	X
	Hardwaretechnische Umsetzung administrativer Zugriffsregeln								
	Softwaretechnische Umsetzung administrativer Zugriffsregeln								
	Funktionsweise des Gesamtsystems								

Alle Diversitätsmerkmale, die sich auf Softwareerstellung beziehen, sind immer dann relevant, wenn die zu betrachtenden Baugruppen und Komponenten Softwarebestandteile enthalten. Daher sind diese Diversitätsmerkmale bei allen Bestandteilen des in Abschnitt 6.2 eingeführten generischen Leittechniksystems, die Softwarebestandteile enthalten, mit Kreuzen gekennzeichnet.

6.3.1.3 Entwicklung und Fertigung der Hardware

Im Bereich Entwicklung und Fertigung der Hardware (siehe auch Tabelle 6.4) werden folgende Diversitätsmerkmale betrachtet:

Hardwareentwicklungsverfahren
Beim Entwicklungsprozess von Hardwarekomponenten eingesetzte Verfahren werden im Folgenden als Hardwareentwicklungsverfahren bezeichnet. Für das Vorliegen von Diversität in diesem Merkmal müssen im Rahmen des Design- und Entwicklungsprozesses der Hardware unterschiedliche Hardwareentwicklungsverfahren zum Einsatz kommen.

Genutzte Software
Software, die zur Unterstützung des Entwicklungs- und Fertigungsprozesses der Hardware zum Einsatz kommt, wird im Folgenden als genutzte Software bezeichnet. Für das Vorliegen von Diversität in diesem Merkmal muss im Rahmen des Design- und Entwicklungsprozesses der Hardware grundlegend unterschiedliche Software zum Einsatz kommen (z. B. unterschiedliche CAD-Programme).

Hersteller einschließlich Unterauftragnehmer
Hier wird neben dem Hersteller einer Hardware auch jeder von diesem beauftragte Unterauftragnehmer betrachtet. Für das Vorliegen von Diversität in diesem Merkmal muss der gesamte Fertigungsprozess bei unterschiedlichen Herstellern erfolgen. Sofern eine Auslagerung einzelner Fertigungsschritte an Unterauftragnehmer erfolgt, muss dies bei unterschiedlichen Firmen erfolgen.

Zulieferer
Hier werden sämtliche Zulieferer betrachtet, die während der Entwicklung und Fertigung der Hardware an den Hersteller oder von ihm beauftragte Unterauftragnehmer Hardwarekomponenten oder Materialen liefern. Für das Vorliegen von Diversität in diesem

Merkmal müssen über den gesamten Fertigungsprozess hinweg die benötigten Hardwarekomponenten und Materialien von unterschiedlichen Zulieferern bezogen werden.

Fertigungsprozess

Der Fertigungsprozess umfasst eine oder mehrere Methoden, mit denen durch die Bearbeitung von Materialien oder zugelieferten Komponenten das gewünschte Produkt hergestellt wird, wobei sämtliche Aspekte des Fertigungsprozesses einschließlich eingesetzter Maschinen und verwendeter Verfahren betrachtet werden. Für das Vorliegen von Diversität in diesem Merkmal muss sich die Fertigung der Hardware bzw. der Hardwarekomponenten grundlegend unterscheiden (z. B. hinsichtlich eingesetzter Maschinen, Verfahren, Programme zur Automatisierung etc.).

Ort der Fertigung

Hier werden insbesondere Eigenschaften des Orts oder der Orte, an dem die Hardware gefertigt wird, betrachtet, die einen Einfluss auf das dort gefertigte Produkt haben können. Für das Vorliegen von Diversität in diesem Merkmal muss die Fertigung der Hardware oder Hardwarekomponenten zur Vermeidung von Fehlfunktionen aufgrund identischer Umwelteinflüsse (z. B. Temperatur, Luftfeuchtigkeit, Partikel in der Luft) an unterschiedlichen Orten erfolgen.

Tab. 6.4 Entwicklung und Fertigung der Hardware – Matrix der Diversitätsmerkmale

		Hardwareentwicklungsverfahren	Genutzte Software	Hersteller mit Unterauftragnehmer	Zulieferer	Fertigungsprozess	Ort der Fertigung
Eingabe	Sonden	X	X	X	X	X	X
	Messumformer ohne Softwarebestandteile	X	X	X	X	X	X
	Messumformer mit Softwarebestandteilen	X	X	X	X	X	X
	Bedienelemente ohne Softwarebestandteile	X	X	X	X	X	X
	Bedienelemente mit Softwarebestandteilen	X	X	X	X	X	X
Verarbeitung	Nicht programmierbare Baugruppen ohne Softwarebestandteile	X	X	X	X	X	X
	Nicht programmierbare Baugruppen mit Softwarebestandteilen	X	X	X	X	X	X
	Programmierbare Baugruppen	X	X	X	X	X	X
	Rechnerbasierte Baugruppen	X	X	X	X	X	X
	Rechner	X	X	X	X	X	X
Ausgabe	Koppelebene ohne Softwarebestandteile	X	X	X	X	X	X
	Koppelebene mit Softwarebestandteilen	X	X	X	X	X	X
	Aktuatoren	X	X	X	X	X	X
	Anzeigen (einschl. Meldeeinrichtungen) ohne Softwarebestandteile	X	X	X	X	X	X
	Anzeigen (einschl. Meldeeinrichtungen) mit Softwarebestandteilen	X	X	X	X	X	X
Stromversorgung	Kabel/Leitungen	X	X	X	X	X	X
	Einrichtungen der Stromversorgung ohne Softwarebestandteile	X	X	X	X	X	X
	Einrichtungen der Stromversorgung mit Softwarebestandteilen	X	X	X	X	X	X
Schutzeinrichtungen	Aggregateschutz ohne Softwarebestandteile	X	X	X	X	X	X
	Aggregateschutz mit Softwarebestandteilen	X	X	X	X	X	X
	Sonstige Schutzeinrichtungen ohne Softwarebestandteile	X	X	X	X	X	X
	Sonstige Schutzeinrichtungen mit Softwarebestandteilen	X	X	X	X	X	X
Kommunikation	Hardwaresysteme zur Realisierung des Datenflusses	X	X	X	X	X	X
	Protokoll						
	Signalwandler ohne Softwarebestandteile	X	X	X	X	X	X
	Signalwandler mit Softwarebestandteilen	X	X	X	X	X	X
Zugriffsmöglichkeiten	Zugriffsmöglichkeiten ohne Softwarebestandteile	X	X	X	X	X	X
	Zugriffsmöglichkeiten mit Softwarebestandteilen	X	X	X	X	X	X
	Hardwaretechnische Umsetzung administrativer Zugriffsregeln	X	X	X	X	X	X
	Softwaretechnische Umsetzung administrativer Zugriffsregeln						
	Funktionsweise des Gesamtsystems						

Alle Diversitätsmerkmale, die sich auf Entwicklung und Fertigung der Hardware beziehen, sind immer dann relevant, wenn die zu betrachtenden Baugruppen und Komponenten Hardware enthalten. Daher sind diese Diversitätsmerkmale bei allen Bestandteilen des in Abschnitt 6.2 eingeführten generischen Leittechniksystems, die Hardware enthalten, mit Kreuzen gekennzeichnet.

6.3.1.4 Tests bei Herstellung und Entwicklung

Im Bereich der Tests bei Herstellung und Entwicklung (siehe auch Tabelle 6.5) werden folgende Diversitätsmerkmale betrachtet:

Tests bei Fertigung und Entwicklung
Während der Fertigung und Entwicklung der Hardware werden Tests durchgeführt. Für das Vorliegen von Diversität in diesem Merkmal dürfen im Rahmen der Fertigung und Entwicklung zur Vermeidung des Einbringens identischer Fehler keine identischen Tests zur Überprüfung einer Eigenschaft oder Funktionalität der zu vergleichenden Baugruppen, Komponenten, Teilsysteme oder Systeme eingesetzt werden.

Tests bei Qualifizierung
Im Rahmen der Qualifizierung der Hardware werden Tests durchgeführt. Für das Vorliegen von Diversität in diesem Merkmal dürfen im Rahmen der Qualifizierung zur Vermeidung des Einbringens identischer Fehler keine identischen Tests zur Überprüfung einer Eigenschaft oder Funktionalität der zu vergleichenden Baugruppen, Komponenten, Teilsysteme oder Systeme eingesetzt werden.

Tab. 6.5 Tests bei Herstellung und Entwicklung – Matrix der Diversitätsmerkmale

		Tests bei Fertigung/Entwicklung	Tests bei Qualifizierung
Eingabe	Sonden	X	X
	Messumformer ohne Softwarebestandteile	X	X
	Messumformer mit Softwarebestandteilen	X	X
	Bedienelemente ohne Softwarebestandteile	X	X
	Bedienelemente mit Softwarebestandteilen	X	X
Verarbeitung	Nicht programmierbare Baugruppen ohne Softwarebestandteile	X	X
	Nicht programmierbare Baugruppen mit Softwarebestandteilen	X	X
	Programmierbare Baugruppen	X	X
	Rechnerbasierte Baugruppen	X	X
	Rechner	X	X
Ausgabe	Koppelebene ohne Softwarebestandteile	X	X
	Koppelebene mit Softwarebestandteilen	X	X
	Aktuatoren	X	X
	Anzeigen (einschl. Meldeeinrichtungen) ohne Softwarebestandteile	X	X
	Anzeigen (einschl. Meldeeinrichtungen) mit Softwarebestandteilen	X	X
Stromver-sorgung	Kabel/Leitungen	X	X
	Einrichtungen der Stromversorgung ohne Softwarebestandteile	X	X
	Einrichtungen der Stromversorgung mit Softwarebestandteilen	X	X
Schutzeinrich-tungen	Aggregateschutz ohne Softwarebestandteile	X	X
	Aggregateschutz mit Softwarebestandteilen	X	X
	Sonstige Schutzeinrichtungen ohne Softwarebestandteile	X	X
	Sonstige Schutzeinrichtungen mit Softwarebestandteilen	X	X
Kommu-nika-tion	Hardwaresysteme zur Realisierung des Datenflusses	X	X
	Protokoll	X	X
	Signalwandler ohne Softwarebestandteile	X	X
	Signalwandler mit Softwarebestandteilen	X	X
Zugriffsmög-lichkeiten	Zugriffsmöglichkeiten ohne Softwarebestandteile	X	X
	Zugriffsmöglichkeiten mit Softwarebestandteilen	X	X
	Hardwaretechnische Umsetzung administrativer Zugriffsregeln	X	X
	Softwaretechnische Umsetzung administrativer Zugriffsregeln	X	X
	Funktionsweise des Gesamtsystems		

Tests bei Herstellung und Entwicklung werden bei allen Baugruppen und Komponenten während des Herstellungs- und Entwicklungsprozesses sowie im Rahmen der Qualifizierung durchgeführt. Daher spielen die Diversitätsmerkmale, die sich auf Tests bei Herstellung und Entwicklung beziehen, bei einzelnen Baugruppen und Komponenten immer eine wichtige Rolle. Aufgrund dessen sind diese Diversitätsmerkmale bei allen Bestandteilen des in Abschnitt 6.2 eingeführten generischen Leittechniksystems mit Kreuzen gekennzeichnet. Einzige Ausnahme bildet die Funktionsweise des Gesamtsystems, da diese erst nach Installation des Gesamtsystems bei Inbetriebnahme getestet wird.

6.3.2 Systemaufbau und Technologie

Im Bereich Systemaufbau und Technologie muss bewertet werden, ob die eingesetzte Software bzw. Hardware oder die Umsetzung der Funktion der Baugruppe, Komponente, des Teilsystems oder des Systems (Logik, Ankopplung an die Verfahrenstechnik) hinreichend diversitär ist, damit ein CCF nicht unterstellt werden muss. Dazu muss bewertet werden, ob in den im Folgenden aufgeführten Diversitätsmerkmalen Diversität vorliegt.

6.3.2.1 Eingesetzte Software

Im Bereich der eingesetzten Software (siehe auch Tabelle 6.6) werden folgende Diversitätsmerkmale betrachtet:

Softwarearchitektur

Die Softwarearchitektur definiert die Organisation der Softwarekomponenten und die zwischen diesen Softwarekomponenten bestehenden Schnittstellen. Für das Vorliegen von Diversität in diesem Merkmal müssen sich die Architekturen der eingesetzten Software, d. h. die Festlegung der grundlegenden Organisation und Interaktion der einzelnen Softwarekomponenten, unterscheiden.

System- und Anwendungssoftware

System- und Anwendungssoftware schließt Betriebssysteme, systemnahe Software sowie den Teil der Software eines leittechnischen Systems ein, durch den Anwendungsfunktionen realisiert werden, wobei hier diejenige System- und Anwendungssoftware gemeint ist, die zur Realisierung der Leittechnikfunktion zum Einsatz kommt. Für das Vorliegen von Diversität in diesem Merkmal muss zur Realisierung der Leittechnik-Funktion

grundlegend unterschiedliche Systemsoftware (z. B. Windows, UNIX etc.) sowie verschiedenartige Anwendungssoftware zum Einsatz kommen. Dies umfasst sowohl schon existierende Softwarebestandteile als auch vorgefertigte Software einschließlich entwickelter Modifikationen.

Programmstrukturen

Als Programmstruktur wird das logische Layout des erstellten Programms bezeichnet. Für das Vorliegen von Diversität in diesem Merkmal müssen sich die erstellten Programme hinsichtlich ihrer Struktur unterscheiden (z. B. Umsetzung einer gleichartigen Aufgabenstellung mittels unterschiedlicher Befehle, unterschiedliche Implementierung).

Datenstrukturen

Als Datenstruktur werden die logischen Beziehungen zwischen verschiedenen Datenelementen bezeichnet. Für das Vorliegen von Diversität in diesem Merkmal müssen sich die erstellten Programme hinsichtlich der Speicherung und Organisation der verwendeten Daten unterscheiden (z. B. Variablentypen, Prinzip der Stapelspeicherung).

Tab. 6.6 Eingesetzte Software – Matrix der Diversitätsmerkmale

		Softwarearchitektur	System- und Anwendungssoftware	Programmstrukturen	Datenstrukturen
Eingabe	Sonden				
	Messumformer ohne Softwarebestandteile				
	Messumformer mit Softwarebestandteilen	X	X	X	X
	Bedienelemente ohne Softwarebestandteile				
	Bedienelemente mit Softwarebestandteilen	X	X	X	X
Verarbeitung	Nicht programmierbare Baugruppen ohne Softwarebestandteile				
	Nicht programmierbare Baugruppen mit Softwarebestandteilen	X	X	X	X
	Programmierbare Baugruppen	X	X	X	X
	Rechnerbasierte Baugruppen	X	X	X	X
	Rechner	X	X	X	X
Ausgabe	Koppelebene ohne Softwarebestandteile				
	Koppelebene mit Softwarebestandteilen	X	X	X	X
	Aktuatoren				
	Anzeigen (einschl. Meldeeinrichtungen) ohne Softwarebestandteile				
	Anzeigen (einschl. Meldeeinrichtungen) mit Softwarebestandteilen	X	X	X	X
Stromver-sorgung	Kabel/Leitungen				
	Einrichtungen der Stromversorgung ohne Softwarebestandteile				
	Einrichtungen der Stromversorgung mit Softwarebestandteilen	X	X	X	X
Schutzeinrich-tungen	Aggregateschutz ohne Softwarebestandteile				
	Aggregateschutz mit Softwarebestandteilen	X	X	X	X
	Sonstige Schutzeinrichtungen ohne Softwarebestandteile				
	Sonstige Schutzeinrichtungen mit Softwarebestandteilen	X	X	X	X
Kommu-nika-tion	Hardwaresysteme zur Realisierung des Datenflusses				
	Protokoll	X	X	X	X
	Signalwandler ohne Softwarebestandteile				
	Signalwandler mit Softwarebestandteilen	X	X	X	X
Zugriffsmög-lichkeiten	Zugriffsmöglichkeiten ohne Softwarebestandteile				
	Zugriffsmöglichkeiten mit Softwarebestandteilen	X	X	X	X
	Hardwaretechnische Umsetzung administrativer Zugriffsregeln				
	Softwaretechnische Umsetzung administrativer Zugriffsregeln	X	X	X	X
	Funktionsweise des Gesamtsystems				

Alle Diversitätsmerkmale, die sich auf die eingesetzte Software beziehen, sind immer dann relevant, wenn die zu betrachtenden Baugruppen und Komponenten Softwarebestandteile enthalten. Daher sind diese Diversitätsmerkmale bei allen Bestandteilen des in Abschnitt 6.2 eingeführten generischen Leittechniksystems, die Softwarebestandteile enthalten, mit Kreuzen gekennzeichnet.

6.3.2.2 Eingesetzte Hardware

Im Bereich der eingesetzten Hardware (siehe auch Tabelle 6.7) werden folgende Diversitätsmerkmale betrachtet:

Art der Baugruppen

Neben Baugruppen, die ausschließlich nichtprogrammierbare Bauelemente enthalten, werden auch Baugruppen, die programmierbare oder rechnerbasierte Bauelemente enthalten, eingesetzt. Für das Vorliegen von Diversität in diesem Merkmal müssen sich die eingesetzten Komponenten und Baugruppen hinsichtlich ihrer Basistechnologie (z. B. nicht programmierbar vs. programmierbar) unterscheiden. Aus diesem Grund handelt es sich bei dem Diversitätsmerkmal Art der Baugruppen um einen Sonderfall. Das Vorliegen von Diversität kann beispielsweise durch den Einsatz einer nichtprogrammierbaren und einer rechnerbasierten Baugruppe erreicht werden. Umgekehrt ist es beispielsweise nicht möglich Diversität in der Art der Baugruppe zu erhalten, wenn beide betrachteten Baugruppen nicht programmierbar und ohne Softwarebestandteile sind. Daher wird für dieses Merkmal beim generischen Leittechniksystem auf die Unterscheidung von Komponenten mit und ohne Softwarebestandteile verzichtet. Dieses ist in der Matrix dadurch gekennzeichnet, dass die entsprechenden Zellen zusammengefasst wurden.

Bauteile und Komponenten

Hier werden die Bauteile und Komponenten der eingesetzten Hardware betrachtet. Für das Vorliegen von Diversität in diesem Merkmal muss sich die eingesetzte Hardware hinsichtlich ihrer Bauteile und Komponenten grundlegend unterscheiden (z. B. Glasfaserkabel oder Kupferkabel, Leittechnikkarten mit unterschiedlichen Bauelementen).

Rechnerarchitektur

Die Rechnerarchitektur bezeichnet die organisatorische Struktur von Rechnern sowie deren internen Aufbau. Dies schließt hier insbesondere das Design des Prozessors bzw. Prozessorkerns ein. Für das Vorliegen von Diversität in diesem Merkmal müssen die Rechnerarchitekturen einschließlich der Prozessor- oder Mikroprozessorarchitekturen

der eingesetzten rechnerbasierten Komponenten und Baugruppen unterschiedlich sein (z. B. AMD64, Intel x86, Motorola 68000).

Datenspeicherung

Die Speicherung von Daten kann auf unterschiedlichen Speichermedien erfolgen. Für das Vorliegen von Diversität in diesem Merkmal muss die Speicherung der verwendeten Daten bei den eingesetzten rechnerbasierten oder programmierbaren Komponenten und Baugruppen auf unterschiedlichen Speichermedien erfolgen (z. B. RAM, Flash, EPROM).

Tab. 6.7 Eingesetzte Hardware – Matrix der Diversitätsmerkmale

		Art der Baugruppen	Bauteile und Komponenten	Rechnerarchitektur	Datenspeicherung
Eingabe	Sonden		X		
	Messumformer ohne Softwarebestandteile	X	X		
	Messumformer mit Softwarebestandteilen		X	X	X
	Bedienelemente ohne Softwarebestandteile	X	X		
	Bedienelemente mit Softwarebestandteilen		X	X	X
Verarbeitung	Nicht programmierbare Baugruppen ohne Softwarebestandteile	X	X		
	Nicht programmierbare Baugruppen mit Softwarebestandteilen		X		
	Programmierbare Baugruppen		X		X
	Rechnerbasierte Baugruppen		X	X	X
	Rechner		X	X	X
Ausgabe	Koppelebene ohne Softwarebestandteile	X	X		
	Koppelebene mit Softwarebestandteilen		X	X	X
	Aktuatoren		X		
	Anzeigen (einschl. Meldeeinrichtungen) ohne Softwarebestandteile	X	X		
	Anzeigen (einschl. Meldeeinrichtungen) mit Softwarebestandteilen		X	X	X
Stromver-sorgung	Kabel/Leitungen		X		
	Einrichtungen der Stromversorgung ohne Softwarebestandteile	X	X		
	Einrichtungen der Stromversorgung mit Softwarebestandteilen		X	X	X
Schutzeinrich-tungen	Aggregateschutz ohne Softwarebestandteile	X	X		
	Aggregateschutz mit Softwarebestandteilen		X	X	X
	Sonstige Schutzeinrichtungen ohne Softwarebestandteile	X	X		
	Sonstige Schutzeinrichtungen mit Softwarebestandteilen		X	X	X
Kommu-nika-tion	Hardwaresysteme zur Realisierung des Datenflusses		X		
	Protokoll				
	Signalwandler ohne Softwarebestandteile	X	X		
	Signalwandler mit Softwarebestandteilen		X	X	X
Zugriffsmög-lichkeiten	Zugriffsmöglichkeiten ohne Softwarebestandteile	X	X		
	Zugriffsmöglichkeiten mit Softwarebestandteilen		X	X	X
	Hardwaretechnische Umsetzung administrativer Zugriffsregeln	X	X		
	Softwaretechnische Umsetzung administrativer Zugriffsregeln				
	Funktionsweise des Gesamtsystems				

Das Diversitätsmerkmal Art der Baugruppen ist immer dann relevant, wenn die Möglichkeit besteht, verschiedene Arten von Baugruppen einzusetzen (z. B. Baugruppen mit oder ohne Softwarebestandteile). Daher sind alle Bestandteile des in Abschnitt 6.2 eingeführten generischen Leittechniksystems, bei denen eine solche Auswahlmöglichkeit besteht, mit Kreuzen gekennzeichnet. Dabei werden die Baugruppen, zwischen denen ausgewählt werden kann, wie oben beschrieben zusammengefasst.

Das Diversitätsmerkmal Bauteile und Komponenten ist immer dann relevant, wenn die zu betrachtenden Baugruppen und Komponenten Hardware enthalten. Daher ist dieses Diversitätsmerkmal bei allen Bestandteilen des generischen Leittechniksystems, die Hardware enthalten, mit Kreuzen gekennzeichnet.

Das Diversitätsmerkmal Rechnerarchitektur ist für alle Rechner sowie rechnerbasierten Baugruppen und Komponenten relevant. Daher ist dieses Diversitätsmerkmal bei allen Bestandteilen des generischen Leittechniksystems, die mindestens einen Mikroprozessor oder Prozessor enthalten können, mit Kreuzen gekennzeichnet.

Das Diversitätsmerkmal Datenspeicherung ist immer dann relevant, wenn die zu betrachtenden Baugruppen und Komponenten Speichermedien enthalten. Daher ist dieses Diversitätsmerkmal bei allen Bestandteilen des generischen Leittechniksystems, die Speichermedien enthalten können, mit Kreuzen gekennzeichnet.

6.3.2.3 Logik

Im Bereich der Logik (siehe auch Tabelle 6.8) werden folgende Diversitätsmerkmale betrachtet:

Verarbeitungsalgorithmus
Mit Verarbeitungsalgorithmus ist hier die Sequenz von eindeutigen Handlungsvorschriften gemeint, die nacheinander angewendet oder ausgeführt werden müssen, um ein gegebenes Problem in einer endlichen Anzahl von Schritten zu lösen. Für das Vorliegen von Diversität in diesem Merkmal müssen bei der Umsetzung der Anforderungsformulierungen unabhängig von der Realisierung mittels Hard- und Software hinreichend unterschiedliche Verarbeitungsalgorithmen zu Grunde gelegt werden.

Verarbeitungslogik

Unter Verarbeitungslogik wird hier die zur Implementierung des Verarbeitungsalgorithmus verwendete Sequenz von Rechenvorschriften und logischen Operationen verstanden. Diese zur Implementierung des Verarbeitungsalgorithmus verwendete Verarbeitungslogik darf nicht identisch sein. Für das Vorliegen von Diversität in diesem Merkmal muss sich die Umsetzung des Verarbeitungsalgorithmus durch die Verarbeitungslogik unterscheiden (z. B. unterschiedliche logische Operationen oder Logikbausteine).

Vorrangschaltung

Unter Vorrangschaltung versteht man die leittechnische Realisierung der Priorisierung von Signalen. Die hardware- bzw. softwaretechnische Umsetzung bei der Priorisierung von Signalen und Befehlen muss unterschiedlich sein. Für das Vorliegen von Diversität in diesem Merkmal müssen zur Realisierung einer geforderten Vorrangschaltung unterschiedliche Baugruppen, Komponenten, Teilsysteme oder Systeme mit ggf. unterschiedlicher Programmierung zum Einsatz kommen.

Überwachungsmethoden

Im Rahmen der Fehlererkennung bzw. Sicherstellung der korrekten Funktionsweise einer Baugruppe oder Komponente bzw. eines Teilsystems oder Systems eingesetzte Methoden zur Überwachung oder Selbstüberwachung werden im Folgenden als Überwachungsmethoden bezeichnet. Für das Vorliegen von Diversität in diesem Merkmal müssen grundlegend unterschiedliche Möglichkeiten zur Überwachung oder Selbstüberwachung genutzt und unterschiedliche Komponenten dafür eingesetzt werden (z. B. verschiedene Arten von Watchdogs).

Tab. 6.8 Logik – Matrix der Diversitätsmerkmale

		Verarbeitungsalgorithmus	Verarbeitungslogik	Vorrangschaltung	Überwachungsmethoden
Eingabe	Sonden				
	Messumformer ohne Softwarebestandteile	X	X		X
	Messumformer mit Softwarebestandteilen	X	X		X
	Bedienelemente ohne Softwarebestandteile	X	X		X
	Bedienelemente mit Softwarebestandteilen	X	X		X
Verarbeitung	Nicht programmierbare Baugruppen ohne Softwarebestandteile	X	X	X	X
	Nicht programmierbare Baugruppen mit Softwarebestandteilen	X	X	X	X
	Programmierbare Baugruppen	X	X	X	X
	Rechnerbasierte Baugruppen	X	X	X	X
	Rechner	X	X	X	X
Ausgabe	Koppelebene ohne Softwarebestandteile	X	X		X
	Koppelebene mit Softwarebestandteilen	X	X		X
	Aktuatoren				X
	Anzeigen (einschl. Meldeeinrichtungen) ohne Softwarebestandteile	X	X		X
	Anzeigen (einschl. Meldeeinrichtungen) mit Softwarebestandteilen	X	X		X
Stromver-sorgung	Kabel/Leitungen				X
	Einrichtungen der Stromversorgung ohne Softwarebestandteile	X	X		X
	Einrichtungen der Stromversorgung mit Softwarebestandteilen	X	X		X
Schutzeinrich-tungen	Aggregateschutz ohne Softwarebestandteile	X	X	X	X
	Aggregateschutz mit Softwarebestandteilen	X	X	X	X
	Sonstige Schutzeinrichtungen ohne Softwarebestandteile	X	X	X	X
	Sonstige Schutzeinrichtungen mit Softwarebestandteilen	X	X	X	X
Kommu-nika-tion	Hardwaresysteme zur Realisierung des Datenflusses				X
	Protokoll	X	X	X	X
	Signalwandler ohne Softwarebestandteile	X	X		X
	Signalwandler mit Softwarebestandteilen	X	X		X
Zugriffsmög-lichkeiten	Zugriffsmöglichkeiten ohne Softwarebestandteile	X	X	X	X
	Zugriffsmöglichkeiten mit Softwarebestandteilen	X	X	X	X
	Hardwaretechnische Umsetzung administrativer Zugriffsregeln	X	X		X
	Softwaretechnische Umsetzung administrativer Zugriffsregeln	X	X		X
	Funktionsweise des Gesamtsystems	X	X		

Die Diversitätsmerkmale Verarbeitungsalgorithmus und Verarbeitungslogik sind immer dann relevant, wenn Informationen verarbeitet werden. Das ist mit wenigen Ausnahmen in allen Baugruppen, Komponenten und Systemen der Fall. Ausnahmen sind Sonden (Messung von Anlagenparametern, die Verarbeitung erfolgt im Messumformer), Aktuatoren (Beeinflussung von Anlagenparametern, Ansteuerung erfolgt über Koppelebene) sowie Kabel oder Leitungen und Hardwaresysteme zur Realisierung des Datenflusses (reine Hardware). Daher sind diese beiden Diversitätsmerkmale bei allen Bestandteilen des in Abschnitt 6.2 eingeführten generischen Leittechniksystems mit Ausnahme von Sonden, Aktuatoren, Kabel oder Leitungen und Hardwaresystemen zur Realisierung des Datenflusses mit Kreuzen gekennzeichnet.

Das Diversitätsmerkmal Vorrangschaltung ist in allen Bereichen relevant, in denen eine Priorisierung von Signalen vorgenommen werden kann Dies ist bei allen Baugruppen und Komponenten der Fall, die für die Realisierung einer Vorrangschaltung eingesetzt werden können. Diese Baugruppentypen sind hier im Bereich Verarbeitung mit erfasst. Außerdem ist dies bei allen Schutzeinrichtungen der Fall, da auch hier zum Schutz von Aggregaten bzw. der Anlage eine Priorisierung implementiert werden kann. Des Weiteren besteht die Möglichkeit einer Priorisierung im Protokoll, indem z. B. einzelne Sender einen Vorrang vor anderen Sendern haben. Außerdem können durch die Zugriffsmöglichkeiten Aktionen mit Priorität ausgelöst werden. Daher ist das Diversitätsmerkmal Vorrangschaltung bei allen genannten Bestandteilen des generischen Leittechniksystems mit Kreuzen gekennzeichnet.

Das Diversitätsmerkmal Überwachungsmethoden ist immer dann relevant, wenn die Funktion der zu betrachtenden Baugruppen und Komponenten überwacht werden kann. Daher ist dieses Diversitätsmerkmal bei allen Bestandteilen des generischen Leittechniksystems mit Ausnahme der Sonden, die nicht gesondert überwacht werden (Überwachung erfolgt mittels Überwachung der Messumformer), mit Kreuzen gekennzeichnet.

6.3.2.4 Ankopplung an die Verfahrenstechnik

Im Bereich der Ankopplung an die Verfahrenstechnik (siehe auch Tabelle 6.9) werden folgende Diversitätsmerkmale betrachtet:

Messprinzip

Unter Messprinzip versteht man das physikalische Prinzip einer Messung. Für das Vor-

liegen von Diversität in diesem Merkmal muss derselbe Anlagenparameter mit unterschiedlichen Messprinzipien erfasst werden, d. h. die Messung muss auf unterschiedlichen physikalischen Prinzipien basieren (z. B. Messung der Fördermenge der Pumpe mittels Druckdifferenz oder Drehzahl).

Anregekriterien

Unter einem Anregekriterium versteht man die Bedingung, unter der eine Schutzaktion ausgelöst wird /KTA14b/. Für das Vorliegen von Diversität in diesem Merkmal müssen für die Auslösung einer Schutzaktion unterschiedliche Anregekriterien herangezogen werden, die aus physikalisch unterschiedlichen Prozessvariablen gebildet werden.

Auslösemechanismus der Schutzaktion

In diesem Zusammenhang werden hierunter neben den Mechanismen, die eine Schutzaktion auslösen (z. B. Auslösung einer RESA durch unterschiedliche Mechanismen) auch technische Realisierungen verstanden, wie die für die Schutzaktion notwendigen Komponenten angesteuert werden (z. B. Arbeits- und Ruhestrom, Pneumatik etc.). Für das Vorliegen von Diversität in diesem Merkmal müssen die Auslösemechanismen für eine Schutzaktion in ihrer Funktionsweise unterschiedlich und unabhängig voneinander sein.

Mechanismen zur Einhaltung eines Schutzziels

Unter Mechanismen zur Einhaltung eines Schutzziels werden hier Schutzaktionen und weitere Maßnahmen verstanden, die erfolgen, um die Anlage in einem sicheren Zustand zu halten und der Einhaltung eines Schutzziels dienen. Für das Vorliegen von Diversität in diesem Merkmal müssen unterschiedliche und in ihrer Funktionsweise voneinander unabhängige Mechanismen zur Einhaltung eines Schutzziels eingesetzt werden (z. B. Einhaltung des Schutzziels Unterkritikalität durch Steuerstäbe oder Aufborieren).

Tab. 6.9 Ankopplung an die Verfahrenstechnik – Matrix der Diversitätsmerkmale

		Messprinzip	Anregekriterien	Auslösemechanismus der Schutzaktion	Mechanismen zur Einhaltung eines Schutzziels
Eingabe	Sonden	X			
	Messumformer ohne Softwarebestandteile				
	Messumformer mit Softwarebestandteilen				
	Bedienelemente ohne Softwarebestandteile				
	Bedienelemente mit Softwarebestandteilen				
Verarbeitung	Nicht programmierbare Baugruppen ohne Softwarebestandteile				
	Nicht programmierbare Baugruppen mit Softwarebestandteilen				
	Programmierbare Baugruppen				
	Rechnerbasierte Baugruppen				
	Rechner				
Ausgabe	Koppelebene ohne Softwarebestandteile			X	
	Koppelebene mit Softwarebestandteilen			X	
	Aktuatoren			X	
	Anzeigen (einschl. Meldeeinrichtungen) ohne Softwarebestandteile				
	Anzeigen (einschl. Meldeeinrichtungen) mit Softwarebestandteilen				
Stromversorgung	Kabel/Leitungen				
	Einrichtungen der Stromversorgung ohne Softwarebestandteile				
	Einrichtungen der Stromversorgung mit Softwarebestandteilen				
Schutzeinrichtungen	Aggregateschutz ohne Softwarebestandteile	X		X	
	Aggregateschutz mit Softwarebestandteilen	X		X	
	Sonstige Schutzeinrichtungen ohne Softwarebestandteile	X		X	
	Sonstige Schutzeinrichtungen mit Softwarebestandteilen	X		X	
Kommunikation	Hardwaresysteme zur Realisierung des Datenflusses				
	Protokoll				
	Signalwandler ohne Softwarebestandteile				
	Signalwandler mit Softwarebestandteilen				
Zugriffsmöglichkeiten	Zugriffsmöglichkeiten ohne Softwarebestandteile				
	Zugriffsmöglichkeiten mit Softwarebestandteilen				
	Hardwaretechnische Umsetzung administrativer Zugriffsregeln				
	Softwaretechnische Umsetzung administrativer Zugriffsregeln				
	Funktionsweise des Gesamtsystems		X	X	X

Das Diversitätsmerkmal Messprinzip ist immer dann relevant, wenn die zu betrachtenden Baugruppen und Komponenten Anlagenparameter erfassen können. Das ist bei den Sonden und allen Schutzeinrichtungen der Fall. Daher ist dieses Diversitätsmerkmal bei den Sonden und den Schutzeinrichtungen des in Abschnitt 6.2 eingeführten generischen Leittechniksystems mit Kreuzen gekennzeichnet.

Das Diversitätsmerkmal Anregekriterien ist immer dann relevant, wenn es um die Bedingungen geht, unter denen eine Schutzaktion ausgelöst wird. Dies ist insbesondere bei der Funktionsweise des Gesamtsystems der Fall.

Das Diversitätsmerkmal Auslösemechanismus der Schutzaktion ist für die Bestandteile eines Leittechniksystems relevant, bei denen es um die technische Realisierung der Auslösung einer Schutzaktion oder die dafür benötigten Komponenten geht. Daher ist es für die Koppelebene und Aktuatoren, den Aggregateschutz und weitere Schutzeinrichtungen sowie die Funktionsweise des Gesamtsystems relevant. Aufgrund dessen ist dieses Diversitätsmerkmal bei den genannten Bestandteilen des generischen Leittechniksystems mit Kreuzen gekennzeichnet.

Das Diversitätsmerkmal Mechanismen zur Einhaltung eines Schutzziels ist insbesondere für die Konzeptionierung des Gesamtsystems relevant, daher ist dieses Diversitätsmerkmal nur bei der Funktionsweise des Gesamtsystems mit einem Kreuz gekennzeichnet.

6.3.3 Betrieb und Instandhaltung

Im Bereich Betrieb und Instandhaltung muss bewertet werden, ob das Hard- und Softwaremanagement sowie die Tests und Prüfungen während des Betriebs hinreichend diversitär sind, damit ein CCF nicht unterstellt werden muss. Dazu muss bewertet werden, ob in den im Folgenden aufgeführten Diversitätsmerkmalen Diversität vorliegt.

6.3.3.1 Hard- und Softwaremanagement

Im Bereich des Hard- und Softwaremanagements (siehe auch Tabelle 6.10) werden folgende Diversitätsmerkmale betrachtet:

Versionsmanagement

Das Versionsmanagement (bezieht sich hier ausschließlich auf die Hardware) regelt, wie mit Bauteilen oder Komponenten umgegangen wird, die aufgrund von Änderungen, Korrekturen oder Verbesserungen in neuen Versionen vorliegen. Dies schließt unter anderem auch die Festlegung von möglichen Zeitpunkten für Inbetriebnahme oder Austausch beispielsweise in verschiedenen Systemen, Teilsystemen und Redundanzen sowie die durchzuführenden Tests ein. Für das Vorliegen von Diversität in diesem Merkmal müssen deutliche Unterschiede in der Behandlung innerhalb des Versionsmanagements bestehen (z. B. bei Inbetriebnahme oder beim Austausch von Komponenten und Bauteilen, der vorab durchzuführenden Prüfungen, der möglichen Zeitpunkte für die Inbetriebnahme bzw. den Austausch etc.).

Patchmanagement

Das Patchmanagement regelt den Umgang mit Patches und Updates für Softwarebestandteile von Systemen oder Komponenten. Dies schließt unter anderem auch die Festlegung von möglichen Zeitpunkten für das Aufspielen von Updates oder Patches sowie durchzuführende Tests ein. Für das Vorliegen von Diversität in diesem Merkmal müssen deutliche Unterschiede in der Behandlung innerhalb des Patchmanagements bestehen (z. B. hinsichtlich des Umgangs mit Updates und Patches, der vorab durchzuführenden Prüfungen, der möglichen Zeitpunkte für das Aufspielen von Updates und Patches etc.).

Tab. 6.10 Hard- und Softwaremanagement – Matrix der Diversitätsmerkmale

		Versionsmanagement	Patchmanagement
Eingabe	Sonden	X	
	Messumformer ohne Softwarebestandteile	X	
	Messumformer mit Softwarebestandteilen	X	X
	Bedienelemente ohne Softwarebestandteile	X	
	Bedienelemente mit Softwarebestandteilen	X	X
Verarbeitung	Nicht programmierbare Baugruppen ohne Softwarebestandteile	X	
	Nicht programmierbare Baugruppen mit Softwarebestandteilen	X	X
	Programmierbare Baugruppen	X	X
	Rechnerbasierte Baugruppen	X	X
	Rechner	X	X
Ausgabe	Koppelebene ohne Softwarebestandteile	X	
	Koppelebene mit Softwarebestandteilen	X	X
	Aktuatoren	X	
	Anzeigen (einschl. Meldeeinrichtungen) ohne Softwarebestandteile	X	
	Anzeigen (einschl. Meldeeinrichtungen) mit Softwarebestandteilen	X	X
Stromver-sorgung	Kabel/Leitungen	X	
	Einrichtungen der Stromversorgung ohne Softwarebestandteile	X	
	Einrichtungen der Stromversorgung mit Softwarebestandteilen	X	X
Schutzeinrich-tungen	Aggregateschutz ohne Softwarebestandteile	X	
	Aggregateschutz mit Softwarebestandteilen	X	X
	Sonstige Schutzeinrichtungen ohne Softwarebestandteile	X	
	Sonstige Schutzeinrichtungen mit Softwarebestandteilen	X	X
Kommu-nika-tion	Hardwaresysteme zur Realisierung des Datenflusses	X	
	Protokoll	X	X
	Signalwandler ohne Softwarebestandteile	X	
	Signalwandler mit Softwarebestandteilen	X	X
Zugriffsmög-lichkeiten	Zugriffsmöglichkeiten ohne Softwarebestandteile	X	
	Zugriffsmöglichkeiten mit Softwarebestandteilen	X	X
	Hardwaretechnische Umsetzung administrativer Zugriffsregeln	X	
	Softwaretechnische Umsetzung administrativer Zugriffsregeln	X	X
	Funktionsweise des Gesamtsystems		

Da es für alle Baugruppen und Komponenten ein Versionsmanagement gibt, ist das Diversitätsmerkmal Versionsmanagement bei allen Baugruppen und Komponenten relevant. Daher ist dieses Diversitätsmerkmal bei allen Bestandteilen des in Abschnitt 6.2 eingeführten generischen Leittechniksystems mit Kreuzen gekennzeichnet.

Das Diversitätsmerkmal Patchmanagement ist immer dann relevant, wenn die Baugruppen oder Komponenten Software enthalten. Daher ist dieses Diversitätsmerkmal bei allen Bestandteilen des generischen Leittechniksystems, die Software enthalten, mit Kreuzen gekennzeichnet.

6.3.3.2 Tests, Prüfungen und Instandhaltung

Im Bereich von Tests, Prüfungen und Instandhaltung (siehe auch Tabelle 6.11) werden folgende Diversitätsmerkmale betrachtet:

Tests bei Inbetriebnahme
Im Rahmen der Inbetriebnahme werden Tests durchgeführt. Für das Vorliegen von Diversität in diesem Merkmal müssen bei der Inbetriebnahme zur Vermeidung des Einbringens identischer Fehler hinsichtlich ihres Zeitpunkts und Prüfgeräts unterschiedliche Tests zum Nachweis der korrekten Arbeitsweise und der Erfüllung der geforderten Aufgabenstellung durchgeführt werden.

WKPs und andere Prüfungen des LT-Systems nach Inbetriebnahme
Nach der Inbetriebnahme werden wiederkehrende Prüfungen (WKPs) und andere Prüfungen durchgeführt. Für das Vorliegen von Diversität in diesem Merkmal müssen sich die WKPs und andere Prüfungen zur Sicherstellung der korrekten Arbeitsweise nach Inbetriebnahme zur Vermeidung des Einbringens identischer Fehler hinsichtlich ihres Zeitpunkts und Prüfgeräts unterscheiden.

Werkzeuge und Hilfsmittel bei der Instandhaltung
Für das Vorliegen von Diversität in diesem Merkmal müssen zur Vermeidung des Einbringens identischer Fehler unterschiedliche Werkzeuge und Hilfsmittel bei der Durchführung der Instandhaltung eingesetzt werden.

Instandhaltungszeitpunkte
Hierbei geht es um die Zeitpunkte, zu denen Instandhaltungsmaßnahmen durchgeführt

werden. Für das Vorliegen von Diversität in diesem Merkmal muss die Instandhaltung generell zu unterschiedlichen Zeitpunkten erfolgen.

Tab. 6.11 Tests und Prüfungen – Matrix der Diversitätsmerkmale

		Tests bei Inbetriebnahme	WKPs und andere Prüfungen des LT-Systems nach Inbetriebnahme	Werkzeuge und Hilfsmittel bei der Instandhaltung	Instandhaltungszeitpunkte
Eingabe	Sonden	X	X	X	X
	Messumformer ohne Softwarebestandteile	X	X	X	X
	Messumformer mit Softwarebestandteilen	X	X	X	X
	Bedienelemente ohne Softwarebestandteile	X	X	X	X
	Bedienelemente mit Softwarebestandteilen	X	X	X	X
Verarbeitung	Nicht programmierbare Baugruppen ohne Softwarebestandteile	X	X	X	X
	Nicht programmierbare Baugruppen mit Softwarebestandteilen	X	X	X	X
	Programmierbare Baugruppen	X	X	X	X
	Rechnerbasierte Baugruppen	X	X	X	X
	Rechner	X	X	X	X
Ausgabe	Koppelebene ohne Softwarebestandteile	X	X	X	X
	Koppelebene mit Softwarebestandteilen	X	X	X	X
	Aktuatoren	X	X	X	X
	Anzeigen (einschl. Meldeeinrichtungen) ohne Softwarebestandteile	X	X	X	X
	Anzeigen (einschl. Meldeeinrichtungen) mit Softwarebestandteilen	X	X	X	X
Stromver-sorgung	Kabel/Leitungen	X	X	X	X
	Einrichtungen der Stromversorgung ohne Softwarebestandteile	X	X	X	X
	Einrichtungen der Stromversorgung mit Softwarebestandteilen	X	X	X	X
Schutzeinrich-tungen	Aggregateschutz ohne Softwarebestandteile	X	X	X	X
	Aggregateschutz mit Softwarebestandteilen	X	X	X	X
	Sonstige Schutzeinrichtungen ohne Softwarebestandteile	X	X	X	X
	Sonstige Schutzeinrichtungen mit Softwarebestandteilen	X	X	X	X
Kommu-nika-tion	Hardwaresysteme zur Realisierung des Datenflusses	X	X	X	X
	Protokoll	X	X		
	Signalwandler ohne Softwarebestandteile	X	X	X	X
	Signalwandler mit Softwarebestandteilen	X	X	X	X
Zugriffsmög-lichkeiten	Zugriffsmöglichkeiten ohne Softwarebestandteile	X	X	X	X
	Zugriffsmöglichkeiten mit Softwarebestandteilen	X	X	X	X
	Hardwaretechnische Umsetzung administrativer Zugriffsregeln	X	X	X	X
	Softwaretechnische Umsetzung administrativer Zugriffsregeln	X	X		
	Funktionsweise des Gesamtsystems	X	X		

Tests und Prüfungen bei Instandsetzung oder während des Betriebs werden bei allen Baugruppen, Komponenten und Systemen durchgeführt. Daher spielen die Diversitätsmerkmale, die sich auf Tests und Prüfungen bei Instandsetzung oder während des Betriebs beziehen, bei der Beurteilung der Diversität immer eine wichtige Rolle, unabhängig davon, ob einzelne Baugruppen oder ganze leittechnische Systeme betrachtet werden. Daher sind diese Diversitätsmerkmale bei nahezu allen Bestandteilen des in Abschnitt 6.2 eingeführten generischen Leittechniksystems mit Kreuzen gekennzeichnet. Ausnahmen bilden hierbei die Protokolle, die softwaretechnische Umsetzung administrativer Zugriffsregeln und die Funktionsweise des Gesamtsystems, für die keine Instandhaltungen durchgeführt werden (für einzelne Komponenten schon, nicht für das gesamte System). Für diese sind daher die mit der Instandhaltung in Verbindung stehenden Diversitätsmerkmale nicht relevant.

6.3.4 Beteiligtes Personal

Im Bereich Beteiligtes Personal muss bewertet werden, ob das Personal bei Herstellung und Entwicklung sowie bei Betrieb und Instandhaltung diversitär ist, damit ein CCF nicht unterstellt werden muss. Dazu muss bewertet werden, ob in den im Folgenden aufgeführten Diversitätsmerkmalen Diversität vorliegt.

Generell ist bei den folgenden Diversitätsmerkmalen zu beachten, dass die Forderung nach unabhängig voneinander arbeitenden Firmen bedeutet, dass sich die von den Firmen eingesetzten Teams aus unterschiedlichem Personal zusammensetzen müssen. Darüber hinaus dürfen die Teams nicht über ihre Arbeit kommunizieren. Auch gemeinsam besuchte Schulungen oder ähnliches in der Gegenwart oder Vergangenheit können für die Diversität problematisch sein.

6.3.4.1 Personal bei Herstellung und Entwicklung

Im Bereich des Personals bei Herstellung und Entwicklung (siehe auch Tabelle 6.12) werden folgende Diversitätsmerkmale betrachtet:

Teams zur Formulierung der Anforderungen
Hier geht es um sämtliches Personal seitens des Auftraggebers, das an der Erstellung der Anforderungsformulierungen beteiligt ist. Für das Vorliegen von Diversität in diesem Merkmal ist bei der Erstellung der Anforderungsformulierungen auf Auftraggeberseite

unterschiedliches Personal einzusetzen. Dabei dürfen die gebildeten Teams weder vor noch während der Erstellung der Anforderungsformulierungen miteinander darüber kommunizieren und müssen unabhängig voneinander arbeiten.

Management des Entwicklungs- und Herstellungsprozesses

Hier geht es um sämtliches Personal seitens der Auftragnehmer, das am Management des Entwicklungs- und Herstellungsprozesses beteiligt ist. Für das Vorliegen von Diversität in diesem Merkmal ist bei Organisation und Management des Entwicklungs- und Herstellungsprozesses auf Auftragnehmerseite unterschiedliches Personal einzusetzen. Dabei müssen Organisation und Management des Entwicklungs- und Herstellungsprozesses in unterschiedlichen, unabhängig voneinander arbeitenden Firmen erfolgen.

Entwicklungs- und Designteams

Hier geht es um sämtliches Personal seitens der Auftragnehmer, das an Entwicklung und Design beteiligt ist. Für das Vorliegen von Diversität in diesem Merkmal ist bei der Umsetzung der Anforderungsformulierungen im Rahmen des Entwicklungs- und Herstellungsprozesses auf Auftragnehmerseite unterschiedliches Personal einzusetzen. Dabei müssen Entwicklung und Design in unterschiedlichen, unabhängig voneinander arbeitenden Firmen erfolgen.

Implementierungsteams

Hier geht es um sämtliches Personal seitens der Auftragnehmer, das an der Implementierung beteiligt ist. Für das Vorliegen von Diversität in diesem Merkmal ist bei der Implementierung im Rahmen des Entwicklungs- und Herstellungsprozesses auf Auftragnehmerseite unterschiedliches Personal einzusetzen. Dabei muss die Implementierung in unterschiedlichen, unabhängig voneinander arbeitenden Firmen erfolgen.

Validierungsteams

Hier geht es um sämtliches Personal seitens der Auftragnehmer, das an der Validierung beteiligt ist. Für das Vorliegen von Diversität in diesem Merkmal ist bei der Validierung im Rahmen des Entwicklungs- und Herstellungsprozesses auf Auftragnehmerseite unterschiedliches Personal einzusetzen. Dabei muss die Validierung in unterschiedlichen, unabhängig voneinander arbeitenden Firmen erfolgen.

Tab. 6.12 Personal bei Herstellung und Entwicklung – Matrix der Diversitätsmerkmale

		Teams zur Formulierung der Anforderungen	Management des Entwicklungs- und Herstellungsprozesses	Entwicklungs-/Designteams	Implementierungsteams	Validierungsteams
Eingabe	Sonden	X	X	X	X	X
	Messumformer ohne Softwarebestandteile	X	X	X	X	X
	Messumformer mit Softwarebestandteilen	X	X	X	X	X
	Bedienelemente ohne Softwarebestandteile	X	X	X	X	X
	Bedienelemente mit Softwarebestandteilen	X	X	X	X	X
Verarbeitung	Nicht programmierbare Baugruppen ohne Softwarebestandteile	X	X	X	X	X
	Nicht programmierbare Baugruppen mit Softwarebestandteilen	X	X	X	X	X
	Programmierbare Baugruppen	X	X	X	X	X
	Rechnerbasierte Baugruppen	X	X	X	X	X
	Rechner	X	X	X	X	X
Ausgabe	Koppelebene ohne Softwarebestandteile	X	X	X	X	X
	Koppelebene mit Softwarebestandteilen	X	X	X	X	X
	Aktuatoren	X	X	X	X	X
	Anzeigen (einschl. Meldeeinrichtungen) ohne Softwarebestandteile	X	X	X	X	X
	Anzeigen (einschl. Meldeeinrichtungen) mit Softwarebestandteilen	X	X	X	X	X
Stromver-sorgung	Kabel/Leitungen	X	X	X	X	X
	Einrichtungen der Stromversorgung ohne Softwarebestandteile	X	X	X	X	X
	Einrichtungen der Stromversorgung mit Softwarebestandteilen	X	X	X	X	X
Schutzeinrich-tungen	Aggregateschutz ohne Softwarebestandteile	X	X	X	X	X
	Aggregateschutz mit Softwarebestandteilen	X	X	X	X	X
	Sonstige Schutzeinrichtungen ohne Softwarebestandteile	X	X	X	X	X
	Sonstige Schutzeinrichtungen mit Softwarebestandteilen	X	X	X	X	X
Kommu-nika-tion	Hardwaresysteme zur Realisierung des Datenflusses	X	X	X	X	X
	Protokoll	X	X	X	X	X
	Signalwandler ohne Softwarebestandteile	X	X	X	X	X
	Signalwandler mit Softwarebestandteilen	X	X	X	X	X
Zugriffsmög-lichkeiten	Zugriffsmöglichkeiten ohne Softwarebestandteile	X	X	X	X	X
	Zugriffsmöglichkeiten mit Softwarebestandteilen	X	X	X	X	X
	Hardwaretechnische Umsetzung administrativer Zugriffsregeln	X	X	X	X	X
	Softwaretechnische Umsetzung administrativer Zugriffsregeln	X	X	X	X	X
	Funktionsweise des Gesamtsystems	X	X	X	X	X

Das eingesetzte Personal ist ein grundlegender Bestandteil bei Herstellung und Entwicklung von Baugruppen, Komponenten und Systemen. Daher spielen Diversitätsmerkmale bezüglich des Personals bei Herstellung und Entwicklung bei der Beurteilung der Diversität immer eine wichtige Rolle, unabhängig davon, ob einzelne Baugruppen oder ganze leittechnische System betrachtet werden. Daher sind diese Diversitätsmerkmale bei allen Bestandteilen des in Abschnitt 6.2 eingeführten generischen Leittechniksystems mit Kreuzen gekennzeichnet.

6.3.4.2 Personal bei Betrieb und Instandhaltung

Im Bereich des Personals bei Betrieb und Instandhaltung (siehe auch Tabelle 6.13) werden folgende Diversitätsmerkmale betrachtet:

Inbetriebnahmeteams
Hier geht es um das Personal, das die Inbetriebnahme vornimmt. Für das Vorliegen von Diversität in diesem Merkmal muss die Inbetriebnahme durch unterschiedliches Personal auf Auftragnehmerseite erfolgen.

Teams für die Durchführung von WKPs und anderen Prüfungen des LT-Systems nach Inbetriebnahme
Hier geht es um das Personal, das wiederkehrende Prüfungen und andere Prüfungen des Leittechniksystems nach dessen Inbetriebnahme durchführt. Für das Vorliegen von Diversität in diesem Merkmal muss auf Auftraggeberseite zur Durchführung von WKPs und anderen Prüfungen der Baugruppen oder Komponenten bzw. des Teilsystems oder Systems nach der Inbetriebnahme unterschiedliches Personal eingesetzt werden.

Teams für die Durchführung von Wartung und Instandhaltung
Hier geht es um das Personal, das für Wartung und Instandhaltung eingesetzt wird. Für das Vorliegen von Diversität in diesem Merkmal muss zur Durchführung von Wartungs- und Instandhaltungsarbeiten der Baugruppen oder Komponenten bzw. des Teilsystems oder Systems unterschiedliches Personal eingesetzt werden.

Tab. 6.13 Personal bei Betrieb und Instandhaltung – Matrix der Diversitätsmerkmale

		Inbetriebnahmeteams	Teams für die Durchführung von WKPs und anderen Prüfungen des LT-Systems nach Inbetriebnahme	Teams für die Durchführung von Wartung und Instandhaltung
Eingabe	Sonden	X	X	X
	Messumformer ohne Softwarebestandteile	X	X	X
	Messumformer mit Softwarebestandteilen	X	X	X
	Bedienelemente ohne Softwarebestandteile	X	X	X
	Bedienelemente mit Softwarebestandteilen	X	X	X
Verarbeitung	Nicht programmierbare Baugruppen ohne Softwarebestandteile	X	X	X
	Nicht programmierbare Baugruppen mit Softwarebestandteilen	X	X	X
	Programmierbare Baugruppen	X	X	X
	Rechnerbasierte Baugruppen	X	X	X
	Rechner	X	X	X
Ausgabe	Koppelebene ohne Softwarebestandteile	X	X	X
	Koppelebene mit Softwarebestandteilen	X	X	X
	Aktuatoren	X	X	X
	Anzeigen (einschl. Meldeeinrichtungen) ohne Softwarebestandteile	X	X	X
	Anzeigen (einschl. Meldeeinrichtungen) mit Softwarebestandteilen	X	X	X
xStrom-versor-	Kabel/Leitungen	X	X	X
	Einrichtungen der Stromversorgung ohne Softwarebestandteile	X	X	X
	Einrichtungen der Stromversorgung mit Softwarebestandteilen	X	X	X
Schutzeinrich-tungen	Aggregateschutz ohne Softwarebestandteile	X	X	X
	Aggregateschutz mit Softwarebestandteilen	X	X	X
	Sonstige Schutzeinrichtungen ohne Softwarebestandteile	X	X	X
	Sonstige Schutzeinrichtungen mit Softwarebestandteilen	X	X	X
Kommu-nika-tion	Hardwaresysteme zur Realisierung des Datenflusses	X	X	X
	Protokoll	X	X	
	Signalwandler ohne Softwarebestandteile	X	X	X
	Signalwandler mit Softwarebestandteilen	X	X	X
Zugriffsmög-lichkeiten	Zugriffsmöglichkeiten ohne Softwarebestandteile	X	X	X
	Zugriffsmöglichkeiten mit Softwarebestandteilen	X	X	X
	Hardwaretechnische Umsetzung administrativer Zugriffsregeln	X	X	X
	Softwaretechnische Umsetzung administrativer Zugriffsregeln	X	X	
	Funktionsweise des Gesamtsystems	X	X	

Das eingesetzte Personal ist ein grundlegender Bestandteil während Betrieb und Instandhaltung von Baugruppen, Komponenten und Systemen. Daher spielen Diversitätsmerkmale bezüglich des Personals bei Betrieb und Instandhaltung bei der Beurteilung der Diversität immer eine wichtige Rolle, unabhängig davon, ob einzelne Baugruppen oder ganze leittechnische System betrachtet werden. Aufgrund dessen sind diese Diversitätsmerkmale bei nahezu allen Bestandteilen des in Abschnitt 6.2 eingeführten generischen Leittechniksystems mit Kreuzen gekennzeichnet. Ausnahmen bilden hierbei die Protokolle, die softwaretechnische Umsetzung administrativer Zugriffsregeln und die Funktionsweise des Gesamtsystems, für die keine Instandhaltungen durchgeführt werden (für einzelne Komponenten schon, nicht für das gesamte System). Für diese ist daher das für Wartung und Instandhaltung eingesetzte Personal als Diversitätsmerkmal nicht relevant.

6.4 Anwendung der Matrix der Diversitätsmerkmale

Die in der Matrix enthaltenen Diversitätsmerkmale sind anwendbar auf:

- Zwei oder mehr Leittechniksysteme, welche dieselbe Funktion erfüllen
- Redundante Stränge eines Leittechniksystems
- Einzelne Komponenten eines Leittechniksystems

Zur Bewertung der Diversität muss geprüft werden, ob zwei Baugruppen oder Komponenten bzw. Teilsysteme oder Systeme, welche dieselbe Funktion erfüllen, hinreichend diversitär realisiert sind, um als Vorsorge gegen CCF auszureichen. Ausreichende Vorsorge gegen CCF bedeutet in diesem Fall, dass dieselbe Ursache nicht bei beiden zu untersuchenden Baugruppen, Komponenten, Teilsysteme oder Systeme zum Auftreten desselben Fehlers führt. Somit ist beim Vorliegen von Diversität nur eine Baugruppe oder Komponente bzw. ein Teilsystem oder System vom Fehler betroffen und die Funktionalität des Gesamtsystems ist weiterhin gegeben.

Mit Hilfe der in Abschnitt 6.3 dargestellten Diversitätsmerkmale kann die Diversität zweier Baugruppen oder Komponenten bzw. Teilsysteme oder Systeme bewertet werden. Bei der Bewertung der Erfüllung der einzelnen Diversitätsmerkmale können Fälle auftreten, in denen einzelne Merkmale nur teilweise erfüllt sind. Ist dies der Fall, muss spezifisch bewertet werden, ob die Vorsorge gegen CCF noch ausreichend ist oder ob

ein andere Baugruppe oder Komponente bzw., ein anderes Teilsystem oder System auszuwählen ist, um die geforderte Diversität sicherzustellen.

Ebenfalls ist von Fall zu Fall zu bewerten, welche Maßnahmen getroffen werden müssen, wenn in einzelnen Merkmalen keine Diversität vorliegt.

6.4.1 Anwendungsbeispiele

Als erstes Beispiel zur Anwendung der Matrix der Diversitätsmerkmale wird das Diversitätsmerkmal Entwicklungs- und Designteams im Bereich Personal bei Herstellung und Entwicklung betrachtet. Die Definition dieses Merkmals sagt aus, dass bei der Umsetzung der Anforderungsformulierungen im Rahmen des Entwicklungs- und Herstellungsprozesses auf der Auftragnehmerseite unterschiedliches Personal einzusetzen ist. Des Weiteren wird in Abschnitt 6.3.1 definiert, dass Entwicklung und Design der zu bewertenden Baugruppen, Komponenten, Teilsysteme oder Systeme in unterschiedlichen, unabhängig voneinander arbeitenden Firmen erfolgen müssen, damit Diversität in diesem Merkmal vorliegt. Das Diversitätsmerkmal Entwicklungs- und Designteams soll jetzt beispielsweise auf Messumformer mit Softwarebestandteilen, also ein Gerät mit Softwarebestandteilen zur Umformung der mittels Sonden gemessenen Anlagenparameter in elektrische Eingangssignale für die Verarbeitungsebene, angewendet werden. Zuerst muss beurteilt werden, ob das zu bewertende Diversitätsmerkmal auf die Komponente angewendet werden muss. Dies ist der Fall, da die Software und Hardware des Messumformers mit Softwarebestandteilen von einem Entwicklungs- und Designteam entwickelt und entworfen werden muss. Anschließend ist zu bewerten, ob das Diversitätsmerkmal erfüllt ist. Die zu untersuchenden Messumformer mit Softwarebestandteilen erfüllen das Diversitätsmerkmal Entwicklungs- und Designteam, wenn die Teams, die aktiv am Entwicklungs- und Designprozess der Messumformer beteiligt sind, aus unterschiedlichen Mitarbeitern bestehen und unabhängig voneinander arbeiten. Außerdem darf keine Kommunikation zwischen den Mitgliedern der Teams über Entwicklung und Design der Komponente stattfinden.

Als weiteres Beispiel wird das Diversitätsmerkmal Vorgefertigte Software im Bereich Softwareerstellung während Herstellung und Entwicklung betrachtet. Durch dieses Merkmal sind alle Arten vorgefertigter Software, welche als Teil der entwickelten Software genutzt werden, abgedeckt. Dies beinhaltet sowohl bereits existierende vorgefer-

tigte Software in der Softwareentwicklungsfirma, welche nicht speziell für die zu betrachtende Komponente entwickelt wurde, als auch zugekaufte Software anderer Hersteller. Die Definition des Merkmals sagt aus, dass, sofern es zur Verwendung vorgefertigter Softwarebestandteile kommt, diese über den gesamten Prozess der Softwareerstellung hinweg von unterschiedlichen Herstellern bezogen werden muss, damit Diversität in diesem Merkmal vorliegt. Des Weiteren muss in allen zutreffenden Diversitätsmerkmalen Diversität vorliegen. Das Diversitätsmerkmal Vorgefertigte Software im Bereich Softwareerstellung soll jetzt beispielsweise auf rechnerbasierte Baugruppen, also Baugruppen die zumindest einen Prozessor enthalten, angewendet werden. Da sowohl die Konfiguration als auch die Funktion der Baugruppe durch die Ausführung von Software in einem Betriebssystem realisiert wird, ist das Diversitätsmerkmal auf die zu bewertende Komponente anzuwenden. Anschließend ist zu bewerten, ob das Diversitätsmerkmal erfüllt ist. Die zu untersuchenden rechnerbasierten Baugruppen erfüllen das Diversitätsmerkmal Vorgefertigte Software im Bereich Softwareerstellung, wenn die genutzten vorgefertigten Softwarekomponenten von verschiedenen, voneinander unabhängigen Softwareentwicklern bezogen werden und in allen zutreffenden Diversitätsmerkmalen Diversität vorliegt.

Als Beispiel für den Nutzen der Matrix von Diversitätsmerkmalen soll ein Fehler in der Fertigung von Hardwarekomponenten betrachtet werden. Ein zugehöriges Diversitätsmerkmal ist der Fertigungsprozess im Bereich Entwicklung und Fertigung der Hardware während Herstellung und Entwicklung. Die Definition dieses Merkmals sagt aus, dass sich die Fertigung der Hardware bzw. der Hardwarekomponenten grundlegend unterscheiden muss (z. B. hinsichtlich eingesetzter Maschinen, Verfahren, Programme zur Automatisierung etc.), damit Diversität in diesem Merkmal vorliegt. Ein weiteres Diversitätsmerkmal im Bereich Entwicklung und Fertigung der Hardware ist Hersteller einschließlich Unterauftragnehmer. Die Definition dieses Merkmals sagt aus, dass der gesamte Fertigungsprozess bei unterschiedlichen Herstellern erfolgen muss, damit Diversität in diesem Merkmal vorliegt. Des Weiteren wird gefordert, dass auch bei der Auslagerung einzelner Fertigungsschritte an Unterauftragnehmer unterschiedliche Firmen beauftragt werden müssen. Käme es jetzt zu einem Fehler in der Fertigung, der eine fehlerhafte Lötung zur Folge hat, welche die betroffene Komponente bei Grenzbelastungen zum Ausfall bringt, gäbe es zwei Möglichkeiten, die Wahrscheinlichkeit für einen CCF zu reduzieren. Zum einen würde die Erfüllung des Diversitätsmerkmals Fertigungsprozess verlangen, dass nicht beide zu bewertenden Komponenten mit dem gleichen Verfahren hergestellt werden. Prinzipiell würde das bedeuten, dass nicht beide Komponenten nach

dem gleichen Verfahren gelötet werden dürfen bzw. nur eine Komponente gelötet werden darf und bei der anderen Komponente die Kontaktierung mittels eines anderen Verfahrens hergestellt werden muss. Da dies praktisch nicht oder nur sehr schwierig umzusetzen ist, ist eine Erfüllung dieses Diversitätsmerkmals eventuell nicht möglich. Wird aber das Diversitätsmerkmal Hersteller einschließlich Unterauftragnehmer erfüllt, ist sichergestellt, dass die beiden zu bewertenden Komponenten bei unterschiedlichen Herstellern gefertigt wurden. Damit wäre dann die Wahrscheinlichkeit für einen oben beschriebenen Chargenfehler stark reduziert. Je nach Zielsetzung könnte die zuständige Aufsichts- und Genehmigungsbehörde in diesem Fall abwägen, ob die Komponente auch dann eingesetzt werden kann, wenn nicht in allen zutreffenden Diversitätsmerkmalen Diversität vorliegt. Dabei ist aber zu bedenken, dass bei der Betrachtung eines herausgegriffenen möglichen Fehlers manche Diversitätsmerkmale relevanter erscheinen als andere. Die Forderung nach Diversität dient in der Regel aber nicht nur dazu, die Wahrscheinlichkeit bereits vorgedachter Fehler sondern auch die Wahrscheinlichkeit des Auftretens noch nicht vorgedachter Fehler zu reduzieren. Von Diversität kann man in diesem Sinne nur dann sprechen, wenn in allen zutreffenden Diversitätsmerkmalen Diversität vorliegt.

7 Zusammenfassung

Ziel des Vorhabens war es, Anforderungen für den Einsatz von Redesign-Komponenten in der Sicherheitsleittechnik von Kernkraftwerken zu entwickeln und nach Kriterien und Kenngrößen zu suchen, um diese zu bewerten.

Zunächst wurde der für das Vorhaben relevante Stand von Wissenschaft und Technik ermittelt und dargestellt. Dabei stellte sich heraus, dass der Begriff „Redesign“ nicht eindeutig definiert ist und mit unterschiedlichen Bedeutungen verwendet wird. Daher wurde in diesem Vorhaben der Begriff „Ersatzbaugruppen“ eingeführt und verwendet. Damit beziehen sich die Aussagen in diesem Bericht auf jegliche Baugruppen, die durch Modifizierung bisher eingesetzter Baugruppen entstehen und diese ersetzen sollen, unabhängig davon, ob es sich um Nachbauten oder Nachfolgemodelle handelt.

Im Rahmen des Vorhabens sollten vor allem Diversitätsmerkmale erarbeitet werden, die bei der Beurteilung der Diversität von Baugruppen, die in redundanten Teilsystemen eingesetzt sind, herangezogen werden können.

Bei der Beurteilung der Diversität gibt es nach Ansicht der GRS zwei wesentliche Punkte:

- Betrachtung relevanter Aspekte des Lebenszyklus von der Formulierung der Anforderungen über Entwicklung und Herstellung bis hin zu Betrieb und Instandhaltung bei der Definition und der Erarbeitung von Diversitätsmerkmalen
- Herstellung des Anwendungsbezugs dieser Diversitätsmerkmale über ihre flexible Anwendbarkeit auf einzelne Baugruppen, verschiedene Redundanzen eines Leittechniksystems oder ganze Leittechniksysteme

Um diese beiden Punkte zu erfüllen, wurden in den ersten beiden Arbeitspaketen folgende Ansätze verfolgt:

Ausgehend vom Stand von Wissenschaft und Technik wurden zunächst Anforderungen speziell an Ersatzbaugruppen aus nationalen und internationalen Normen und Regelwerken zusammengetragen. Des Weiteren wurden die in diesen Normen und Regelwerken enthaltenen Aussagen und Anforderungen hinsichtlich der Diversität, Zuverlässigkeit und des CCF-Potentials von programmierbaren oder rechnerbasierten Baugruppen, Komponenten, Teilsystemen und Systemen und die darin beschriebenen Diversitäts-

merkmale recherchiert und aufbereitet. Die Ergebnisse wurden als Diskussionsgrundlage für die Erarbeitung und Definition der in diesem Bericht beschriebenen Diversitätsmerkmale verwendet.

Parallel dazu wurde jeweils eine FMEA für generische nicht programmierbare, programmierbare und rechnerbasierte Baugruppen durchgeführt, wobei insbesondere mögliche Failure Modes dieser Baugruppen aufgezeigt wurden. Dies lieferte wertvolle Hinweise zum einen für die Erarbeitung und Definition der Diversitätsmerkmale, und zum anderen für die Charakterisierung eines generischen Leittechniksystems.

Aufbauend auf den Ergebnissen aus diesen Arbeitspaketen wurde von der GRS zunächst eine generische Darstellung eines Leittechniksystems erarbeitet. Dabei wurden sowohl die für die Ausführung der Leittechnik-Funktionen wichtigen Bestandteile des Leittechniksystems berücksichtigt als auch weitere technische Aspekte des Leittechniksystems, die nicht direkt für die Ausführung der Leittechnik-Funktionen verantwortlich sind wie beispielsweise hard- und softwaretechnische Zugriffsmöglichkeiten.

Im nächsten Schritt wurden Diversitätsmerkmale erarbeitet und definiert, welche die für die Beurteilung der Diversität relevanten Aspekte des Lebenszyklus dieses generischen Leittechniksystems abdecken. Da nicht alle Diversitätsmerkmale auf jeden Teil einer Baugruppe, Komponente bzw. eines Teilsystems oder Systems anzuwenden sind, wurde von der GRS eine Matrix erstellt, welche die Bestandteile des generischen Leittechniksystems mit den Diversitätsmerkmalen verknüpft.

Bei der Aufbereitung des Standes von Wissenschaft und Technik sowie der Bearbeitung der weiteren Arbeitspakete wurde schnell deutlich, dass weder hinsichtlich der Kriterien und Kenngrößen zu ihrer Bewertung noch bezüglich der Frage nach Diversität wesentliche Unterschiede zwischen Ersatzbaugruppen und Baugruppen, die im Zuge einer Umrüstung der Leittechnik, der Inbetriebnahme eines weiteren Systems oder im Rahmen eines Neubauprojektes zum Einsatz kommen sollen, bestehen. Daher ist die Anwendbarkeit dieser Matrix nicht auf Ersatzbaugruppen beschränkt. Vielmehr ist diese Matrix fallspezifisch und flexibel im Rahmen der Beurteilung der Diversität anwendbar. Dies umfasst sowohl die Anwendung für ganze Leittechniksysteme (z. B. wenn ein System das Backupsystem eines anderen Systems darstellen soll) als auch für redundante Stränge eines Leittechniksystems (Teilsysteme) oder für einzelne Baugruppen oder Komponenten (unabhängig davon, ob sie im selben Teilsystem oder System eingesetzt sind oder in verschiedenen Teilsystemen oder Systemen).

Die im Rahmen des Vorhabens entwickelte Matrix der Diversitätsmerkmale ist also wesentlich vielseitiger einsetzbar, als in der ursprünglichen Vorhabensplanung vorgesehen war. Die Bewertung der Diversität von Ersatzbaugruppen ist einer der möglichen Anwendungsfälle.

8 Literaturverzeichnis

/ACT03/ ACTEL Corporation, Reliability Considerations for Automotive FPGAs White Paper, http://www.eet-china.com/ARTICLES/2006OCT/PDF/AUCOL_2006OCT26_BOE_TA_488.pdf?SOURCES=DOWNLOAD

/BAT11/ N. Battezzati, L. Sterpone, M. Violante, Reconfigurable Field Programmable Gate Arrays for Mission-Critical Applications, Springer 2011

/BMU12/ Sicherheitsanforderungen an Kernkraftwerke, Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit, November 2012

/BMU13/ Interpretationen zu den Sicherheitsanforderungen an Kernkraftwerke, Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit, November 2013

/DIN06/ DIN EN 60812, „Analysetechniken für die Funktionsfähigkeit von Systemen – Verfahren für die Fehlerzustandsart- und -auswirkungsanalyse (FMEA)“, (IEC 60812:2006); Deutsche Fassung EN 60812:2006, November 2006

/DIN10a/ DIN IEC EN 60880 (VDE 0491-3-2), „Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Softwareaspekte für rechnerbasierte Systeme zur Realisierung von Funktionen der Kategorie A“, (IEC 60880:2006); Deutsche Fassung EN 60880:2009, März 2010

/DIN10b/ DIN IEC 62138 (VDE 0491-3-3), Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Softwareaspekte für rechnerbasierte Systeme zur Realisierung von Funktionen der Kategorie B oder C, März 2010

/DIN10c/ DIN IEC 60987 (VDE 0491-3-1), Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Anforderungen an die Hardwareauslegung rechnerbasierter Systeme, März 2010

/DIN10d/ DIN EN 62340 (VDE 0491-10), Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Anforderungen zur Beherrschung von Versagen aufgrund gemeinsamer Ursache, Dezember 2010

/DIN10e/ DIN EN 61226 (VDE 0491-1), Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Kategorisierung leittechnischer Funktionen, Stand August 2010

/DIN13/ DIN IEC 61513 (VDE 0491-2), Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Allgemeine Systemanforderungen, Stand September 2013

/EPR08/ EPRI 1016731, Operating Experience Insights on Common-Cause Failures in Digital Instrumentation and Control Systems,
EPRI Report 1016731, Dezember 2008

/GRS00/ Beitrag zum "Alterungsbericht", Störungen im Zusammenhang mit dem Austausch von kompatiblen oder verbesserten Komponenten, abgeleitet aus der internationalen Betriebserfahrung, 24.01.2000

/GRS10/ GRS Reaktorsicherheitsforschung-Vorhaben RS1180, Weiterentwicklung und Erprobung von Methoden und Werkzeugen für probabilistische Sicherheitsanalysen,
GRS-A-3550, Entwicklung eines aktualisierten Ansatzes zur Berücksichtigung softwarebasierter Sicherheitsleittechnik in der PSA, August 2010

/GRS14b/ „Diversity criteria for digital instrumentation and control systems in nuclear power plants”, Beitrag zum International Automation Congress 2014 in Budapest, GRS, Oktober 2014

/GRS15a/ Entwicklung und Einsatz von Analysemethoden zur Beurteilung softwarebasierter leittechnischer Einrichtungen in deutschen Kernkraftwerken (3610R01361), ISBN 978-3-944161-36-5, GRS-355, 2015

/GRS15b/ Sicherheitstechnische Analyse zum Einsatz und Betrieb elektrotechnischer Einrichtungen in deutschen Kernkraftwerken, Überwachung und Schutz gegen sicherheitstechnisch bedeutsame Einwirkungen aus dem Verbundnetz sowie anderen äußeren Quellen (3610R01363), ISBN 978-3-944161-37-2, GRS-356, 2015

/IAE12/ IAEA NS-G-1.3, IAEA, Instrumentation and Control Systems Important to Safety in Nuclear Power Plants,
Safety Guide NS-G-1.3, März 2012

/IEE08/ IEEE Std. 1633-2008; IEEE Recommended Practice on Software Reliability,
IEEE Std 1633-2008, Juni 2008

/IEE09/ IEEE Std. 603-2009; IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations,
IEEE Std 603-2009, November 2009

/IEE10/ IEEE Std. 7-4-3-2-2010, IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations,
IEEE Std 7-4.3.2-2010, August 2010

/IST14/ ISTec-A-2158, „Aufstellung von Kriterien und Kenngrößen zur de-terministischen Prüfung der Eignung von Redesign-Baugruppen für den Einsatz in der Sicherheitsleit-technik von KKW“, TÜV Rheinland ISTec GmbH, Dezember 2014

/KTA06/ KTA 3504, Elektrische Antriebe des Sicherheitssystems in Kernkraftwerken, November 2006

/KTA13/ KTA 3503, Typprüfung von elektrischen Baugruppen der Sicherheitsleittechnik, Regeländerungsentwurf, Fassung November 2013

/KTA14a/ KTA 3507, Werksprüfungen, Prüfungen nach Instandsetzung und Nachweis der Betriebsbewährung der Baugruppen und Geräte der Sicherheitsleittechnik, November 2014

/KTA14b/ KTA3501, Reaktorschutzsystem und Überwachungseinrichtungen des Sicherheitssystems, Regeländerungsentwurf (Gründruck), Fassung November 2014

/NUR94/ NUREG 6303, US NRC, Method for performing diversity and defense-in-depth analyses of reactor protection systems,
NUREG-6303, Dezember 1994

/NUR00/ NUREG 6680, US NRC, Review templates for computer-based reactor protection systems,
NUREG-6680, August 2000

/NUR07/ NUREG 0800, US NRC, Guidance for evaluation of diversity and defense-in-depth in digital computer-based instrumentation and control systems,
NUREG-0800, Branch Technical Position 7-19, Rev. 5, März 2007

/NUR10/ NUREG 7007, US NRC, Diversity strategies for nuclear power plant instrumentation and control systems,
NUREG-7007, Februar 2010

/QUI08/ H. Quinn, P. Graham, K. Morgan, J. Krone, M. Caffrey, M. Wirthlin, An Introduction to Radiation-Induced Failure Modes and Related Mitigation Methods for Xilinx SRAM FPGAs, The International Conference on Engineering of Reconfigurable Systems and Algorithms (ERSA), Las Vegas, Nevada, USA, July 14 – 17, 2008

/RAN11/ Jukka Ranta, The current state of FPGA technology in the nuclear domain, VTT Technology, 10, 2011

/RSK96/ RSK-Leitlinien für Druckwasserreaktoren, Änderungsstand 15.11.1996, (4. Änderung: Berichtigung (BMU-Bekanntmachung vom 29.10.1996), BAnz Nr. 214 vom 15.11.1996)

/RSK12/ RSK-Stellungnahme, Redesign von leittechnischen Baugruppen und Komponenten in Kernkraftwerken, September 2012

/TÜV10/ Nutzerprogrammierbare Hardware (NPHW) zur Realisierung von Funktionen der Kategorie A
Stellungnahme des TÜV Süd vom 23.08.2010, IS-ETL 3-MUC/be

/VAL14/ Janne Valkonen, VTT Technical Research Centre of Finland, Vortrag im Rahmen des EU-China-Projektes “NPP I&C Training Course”, „Field-programmable gate array (FPGA) technology in NPP safety automation
– Introduction”, Oktober 2014, Beijing, China

/VDI11/ VDI/VDE 3528, VDI/VDE 3528, Anforderungen an Serienprodukte und für deren Einsatz in der Sicherheitsleittechnik in Kernkraftwerken, August 2011

/VGB11/ VGB Powertech e.V., Ersatzbeschaffung von technischen Einrichtungen der E- und L-Technik für KKW VGB-AK „Gerätequalifizierung E- und L-Technik in KKW“ E. Sander (EnKK) und W. Schroeder (VENE „WIL“), Folienvortrag zum TOP 6 der 213. Sitzung des RSK-Ausschusses „Elektrische Einrichtungen“ am 19.10.2011 im BMU

/VGB11b/ VGB-Arbeitskreis Gerätequalifizierung E+L in KKW, Richtlinie Nr. RL005/A „Design/Redesign von technischen Einrichtungen in Kernkraftwerken“, Rev. A, 2011

/WAN98/ Markus Wannemacher: Das FPGA-Kochbuch, 1998
http://www.aufzu.de/FPGA/kochbuch/index.html

/ZEI06a/ Bob Zeidman: All about FPGAs, 2006
http://www.eetimes.com/document.asp?doc_id=1274496&print=yes

/ZEI06b/ Bob Zeidman: Introduction to CPLD and FPGA Design, 2006
http://pldworld.org/html/technote/intro.cpld.fpga.design.pdf

Abbildungsverzeichnis

Tabellenverzeichnis

Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH

Schwertnergasse 1
50667 Köln
Telefon +49 221 2068-0
Telefax +49 221 2068-888

Forschungszentrum
85748 Garching b. München
Telefon +49 89 32004-0
Telefax +49 89 32004-300

Kurfürstendamm 200
10719 Berlin
Telefon +49 30 88589-0
Telefax +49 30 88589-111

Theodor-Heuss-Straße 4
38122 Braunschweig
Telefon +49 531 8012-0
Telefax +49 531 8012-200

www.grs.de

ISBN 978-3-944161-76-1