„Rechnerbasierte Sicherheitsleittechnik für den Einsatz in der höchsten Sicherheitskategorie in deutschen Kernkraftwerken“

Darstellung der Beratungsergebnisse der RSK-Arbeitsgruppe EINSATZ RECHNERBASIERTE LEITTECHNIK (ERL)

20.09.2011

INHALTSVERZEICHNIS

1 Anlass der Beratung ... 3

2 Begriffe und Abkürzungen ... 4

2.1 Begriffsdefinitionen ... 4

2.2 Verwendete Abkürzungen ... 7

3 Beratungsverlauf ... 7

4 Sicherheitsrelevante Aspekte eines Einsatzes rechnerbasierter Sicherheitsleittechnik ... 7

5 Anforderungen des nationalen und internationalen Regelwerkes und Anpassungsnotwendigkeiten ... 9

5.1 Anforderungen im bestehenden deutschen Regelwerk ... 9

5.2 Übersicht über Regelungsinhalte im IEC, DIN IEC und DIN EN Regelwerk zum Lebenszyklus rechnerbasierter Sicherheitsleittechnik ... 12

6 Aspekte zur CCF Vermeidung ... 16

6.1 Aspekte zur Arbeitsweise rechnerbasierter Sicherheitsleitsysteme, die Kategorie-A Funktionen ausführen ... 16

6.2 Aspekte grundlegender Qualitätsanforderungen an der Schnittstelle Verfahrenstechnik / Leittechnik ... 18

7 Diversität als Beitrag zur CCF Vermeidung / Beherrschung ... 19

7.1 Diversifizierung interner Zustände der Rechner ... 19

7.2 Gegenüberstellung realisierter Architekturen in den USA, in Frankreich, in Japan, und in Finnland im Hinblick auf Verwendung diversitärer Systeme ... 22

8 Darstellung von zwei Architekturen zur Beherrschung des CCF im Rahmen des gestaffelten Sicherheitskonzepts ... 25

9 Auswirkungen von CCF Postulaten an der Schnittstelle Leittechnik/Verfahrenstechnik ... 32

9.1 Folgen fehlerhaft generierter Reaktorschutzsignale ... 32

9.2 Beherrschung von aktivem und passivem Funktionsversagen im Kontext unterschiedlicher Architekturen ... 33

9.3 Ableitung vitaler Funktionen ... 37

10 Zusammenstellung von Konsequenzen für Entwicklung, Implementierung und Betrieb aus der Realisierung der beiden Architekturen zur Beherrschung des CCF ... 38

11 Instandhaltungs- und Änderungsmaßnahmen ... 41

12 Qualifizierung und Komplexität; Abgrenzung zwischen Typprüfung und Eignungsüberprüfung ... 43

In Bezug genommene Unterlagen ... 46

Anhang 49

1 Anlass der Beratung

In seiner 200. Sitzung am 04.06.2009 hat der RSK-Ausschuss ELEKTRISCHE EINRICHTUNGEN sein Positionspapier „Rechnerbasierte Sicherheitsleittechnik für den Einsatz in der höchsten Sicherheitskategorie in deutschen Kernkraftwerken“ [1.1] verabschiedet. In dem Positionspapier werden fünf Einzelaspekte behandelt:

- Maßnahmen zur Vermeidung und Beherrschung des Common-Cause-Failure (CCF);
- Qualifizierung und Komplexität; Abgrenzung zwischen Typprüfung und Eignungsüberprüfung;
- Instandhaltungsmaßnahmen und Änderungen an rechnerbasierter Leittechnik;
- Security;
- Zuverlässigkeit und Einbeziehung der Probabilistik.

Zu den letzten vier Aspekten wurde ein einvernehmlicher Standpunkt erarbeitet, der von allen Mitgliedern des Ausschusses ELEKTRISCHE EINRICHTUNGEN getragen wurde. Zu den Maßnahmen zur Vermeidung und Beherrschung des CCF konnte kein einvernehmlicher Standpunkt erarbeitet werden.

Vor diesem Hintergrund ist in der 425. Sitzung der RSK am 15.04.2010 die RSK Ad-Hoc Arbeitsgruppe „Einsatz Rechnerbasierter Leittechnik“ (AG ERL) eingesetzt und in der 426. Sitzung der RSK am 20.05.2010 beauftragt worden, eine Vorlage zu erarbeiten für RSK Beratungen zu übergeordneten Anforderungen an eine rechnerbasierte Sicherheitsleittechnik.

Seitens der Arbeitsgruppe sind somit Vorschläge für übergeordnete Anforderungen an eine rechnerbasierte Sicherheitsleittechnik für den Einsatz in Reaktorschutzsystemen zusammenzustellen und zu begründen. Insbesondere ist einzugehen auf Anforderungen, die die Vermeidung / Beherrschung systematischer Ausfälle (Ausfall aufgrund gemeinsamer Ursache – GVA)[1] rechnerbasierter Leittechnikfunktionen im Rahmen des gestaffelten Sicherheitskonzepts sicherstellen sollen. Die Zusammenstellung soll eine nachvollziehbare Grundlage für die darauf aufbauenden RSK Beratungen liefern.

Im Zuge der Beratungen der AG soll eine Bestandsaufnahme über den internationalen Stand der Diskussionen unter Einbeziehung der Anforderungen erfolgen, die den geplanten und bereits erfolgten Implementierungen rechnerbasierter Sicherheitsleittechnik zu Grunde liegen. Hierbei sind seitens der Arbeitsgruppe relevante internationale Normen und Normenentwürfe sowie weitere relevante Quellen heranzuziehen.

Die Arbeitsgruppe soll in ihre Beratungen neben den leittechnischen auch verfahrenstechnische Fragestellungen einbeziehen.

[1] Nachfolgend wird ausschließlich der Begriff CCF benutzt.

Die Beratungsergebnisse der RSK-Arbeitsgruppe ERL sind nachfolgend dargestellt. Die AG ERL hat die in dem Positionspapier [1.1] enthaltenen Empfehlungen zu den Punkten

- Qualifizierung und Komplexität; Abgrenzung zwischen Typprüfung und Eignungsüberprüfung

- Instandhaltungsmaßnahmen und Änderungen an rechnerbasierter Leittechnik

in ihre Empfehlungen übernommen. Der in [1.1] betrachtete Aspekt „Security“ ist von der AG ERL nicht beraten worden.

2 Begriffe und Abkürzungen

2.1 Begriffsdefinitionen

- **Ausfall**: Verlust der Fähigkeit einer Komponente, bei Einhaltung spezifizierter Bedingungen die geforderte Funktion zu erfüllen.

  Anmerkung: Bezieht sich nur auf Hardware, also auf Objekte, die ihre körperliche Beschaffenheit ändern und somit ausfallen können. Das Ereignis "Ausfall" markiert den Zeitpunkt des Übergangs von der Korrektheit zu einem Fehler (in diesem Sinne werden die Begriffe in [2.1] bis [2.3] verwendet).

- **closed-loop Simulation**: Simulation der Leittechnik in einem geschlossenen Regelkreis, bei dem Ausgangs- und Eingangswerte der Leittechnik mit einem Prozessmodell gekoppelt werden.

- **Common Cause Failure (CCF)**: Versagen von zwei oder mehreren Strukturen, Systemen/Teilsystemen oder Komponenten infolge eines einzigen spezifischen Ereignisses oder Grundes.
  (Quelle: [2.4])

- **Diversität**: Vorhandensein von zwei oder mehreren unterschiedlichen Verfahren oder Mitteln, um ein bestimmtes Ziel zu erreichen. Diversität wird insbesondere als Schutzmaßnahme gegen CCF-Versagen eingesetzt. Sie kann erreicht werden, indem physikalisch unterschiedliche Systeme eingesetzt werden, oder durch funktionale Diversität, bei der gleichartige Systeme ein bestimmtes Ziel über unterschiedliche Verfahren erreichen.
  (Quelle: [2.5])

- **Dissimilarität:** spezielle Form der Diversität für rechnerbasierte Systeme mit den im Rahmen der VDI/VDE 3528 [2.6] genannten Diversitätsmerkmalen:
  „Eine dissimilare Technik verwendet Geräte, die nachweisbar hinsichtlich Hardware, Software, Entwicklungswerkzeugen, Entwicklungsteams, Fertigung, Test und Instandhaltung hinreichend unähnlich bzw. ungleichartig sind.

  Anmerkung 1: Ziel ist es, unabhängige Systeme oder Teilsysteme so aufzubauen, dass deren sicherheitstechnisch unverzichtbare Funktionen auch beim postulierten systematischen Versagen von einem der unabhängigen Systeme oder Teilsysteme erhalten bleiben. Dazu muss der Grad der Dissimilarität in den zur Fehlerbeherrschung wichtigen Eigenschaften aufgezeigt werden."

  Anmerkung 2: Rechnerbasierte Systeme können auch in Einzelaspekten diversitär aber nicht dissimilar ausgeführt sein; in diesem Fall wird im Folgenden allgemein vom Vorliegen von Diversitätsmerkmalen gesprochen.

- **Emulation:** Nachbildung der Verhaltensweise eines Systems oder Geräts.

- **Fehler**: Mangel an einer Hardware-, Software- oder Systemkomponente.
  (Quelle: [2.4])

- **Funktionale Diversität:** Anwendung der Diversität auf der Funktionsebene (z. B. Ableitung eines Abschaltkriteriums sowohl aus Druck- als auch Temperaturgrenzwerten).
  (Quelle: [2.4])

- **Funktionsversagen, aktives:** Versagen eines leittechnischen Systems derart, dass von der Aufgabenspezifikation nicht vorgesehene Auslösesignale ausgegeben werden.

- **Funktionsversagen, passives**: Versagen eines leittechnischen Systems derart, dass von der Aufgabenspezifikation vorgesehene Auslösesignale nicht ausgegeben werden.

- **Kategorie einer leittechnischen Funktion**: eine von drei möglichen Sicherheitszuordnungen (A, B, C) von leittechnischen Funktionen, die aus der Sicherheitsrelevanz der durchzuführenden Funktionen resultieren. Wenn die Funktion für die Sicherheit nicht signifikant ist, erfolgt keine Sicherheitszuordnung (Kategorisierung).
  (Quelle: [2.4])

  Anmerkung: Vorgaben zur Kategorisierung leittechnischer Funktionen enthält die DIN EN 61226 [2.7].

- **Klasse eines leittechnischen Systems:** eine von drei möglichen Zuordnungen (1, 2, 3) sicherheitstechnisch wichtiger leittechnischer Systeme, entsprechend der Anforderung, leittechnische Funktionen unterschiedlicher Sicherheitsrelevanz zu realisieren. Wenn mit einem leittechnischen System keine sicherheitstechnisch wichtige Funktion realisiert wird, erfolgt keine Sicherheitszuordnung (Klassifizierung)
  (Quelle: [2.4])

- **Komplexität:** Schwierigkeitsgrad der Verständlichkeit und Verifizierbarkeit eines Systems oder einer Komponente aufgrund von Auslegung, Realisierung oder Verhalten.

(Quelle: [2.4])

- **Lebenszyklus:** Erforderliche Aktivitäten in Zusammenhang mit der Realisierung von sicherheitstechnisch wichtigen Systemen und Geräten der leittechnischen Architektur, beginnend mit der Herleitung der Leittechnik-Anforderungen aus der sicherheitstechnischen Auslegungsbasis der Anlage bis zu dem Zeitpunkt, in dem keines der leittechnischen Systeme für die Nutzung zur Verfügung steht.
  (Quelle: [2.4])

- **Rechnerbasiertes System:** Leittechnisches System, dessen Funktionen zum größten Teil oder auch vollständig von Mikroprozessoren, programmierbaren elektronischen Geräten oder Rechnern abhängen bzw. durchgeführt werden.
  (Quelle: [2.4])

- **Unabhängige leittechnische Systeme:** Unabhängige Systeme weisen folgende Eigenschaften auf:
  a) Die Fähigkeit eines jeden der beiden Systeme, die gewünschte Funktion auszuführen, wird durch Betrieb oder Versagen des anderen Systems nicht beeinflusst.
  b) Die Fähigkeit der Systeme, ihre Funktionen auszuführen, wird nicht von Effekten beeinflusst, die von dem angenommenen auslösenden Ereignis herrühren, für das diese Funktionen gefordert sind.
  c) Hinreichende Robustheit gegen gemeinsame externe Einflüsse (z. B. Erdbeben und Elektromagnetische Beeinflussung) wird durch die Auslegung der Systeme sichergestellt. (Quelle: [2.5])

  Anmerkung 1: Auslegungsmittel zur Erzielung von Unabhängigkeit sind elektrische und physikalische Trennung, unabhängige Kommunikation und Rückwirkungsfreiheit von den zu steuernden Prozessen.

  Anmerkung 2: Die derart definierte Unabhängigkeit ist zwar eine notwendige Voraussetzung, dass Systeme nicht gemeinsam versagen, wird aber in dieser Form im Kontext des vorliegenden Textes nicht als hinreichend zur Beherrschung von CCF angesehen.

- **Versagen**: Abweichen des vorliegenden Verhaltens von dem beabsichtigten Verhalten. (Quelle: [2.8])

- **Versagen, gerichtetes**: Versagen eines leittechnischen Systems in einer vordefinierten Weise (Richtung) derart, dass sich an den Ausgängen ein definierter Zustand einstellt.

2.2 Verwendete Abkürzungen

CC	Common Cause
CCA	Common Cause Analysis
CCF	Common Cause Failure
CCI	Common Cause Initiator
COTS	Commercial-of-the-shelf
EMV	Elektromagnetische Verträglichkeit
EN	Europäische Norm
FMEA	Failure Mode and Effects Analysis
FTA	Fault Tree Analysis
HALT	Highly Accelerated Lifetime Testing
HW	Hardware
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
RS	Reaktorschutz
RSS	Reaktorschutzsystem
SW	Software
V&V	Verifikation und Validierung
WKP	wiederkehrende Prüfung
ZLE	Zusätzliche leittechnische Einrichtungen

3 Beratungsverlauf

Die Arbeitsgruppe hat in insgesamt neun Sitzungen beraten. In der 1. Sitzung am 21.05.2010 nahm die Arbeitsgruppe entsprechend der Aufgabenstellung der RSK ihre Arbeit auf und erstellte einen Ablaufplan für die weiteren Beratungen. Eine ausführlichere Darstellung des Beratungsverlaufs mit Auflistung der Beratungsunterlagen findet sich in Anhang 1.

4 Sicherheitsrelevante Aspekte eines Einsatzes rechnerbasierter Sicherheitsleittechnik

Der Einsatz rechnerbasierter Leittechnik entspricht mittlerweile dem nationalen und internationalen Stand der Technik in der Mess-, Regel- und Automatisierungstechnik. Auch in der Kerntechnik hat diese Technologie Eingang in der Leittechnik gefunden, national gesehen insbesondere im betrieblichen Bereich der Leittechnik und in den Begrenzungen , international gesehen auch im Bereich des Reaktorschutzes.

Insofern stellt sich insbesondere bei Nachrüstungen oder Modernisierungsprojekten die Frage, ob ein Einsatz rechnerbasierter Leittechnik in Reaktorschutzsystemen erfolgen kann. In diesem Zusammenhang ist auch zu berücksichtigen, dass im Bereich der Peripheriegeräte des Reaktorschutzsystems der Einsatz softwarebasierter Gerätetechnik zunehmend an Bedeutung gewinnt, da die Gerätetechnik auf analoger Basis

vielfach nicht mehr verfügbar ist. Hierbei kommt, je nach Anwendung, z. T. komplexe Technik zum Einsatz, da es sich in der Regel um Geräte für einen weiten kommerziellen Anwendungsbereich handelt.

Rechnerbasierte Sicherheitsleittechnik weist sowohl Vor- als auch Nachteile gegenüber fest verdrahteter analoger oder digitaler Technik aus. Zu den Vorteilen zählen:

- Bessere Wartbarkeit;
- Inhärente Möglichkeit der Selbstüberwachung und der Fehlererkennung;
- Teilautomatisierte Projektierung (fehlervermeidende Generierung von Detail-Spezifikationen und Code aus Aufgabenstellungen);
- Reduzierung der Fehlerrate bei der Umsetzung durch werkzeuggestützte Plausibilitätsprüfung;
- Automatisierte Dokumentation der Funktionalität und des Änderungsmanagements;
- Automatisierte Prüfung der Funktionalität;
- Keine Drift der eingestellten Grenzwerte;
- Bei Störungen ermöglichen Diagnosetools eine umfassendere und schnellere Störungsanalyse als bei der derzeit implementierten analogen Technik;
- Es ist auf einfache Weise möglich, Emulationen der leittechnischen Funktionen auf Simulatoren zu implementieren und die Simulatoren bei funktionalen Änderungen auf dem neuesten Stand zu halten. Der Simulator erlaubt dadurch eine umfangreiche Unterstützung bei Analysen von Ausfallszenarien und eine realistische Ausbildung des Bedienpersonals bereits vor der Durchführung von Änderungen.

Abhängig von der konkreten Aufgabenstellung kommen nicht alle der o. a. Aspekte zum Tragen.

Prinzipielle Nachteile der rechnerbasierten Leittechnik sind:

- Hohe Funktionsdichte auf einzelnen Baugruppen und damit Fehlerauswirkungen auf viele Funktionen bei einem Baugruppenausfall;
- Kurze Innovationszyklen erzwingen Änderungen;
- Verwendung von komplexeren, nicht nach nuklearem Regelwerk entwickelten Komponenten (COTS), z. B. Prozessoren, Firmware;
- Es gibt neue Angriffsmöglichkeiten für Störmaßnahmen von Dritten (IT-Security);

- Für Betreiber und Sachverständige sind Updates, die vom Hersteller geliefert werden, nur mit hohem Aufwand nachvollziehbar (Einschränkung des Vieraugen-Prinzip); dies gilt ebenso für die Hersteller bzgl. ihrer Zulieferungen von Unterlieferanten;

- Hoher Aufwand bei Erwerb des Systemverständnisses;

- Eingeschränkte / erschwerte Bewertung der Zuverlässigkeit;

- Das Design von Hardware und Software erfolgt unter den Gesichtspunkten vielseitiger Verwendbarkeit und ist damit umfangreicher und komplexer als erforderlich;

- Keine vollständige Prüfbarkeit möglich durch hohe Komplexität der anwendungsunabhängigen Systemhardware und –software.

Es verbleibt ein Potenzial für CCF insbesondere im Bereich der Systemsoftware, das bei homogenen Systemen zusätzliche Maßnahmen erforderlich macht.

5 Anforderungen des nationalen und internationalen Regelwerkes und Anpassungsnotwendigkeiten

5.1 Anforderungen im bestehenden deutschen Regelwerk

In Bezug auf die Vermeidung bzw. Beherrschung von CCF im Reaktorschutzsystem sind im deutschen kerntechnischen Regelwerk zu betrachten:

- BMI-Sicherheitskriterien für Kernkraftwerke vom Oktober 1977 (SiKri)

- RSK-Leitlinien für Druckwasserreaktoren, Stand 1996

- KTA 3501 „Reaktorschutzsystem und Überwachungseinrichtungen des Sicherheitssystems“, Fassung 06/1985

- KTA 3503 „Typprüfung von elektrischen Baugruppen der Sicherheitsleittechnik“, 11.2005

- KTA 3506 „Systemprüfung der leittechnischen Einrichtungen des Sicherheitssystems von Kernkraftwerken“, 11.1984

Anforderungen im internationalen DIN IEC- bzw. DIN EN-Regelwerk, das auch national gültig ist, werden in Kapitel 5.2 dargestellt.

In den **BMI-Sicherheitskriterien für Kernkraftwerke** vom Oktober 1977 werden im Kriterium 6.1 Anforderungen an das Reaktorschutzsystem gestellt. Demnach muss ein Kernkraftwerk mit einem zuverlässigen Reaktorschutzsystem ausgerüstet sein, das bei Erreichen festgelegter Ansprechwerte Schutzaktionen auslöst. Es muss so beschaffen sein, dass es auch während Instandhaltungsvorgängen bei gleichzeitigem Auftreten eines Einzelfehlers im System seine sicherheitstechnische Aufgabe erfüllen kann. Von Hand gegebene Befehle dürfen notwendige Schutzaktionen weder beeinträchtigen noch verhindern können. In der Fußnote 5) wird weiter konkretisiert, wie die Forderung nach einem „zuverlässigen Reaktorschutzsystem“ im Sinne des Sicherheitskriteriums erfüllt werden kann:

> *„Als Mittel zur zuverlässigen Auslegung des Reaktorschutzsystems sollen vorzugsweise angewendet werden:*
>
> - *redundante Auslegung von Komponenten, Baugruppen und Untersystemen, räumlich getrennte Installation entsprechend dem Wirkungsbereich möglicher versagensauslösender Ereignisse,*
> - *Verwendung von Geräten unterschiedlicher Bauart (Diversitätsprinzip),*
> - *weitgehend selbsttätige Überwachung auf einen Ausfall hin,*
> - *Anpassung der Komponenten an die möglichen Umgebungsbedingungen.“*

Der Abschnitt 7.3 der **RSK-Leitlinien für Druckwasserreaktoren** behandelt die Sicherheitsleittechnik, wobei die Leittechnikfunktionen in drei Kategorien eingeteilt werden. Die Funktionen des Reaktorschutzsystems fallen dabei in die Kategorie 1. In Bezug auf die Vermeidung bzw. Beherrschung systematischer Ausfälle sind die folgenden Anforderungen an die Sicherheitsleittechnik der Kategorie 1 hervorzuheben:

> *„Abschnitt 7.3.2 Allgemeine Anforderungen*
>
> *(4) Der Aufbau der Sicherheitsleittechnik der Kategorie 1 soll einfach sein. Er soll erforderliche Nachweise zur Qualifizierung des Systems zuverlässig ermöglichen.*
>
> *(5) Bei der Auslegung der Sicherheitsleittechnik der Kategorie 1 ist Vorsorge gegen systematische Ausfälle zu treffen.*
>
> *(6) Es ist nachzuweisen, dass die Sicherheitsleittechnik der Kategorie 1 ihre Aufgaben auch dann erfüllt, wenn zusätzlich zum Störfall ein Zufallsausfall und ein systematischer Ausfall und Folgeausfälle eintreten. Ein systematischer Ausfall braucht dabei nicht angenommen zu werden, wenn ausreichende Maßnahmen zu seiner Vermeidung nachgewiesen werden. Während eines Instandhaltungsfalls ist auch ein Störfall zu unterstellen. Dabei brauchen innerhalb einer Zeitspanne von 100 h der systematische Ausfall und der Zufallsausfall nicht überlagert zu werden.*

(9) Fehlerhaftes Ansteuern des Sicherheitssystems ist unter Berücksichtigung der Ausfallkombinationen nach 7.3.2 (6) zu verhindern, wenn dadurch Störfälle mit nichttolerablen Auswirkungen auftreten können.

(10)Die Sicherheitsleittechnik darf die Unverfügbarkeit des Sicherheitssystems nicht bestimmen."

In der **KTA 3501 „Reaktorschutzsystem und Überwachungseinrichtungen des Sicherheitssystems"** werden die Anforderungen an das Reaktorschutzsystem weiter konkretisiert. Hinsichtlich der Vermeidung bzw. Beherrschung systematischer Ausfälle sind insbesondere die folgenden Anforderungen zu beachten (den RSK-Leitlinien wortgleiche Anforderungen werden nicht wiederholt):

Abschnitt 4 Auslegungsgrundlagen für das Reaktorschutzsystem
4.4 Ausfallkombinationen
4.4.1 Grundannahmen

(2) Es ist nachzuweisen, dass das Reaktorschutzsystem im Zusammenwirken mit aktiven und passiven Sicherheitseinrichtungen zusätzlich zum Störfall

a) einen Zufallsausfall	*Z,*
b) und einen systematischen Ausfall (soweit er nicht nach Absatz (5) ausgeschlossen werden kann)	*S,*
c) und Folgeausfälle	*F*

beherrscht.

(3) Während des bestimmungsgemäßen Betriebs der Reaktoranlage ist die Ausfallkombination nach Bild 4- 1 bezüglich eintretender Störfälle zu beherrschen, wobei im Instandhaltungsfall (l) nicht angenommen werden muss, dass während einer Zeitspanne von 100 h der systematische Ausfall (S) und der Zufallsausfall (Z) gleichzeitig auftreten.
…

(5) Die Auswirkungen systematischer Ausfälle im Reaktorschutzsystem sind zu analysieren. Abhängig vom Ergebnis der Analysen sind zusätzliche Maßnahmen zur Minderung der Eintrittswahrscheinlichkeit systematischer Ausfälle oder ihrer Auswirkungen zu treffen.

H i n w e i s:
Die Eintrittswahrscheinlichkeit systematischer Ausfälle kann zum Beispiel durch die Auswahl geeigneter Gerätesysteme, Prüfzyklen, Grenzbelastungsprüfungen so weit herabgesetzt werden, daß die systematischen Ausfälle in der Ausfallkombination nach Abschnitt 4.4.1 Absatz (2) nicht mehr betrachtet zu werden brauchen. Die Minderung der Auswirkungen kann zusätzliche Maßnahmen außerhalb des Reaktorschutzsystems erfordern.

4.4.3.2 Nicht eindeutig sicherheitsgerichtete Schutzteilaktionen

H i n w e i s:
Unter den hier betrachteten Schutzteilaktionen werden solche verstanden, die bei Fehlauslösung andere Schutzaktionen verhindern können.

(1) Die Auslösung der nicht eindeutig sicherheitsgerichteten Schutzteilaktionen muss bei den Grundannahmen nach Abschnitt 4.4.1 so sichergestellt sein, dass die aufgrund der angenommenen Ausfallkombinationen verbleibenden Schutzteilaktionen die erforderliche sicherheitstechnische Aufgabe erfüllen.

(3) Bezüglich der Fehlauslösungen nicht eindeutig sicherheitsgerichteter Schutzteilaktionen durch systematische Ausfälle sind die Forderungen von Abschnitt 4.4.1 Absatz 5 anzuwenden.

H i n w e i s:
Bei der Auslegung dieses Teils des Reaktorschutzsystems ist besonders auf auslösegerichtete Ausfälle zu achten, da Fehlauslösungen die Wirksamkeit des Sicherheitssystems in unzulässiger Weise vermindern können.

4.4.4 Fehlauslösungen von Schutzaktionen

Fehlauslösungen von Schutzaktionen sind unter Einhaltung der Grundannahmen nach Abschnitt 4.4.1 zu verhindern, wenn sie zu einem Schaden führen können, der über die Auswirkungen der zu betrachtenden Störfälle hinausgeht. Auch während des Instandhaltungsfalls im Sicherheitssystem dürfen durch einen Zufallsausfall im Reaktorschutzsystem einschließlich Folgeausfällen keine Störfälle mit Schadensfolge herbeigeführt werden.

Die in den nationalen Regeln auf der Geräteebene

- KTA 3503 „Typprüfung von elektrischen Baugruppen der Sicherheitsleittechnik“, 11.2005

- KTA 3506 „Systemprüfung der leittechnischen Einrichtungen des Sicherheitssystems von Kernkraftwerken“, 11.1984

definierten Prüfanforderungen berücksichtigen das Themenfeld CCF nicht.

5.2 Übersicht über Regelungsinhalte im IEC, DIN IEC und DIN EN Regelwerk zum Lebenszyklus rechnerbasierter Sicherheitsleittechnik

Mit der Normenreihe IEC-SC45A wurde in den letzten Jahren ein geschlossenes Regelwerk zum Einsatz von Leittechnik für Systeme mit sicherheitstechnischer Bedeutung speziell in Kernkraftwerken entwickelt. Das Eingangsdokument zur IEC-SC45A-Normenreihe bildet die IEC 61513 [5.1], die allgemeine Anforderungen an die leittechnischen Systeme und Geräte zur Ausführung sicherheitstechnisch wichtiger Funktionen in Kernkraftwerken beinhaltet.

Die IEC 61513 „Nuclear power plants - Instrumentation and control for systems important to safety - General requirements for systems“ verweist als Norm der ersten Ebene auf weitere Normen der IEC-SC45A-Serie, die allgemeine Themen wie die Kategorisierung von Funktionen und die Klassifizierung von Systemen, Software-Anforderungen, Hardware-Aspekte rechnerbasierter Systeme, Qualifizierung, Trennung von Systemen, Maßnahmen gegen Versagen aufgrund gemeinsamer Ursache sowie Auslegung von Warten behandeln (Normen der zweiten Ebene). Die Normen der dritten Ebene der IEC-SC45A-Normenreihe behandeln spezielle Gerätschaften, technische Methoden oder spezifische Aktivitäten.

In den einleitenden Beschreibungen der Normen der IEC-SC45A-Serie wird dargelegt, dass die darin enthaltenen Anforderungen auf den Prinzipien und den grundsätzlichen Sicherheitsaspekten des IAEA-Codes für die Sicherheit von Kernkraftwerken und der IAEA-Sicherheitsserie umgesetzt werden. Hierzu werden insbesondere die Requirements NS-R-1 „Safety of Nuclear Power Plants: Design” [5.2] und der Safety-Guide NS-G-1.3 “Instrumentation and control systems important to safety in Nuclear Power Plants” [5.3] benannt. In der IEC-SC45A-Normenreihe stimmen die Terminologie und die Definitionen mit den von der IAEA angewandten überein.

Die Normenreihe IEC-SC45A wurde vom DKE-Gremium UK 967.1, das das nationale Spiegelgremium zur IEC-SC45A darstellt, als DIN-IEC respektive aktuell auch als DIN-EN-Normen in das deutsche Regelwerk überführt.

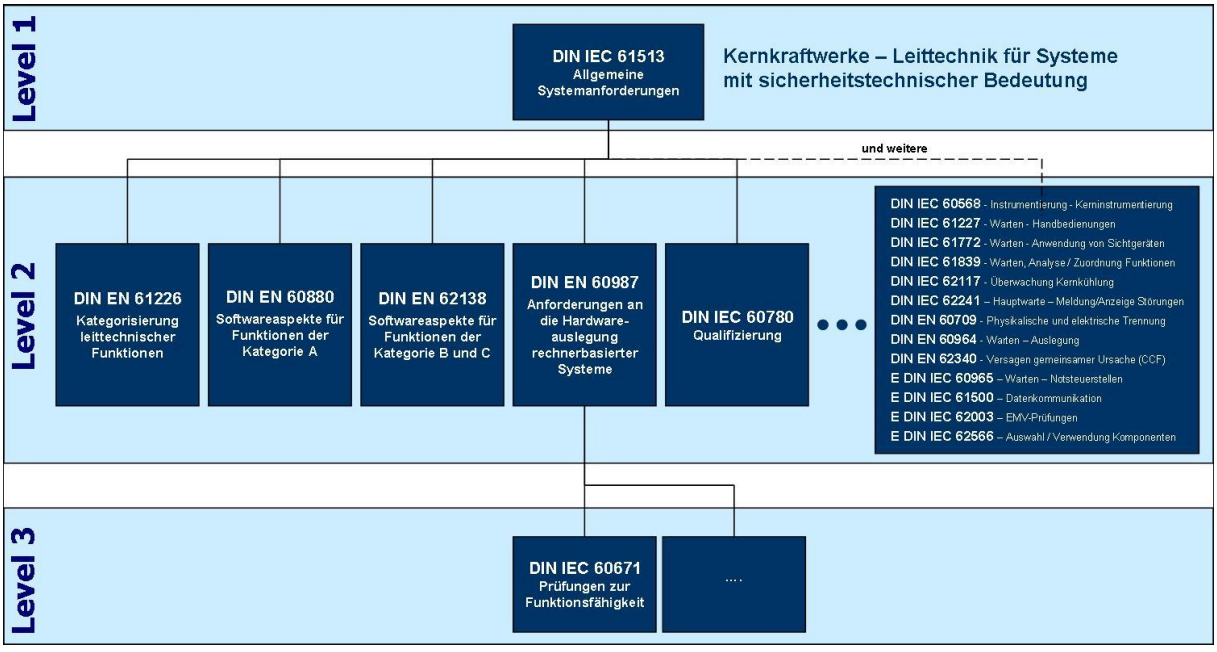

Abbildung 1: Übersicht über die in Deutschland gültigen DIN-IEC- und DIN-EN-Normen zur Leittechnik für Systeme mit sicherheitstechnischer Bedeutung in Kernkraftwerken

Das IEC-Regelwerk definiert mit der Normenreihe IEC-SC45A, die durch DIN-IEC- und DIN-EN-Normen in das deutsche Regelwerk überführt wurde bzw. wird, umfangreiche Anforderungen an die Projektierung und Dokumentation des Sicherheitslebenszyklus rechnerbasierter Leittechnik mit sicherheitstechnischer

Bedeutung in Kernkraftwerken. In diesen Normen sind Basisanforderungen zur Vermeidung und Beherrschung von CCF in rechnerbasierten Leittechniksystemen enthalten.

5.3 Anpassungsbedarf im deutschen Regelwerk

Die genannten nationalen Regelwerke spezifizieren infolge ihrer Stellung in der Regelwerkshierarchie keine detaillierten Nachweisverfahren und zugehörige Anforderungen.

Bei der Realisierung rechnerbasierter Leittechniksysteme verbleibt aufgrund der Komplexität der verwendeten Gerätetechnik sowie der Auslegung zu bewerten, ob die für eine Leittechnikarchitektur konzipierte Diversität bzw. Dissimilarität ausreichend zur Vermeidung und Beherrschung von CCF ist, da das Regelwerk diesbezüglich keine konkretisierten Bewertungskriterien und detaillierten Nachweisanforderungen enthält. Von besonderer Bedeutung für die Diskussion um die Auslegung rechnerbasierter Leittechniksysteme ist die Tatsache, dass der Nachweis vollständig fehlerfreier Systeme nicht möglich ist und somit latente Fehler prinzipiell nicht auszuschließen sind. Da deshalb für rechnerbasierte Leittechniksysteme ein CCF nicht ausgeschlossen werden kann, sind die in den Regelwerken enthaltenen Anforderungen zu Analysen und Nachweisführungen zu erfüllen, um die Wahrscheinlichkeit des Auftretens eines CCF innerhalb eines Teilsystems ausreichend zu reduzieren und das Auftreten eines CCF durch eine geeignete Gesamtarchitektur auf Teilsysteme zu beschränken und damit zu beherrschen.

Maßnahmen auf Geräteebene und zur Qualitätssicherung dienen der weitgehenden Vermeidung von CCF durch Sicherstellung einer hohen Qualität und Robustheit. Demgegenüber sind Maßnahmen zur Beherrschung von CCF in erster Linie auf Systemebene sinnvoll, so dass entsprechende Änderungen in den vorgenannten Systemregeln RSK-LL und KTA 3501 erforderlich sind.

Die kerntechnischen Normen des IEC-, DIN-IEC und DIN-EN liefern einen Rahmen für die Betrachtung von CCF und benennen bevorzugte Gegenmaßnahmen. Dies sind überwiegend Defence-in-Depth und die Anwendung funktionaler Diversität zusammen mit Maßnahmen zur Vermeidung einer Fehlerausbreitung. Sie bleiben mit ihren vorgeschlagenen Maßnahmen auf der Systemebene und behandeln die Ermittlung möglicher Common Cause (CC) Auslöser und Schwachstellen auf Geräteebene nur unzureichend.

Allerdings müssen für eine optimale und nachweisbare CCF Auslegung auf Systemebene zusätzlich die konkreten von der Systemebene abzudeckenden CC Auslöser und CC Schwachstellen auf Geräteebene soweit als möglich bekannt sein. Diesbezüglich ist nach Auffassung der AG ERL eine Anwendung von Verfahren, die über den gegenwärtigen Stand in den Normen des kerntechnischen Regelwerks hinausgehen, erforderlich (siehe Kapitel 5.4). Wie oben dargestellt, berücksichtigen die in den nationalen Regeln auf der Geräteebene

- KTA 3503 „Typprüfung von elektrischen Baugruppen der Sicherheitsleittechnik“, 11.2005

- KTA 3506 „Systemprüfung der leittechnischen Einrichtungen des Sicherheitssystems von Kernkraftwerken“, 11.1984

definierten Prüfanforderungen das Themenfeld CCF nicht. Zwar ist es gängige Praxis, neben der reinen Prüfung der Komponenten auch im Hinblick auf die CCF Problematik relevante Systemmerkmale in die Typprüfung mit einzubinden, jedoch hat diese Praxis derzeit noch keinen Niederschlag im nationalen Regelwerk gefunden. Mit gegenwärtigem Regelwerksstand sind somit zusätzliche Anforderungen erforderlich. Im Rahmen der anstehenden Überarbeitung der KTA 3503 ist eine entsprechende Ergänzung zusätzlich zu berücksichtigen. Hierauf wird in Kapitel 12 weiter eingegangen.

Wird der Ansatz gerätetechnischer Dissimilarität verfolgt, so erfordert dies eine Bewertung der angemessenen Dissimilarität. Somit muss zu dem bisherigen Nachweisumfang eine Prüfung und Bewertung der Unterschiedlichkeit der Gerätetechniken ergänzt werden, die wie die Typprüfung gegenüber der Anwendersicht vertiefte Systeminformationen auf Entwicklungsebene erfordert. Entsprechende Anforderungen sind hierzu noch festzulegen.

5.4 CCF Analyse

Wirksame Vorkehrungen zum Vermeiden oder Beherrschen von CCF setzen eine systematische Analyse der potenziellen CCF Mechanismen und Common Cause Auslöser für die jeweiligen Einsatzbedingungen voraus. Ziel der Analysen sollte sein, die potenziellen Common Cause- Mechanismen und Auslöser besser zu verstehen und davon ausgehend u.a. Funktions- oder/und Gerätediversität gezielt und wirksam einzusetzen. CCF Analysen können dabei sowohl als Verifikations- als auch Design-Methode eingesetzt werden.

Insgesamt ergeben sich hinsichtlich der Durchführung von CCF Analysen folgende Ergebnisse und Empfehlungen:

- CCF Analyse: Jede redundante Systemkonfiguration muss im Rahmen einer CCF Analyse auf ihr Verhalten in Bezug auf anzunehmende Common Cause Auslöser (CCI – Common Cause Initiator) untersucht werden, unabhängig davon, ob die Systemkonfiguration homogen redundant oder diversitär redundant aufgebaut ist.

- Analyseleitfaden: Das kerntechnische Regelwerk enthält derzeit keine Anforderungen bzgl. der CCF-Analyse. Die AG ERL empfiehlt daher zur Schaffung einer Basis für ein einheitliches Vorgehen zeitnah einen Leitfaden zur Durchführung von CCF Analysen auf Geräte- und Systemebene zu entwickeln, der die in verschiedenen Normen genannten Einzelverfahren FTA (Fehlerbaumanalyse), FMEA und CCA zusammenführt. Zusätzlich zu den kerntechnischen Normen des IEC Regelwerks sollen hierbei insbesondere die Normen [5.4] bis [5.9] herangezogen werden.

- CCI Katalog: Als Grundlage für die CCF Analysen sollte in diesem Rahmen ein Katalog mindestens zu betrachtender Auslöser für Software und Hardware CCF zusammengestellt werden. Der Katalog soll auf dem aktuellen Kenntnisstand hinsichtlich möglicher CCI basieren. Hierbei sind auch Erfahrungen mit in der Kerntechnik eingesetzten Leittechniksystemen einzubeziehen. Der Katalog soll von einer hierzu beauftragten Stelle auf aktuellem Stand gehalten werden. Hierzu sind Informationen zu möglichen CCI zu sammeln und zu bewerten. Dabei sollen Service Letter, die von Herstellern der in deutschen Anlagen eingesetzten, rechnerbasierten Sicherheitsleittechniksystemen herausgegeben werden, einbezogen werden.

- HALT Tests: In der Luftfahrt ist das HALT Testverfahren eingeführt (Highly Accelerated Lifetime Testing), das die Widerstandskraft eines Teilsystems gegenüber einem gleichzeitigen Einwirken einer Vielzahl externer Einflüsse ermittelt. Die Tests werden üblicherweise bis zum Ausfall der ersten Komponenten durchgeführt. Für rechnerbasierte Systeme, die im Rahmen von Reaktorschutzanwendungen eingesetzt werden sollen, sollte der HALT Test angewendet werden, außer es sind hieraus keine zusätzlichen Erkenntnisse zu erwarten. Für die Beurteilung, ob HALT Tests erforderlich sind, sollten die Testergebnisse aus der Typprüfung sowie der o.g. CCI Katalog herangezogen werden. Die in den HALT Tests komponentenspezifisch zu berücksichtigenden Stressoren sollten aus dem o.g. CCI Katalog abgeleitet werden.

- Verfolgung von Betriebserfahrung: Für rechnerbasierte Leittechniksysteme und Feldgeräte, die in Deutschland für Kategorie A und B eingesetzt werden, ist es zur Sicherstellung des erforderlichen hohen Zuverlässigkeitsniveaus wichtig, dass die Einsatzerfahrungen und Systeminformationen in einem gesicherten Informationsaustausch auch Behörden und Gutachtern bereitgestellt werden, damit die Umsetzung von eventuell erforderlichen Maßnahmen gewährleistet ist. Diese Informationen werden vom Hersteller i. A. in Form von Produktmitteilungen seinen Kunden mitgeteilt. Für den Informationsaustausch ist eine geeignete Vorgehensweise festzulegen, z. B. in Form von regelmäßigen bzw. im Anforderungsfall getriggerten Systemreports der Betreiber mit den vom Hersteller mitgeteilten Produktinformationen und den davon abgeleiteten Maßnahmen in der Anlage.

6 Aspekte zur CCF Vermeidung

6.1 Aspekte zur Arbeitsweise rechnerbasierter Sicherheitsleitsysteme, die Kategorie-A Funktionen ausführen

Die IEC Normen fordern für rechnerbasierte Sicherheitsleitsysteme eine Arbeitsweise, die diese Technik robust machen soll gegenüber einem triggernden Ereignis über den Prozess. Gemäß DIN IEC 61513 (Abschnitt 5.3.1.5) [6.1] sollen leittechnische Systeme der Klasse 1 und ihre Hilfssysteme so ausgelegt sein, dass sie unabhängig von Einflussfaktoren der Anlagenprozesse sind. Weiterhin wird in der DIN IEC 61513 (Abschnitt 6.1.1.2.2) u. a. die Anforderung gestellt, dass für Einrichtungen der Klasse 1 bestimmte Entwicklungstechniken anzuwenden seien, um ein hohes Maß von Verlässlichkeit bezüglich des

deterministischen Verhaltens sicherzustellen.[2] In der DIN EN 62340 [6.2] wird in Abschnitt 8.1 für leittechnische Systeme, die Kategorie-A Funktionen ausführen, gefordert, dass sie in ihrer Betriebs- und Arbeitsweise keine Abhängigkeit vom Anforderungsprofil aufweisen. Diese übergeordnete Anforderung wird durch Einzelanforderungen unterlegt.

Nach IEC Regelwerk ausgelegte softwarebasierte digitale Automatisierungsgeräte für Reaktorschutzsysteme sollen somit sequenziell und zyklisch arbeiten und ein hohes Maß von Verlässlichkeit bezüglich eines deterministischen Verhaltens aufweisen. Diese Anforderungen des IEC Regelwerks gelten für alle leittechnischen Systeme, die Kategorie-A Funktionen ausführen, das heißt u. a. für:

- Messwerterfassung für das Reaktorschutzsystem;
- Reaktorschutzsystem;
- Vorrangsteuerung incl. vorrangiger Aggregateschutz;
- Leittechnik der benötigten Hilfssysteme (z. B. Notstromversorgung).

Es ist festzustellen, dass in der Praxis außerhalb der zentralen Leittechnik (Reaktorschutzsystem) auch für Kategorie-A Funktionen in Einzelfällen Geräte eingesetzt werden, die nicht allen Anforderungen des IEC Regelwerks genügen. Hintergrund ist, dass nicht für alle Anwendungen gemäß IEC ausgelegte Gerätetechnik zur Verfügung steht und somit auf industrielle Standardprodukte zurückgegriffen werden muss. Hieraus leiten sich folgende Anforderungen ab:

- Für die Ausführung von Kategorie-A Funktionen sind grundsätzlich Geräte einzusetzen, die den Anforderungen des IEC Regelwerks zur Arbeitsweise rechnerbasierter Leittechnik, die Kategorie-A Funktionen ausführt, genügen (insbesondere IEC 61513, 60880, 62340). Insbesondere sollen alle rechnergestützten Geräte der Kategorie-A Leittechnik (Zentralgeräte, Peripherie) auf einer streng sequentiellen und zyklischen SW-Verarbeitung basieren und ein hohes Maß von Verlässlichkeit bezüglich eines deterministischen Verhaltens aufweisen (Predictability). Eingriffe in die zeitliche Abarbeitung und in die Abarbeitungsreihenfolge, wie beispielsweise durch Interrupts oder andere HW-Einheiten, und Eingriffe auf Daten durch andere HW-Einheiten müssen begründet sein und durch zusätzliche Sicherheitsmaßnahmen beherrscht werden.

- Sofern in Einzelfällen für Kategorie-A Funktionen keine Gerätetechnik, die den Anforderungen des IEC Regelwerks zur Arbeitsweise rechnerbasierter Leittechnik entspricht, zur Verfügung steht, sind Abweichungen der Arbeitsweise auszuweisen und es ist nachzuweisen, dass durch diese Arbeitsweise und damit zu unterstellende CCF keine unzulässigen sicherheitstechnischen Auswirkungen in der Anlage resultieren können.

[2] "c) In order to provide a high degree of assurance of deterministic behaviour, class 1 systems should be developed using techniques such as those of appendix B of IEC 60880 (notably B2.d on execution time and B2.e on interrupts). Techniques using static scheduling of operations (see note 2) are preferable to those using interrupts."

6.2 Aspekte grundlegender Qualitätsanforderungen an der Schnittstelle Verfahrenstechnik / Leittechnik

In der DIN EN 62340 [6.2] wird der Anwendung funktionaler Diversität als Mittel zur Gewährleistung von Unabhängigkeit und zur CCF Beherrschung eine hohe Bedeutung beigemessen. Hintergrund ist, dass funktionale Diversität durch unterschiedliche Aufgabenstellungen dazu beiträgt, die Auswirkungen der beiden folgenden Fehlerarten einzugrenzen:

a) Fehler in der Aufgabenstellung;
b) Fehler bei der Implementierung der Aufgabenstellung (betrifft die Anwendungssoftware).

Die Umsetzung funktionaler Diversität ist in den bestehenden deutschen Anlagen nur bedingt möglich.

Da die hohe Qualität bei der Erstellung und Umsetzung der Aufgabenstellung eine wichtige Grundlage dafür ist, dass die Wahrscheinlichkeit für einen CCF minimiert werden kann, gewinnen Qualitätssicherungsmaßnahmen zur Vermeidung der genannten Fehlerarten eine zusätzliche Bedeutung. Dazu sollte die Aufgabenstellung in einer Sprache spezifiziert werden, die zum einen eindeutig ist und zum anderen von Leittechnikern und Verfahrenstechnikern gleichermaßen verstanden wird. Hinzu kommen zusätzliche Anstrengungen zur Fehleraufdeckung wie erweiterte Prüfverfahren, closed-loop Simulationen und Simulationen unter Einbeziehung der Verfahrenstechnik. Hieraus leiten sich insgesamt folgende Anforderungen ab:

- Durch hohe Qualität bei der Erstellung der verfahrenstechnischen Aufgabenstellung und bei der Bearbeitung der Aufgabenstellung an der Schnittstelle Leittechnik / Verfahrenstechnik sowie durch geeignete Prüfverfahren und Simulationen muss die Vollständigkeit und korrekte Implementierung der Aufgabenstellung sichergestellt werden.

  Die verfahrenstechnische Aufgabenstellung muss demnach:

  - alle sicherheitsrelevanten Merkmale berücksichtigen (Vollständigkeit);
  - eindeutig sein und in formalisierter Weise spezifiziert werden;
  - einfach sein, so dass eine vollständige Prüfung möglich ist;
  - auch Testfälle und die erwarteten Testergebnisse umfassen, durch welche die Korrektheit der Implementierung geprüft werden kann.

  Geeignete Prüfverfahren und Simulationen im Hinblick auf die Vollständigkeit und korrekte Implementierung der Aufgabenstellung sind insbesondere:

  - Closed Loop Simulationen („wissende Tests“) mit Berücksichtigung der Rückwirkungen aus dem Prozess (z. B. gestaffelte Ansteuerungen von Komponenten);
  - Systemprüfung im Prüffeld (Integrationstest).

Zu beachten ist weiterhin, dass alle Anlagenzustände in der Spezifikation ausreichend berücksichtigt werden müssen. Die bedeutet, dass auch Sonderzustände, die in den Anlagen auftreten können (z. B. Freischaltungen), in der ausreichenden Tiefe betrachtet werden müssen. Die verfahrenstechnische Aufgabenstellung muss demnach explizite Aussagen enthalten,

- in welchen Betriebszuständen die entsprechende Funktion verfügbar sein muss,
- welche Zustände an den Schnittstellen aufgrund von Prüf- und Reparaturtätigkeiten zu berücksichtigen sind.

Im Hinblick auf die Fehlerart b) kann eine unabhängige Implementierung der Aufgabenstellung mittels unterschiedlicher Entwicklungsumgebungen durch verschiedene Entwicklerteams die Wahrscheinlichkeit für identische implementierungsbedingte Fehler reduzieren. Dies ist z. B. dann der Fall, wenn unterschiedliche Gerätetechnik mit von unterschiedlichen Herstellern entwickelter Anwendungssoftware eingesetzt wird.

7 Diversität als Beitrag zur CCF Vermeidung / Beherrschung

7.1 Diversifizierung interner Zustände der Rechner

Fehler, die sich aufgrund bestimmter interner Zustände von Rechnern ergeben, können durch Eingrenzung auf wenige Rechner beherrscht werden, sofern ausreichend unterschiedliche interne Zustände der Rechner erzwungen werden. Das DIN IEC Regelwerk verlangt, dass unabhängige leittechnische Systeme bei unterschiedlichen Signaltrajektorien betrieben werden (DIN IEC 61513 [7.1] – Ziffer 5.3.1.5). Hintergrund dieser Anforderung ist, dass identische innere Zustände der Rechner vermieden werden sollen. Gemäß DIN IEC 61513 kann dies durch Diversität sichergestellt werden (z. B. Gerätediversität oder funktionale Diversität).

In der DIN IEC 62340 (Ziffer 5.5) [7.2] wird festgestellt, dass die Zuordnung von diversitären Funktionen zu unabhängigen leittechnischen Systemen als ein Mittel benutzt werden kann, um unterschiedliche Signaltrajektorien beim Betrieb der leittechnischen Systeme sicherzustellen. In Abschnitt 7.3.1 wird gefordert, dass funktionale Diversität angewendet werden muss, um die „Eingangssignal“-Komponente der Signaltrajektorien zu diversifizieren.

Im Wesentlichen bestimmen die Sicherheitsfunktionen die internen Zustände der jeweiligen Rechner. Sie stellen für die Hardware und das Betriebssystem die Lasten dar. Makroskopisch über das ganze System gesehen sind keine Laständerungen vorhanden, mikroskopisch bezogen auf die einzelnen CPU allerdings sehr wohl. Die Kette „Unterschiedliche Sicherheitsfunktionen → unterschiedliche Lasten auf mikroskopischer Ebene → unterschiedliche innere Zustände der Rechner“ bildet den Hintergrund dafür, dass die funktionale Diversität als mögliches Mittel zur Eingrenzung eines CCF durch Diversifizierung der

internen Zustände der Rechner eingestuft wird[3]. Wie bereits festgestellt, ist die Umsetzung funktionaler Diversität in den bestehenden deutschen Anlagen nur bedingt möglich. Daher sind andere Maßnahmen zur Diversifizierung der internen Rechnerzustände erforderlich. Hieraus leiten sich folgende Mindestanforderungen ab:

- Die Diversifizierung der internen Zustände der Rechner muss bei fehlender funktionaler Diversität durch leittechnische Mittel oder Gerätediversität erreicht werden. Geeignete Maßnahmen zur Diversifizierung der internen Zustände bei homogener Gerätetechnik können insbesondere sein:

  - unterschiedliche Belegung der Ein-/Ausgabekanäle,
  - unterschiedliche Abarbeitungsfolge der leittechnischen Funktionen,
  - unterschiedliche Normierung der verwendeten Messsignale,
  - Unsymmetrische Implementierung zusätzlicher Überwachungsfunktionen,
  - Unterschiedliche Implementierung der Funktionen.

Für die realisierten Maßnahmen ist aufzuzeigen, dass sie im Hinblick auf die Diversifizierung innerer Zustände eine ausreichende Wirksamkeit entfalten.

Wird unterschiedliche Gerätetechnik mit unterschiedlicher Betriebssystemsoftware eingesetzt, sind unterschiedliche interne Zustände der unterschiedlichen Rechner auslegungsbedingt gegeben.

[3] **Kommentar Dr. Graf:**
Die Diversifizierung der internen Zustände dient der Eingrenzung eines möglichen CCF für nicht zyklische Lastfälle. Für rein zyklisch benutzte Dienste (HW +SW) kann nach Ablauf eines Zyklus der CCF ausgeschlossen werden, da es keinen Auslöser gibt. Über die Anwendung gibt es aber auch nicht zyklische Lastfälle. Da die Messsignale vom Prozess sich nicht zyklisch ändern, wird beispielsweise der Speicherbereich, in welchem die davon abgeleiteten Rechenergebnisse abgelegt sind, von stetig unterschiedlichen Werten belegt. Bei genau diesen nicht zyklisch benutzen Diensten wirkt die von IEC geforderte Diversifizierung.

1. Kommentar von Vertretern der Architektur 1: *Beschreibung Architektur: siehe Kapitel 8*

Im Gegensatz zu dem großen Nutzen der funktionalen Diversität für die Fehlertypen a) und b) des Abschnitts 6.2 in der Anwendersoftware wird der Effekt für eine Erzwingung von unterschiedlichen Zuständen für die System-HW und SW als nicht wirksam bewertet.

Eine Diversifizierung der inneren Zustände der System-HW und -SW (d.h. nicht in der Anwendersoftware, die die programmtechnische Umsetzung der Funktionspläne darstellt) ist aufgrund der gemäß DIN EN 60880 geforderten Eigenschaften nicht realisierbar. So widerspricht sich die geforderte streng zyklische Arbeitsweise der Systemsoftware, die unabhängig von der Einflussfaktoren des Anlagenprozesses und getrennt von der Anwendersoftware sein soll, und die Invarianz von Verarbeitungs- und Kommunikationslast mit der beabsichtigten Beeinflussung der inneren Zuständen der System-HW und -SW durch die Messsignale des Anlagenprozesses. Dies gilt sowohl für die funktionale Diversität als auch die Verwendung diversitärer Messgeräte. Hierbei ist zu beachten, dass bei der Verwendung diversitäter Messgeräte für die gleiche physikalische Messgröße nur Sensoriken mit unterschiedlichen physikalischen Messprinzipien genutzt werden. Von den analogen Messumformern wird im Allgemeinen ein Signal von 0/4 - 20 Milliampere ausgegeben und wird anschließend in den meisten Fällen in ein 0 – 10 V Signal umgewandelt. Die unterschiedlichen Messprinzipien und die Signalwandlung führen jedoch nicht dazu, dass die Trajektorien der Signale sich unterscheiden. Über die in der Spiegelstrichliste genannten Ersatzmaßnahmen wird im Allgemeinen eine noch geringere Diversifizierung der Eingangssignale erreicht. Das bedeutet, dass der Nachweis der Wirksamkeit der vorgeschlagenen Diversifizierungsmaßnahmen hinsichtlich der Verhinderung von CCF nicht erbracht werden kann.

Bereits in der DIN EN 62340, 5.5 wird zur Sicherstellung von unterschiedlichen Signaltrajektorien (die entsprechend der Definition auch die inneren Zustände des Rechnersystems umfassen) neben der funktionalen Diversität auch die Gerätediversität (hier Dissimilarität) als Maßnahmen genannt. Ebenso wird unter 7.3 der Effekt der funktionalen Diversität auf die „Eingangssignal“-Komponente der Signaltrajektorie eingeschränkt und darauf hingewiesen dass auch die anderen Teile der Trajektorie, wie z. B. die inneren Zustände, betrachtet werden müssen. Ein Effekt für eine Erzwingung von unterschiedlichen inneren Zustände kann sich nur durch den Einsatz von nachgewiesen dissimilaren Verarbeitungsebenen ergeben.

1. Kommentar von Vertretern der Architektur 2 *Beschreibung Architektur: siehe Kapitel 8*

Die nach DIN IEC 62340 geforderten Systemeigenschaften stellen sicher, dass sich die weit überwiegenden Anzahl der internen Zustände eines Rechners nicht ändern oder aber zyklisch ändern und somit keinen CCF auslösen können. Jedoch verbleiben einige wenige interne Zustände, die über die berechneten Funktionen beeinflusst werden, da z.B. auch die Ergebnisse der Berechnung einer Funktion in Speicherbereichen abgelegt werden und damit eine Teilmenge der internen Zustände sind. Um einen CCF einzugrenzen, der über diese wenigen beeinflussbaren internen Zustände ausgelöst werden könnte, fordert die DIN IEC 62340, diversitäre Funktionen in unabhängigen leittechnischen Systemen zu implementieren. Der Gedanke zur

CCF-Vermeidung beruht hier darauf, dass ein latenter, bisher evtl. nicht entdeckter systematischer Fehler in verschiedenen Strängen gleichzeitig getriggert werden müsste, um zu einem CCF zu kommen. Entsprechend wird angestrebt, dass in den unabhängigen Teilsystemen identische Zahlen, Zahlenkombinationen und Abfolgen nicht gleichzeitig auftreten. Für die Wirksamkeit dieser Maßnahme ist es dabei völlig unerheblich, ob tatsächlich physikalisch diversitäre Funktionen implementiert werden oder ob dieselben Funktionen in unterschiedlicher Weise implementiert werden. Beide Maßnahmen haben zur Folge, dass die wenigen internen Zustände der Rechner, die über diese Funktionen beeinflusst werden können, unterschiedlich sind.

7.2 Gegenüberstellung realisierter Architekturen in den USA, in Frankreich, in Japan, und in Finnland im Hinblick auf Verwendung diversitärer Systeme

In diesem Kapitel wird dargestellt, welche Lösungen für digitale Sicherheitsleittechnik in Kernkraftwerken in unterschiedlichen Ländern von den Genehmigungsbehörden akzeptiert wurden und auf dieser Basis realisiert wurden oder in der Realisierung befindlich sind. Die Darstellung konzentriert sich auf die Architekturprinzipien und die Einordnung in das Sicherheitskonzept sowie die Verwendung einer diversitärer Auslegung für leittechnischen Einrichtungen, die identischen oder unterschiedlichen Sicherheitsebenen zugeordnet sind. Unter dem Begriff „Sicherheitsleittechnik“ werden hier der Reaktorschutz sowie weitere leittechnische Einrichtungen zur Beherrschung von Störfällen mit Überlagerung von CCF zusammengefasst.

USA

Als Beispiel für ein in den USA akzeptiertes Auslegungskonzept für die digitale Sicherheitsleittechnik wird die Nachrüstung für das Reaktorschutzsystem im Kernkraftwerk Oconee, Blöcke 1 bis 3, herangezogen, für die von der U.S. NRC im Januar 2010 die Genehmigung erteilt wurde. Die folgende Darstellung basiert auf dieser Genehmigung [7.3].

Das neue Reaktorschutzsystem im Kernkraftwerk Oconee besteht aus einer Kombination eines primären, redundanten digitalen Reaktorschutzsystems mit diversitären redundanten Backup-Systemen in unterschiedlicher technischer Ausführung.

Das primäre digitale Sicherheitsleittechniksystem ist aufgeteilt in das Reactor Protection System (RPS) zur Anregung der Reaktorschnellabschaltung (RESA) und das Engineered Safeguards Protection System (ESPS) zur Ansteuerung der Sicherheitssysteme. Das RPS ist vierkanalig aufgebaut (2v4-Auswahl), das ESPS in zwei Teilsystemen mit je drei Kanälen (2v3-Auswahl). Dabei ist das eine ESPS-Teilsystem auf den Hardwarekomponenten von drei Kanälen des RPS implementiert, das andere ESPS-Teilsystem auf eigenen Komponenten. Die ESPS-Teilsysteme sind auf identischer Hardware mit identischer Software realisiert, d.h. ohne Diversitätsmerkmale.

Die diversitären Backup-Funktionen zur Beherrschung von Auslegungsstörfällen mit einem überlagerten Software-CCF sind auf mehrere Systeme aufgeteilt. Zum einen wird ein bereits bislang bestehendes, zweikanaliges ATWS-System (PLC-Technik) zur Abdeckung von Transienten verwendet, zum anderen

wurde ein festverdrahtetes, dreikanaliges System (mit 2v3-Auswahl) zur Beherrschung von kleinen und großen Kühlmittelverluststörfällen nachgerüstet. Die Backup-Systeme sind ständig aktiv und verfügen über eigene Anregekriterien. Sie erfüllen Qualitätsanforderungen basierend auf den Anforderungen für Standard-Industriesysteme.[4] Von Handmaßnahmen wird (mit einer, von der NRC bewerteten Ausnahme) nur Kredit genommen, wenn sie nicht in den ersten 30 Minuten nach Störfalleintritt erforderlich sind.

Der Gesamtaufbau der Sicherheitsleittechnik umfasst damit ein redundantes Reaktorschutzsystem kombiniert mit diversitären Backup-Systemen mit einem hinsichtlich des betrachteten Ereignisspektrums weitgehend abdeckenden Funktionsumfang in redundanter Ausführung.

Frankreich

Die französische Praxis wird hier mit Bezug auf die Auslegung der Sicherheitsleittechnik des 1996 in Betrieb genommenen Kernkraftwerkes Chooz B aus der Reaktorserie N4 dargestellt.

Gemäß den Darstellungen in NUREG/CR-7007 [7.4] besteht die Sicherheitsleittechnik des N4 aus einem primären Reaktorschutzsystem und einem dazu diversitären Backup-System, wobei es sich bei beiden Systemen um softwarebasierte digitale Leittechniksysteme handelt.

Das primäre Reaktorschutzsystem ist grundsätzlich viersträngig aufgebaut mit 2v4-Auswahlschaltungen, in Teilen zweimal viersträngig. Im primären Reaktorschutzsystem sind Elemente der funktionalen Diversität und unterschiedliche Signalpfade durch die Verwendung diversitärer Prozessgrößen verwirklicht, unterstützt durch die Implementierung von Rechenschaltungen für verschiedene Funktionen auf unterschiedlichen Prozessoren.

Das sekundäre Backup-System (ATWS-System) beherrscht ein eingeschränktes Spektrum auslösender Ereignisse. Es wird gemäß NUREG/CR-7007 ausschließlich über das Kriterium „niedriger Dampferzeugerfüllstand“ angeregt, das die nach probabilistischen Analysen häufigsten Transienten abdeckt. Das Backup-System ist auf einer zum primären Reaktorschutzsystem unterschiedlichen Hardware und mit einer anderen Programmiersprache auf der Anwendungsebene implementiert. An das System werden – abgestufte – Qualitätsanforderungen gestellt.

Grundsätzlich ist damit ein Gesamtsystem mit hohem Redundanzgrad im primären Reaktorschutzsystem und vermindertem Funktionsumfang für die Leittechnik des diversitären Backupsystems realisiert.

Japan

Auch diese Darstellung fußt auf den Ausführungen in NUREG/CR-7007 [7.4], in diesem Fall für die Referenzanlagen Kashiwazaki-Kariwa 6 und 7, die 1996 bzw. 1997 in Betrieb genommenen ersten Advanced boiling-water reactors (ABWR).

[4] NRC Generic Letter 85-06, „Quality Assurance Guidance for ATWS Equipment“.

Die Sicherheitsleittechnik dieser Kernkraftwerke besteht aus einem primären, digitalen Reaktorschutzsystem und einem festverdrahteten Backup-System (ATWS-System).

Das primäre Reaktorschutzsystem ist vierfach redundant mit 2v4 Auswahlschaltungen in digitaler Technik aufgebaut. Im Reaktorschutzsystem wird soweit möglich funktionale Diversität verwendet. Dabei wird bei mehreren Sicherheitsfunktionen auf diversitäre technische Realisierungen zurück gegriffen (z.B. zwei unterschiedlich Hochdruck-Einspeisesysteme). Der Einführung der Digitaltechnik im Reaktorschutzsystem ging ein langjähriger Prozess für die Einführung von digitalen Leittechniksystemen in japanischen Kernkraftwerken voraus, zunächst auf der betrieblichen Ebene, dann bei der Steuerung von Sicherheitssystemen. Aufgrund dieser langjährigen Erfahrung und der Verwendung bewährter Software-Entwicklungstools wird das CCF-Potenzial in Japan als niedrig eingeschätzt.

Das diversitäre Backup-System (ATWS-System) in festverdrahteter Technik verfügt über einen begrenzten Funktionsumfang. Es kann die Reaktorschnellabschaltung über einen diversitären Mechanismus und das Herunterfahren der Zwangsumwälzpumpen auslösen. Darüber hinaus wird von der Handanregung von Sicherheitsfunktionen Kredit genommen. Dazu ist ein eigenes, festverdrahtetes Leittechniksystem installiert, mit dem über Hardware-Schalter und -Logikschaltungen einige ausgewählte Sicherheitsfunktionen vom Personal von der Warte aus ausgelöst werden können. Die Auslösewege sind unabhängig von und diversitär zum digitalen Schutzsystem.

Damit entspricht der Aufbau der Sicherheitsleittechnik in den japanischen Anlagen Kashiwazaki-Kariwa 6 und 7 einer Kombination aus Redundanz im Reaktorschutzsystem unter Einsatz funktionaler Diversität und einem diversitären Backup-System mit eingeschränktem Funktionsumfang.

Finnland

Auch beim EPR in Finnland wird gemäß NUREG/CR-7007 [7.4] für die Sicherheitsleittechnik eine Kombination aus einem redundanten primären digitalen Reaktorschutzsystem und einem Backup-System in anderer technischer Ausführung verwendet.

Das primäre Reaktorschutzsystem in digitaler Technik besteht aus zwei Teilsystemen, die jeweils vierfach redundant aufgebaut sind. Für die Teilsysteme wird gemäß NUREG/CR-7007 funktionale Diversität angewandt durch Verwendung unterschiedlicher Parameter und funktionaler Beziehungen für die auslösenden Ereignisse. Das soll zu unterschiedlich programmierter Anwendungssoftware bei identischer Hardware und identischem Betriebssystem führen.

Das Backup-System besteht zum einen aus einem digitalen Leittechniksystem mit vom Reaktorschutzsystem unterschiedlicher Hard- und Software für die Beherrschung der häufigeren auslösenden Ereignisse. Zudem gibt es ein HW-Backup-System mit programmierbaren Logikbausteinen (PLD-Technologie), das zur diversitären Auslösung der Reaktorschnellabschaltung dient, sowie die Möglichkeit zur manuellen Auslösung von Schutzaktionen. Das digitale Backup-System ist zweifach redundant aufgebaut, das HW-Backup-System vierkanalig (2v4-Auswahl).

Damit liegt ein Gesamtsystem mit Diversitätsmerkmalen auf der Ebene des Reaktorschutzsystems kombiniert mit einem diversitären (hier sogar doppelt diversitär) Backup-System mit eingeschränktem Funktionsumfang vor.

8 Darstellung von zwei Architekturen zur Beherrschung des CCF im Rahmen des gestaffelten Sicherheitskonzepts

In der AG ERL sind vertieft zwei Architekturansätze für den Einsatz rechnerbasierter Technik in Reaktorschutzsystemen diskutiert worden. Der erste Ansatz beruht auf dem Einsatz dissimilarer Gerätetechnik, der zweite Ansatz beruht auf dem Einsatz von zwei unabhängigen RS-Teilsystemen mit Diversitätsmerkmalen[5] sowie von „Zusätzlichen Leittechnischen Einrichtungen“ (ZLE). Darüber hinaus sind auch noch andere Architekturen denkbar, die aber von der AG ERL nicht beraten wurden.

Hinsichtlich der Notwendigkeit eines Einsatzes von Diversität zur CCF Beherrschung gilt nach Auffassung der AG ERL für beide Ansätze:

- Für ein (weitgehend) homogenes, redundant aufgebautes und rechnerbasiertes System kann das Auftreten eines CCF als nicht so unwahrscheinlich angesehen werden, dass dieser bei Einsatz des Systems im Reaktorschutz auf der SE 3 nicht unterstellt werden müsste. Somit sind zur CCF Beherrschung mindestens zwei unabhängige (Teil)Systeme einzusetzen.[6]

- Diversität ist ein notwendiges (aber nicht hinreichendes) Mittel zur Sicherstellung eines unabhängigen Versagensverhaltens von Teilsystemen der Sicherheitsleittechnik. Zur Beherrschung des CCF Potenzials rechnerbasierter Systeme ist im Rahmen der Gesamtarchitektur der Einsatz diversitärer Teilsysteme erforderlich.

- Diversität ist gezielt und unter Berücksichtigung möglicher CCF Mechanismen einzusetzen (d.h. es sind für das angestrebte Ziel geeignete Diversitätsentscheidungen zu treffen). Hierfür sind entsprechende CCF Analysen vorzunehmen (siehe DIN IEC 61513 und zugehörige Normen).

- Mittels CCF Analysen kann nicht gänzlich ausgeschlossen werden, dass bislang unbekannte und in den Analysen daher unberücksichtigte Fehlertypen oder Auslöser zu einem CCF führen.

Hinsichtlich einer geeigneten leittechnischen Gesamtarchitektur bestehen in der AG ERL unterschiedliche Auffassungen. Sie liegen begründet in unterschiedlichen Einschätzungen zur Belastbarkeit der Ergebnisse von CCF Analysen – das heißt in der Wahrscheinlichkeit, dass in den Analysen nicht berücksichtigte CCF Mechanismen wirksam werden – sowie zur Belastbarkeit von Nachweisen bzgl. der Wirksamkeit von implementierten Funktionen für ein gerichtetes Versagensverhalten (zu diesem wesentlichen Aspekt siehe Kapitel 9). Hieraus ergeben sich zwei unterschiedliche Ansätze für die Gesamtarchitektur.

[5] Dissimilarität zwischen den RS-Teilsystemen wird nicht gefordert.

[6] Anforderungen an unabhängige leittechnische Systeme sind u. a. in den Abschnitten 7.1 und 7.2 der Norm IEC 62340 enthalten.

Die **Architektur 1** legt den Schwerpunkt bei den CCF Maßnahmen nicht allein auf die Gerätequalität die im Rahmen der Typprüfung nachgewiesen wird, da ein vergleichbar tiefgreifendes Verständnis aller Eigenschaften der Geräte wie bei der bisherigen Technik bei der modernen Gerätetechnik als nicht erreichbar angesehen wird. Deshalb werden zusätzlich ergänzende architektonische Lösungsansätze mit dem Einsatz dissimilarer Gerätetechnik im Rahmen einer darauf abgestimmten Gesamtarchitektur als erforderlich angesehen. Die Bewertung der angemessenen Dissimilarität, d. h. eine Prüfung und Bewertung der Unterschiedlichkeit der Gerätetechniken, muss zu dem bisherigen Nachweisumfang ergänzt werden, wobei Informationen aus den Typprüfungen bei der Bewertung der Dissimilarität genutzt sollten. Wie bei der Typprüfung sind für diese Prüfung Informationen über die Geräteentwicklung erforderlich, um die Unterschiedlichkeit der Funktions- und Implementierungsprinzipien sowie das Fehlen von Gemeinsamkeiten z. B. bei Algorithmen, HW- und SW-Komponenten und Werkzeugen festzustellen.

Architektur 1 erfordert den Einsatz von mindestens zwei unabhängigen und dissimilaren RS-Teilsystemen. In Abhängigkeit von den möglichen Konsequenzen aktiven Funktionsversagens sind für bestimmte Funktionen ggf. drei unabhängige und dissimilare RS-Teilsysteme sowie evtl. eine Auswahlschaltung (Voter) erforderlich oder eine Realisierung in festverdrahteter Technik auf Basis diskreter Bauelemente (siehe Kapitel 9). Ein durch die Gerätetechnik verursachter CCF, der mehr als ein RS-Teilsystem betrifft, wird infolge der dissimilaren Auslegung als so unwahrscheinlich angesehen, dass dies praktisch ausgeschlossen wird. Im Falle eines CCF eines der RS-Teilsysteme steht somit immer das dazu dissimilare Teilsystem (bzw. die dissimilaren Teilsysteme) zur Ereignisbeherrschung zur Verfügung. Zusätzliche Maßnahmen auf der SE 4 werden nicht gefordert, da mit den auf SE 3 vorgesehenen Maßnahmen bereits eine Beherrschung von CCF erreicht werden muss.

2. Kommentar der Vertreter der Architektur 2:

Zur Beherrschung des aktiven Funktionsversagens fordert die Architektur 1 drei dissimilare RS-Teilsysteme, die über eine Auswahlschaltung (Voten) verknüpft sind. Genau in dieser Verknüpfung der drei unterschiedlichen Gerätesysteme auf Systemebene wird eine nicht zu vernachlässigende Gefahr von neuen und noch komplexeren Fehlermodi mit dem Potential zum CCF Versagen gesehen. Die Auswahlschaltung schafft zum einen Abhängigkeiten zwischen den dissimilaren RS-Teilsystemen, indem sie Schutzanforderungen erst dann auslösen, wenn sie mindestens bei zwei der drei RS-Teilsysteme anstehen und da sie damit gleichzeitig auch das Zeitverhalten der Schutzanforderungen verändern.

Es gibt im Bereich der Kerntechnik weltweit keinerlei Betriebserfahrung mit derartigen Systemarchitekturen in Reaktorschutzanwendungen, so dass der Vorteil dieser neuen Systemarchitektur gegenüber den weltweit bewährten Backup-Lösungen nicht nachvollziehbar ist.

Architektur 1 ist wie folgt begründet:

- Komplexität der modernen Gerätetechnik: Mit der Einführung der rechnerbasierten Leittechnik ist eine starke Konzentration der Leittechnikfunktionen (LEFU) auf nur wenige Baugruppen verbunden. Weiter besitzt die Gerätetechnik der rechnerbasierten Leittechnik gegenüber der festverdrahteten eine höhere Funktionalität und Varianz. Weiterhin ist durch den Übergang auf

serielle Verarbeitung, die neuen Entwicklungs- und Fertigungstechnologien mit hochintegrierten Commercial-of-the-shelf-(COTS-)Bauteilen und -Softwareelementen in die moderne Gerätetechnik ein weit höherer Entwicklungsaufwand eingeflossen als bei der bisherigen Technik. Dies führt insgesamt zu einer erheblichen Erhöhung der Komplexität innerhalb der Gerätetechnik und damit zu einem schwerer zu prognostizierenden Verhalten bei Ausfällen bzw. Versagen, was nicht allein über das bisherige Verfahren zur Typprüfung angemessen aufgefangen werden kann.
Diese Argumente werden auch bei Nutzung einfacher Funktionsprinzipien nicht entkräftet. Auch wenn in der Gerätetechnik Funktionsprinzipien in der Systemsoftware analog zu den Forderungen des IEC-Regelwerks (siehe Kapitel 6.1) implementiert werden und damit eine höhere Robustheit erreicht wird, bestehen weiterhin die aufgeführten Problematiken z. B. zur Komplexität und Einschränkung der Prüfbarkeit. In Hinblick auf mögliche CCF kann die Beurteilung der Gerätetechnik nicht auf diese „einfachen Funktionsprinzipien“ reduziert werden und damit die Technik als „einfach“ vergleichbar zu der eingesetzten festverdrahteten Technik eingestuft werden.

- Kurze Innovationszyklen; Ein Betriebsbewährungsnachweis ist wegen des schnellen Innovationswandels und der hohen Komplexität der rechnerbasierten Technik nur noch eingeschränkt zielführend.

- Prüfbarkeit; Die in der rechnerbasierter Gerätetechnik verwendeten COTS-Bauteile entziehen sich oftmals einer detaillierten Beurteilung (Fehlen von entsprechenden Entwicklungsunterlagen usw.). Dies betrifft sowohl den Hersteller der Gerätetechnik, den Betreiber als auch die Sachverständigen. Die damit zusammenhängenden Schwierigkeiten werden am Beispiel des Sachverständigen dargestellt, gelten aber auch für die anderen am Prozess Beteiligten. Zusätzlich führt eine kaum überschaubare Vielfalt von Prozessortypen, Rechnerarchitekturen , Betriebssystemen, Programmiersprachen, Engineeringtools, spezifischen Controller-Bausteinen, Kommunikationsprotokollen usw. dazu, dass die Prüfer nur noch relativ gering in die Tiefe gehen können. Die Erfahrung zeigt, dass die Prüfungen letztlich dazu dienen, die Dokumente auf einem regelkonformen Stand zu halten, die grundlegenden funktionalen Anforderungen nachzuweisen und aufzuzeigen, ob autorisierte Stellen die erforderlichen Umweltprüfungen durchgeführt haben. Softwareprüfungen im Sinne einer Codeinspektion oder auch sehr umfangreiche Tests an der Maschine, um systematische Fehler auszuschließen, sind langfristig gesehen an einem fertigen Produkt nicht mehr abbildbar. Das in der Vergangenheit oft propagierte Verfahren der entwicklungsbegleitenden Begutachtung/Prüfung ist unter den heute herrschenden Marktrandbedingungen nicht mehr durchführbar. Diese Situation verschärft sich noch für Änderungstypprüfungen, die aufgrund der schnellen Innovationszyklen der COTS-Bauelemente und dem praktisch nicht führbaren Nachweis der Rückwirkungsfreiheit von Kleinständerungen eine noch größere Schieflast zwischen dem erforderlichen Prüfaufwand und der zur Verfügung stehenden Prüfzeit aufweisen.

- Änderungen; Das Eintragen von Fehlern im Rahmen von künftigen Änderungen gewinnt aufgrund der Komplexität an Bedeutung, insbesondere wenn die ursprünglichen Entwickler des Systems nicht mehr verfügbar sind.

- CCF Analysen; Die Aussagekraft von CCF Analysen ist nicht ausreichend, um auf dieser Basis den CCF auf der SE 3 ausschließen zu können. Dies ist darin begründet, dass ein derart tief greifendes Systemverständnis für rechnerbasierte Leittechnik nicht zu erzielen ist[7], sowie, dass nur gegen bekannte CCF Mechanismen ausgelegt werden kann. Die Auswertung von Betriebserfahrung in verschiedenen Bereichen der Technik zeigt, dass immer wieder neue Mechanismen auftreten, die zuvor in der weltweiten Erfahrung nicht beobachtet worden sind.

- Gerichtetes Versagensverhalten; Die Auswirkungen eines CCF können durch Analysen der Systemeigenschaften nicht soweit eingegrenzt werden, dass ein Versagen abweichend von einem implementierten, gerichteten Versagensverhalten auf der Sicherheitsebene 3 nicht mehr unterstellt werden muss. Gründe sind z. B. Schaden verursachende Software (Malware)[8] oder Hardwarefehler oder fertigungsbedingte Fehler.

Die **Architektur 2** legt den Schwerpunkt auf ein tiefgreifendes Systemverständnis, ergänzt um den Einsatz von Diversität im Rahmen einer abgestuften Gesamtarchitektur.

Architektur 2 erfordert den Einsatz von zwei unabhängigen RS-Teilsystemen mit Diversitätsmerkmalen sowie von „Zusätzlichen Leittechnischen Einrichtungen“ (ZLE). Die Diversitätsmerkmale der RS-Teilsysteme werden im Rahmen der CCF Analyse abgeleitet, d.h. es wird (mindestens) das Maß an Diversität realisiert, das zur Beherrschung der betrachteten CCI erforderlich ist. Jedes RS-Teilsystem hat vollen Funktionsumfang. Ein CCF, der ein RS-Teilsystem betrifft, wird der SE 3 zugeordnet und durch das zweite RS-Teilsystem beherrscht. Ein CCF, der beide RS-Teilsysteme betrifft, wird auf Grundlage der CCF Analyse als so unwahrscheinlich angesehen, dass er der SE 4 zugeordnet werden kann.[9]

2. Kommentar von Vertretern der Architektur 1:

Beim Vorschlag zur Architektur 2 ist festgelegt, dass der CCF beider RS-Teilsysteme der Sicherheitsebene 4 zuzuordnen ist. Dies wäre nur dann zulässig, wenn praktisch ausgeschlossen wäre, dass der CCF beide Teilsysteme treffen könnte. Der praktische Ausschluss wäre dann gegeben, wenn die Häufigkeit für diesen Fall wie für das bisherige eingesetzte festverdrahtete RSS bei $< 10^{-7}$/a liegen würde. Da es zur Zeit keine probabilistische Methode zur Bewertung der Zuverlässigkeit von rechnerbasierter Leittechnik gibt, ist ein solcher Ausschluss nicht nachweisbar. Aus der Betriebserfahrung können solche Werte für den CCF auch nicht abgeleitet werden. Das bedeutet letztendlich, dass die Einrichtung für die "zusätzlichen Leittechnikfunktionen" (ZLE) der Sicherheitsebene 3 zuzuordnen ist.

[7] Dies gilt sowohl für den Hersteller als auch der Gutachter (4-Augenprinzip).
[8] Siehe hierzu WLN 2010/07.
[9] Daher kommen der Qualität der CCF Analyse und des CCF Leitfadens sowie der Vollständigkeit des CCI Katalogs (siehe Kapitel 5.4) hohe Bedeutung zu.

3. Kommentar der Vertreter der Architektur 2:

Die Aussage, es gebe z. Zt. keine probabilistische analytische Methode zur Bewertung der Zuverlässigkeit von Rechner-basierter Leittechnik gilt für beide Architekturen. Dies betrifft auch die Voter Problematik (siehe Kommentar 2).
Es besteht jedoch sehr wohl die Möglichkeit, Abschätzungen der Zuverlässigkeit bzw. der Fehlerhäufigkeit aus Betriebserfahrungen abzuleiten. Diese Vorgehensweise wird international auch mit herangezogen, um zu den Aussagen zu kommen, dass die Wahrscheinlichkeit für einen CCF bei Anforderung < 10^{-x} ist. Natürlich ist es für Auswertungen von Betriebserfahrungen so, dass bei evtl. Änderungen in Komponenten oder Systemen zu bewerten ist, ob diese Änderungen hinsichtlich des CCF- Potenzials relevant sein können, was wiederum ein Systemverständnis bezüglich möglicher CCF- Mechanismen voraussetzt. Dies ist aber nichts besonderes, da auch etwa für eine Dissimilaritätsprüfung ein solches Systemverständnis bezüglich möglicher CCF- Mechanismen vorliegen muss.

Für den Fall, dass ein CCF beide RS-Teilsysteme betrifft, stehen „Zusätzliche Leittechnische Einrichtungen“ (ZLE) zur Vermeidung von Schutzzielverletzungen bei unterstelltem CCF im Reaktorschutzsystem zur Verfügung. Die ZLE sollten vorzugsweise in anderer Technologie als die RS-Teilsysteme ausgeführt sein (z.B. HW-basiert), so dass keine Beeinflussung durch Software-Änderungen gegeben ist. Sie sind technisch wie folgt charakterisiert:

- Die ZLE unterliegen nachzuweisenden Qualitätsanforderungen, die noch festzulegen sind.

- Die ZLE sollen bei Auftreten eines CCF des gesamten RSS wirksam werden und die Störfallbeherrschung bei korrekter Funktion des RSS nicht beeinträchtigen (Rückwirkungsfreiheit). Die Rückwirkungsfreiheit kann dadurch sichergestellt werden, dass

    - entweder die ZLE erst bei einem CCF im RSS mit dem durch die Gesamtheit der Überwachungseinrichtungen (innere und externe Überwachungen) ausgelösten Abschalten der zugeordneten Redundanten des RSS redundanzbezogen frei gegeben werden sollen. Dies setzt Überwachungseinrichtungen der Rechner des RSS voraus, die einen CCF im RSS mit hoher Sicherheit erkennen und eine zuverlässige Aktivschaltung der ZLE bewirken;
    - oder für ZLE, die ständig im Eingriff sind (Ansteuerung von Komponenten bei Erreichen nachgelagerter Grenzwerte), ein aktives Funktionsversagen ausgeschlossen werden kann oder keine unzulässigen Folgen hat. Eine Aktivschaltung durch eine CCF-Überwachung ist nicht erforderlich.

- Sie sollen „einfach“ aufgebaut sein, um bereits hierdurch eine hohe Zuverlässigkeit und weitgehende Fehlerfreiheit zu erreichen. Dies bedeutet gegenüber dem RSS reduzierten Funktionsumfang:

    - Keine Analyserandbedingungen der SE3 (insbesondere keine Anwendung Einzelfehlerkonzept);

- Beherrschung von Teilen des Ereignisspektrums durch Gewährleistung vitaler Funktionen (siehe Kapitel 9.3).

3. Kommentar von Vertretern der Architektur 1:

Die Grundproblematik von ZLE, insbesondere wenn sie geringeren Qualitäts- und Auslegungsanforderungen genügen, besteht darin, dass einerseits eine Belastung der Funktion im Anforderungsfall (CCF im RS) erfolgen soll, aber andererseits keine ungewollten Rückwirkungen möglich sein sollen.

Für ZLE werden zwei Möglichkeiten genannt. Bei der ersten Möglichkeit werden neben den Teilsystemen des RS auch noch externe Überwachungen (ExtÜ) für jedes Teilsystem notwendig. Durch das "Unscharfschalten" der ZLE während des Normalbetriebs werden Rückwirkungen sicher verhindert, es besteht aber das Problem der sicheren Erkennung einer aktiven oder passiven Fehlansteuerung durch des RS allein durch die Beobachtung des RS (nicht des Prozesses!). Derzeit gibt es keine konkreten Angaben zum Funktionsumfang der Testfunktion der ExtÜ (siehe Fußnote 10 in Kap. 9.2).

Bei der anderen Variante sind die ZLE immer im Eingriff. Es ist nicht klar, wie technisch „ein aktives Funktionsversagen ausgeschlossen“ werden soll, insbesondere mit einer Gerätetechnik, die gegenüber dem Reaktorschutz abgestuften Qualitätsanforderungen unterliegt. Eine notwendige, aber nicht hinreichende Anforderung hierzu wäre, dass die ZLE zumindest das Einzelfehlerkriterium erfüllen muss und die Qualitätsanforderung entsprechend dem Reaktorschutz erfüllt werden müssen.
Weitere Kommentare: siehe Anmerkungen zu Kap. 9.2 Architektur 2.

Architektur 2 ist wie folgt begründet:

- Komplexität der modernen Gerätetechnik; Bewusster Verzicht auf solche Merkmale moderner Gerätetechnik, die für deren Komplexität verantwortlich sind (u. a. Vermeidung nebenläufiger Prozesse, Vermeidung prozessbedingter Interrupts). Verwendung eines Gerätesystems mit einfachen und prüfbaren Funktionsprinzipien, das in seinem Betriebs- und Fehlerverhalten alle Merkmale von kontinuierlich und deterministisch arbeitenden Systemen aufweist, die in Normalbetrieb wie im Störfall die gleichen Funktionen in derselben Art und Weise ausführen. Damit verbunden ist eine entsprechend einfache Hardwareauslegung, welche die wesentlichen Merkmale der bewährten Reaktorschutzsysteme bewahrt.
  Beibehaltung der einfachen Aufgabenstellung für die Sicherheitsleittechnik in Kernkraftwerken und Unterstützung der Projektierung durch problemorientierte Projektierungswerkzeuge mit umfangreichen Prüf- und Testmöglichkeiten. Diese Projektierungswerkzeuge erlauben eine viel tiefer gehende Verifikation der Aufgabenstellung, als dies mit festverdrahteter Gerätetechnik möglich wäre.

- Kurze Innovationszyklen; Bewusster Verzicht auf kontinuierliche Fertigungsprozesse mit den daraus resultierenden kurzen Innovationszyklen und Übergang auf eine Batch-Fertigung mit

entsprechender Lagerhaltung, so dass Innovationen planbar werden und gezielt durchgeführt werden können.

- Prüfbarkeit; Die Prüfbarkeit einer Gerätetechnik definiert sich über die erreichbare Prüftiefe, die wiederum im Wesentlichen durch deren interne Funktionsprinzipien bestimmt wird. Bei der gezielten Verwendung einer Gerätetechnik mit einfachen Funktionsprinzipien kann daher in Bezug auf die Sicherheitsfunktionen eine extrem hohe Prüftiefe erreicht werden, die sogar über die erreichbare Prüftiefe einer festverdrahteten Gerätetechnik hinausgeht. So können beispielsweise während einer Prüfung nicht nur die Eingangs- und Ausgangssignale beobachtet werden, sondern alle internen Speicher und Signale einer Funktion sind während der Prüfung von außen beobachtbar, so dass auch Fehler erkannt werden können, die sich zunächst nicht auf die Ausgangssignale auswirken. Ein wesentlicher Vorteil gegenüber der festverdrahteten Gerätetechnik besteht darin, dass „in Anlage eingebaut“ praktisch gleich „geplant und im Prüffeld aufgebaut“ ist, so dass die z. T. nicht einfach auffindbaren Fehler bei der Verdrahtung in der Montage auf der Anlage minimiert sind. Dies betrifft besonders auf der Anlage durchzuführende Verdrahtungsänderungen.

- Änderungen; Grundsätzlich stehen für Änderungen alle Projektierungs- und Prüfwerkzeuge zur Verfügung, die auch bei der Auslegung der Systeme zur Anwendung kommen. Daher sind Änderungen in gleicher Qualität möglich, wie die Auslegung der Systeme selbst. Die Verwendung eines Ansatzes mit einheitlicher Gerätetechnik bringt in Bezug auf die Mensch-Maschine-Nahtstelle große Vorteile. Dies betrifft beispielsweise die Durchgängigkeit der Dokumentation, die Schulung des Personals oder die Einheitlichkeit von Meldungen auf der Warte.

- CCF Analysen; Durch die Beschränkung auf einfache Funktionsprinzipien werden auch die möglichen Auswirkungen latenter Fehler sehr stark eingeschränkt. Die Aussagekraft einer entsprechenden CCF Analysen ist bei geeigneter Durchführung ausreichend, um auf dieser Basis einen CCF, der zum Versagen beider RS-Teilsysteme führt, auf der SE 3 ausschließen zu können. Das hierfür erforderliche tief greifende Systemverständnis ist bei der Beschränkung auf entsprechend einfache Funktionsprinzipien auch für rechnerbasierte Leittechnik erzielbar. Ein CCF des RSS, der zum Versagen von beiden RS-Teilsystem führt, ist der SE 4 zuzuordnen und wird über eine geeignete Gesamtarchitektur mittels der ZLE beherrscht.

- Gerichtetes Versagensverhalten; Durch die Beschränkung auf einfache Funktionsprinzipien können auch die Auswirkungen eines CCF soweit eingegrenzt werden, dass ein Versagen abweichend von einem implementierten, gerichteten Versagensverhalten nicht unterstellt werden muss. Durch die einfachen Funktionsprinzipien ist es möglich, dass die Versagensmechanismen ausreichend analysiert werden können. Auf Grund der bekannten Versagensmechanismen können einerseits wirksame Überwachungsmechanismen implementiert werden, die dieses Versagen erkennen und dann die betroffenen Geräte in einen definierten Zustand überführen. Es können weiterhin gezielt Maßnahmen zur Diversifizierung möglicher triggernder Systemzustände

implementiert werden, so dass der Auswirkungsbereich eines möglichen abhängigen Versagens auf eine Gruppe von sonst baugleichen Geräten eingegrenzt wird.

9 Auswirkungen von CCF Postulaten an der Schnittstelle Leittechnik/Verfahrenstechnik

Falls bei einem CCF im Reaktorschutzsystem Reaktorschutzsignale nicht (passives Funktionsversagen) oder fehlerhaft (aktives Funktionsversagen) generiert werden, hat dies Konsequenzen für die verfahrenstechnischen Abläufe in der Anlage.

Ein aktives Funktionsversagen infolge eines CCF von Teilsystemen des RSS kann dazu führen, dass

- fehlerhaft Reaktorschutzsignale generiert werden oder

- Ansteuerungen, die eine Koordination erfordern, so erfolgen, dass die Koordination nicht mehr gegeben ist und an Sicherheitseinrichtungen Schäden verursacht werden(z.B. Start einer Pumpe, aber kein Start der zugehörigen Schmierölpumpe).

Aktives Funktionsversagen kann sowohl während des Normalbetriebs als auch im Zuge der Beherrschung anderweitig ausgelöster Ereignisse zum Tragen kommen.

Passives Funktionsversagen infolge eines CCF von Teilsystemen des RSS kommt nur bei anderweitig ausgelösten Ereignissen zum Tragen, indem diese Teilsysteme erforderliche Reaktorschutzfunktionen nicht ausführen. Passives Funktionsversagen löst somit keine Transienten oder Störfälle aus. Die Beherrschung von passivem Funktionsversagen setzt voraus, dass die verbleibenden Leittechnikfunktionen ausreichend sind für die Ereignisbeherrschung.

9.1 Folgen fehlerhaft generierter Reaktorschutzsignale

Fehlerhaft generierte Reaktorschutzsignale (aktives Funktionsversagen) können Anlagentransienten, evtl. auch Störfälle auslösen.

Dies gilt auch für kurzzeitig anstehende Fehlsignale. Angesteuerte Stellantriebe verlassen bis auf wenige Ausnahmen, wie z. B. Regelantriebe, ihre ursprüngliche Stellung (AUF oder ZU) und steuern erst bei Erreichen der Endlage (ZU oder AUF) ab. Ebenso werden die meisten Leistungsschalter für Pumpen, Lüfter, Generatorleistungsschalter von Notstromdieseln eingeschaltet bleiben. Ein Eingriff von Hand oder das Ansprechen des Aggregateschutzes ist in den meisten Fällen erst dann möglich, wenn das betroffene Reaktorschutzsignal nicht mehr ansteht.

Ist von den Fehlsignalen nur ein Teil der verfügbaren verfahrenstechnischen Redundanten betroffen, so stehen die anderen zur Beherrschung des ausgelösten Ereignisses zur Verfügung. Es ist

- vom Anlagentyp (DWR oder SWR),
- von der leit- und verfahrenstechnischen Auslegung der Anlage,
- von der Kombination von Fehlsignalen,
- von der Zeitdauer, über die Fehlsignale anstehen,
- von Art und Umfang der von den Fehlsignalen betroffenen Einrichtungen, sowie
- von den technischen Möglichkeiten und den zeitlichen Randbedingungen für vom Reaktorschutzsystem unabhängigen Handmaßnahmen

abhängig, in welchem Ausmaß die Ereignisbeherrschung beeinflusst, erschwert oder verhindert wird.

Dies gilt ebenso, wenn unterstellt wird, dass in Teilsystemen des RSS ein CCF mit aktivem Funktionsversagen zusätzlich zu einem aus anderen Gründen ausgelösten Ereignisablauf auftritt.

Hinsichtlich unkoordinierter Ansteuerungen ist festzustellen, dass das RSS in einem repräsentativen Siemens- DWR ca. 40 Auslösesignale hat, von denen größenordnungsmäßig 600 bis 800 Komponenten-Funktionen angesteuert werden (EIN/AUS oder AUF/ZU). Für eine Reihe von Funktionen müssen mehrere Komponenten koordiniert (in der Regel jeweils bezogen auf die einzelnen verfahrenstechnischen Stränge) angesteuert werden. Diese Koordinierung der Ansteuerung erfolgt für Sicherheitssysteme bisher überwiegend im RSS (Steuerebene), so dass die WKP der entsprechenden leittechnischen Maßnahmen in die WKP des RSS integriert werden konnte. Wird unterstellt, dass bei einem unterstellten aktiven Funktionsversagen die einem Auslösesignal zugeordneten Komponenten unterschiedlich angesteuert werden, können Schäden an sicherheitsrelevanten Komponenten nicht ausgeschlossen werden.

Für die Betrachtung der Fälle ist auch relevant, ob sie unter SE 3 Analyserandbedingungen beherrscht werden müssen oder nicht. Ein Nachweis der Ereignisbeherrschung unter SE 3 Randbedingungen bedeutet u.a., dass der Notstromfall anzunehmen (sofern ungünstig) und das Einzelfehlerkonzept anzusetzen ist.

9.2 Beherrschung von aktivem und passivem Funktionsversagen im Kontext unterschiedlicher Architekturen

Architektur 1 geht davon aus, dass für die modernen rechnerbasierten Gerätetechniken die Aussagekraft von CCF Analysen nicht ausreichend ist, um auf dieser Basis den CCF auf der SE 3 ausschließen zu können. Da gemäß Ansatz 1 im Falle eines CCF ein Versagen abweichend von einem implementierten, gerichteten Versagensverhalten auf der Sicherheitsebene 3 unterstellt werden muss, ist bei homogenen rechnerbasierten Teilsystemen das Auftreten von aktivem und passivem Funktionsversagen zu unterstellen und durch eine geeignete Gesamtarchitektur unter Einsatz dissimilarer Teilsysteme zu beherrschen. Dies bedeutet:

- Verfahrenstechnische Analyse: Es ist eine verfahrenstechnische Analyse durchzuführen, auf deren Basis die Auswirkungen von aktivem und passivem Funktionsversagen zu ermitteln sind.

- Betrachtung von Funktionsversagen: Führt passives Funktionsversagen oder aktives Funktionsversagen auch unter Berücksichtigung von möglichen, vom Reaktorschutz unabhängigen Handmaßnahmen und dem 30-Minutenkriterium zu unzulässigen Auswirkungen, muss die Funktion von dissimilaren Teilsystemen ausgeführt werden können. Andernfalls wird eine Realisierung in einer homogenen Gerätetechnik, wie in der derzeit in den Anlagen bestehenden festverdrahteten Auslegung des Reaktorschutzes, unter Berücksichtigung der geforderten Maßnahmen zur Fehlervermeidung als angemessen betrachtet.
  Ist für einzelne Funktionen sowohl das aktive als auch das passive Funktionsversagen zu betrachten, würde dies bei Einsatz der modernen rechnerbasierten Technik drei dissimilare Teilsysteme erfordern. Die Auslösung / Ansteuerung der Komponenten müsste dann über einen Voter (2v3) erfolgen, wobei für den Voter eine ausreichende Sicherheit gegen CCF erreicht werden müsste. Stattdessen ist in Hinblick auf die Forderung nach Einfachheit für den Reaktorschutz eine Realisierung der Funktion in homogener festverdrahteter Technik auf der Basis von diskreten Bauelementen, die analog zum bisherigen Vorgehen geprüft werden kann, vorzuziehen.

4. Kommentar von Vertretern der Architektur 2: siehe 2. Kommentar.

- Zuordnung der dissimilaren Gerätetechnik auf die redundanten Teilsysteme: Anstelle der parallelen Bearbeitung von Funktionen durch die dissimilaren Teilsysteme mit anschließenden Voting kann für Funktionen, die Komponenten strangweise ansteuern (z.B. 4 Pumpen), auch eine Auslegung mit strangweiser Zuordnung der dissimilaren Gerätetechnik (z.B. 2x2) erfolgen. Hierdurch werden dann die Auswirkungen von einem CCF eines Teilsystems sicher auf nur einen Teil der verfahrenstechnischen Stränge begrenzt. Dies ist in Hinsicht auf die erforderliche Koordination der Ansteuerungen von mehreren Komponenten in unterschiedlichen Strängen, eine vorteilhafte, einfache Realisierungslösung. Hierfür sind jedoch folgende Aspekte zu betrachten:

  - Überlagerung CCF im RSS mit Einzelfehlerkonzept: Gemäß der derzeitigen KTA 3501 ist die Überlagerung von CCF und Versagen aufgrund von Einzelfehlern oder Instandhaltungsfall zusätzlich zum Störfall zu beherrschen. Die derzeitige Anlagenauslegung basiert jedoch auf dem Ausschluss des CCF im Reaktorschutz, so dass die Überlagerung nicht betrachtet werden musste. Wenn eine Überlagerung zu betrachten wäre, würde das zu sehr komplexen Realisierungen mit 3 bzw. 4 dissimilaren Teilsystemen führen. Hierzu ist festzustellen, dass ein Fehler, der zum systematischen Versagen führt, unter Voraussetzung einer anforderungsgerechten Auslegung der Leittechnik einen sehr seltenen Spezialfall des Einzelfehlers darstellt und damit nicht gleichzeitig zum Einzelfehler zu unterstellen ist. Dies wird damit begründet, dass bei einer Auslegung gegen Versagen aufgrund von Einzelfehlern und der sehr hochwertigen Maßnahmen zur Beherrschung und Vermeidung von systematischem Versagen eine zeitliche Koinzidenz beider Versagensmechanismen als hinreichend unwahrscheinlich anzusehen ist, wenn administrativ geeignete Maßnahmen zur Reduzierung der Fehlererkennungs- und -reparaturzeit getroffen werden. Dies ist insbesondere im Kontext mit den hochentwickelten Selbstüberwachungsmaßnahmen zu sehen, die eine geringe Aufenthaltsdauer von mit der Selbstüberwachung erkennbaren Fehlern in digitalen leittechnischen Systemen bedingen.

- Datenaustausch zwischen Redundanten: In den meisten Anlagen sieht das vorhandene RSS-Konzept vor, dass für einzelne Auslösesignale nicht eine nur strangbezogene Erfassung, Verarbeitung und Ansteuerung, sondern auch ein Datenaustausch zwischen Redundanten vorgesehen ist (z.B. für Absperr-Auslösesignale wie DAF 2 > max). Da diese Redundanzverknüpfungen die geforderte Unabhängigkeit der Redundanzen beschränkt, ist bei strangweiser Zuordnung anlagenspezifisch die Notwendigkeit dieser Redundanzverknüpfungen zu bewerten. Bei der Notwendigkeit von redundanzübergreifendem Signalaustausch sind Analysen zur Kopplung der dissimilaren Teilsysteme erforderlich z. B. zu den Signallaufzeiten, zu Möglichkeiten von Fehlerfortpflanzung, etc.

Die sich aus diesem Ansatz ergebenden Anforderungen sind in der Stellungnahme des VdTÜV zu den erforderlichen Vorsorgemaßnahmen gegen systematisches Versagen von digitalen leittechnischen Einrichtungen [9.1] und in den BMU „Sicherheitskriterien für Kernkraftwerke, Modul 5“ Kapitel 3.2 (11) enthalten.

Die **Architektur 2** setzt voraus, dass die Auswirkungen eines CCF soweit eingegrenzt werden können, dass ein Versagen abweichend von einem implementierten, gerichteten Versagensverhalten nicht unterstellt werden muss. Das gerichtete Versagensverhalten setzt die Wirksamkeit interner und ggf. zusätzlicher externer Überwachungen durch Einrichtungen, die diversitär zu den software-gesteuerten Rechnern des RSS sind, voraus. Die Überwachungen benötigen eine endliche Zeit, bis sie einen definierten Zustand an den Ausgängen sicherstellen. Bei TELEPERM XS wird dies durch Abschalten der Laststromversorgung der Signalausgaben erreicht. Bei Rechner-bezogenen (internen) Überwachungen, die innerhalb eines Bearbeitungszyklus wirken, ist davon auszugehen, dass es i. d. R. nicht zu einer Fehlansteuerung (aktives Funktionsversagen) kommt. Bei einer externen Überwachung[10], die u. U. mehrere Rechner auf einem

10 Erläuterung zur Funktionsweise der externen Überwachung (ExtÜ): Nach aller Erfahrung führen HW-Ausfälle oder die Triggerung von Fehlern, auch solcher mit CCF Potenzial, letztlich dazu, dass der zyklische Betrieb des Automatisierungsgerätes unterbrochen wird. Diese Unterbrechung wird durch die mehrstufigen internen Überwachungen zuverlässig erkannt, so dass die Laststromversorgung der Ausgabebaugruppe ausgeschaltet und ein definierter Zustand sichergestellt wird. Wird trotz der Erfahrungen postuliert, dass ein Fehler so geartet ist, dass der zyklische Betrieb nicht unterbrochen wird, aber zu einer Beeinflussung der Reaktorschutz-Leittechnikfunktionen führt, muss jedenfalls eine entsprechende Veränderung in der Hardware, der Software oder der inneren Zustände vorliegen.
Das Konzept der ExtÜ sieht vor, dass in jedem Bearbeitungszyklus auch eine Signalfolge aus der ExtÜ in den jeweils überwachten Baugruppenträger des RSS eingespeist, durch eine spezielle Testfunktion verarbeitet und das Ergebnis der Verarbeitung mit dem bei ungestörtem Betrieb zu erwartenden Signal verglichen wird. Für die Testfunktion werden alle Hardware- und Software-Komponenten verwendet, die auch für die eigentlichen Reaktorschutzfunktionen eingesetzt werden und für die ein CCF Potenzial nicht hinreichend ausgeschlossen werden kann. Wenn in diesen Komponenten eine Veränderung unterstellt wird, die zwar nicht den zyklischen Betrieb, aber das Ergebnis der Leittechnikfunktionen beeinflusst, muss es auch zu Veränderungen des Ergebnisses der Testfunktionen kommen, die von dem zu erwartenden Ergebnis abweichen. Diese Abweichung würde dann zum Abschalten der Laststromversorgung der Baugruppe und damit zu einem definierten Zustand führen, d.h. ein aktives Funktionsversagen würde auch in diesem Fall verhindert.
Die ExTü ist Teil des Reaktorschutzsystems und unterliegt den entsprechenden Qualitäts- und Auslegungsanforderungen.

Baugruppenträger überwacht, kann die Abschaltung der Laststromversorgung ggf. erst nach mehr als einem Bearbeitungszyklus sichergestellt werden. Kurzzeitig (<< 1 s) anstehende Fehlsignale im Zeitraum bis zum Ansprechen der Überwachungen können deshalb nicht ausgeschlossen werden.

Insgesamt ergeben sich für Architektur 2 folgende Konsequenzen hinsichtlich der Schnittstelle Leit-/Verfahrenstechnik:

- Verzögerung der Auslösung: Grundsätzlich besteht die Möglichkeit, durch Verzögerung der Auslösung aller Ansteuerungen (mit Ausnahme der RESA) um ca. 1 s (außerhalb der RSS-Rechner) Fehlauslösungen infolge kurzzeitig anstehender Fehlsignale zu vermeiden. Dafür sind zwar die Störfallanalysen mit 1 s Verzögerungszeit für die verfahrenstechnischen Funktionen durchzuführen, dies lässt für die Einhaltung der Kriterien in den Nachweisen jedoch keine Probleme erwarten. Allerdings wäre eine solche generelle Lösung bei ca. 600 bis 800 vom RSS angesteuerten Komponenten recht aufwendig. Falls diese Lösung nicht sinnvoll eingesetzt werden kann, sind die Funktionen im Zuge einer verfahrenstechnischen Analyse unter Berücksichtigung der verwendeten leittechnischen Komponenten im Einzelnen hinsichtlich kurzzeitiger Fehlansteuerung zu bewerten.

- Verfahrenstechnische Analyse: Zu untersuchen ist, ob fehlerhaft ausgelöste Funktionen zu unzulässigen Auswirkungen führen oder nicht. Unzulässige Auswirkungen werden vermieden, wenn durch Fehlansteuerungen zwar ggf. Transienten ausgelöst werden, diese aber durch das nicht vom CCF betroffene RS-Teilsystem (SE 3) beherrscht werden oder Schutzzielverletzungen im Falle eines CCF des gesamten RSS (SE 4) durch diversitäre Zusätzliche Leittechnische Einrichtungen beherrscht werden. Hierbei wirkt sich günstig aus, dass aufgrund des an den Ausgängen definierten Zustands, der durch die Überwachungen nach Bruchteilen einer Sekunde sichergestellt wird, eine Ansteuerung nicht mehr ansteht. Z. B. können damit Schäden durch den Aggregateschutz verhindert werden. Zu unzulässige Auswirkungen infolge kurzzeitiger Fehlansteuerungen sind geeignete Gegenmaßnahmen festzulegen.

- Passives Funktionsversagen: Passives Funktionsversagen eines RS-Teilsystems infolge CCF (SE 3) wird durch das zweite RS-Teilsystem beherrscht. Passives Funktionsversagen beider RS-

4. Kommentar von Vertretern der Architektur 1 zu Fußnote 10:
Für die hier erforderliche, hoch wirksame Erkennung eines Funktionsversagens eines Teilsystems nur auf Basis des Geräteverhaltens und der inneren Zustände sind die genannten Überwachungsfunktionen bei weitem nicht ausreichend. Hierzu müsste auf der Basis von detaillierten CCF-Analysen aller HW- und SW-Komponenten umfangreiche und tiefgreifende Überwachungsmaßnahmen entwickelt werden.

5. Kommentar von Vertretern der Architektur 2 zu Fußnote 10:
Auf der Basis eines ausreichenden Systemverständnisses in Verbindung mit den erforderlichen CCF-Analysen kann durchaus gezeigt werden, dass mit kompakten Überwachungsfunktionen in der ExtÜ, die die internen Überwachungen ergänzt, eine ausreichende Überwachung darstellbar ist.

Teilsysteme infolge CCF (SE 4) wird durch Zusätzliche Leittechnische Einrichtungen für einen Teil des Ereignisspektrums (Festlegung vitaler Funktionen) beherrscht.

- Aktives Funktionsversagen: Aktives Funktionsversagen über kurzzeitige Fehlansteuerungen hinaus ist aufgrund des gerichteten Versagensverhaltens nicht zu unterstellen. Die Beherrschung kurzzeitiger Fehlansteuerungen erfolgt entweder über Zeitverzögerungen um 1 s oder es wird im Rahmen der verfahrenstechnischen Analyse (ggf. ergänzt um einzelne Gegenmaßnahmen) gezeigt, so dass letztlich nur passives Funktionsversagen zu beherrschen ist.

- Strangweise Auslegung: Da der CCF eines RS-Teilsystems der SE 3 zugeordnet wird und zudem unter den Analyserandbedingungen der SE 3 beherrscht werden soll, muss jedes RS-Teilsystem alle vier Redundanzen ansteuern können (Ansteuerung der Komponenten über ein ODER, das die Signale der jeweiligen Ausgänge der beiden vierfach redundanten, unabhängigen RS-Teilsysteme aufnimmt). Ansonsten würde der CCF überlagert mit dem Einzelfehlerkonzept nicht beherrscht. Weiterhin sieht das vorhandene RSS-Konzept in den meisten DWR Anlagen für einzelne Auslösesignale nicht eine nur strangbezogene Erfassung, Verarbeitung und Ansteuerung, sondern auch einen Datenaustausch zwischen Redundanten vor (z.B. für Absperr-Auslösesignale wie DAF 2 > max), allerdings mit Datenaustausch nur zwischen den Redundanten des jeweiligen vierfach redundanten, RS-Teilsystems.

- Überlagerung CCF im RSS mit Einzelfehlerkonzept: Eine Überlagerung eines CCF in einem RS-Teilsystem (SE 3) mit dem Einzelfehlerkonzept wird für alle Auslegungsstörfälle beherrscht.

9.3 Ableitung vitaler Funktionen

Für Architektur 1 wird mittels einer verfahrenstechnischen Analyse und der Betrachtung von passivem und aktivem Funktionsversagen (siehe Kapitel 9.2) die Auswahl der dissimilar zu realisierenden Funktionen aus dem Gesamtumfang der zu realisierenden Funktionen ermittelt.

Architektur 2 erfordert die Festlegung des Funktionsumfangs der Zusätzlichen Leittechnischen Einrichtungen, die nachfolgend als „vitale Funktionen“ bezeichnet werden. Aufgabe der sog. „vitalen“ Systemfunktionen ist es, die Anlage bei einem unterstellten Versagen des RSS infolge CCF beider RS-Teilsysteme (SE 4) kurzfristig so zu stabilisieren, dass unter Berücksichtigung von später durch das Anlagenpersonal eingeleiteten Maßnahmen unzulässige Auswirkungen auf die Umwelt vermieden werden. Dabei wird ein aktives Funktionsversagen der RS-Teilsysteme mit länger anstehenden Fehlanregungen verfahrenstechnischer Systeme nicht unterstellt (siehe Kapitel 9.2).

Die Auslösung einer Anlagentransiente durch kurzzeitig anstehende Fehlsignale infolge CCF von Teilsystemen des RSS (CCF als Auslöser des Ereignisses) soll durch eine Teilmenge der vitalen Funktionen beherrscht werden – beim DWR sind dies RESA/TUSA sowie Wärmeabfuhr über die Frischdampfarmaturen.

Als vitale Systemfunktionen werden solche verfahrenstechnische Funktionen bezeichnet, die zur Behandlung der Ereigniskombinationen innerhalb 30 Minuten notwendig sind, um die Schutzziele einzuhalten. Die Auswahl vitaler Systemfunktionen ist abhängig vom Störfallbeherrschungskonzept der betrachteten Anlage. Da z.B. bei den Siemens-DWR das Störfallbeherrschungskonzept ähnlich ist, ist auch der Umfang der vitalen Systemfunktionen ähnlich. Eine mögliche Vorgehensweise zur Ableitung vitaler Funktionen für DWR basiert auf den Ergebnissen von Sicherheitsstatusanalysen (SSA) – beispielhaft dargestellt in [9.2].

10 Zusammenstellung von Konsequenzen für Entwicklung, Implementierung und Betrieb aus der Realisierung der beiden Architekturen zur Beherrschung des CCF

Für beide Architekturen gilt, dass die jeweils erforderliche Zuverlässigkeit des RSS bzw. des Gesamtsystems (RSS und ZLE) nicht allein durch die gewählte Architektur sichergestellt werden kann sondern auch für die eingesetzte Gerätetechnik nachgewiesen werden muss. Dies erfordert u. a. eine hohe Qualität des Gerätesystems, die in einer geeigneten Typprüfung nachgewiesen werden muss, und eine CCF Analyse (siehe Kapitel 5.4). Zusammengefasst wird bei der Architektur 2 ein geringeres Maß an Diversität zwischen den beiden RS-Teilsystemen realisiert als bei der Architektur 1 (Dissimilarität), dafür werden bei Variante 2 die ZLE auf SE 4 vorgesehen. Jede Variante hat spezifische Implikationen für Design, Installation, Betrieb und Wartung der leittechnischen Einrichtungen.

Im Falle einer Realisierung der **Architektur 1** ergeben sich folgende wesentliche Konsequenzen:

- Es wird zugrundegelegt, dass die Ereignisbeherrschung ganz oder teilweise mittels rechnerbasierter Systeme erfolgen kann.

- Der Einsatz dissimilarer RS-Teilsysteme erfordert unterschiedliche Gerätetechniken für die Teilsysteme. Der Betreiber hat die gemäß IEC 61513 erforderliche Gesamtplanung des aus dissimilaren Teilsystemen bestehenden RSS und die Gesamtintegration der RS-Teilsysteme in ein leittechnisches Gesamtsystem sowie die Inbetriebsetzung des Gesamtsystems sicherzustellen.

- Festgestellte Fehler, Auslassungen oder missverständliche Vorgaben in den Spezifikationen für die RS-Teilsysteme sind zwischen den einzelnen Herstellern und dem Verantwortlichen für die Gesamtplanung zu kommunizieren. Dabei darf die Unabhängigkeit der Entwicklungen der einzelnen Hersteller nicht in Frage gestellt werden.

- Der gesamte Entwicklungsprozess mit den dabei bestehenden Fehlermöglichkeiten (z. B. bei der Umsetzung von Spezifikationen) ist für die RS-Teilsysteme zweifach bzw. ggf. dreifach durchzuführen. Somit sind tendenziell insgesamt mehr Fehler zu erwarten als bei Architektur 2, allerdings bei gleichzeitig erwarteter geringerer Wahrscheinlichkeit dafür, dass in beiden Teilsystemen „gleiche“ Fehler vorliegen.

- Der Einsatz dissimilarer RS-Teilsysteme erfordert eine Dissimilaritätsanalyse. Hierfür sind vorab geeignete Kriterien für die Dissimilaritätsbeurteilung zu entwickeln. Die Wirksamkeit der einzelnen realisierten Diversitäten im Hinblick auf die Beherrschung von CCF Mechanismen ist zu begründen, damit ein gleichzeitiges Versagen dissimilarer Teilsysteme infolge CCF auf der SE 3 praktisch ausgeschlossen werden kann.

- Im Betrieb sind die Betriebserfahrungen aus der eigenen und aus anderen Anlagen und andere neue Erkenntnisse im Hinblick auf die Beherrschung von CCF Mechanismen zu verfolgen und ggf. erforderliche Maßnahmen zu treffen (siehe Kap. 5.4).

- Die Nachweisführung und Begutachtung ist zweifach bzw. ggf. dreifach für unterschiedliche RS-Teilsysteme durchzuführen.

- Die im Design realisierte Diversität / Dissimilarität ist über die Betriebsdauer für die Produkte unterschiedlicher Hersteller aufrecht zu erhalten. Die Wartungskompetenz ist für RS-Teilsysteme unterschiedlicher Hersteller erforderlich, mit dem Vorteil, dass das Eintragen von CCF- Fehlern bei Wartung und Änderungen reduziert wird und zusätzlich ein Schutz gegen Malware mit CCF Potential aufgebaut wird.

- Die kerntechnischen Applikationen müssen auf die dissimilaren RS-Teilsysteme zweifach bzw. ggf. dreifach implementiert werden. Dabei müssen die dissimilaren Systeme so arbeiten, dass eine zeitlich gesicherte Auslösung durch die sich überlagernden Teilsystemauslösungen gewährleistet ist. Alternativ ist in Hinblick auf die Forderung nach Einfachheit für den Reaktorschutz eine Realisierung der Funktion in homogener festverdrahten Technik auf der Basis von diskreten Bauelementen möglich (siehe Kapitel 9.2).

Die Realisierung der **Architektur 2** hat folgende wesentliche Konsequenzen:

- Werden die ZLE HW-basiert ausgeführt, stehen für die Gewährleistung vitaler Funktionen (Einhaltung der Schutzziele bei einem CCF des gesamten Reaktorschutzsystems für einen Teil des Ereignisspektrums) Systeme in unterschiedlicher Technologie zur Verfügung.

- Es ist nachzuweisen, dass die ZLE bei einem CCF des Reaktorschutzsystems wirksam werden. Der CCF des RSS darf nicht den Eingriff der ZLE blockieren.

- Die Entwicklung der rechnerbasierten RS-Teilsysteme mit Diversitätsmerkmalen kann ggf. von einem Hersteller mittels unterschiedlicher Entwicklerteams und firmeninternem Diversitätsmanagement erfolgen. Zu entscheiden ist, ob die ZLE von einem anderen Hersteller stammen sollen. Der Betreiber hat die gemäß IEC 61513 erforderliche Gesamtplanung des aus RSS und ZLE bestehenden Gesamtsystems, die Gesamtintegration sowie die Inbetriebsetzung des Gesamtsystems sicherzustellen.

- Festgestellte Fehler, Auslassungen oder missverständliche Vorgaben in den Spezifikationen für die RS-Teilsysteme sind ggf. nur innerhalb eines Herstellers zwischen unterschiedlichen Entwicklerteams so zu kommunizieren, dass dabei die Unabhängigkeit von deren Entwicklungen nicht in Frage gestellt wird.

- Der gesamte Entwicklungsprozess mit den dabei bestehenden Fehlermöglichkeiten (z. B. bei der Umsetzung von Spezifikationen) wird für die RS-Teilsysteme nicht vollständig zweifach durchgeführt. Somit sind tendenziell insgesamt weniger Fehler zu erwarten als bei Architektur 1, allerdings bei gleichzeitig erwarteter höherer Wahrscheinlichkeit dafür, dass in beiden RS-Teilsystemen „gleiche“ Fehler vorliegen.

- Die Diversitätsmerkmale der beiden RS-Teilsysteme sind gezielt und unter Berücksichtigung möglicher CCF Mechanismen festzulegen. Hierfür sind vorab geeignete Kriterien für Diversitätsentscheidungen zu entwickeln. Die Wirksamkeit der einzelnen Diversitätsmerkmale im Hinblick auf die Beherrschung von CCF Mechanismen ist zu begründen, da ein gleichzeitiges Versagen beider RS-Teilsysteme infolge CCF auf der SE 3 nicht unterstellt wird.

- Im Betrieb sind die Betriebserfahrungen aus der eigenen und aus anderen Anlagen und andere neue Erkenntnisse im Hinblick auf die Beherrschung von CCF Mechanismen zu verfolgen und ggf. erforderliche Maßnahmen zu treffen.

- Für die ZLE gilt eine andere Aufgabenspezifikation, die nur einen Teil der Funktionen (vitale Funktionen) umfasst.

- Dem gerichteten Versagensverhalten der RS-Teilsysteme kommt zentrale sicherheitstechnische Bedeutung zu, so dass diesbezüglich sehr hohe Nachweisanforderungen bestehen. Auf der Ebene der Teilsysteme muss das Versagensverhalten der Teilsysteme ermittelt und belegt werden, dass jedes Teilsystem einen vordefinierten sicheren Zustand einnimmt. Fehler, die zusammen mit möglichen Common Cause Auslösern zu keinem derartigen sicheren Zustand der RS-Teilsysteme und der ZLE führen, sind mit hoher Zuverlässigkeit zu ermitteln und zu beseitigen. Ggf. kurzzeitig anstehende Fehlsignale aus dem RSS müssen beherrscht werden (bei CCF in einem RS-Teilsystem durch das andere RS-Teilsystem, bei einem CCF des gesamten RSS durch die ZLE, andere leittechnische Einrichtungen wie z.B. Aggregateschutz sowie – bei entsprechenden Karenzzeiten – durch Handmaßnahmen). Sofern ein Konzept verfolgt wird, bei dem die ZLE nicht erst infolge der Abschaltung der jeweiligen Redundanten des RSS freigegeben werden, sondern – z.B. mit nachgelagertem Grenzwert – immer in Eingriff sind, sind die Anforderungen für ein gerichtetes Versagensverhalten auch für die ZLE zu erfüllen.

- Die im Design realisierte Diversität / Dissimilarität ist über die Betriebsdauer für die RS-Teilsysteme eines Herstellers aufrecht zu erhalten. Die Wartungskompetenz ist für RS-Teilsysteme eines Herstellers erforderlich. Für die ZLE ist zusätzliche Wartungskompetenz erforderlich.

Für beide Architekturen gilt, dass auch bei Einbau in vorhandene Anlagen eine vollständige Anforderungsspezifikation vorliegen oder ggf. neu erzeugt werden muss, inklusive der zu unterstellenden elektrischen Umgebungsbedingungen und anderer Umgebungseinflüsse. Es muss nachgewiesen werden, dass die neue Technik verträglich mit den worst-case Bedingungen ist.

Für beide Architekturen ist zu untersuchen, ob Umgebungseinflüsse bestehen, gegen die die neue rechnerbasierte Technik empfindlicher ist als die bislang eingesetzte konventionelle RS-Technik (Beispiel: Spannungsschwankungen, EMV und Strahlung, die zu Datenveränderungen (Soft-Errors) führen können). Sofern dies der Fall ist, sind entsprechende Gegenmaßnahmen zu ergreifen.

11 Instandhaltungs- und Änderungsmaßnahmen

Durch Instandhaltungs- und Änderungsmaßnahmen können Fehler in rechnerbasierte Systeme eingetragen werden. Die Instandhaltungs- und Änderungsmaßnahmen an leittechnischen Systemen unterliegen als Teile des Systemlebenszyklus den Anforderungen der Normenserie der DIN IEC 61513.

Zur Vermeidung eines Eintrags von Fehlern bei Instandhaltungs- und Änderungsmaßnahmen sind folgende allgemeine Anforderungen zu erfüllen:

- Alle Instandhaltungs- und Änderungsmaßnahmen sind auf der Basis der kraftwerksspezifisch erforderlichen Verfahrensreglungen für Instandhaltungsmaßnahmen und Änderungen durch geschultes Personal auszuführen. Dabei sind Kenntnisse sowohl zur Anlagentechnik als auch zu den Gerätesystemen notwendig. Abhängig von den möglichen Auswirkungen der Instandhaltungsmaßnahmen oder Änderungen ist der jeweils notwendige Anlagenzustand (Volllast, Teillast oder Stillstand) vor dem Beginn der Arbeiten herzustellen. Die geladene Software ist einer Identitäts- und Konsistenzprüfung zu unterziehen.

- Es ist ein formalisiertes Änderungs- und Konfigurationsmanagement anzuwenden, sodass jederzeit nachvollziehbar ist, zu welchem Zeitpunkt die Anlage in welcher Konfiguration betrieben wurde.

- Sich wiederholende Instandhaltungsmaßnahmen wie z. B. WKP oder Parameteränderungen (z. B. für Streckbetrieb) sind mit ergonomisch gestalteten Eingabemasken zu unterstützen. Die Eingaben sind hinsichtlich korrekter Syntax (Komma; Punkt; unsichtbares Steuerzeichen) und korrekter Werteeingaben (Dezimalstellen; Werteveränderung) zu prüfen. Die Auswahl von vordefinierten Einstelloptionen ist der alphanumerischen Wertevorgabe vorzuziehen.

- Wiederkehrende Instandhaltungsmaßnahmen sind nach geprüften Anweisungen durch geschultes Fachpersonal durchzuführen, wobei die Maßnahme an dem jeweiligen Anlagenzustand zu spiegeln ist.

- Instandhaltungsmaßnahmen sind, sofern Verfügbarkeitsanforderungen an das betroffene leittechnische System bestehen, grundsätzlich auf eine Scheibe zu beschränken. Ein durch Instandhaltungsvorgänge initiierter Wechsel auf die nächste Scheibe setzt die Kontrolle auf die Korrektheit der Arbeiten und die Funktionsfähigkeit der zuvor bearbeiteten Scheibe voraus. Das schließt auch die Beachtung und Auswertung von Fehlermeldungen und Warnungen des Systems mit ein. Sollten scheibenübergreifende Instandhaltungsmaßnahmen notwendig werden, sind entsprechende sicherheits- und sicherungstechnische Maßnahmen, insbesondere die Durchführung in Anlagenzuständen ohne Verfügbarkeitsanforderung an das betroffene System, vorzusehen. Diese sind zeitlich und technisch so zu planen, dass ein bisher nicht erkannter Fehler im geänderten Anlagensystem oder in den genutzten Prüf- und Programmiereinrichtungen möglichst bereits schon beim Einbringen in der 1. Redundanz und vor Einbringung in die weiteren Redundanz erkannt wird.

- Vor der erstmaligen Durchführung von Instandhaltungsmaßnahmen oder vor erstmaligem Einsatz geänderter Komponenten sind die Möglichkeiten ungewollter Wechselwirkungen mit anderen Komponenten zu analysieren, praktisch zu prüfen und gegebenenfalls durch geeignete Maßnahmen auszuschließen.

- Es sollte überprüft werden, ob die Instandhaltungsordnung bzw. weitere betriebliche Unterlagen entsprechend den o. a. Anforderungen angepasst werden müssen.

Die internationale Betriebserfahrung zeigt, dass insbesondere Änderungen an rechnerbasierten leittechnischen Systemen eine relevante Quelle für den Eintrag von (zusätzlichen) Fehlern darstellen. Daraus leiten sich folgende Anforderungen ab:

- Anzahl/Umfang von zukünftigen Änderungen sollte durch eine geeignete Planung, Auslegung und entsprechende Beschaffungs- und Fertigungsstrategien minimiert werden. Dies bedeutet insbesondere, dass auf kontinuierliche Fertigungsprozesse mit den daraus resultierenden kurzen Innovationszyklen verzichtet werden sollte. Stattdessen sollte eine Batch-Fertigung mit entsprechender Lagerhaltung erfolgen, so dass Innovationen zeitlich planbarer werden.

Zur Vermeidung des Eintrags von Fehlern bei dennoch erforderlichen Änderungen sollten insbesondere folgende Grundsätze angewandt werden:

- Für die Durchführung von Änderungen einschließlich Prüfung und Freigabe sind zumindest Verantwortlichkeiten für folgende Tätigkeiten festzulegen:

    - Vorschlag für eine Änderungen,
    - Prüfung des Vorschlages für die Änderung,
    - Entscheidung über die Durchführung der Änderung,
    - Durchführung der Änderung,
    - Prüfung der korrekten Umsetzung der Änderung.

Dabei ist sicherzustellen, dass die jeweils prüfende Stelle unabhängig von der vorschlagenden oder durchführenden Stelle ist, und dass die entscheidende Stelle unabhängig von der vorschlagenden Stelle ist.

- Änderungen sind sorgfältig zu planen mit ausreichend bemessenen Zeiträumen für Entwicklung und Implementierung, Begutachtung und Tests.

- Die Begründung, die Zielstellung und die Randbedingungen für die Änderung sind klar darzustellen.

- Für die Änderung ist eine Analyse der Auswirkungen auf das betroffene rechnerbasierte System selbst, auf die mit dem betroffenen rechnerbasierten System verbundenen (rechnerbasierten) Systeme und auf das zu steuernde verfahrenstechnische System vorzunehmen.

- Die durchzuführenden Tests und Simulationen sind zu definieren und zu begründen.

- Es ist zu bewerten, welche Teile der Typ- und Eignungsprüfung neu durchzuführen sind.

- Änderungen sind nur nach vorlaufender Verifikation in einer geeigneten Simulationsumgebung oder in der Anlage in einem geeigneten Anlagenzustand zulässig. Dabei ist nicht nur die geänderte Sollfunktionalität zu testen sondern auch die Erhaltung der nicht geänderten Funktionalitäten (z. B. Regressionstest, Tests abgeleitet aus der Analyse der Auswirkung der Änderung).

- Die Dokumentation der Änderung ist in die Dokumentation des rechnerbasierten Systems aufzunehmen.

12 Qualifizierung und Komplexität; Abgrenzung zwischen Typprüfung und Eignungsüberprüfung

Die gegenwärtige Fassung der KTA 3503 „Typprüfung von elektrischen Baugruppen der Sicherheitsleittechnik“ (Fassung: 11.2005) ist im Hinblick auf geeignete Prüfverfahren für rechnerbasierte Gerätetechnik ergänzungsbedürftig. Gleichzeitig stellt die Komplexität rechnerbasierter Sicherheitsleittechnik neue und erhöhte Anforderungen an die Typ- und Eignungsprüfung.

Im Rahmen einer Typprüfung ist der Nachweis zu erbringen, dass während der Entwicklung genügend Maßnahmen ergriffen worden sind, um die im Regelwerk festgelegten Anforderungen zu erfüllen, sowie dass die spezifizierten Funktionen enthalten und entsprechend durch praktische Tests geprüft sind. Die Eignung der Komponente für den Einsatzfall wird im Rahmen der Eignungsüberprüfung unter Berücksichtigung der Typprüfung geprüft.

Bisher stellt die Typprüfung nach Regelwerk eine reine Komponentenprüfung dar. Im Rahmen der Eignungsüberprüfung werden die anlagenspezifische Zusammenstellung (Funktion des Systems) und das Zusammenwirken der Komponenten geprüft.

Sofern die Typprüfungen keine Prüfaussagen bezüglich relevanter Systemeigenschaften zulassen, sollen ergänzende Prüfungen durchgeführt werden.

Hierzu sind für die Komponenten, die im funktionalen Zusammenhang stehen, Prüfungen der relevanten Systemeigenschaften und des Zusammenwirkens der Komponenten vorzusehen. Dies betrifft Merkmale wie Zeitverhalten, gerichtetes Versagensverhalten, die Wirksamkeit der Selbstüberwachung.

Die so genannten Feldgeräte (wie z. B. Messumformer, Schaltgeräte, Schutzeinrichtungen) müssen ebenso wie die leittechnischen Komponenten nach dem kerntechnischen Regelwerk unter Einbeziehung der CCF-Problematik qualifiziert werden.

Die Eignungsüberprüfung erfolgt im Allgemeinen von einem anderen Gutachter als die Typprüfung. Für die effektive Durchführung der Eignungsprüfung ist es wichtig, dass die im Rahmen der Typprüfung durchgeführten Prüfungen hinsichtlich Umfang und Tiefe nachvollzogen werden können. Damit die Typprüfung eines Gutachters später von dem Gutachter, der die Eignungsüberprüfung durchführt, anerkannt wird, ist es erforderlich, dass Tiefe und Umfang zwischen den Gutachtern abgestimmt werden. Hierzu wurde von der TÜV-Leitstelle Kerntechnik der Weisungsbeschluss 35 [12.1] erstellt. Wichtige Informationen in der Typprüfdokumentation sind u. a.:

- Detaillierte Beschreibung des Prüflings hinsichtlich der vorhandenen Geräte, Konfigurationen, Funktionen, Schnittstellen.

- Anforderungen des Herstellers an den Prüfling und Detailbeschreibung der technische Umsetzung der Anforderungen

- Angaben der der Prüfung zu Grunde gelegten Dokumente des Herstellers.

- Konkrete Angabe der berücksichtigten Anforderungen der verwendeten Prüfnormen. Bei der Auswahl der für die Prüfung relevanten Normenanforderungen kann die Verwendung eines Datenbanktools, mit dessen Hilfe eine Vorabfilterung der abzudeckenden wichtigsten Anforderungen möglich ist und das beispielhafte akzeptable Lösungen enthält, sinnvoll sein.

- Detaillierte Darstellung des Prüfumfangs (z. B. Functional Safety, Basic Safety (electrical, mechanical), EMV, Security, Verfügbarkeit). Hierbei sind auch die Prüfungen zur Software sowie Prüfungen zur Rückwirkungsfreiheit auf Sicherheitsteile von nicht sicherheitsrelevanten Komponenten/Teilsystemen anzugeben.

- Vollständige Angabe der eingesetzten Prüfmethoden und –verfahren.

- Vollständige Darstellung der Ergebnisse der einzelnen Prüfungen wie z. B.

    - wie konkret die Umsetzung der an den Prüfling gestellten Anforderungen erfolgt ist (vgl. safety case nach IEC 61508);
    - ob die spezifizierte Funktionalität eingehalten wird;
    - ob die in den Normen spezifizierten Qualitätsanforderungen (auch für Software) eingehalten werden;[11]
    - welches Fehlerverhalten die geprüfte Komponente aufweist.

- Teilweise kann das Fehlerverhalten einer Baugruppe, insbesondere von Software-Komponenten, nur in der Ablaufumgebung oder auf der Systemebene festgestellt werden. In diesen Fällen sollte in der Typprüfungsdokumentation ein entsprechender Hinweis vermerkt werden.

- Vollständige Darstellung der Einhaltung / Nichteinhaltung der relevanten Normanforderungen

Zusätzliche Erkenntnisse, die sich aus der Eignungsprüfung ergeben und auf Defizite bei der Typprüfung hinweisen, sollten im Rahmen einer Fortentwicklung der Typprüfverfahren berücksichtigt werden (Erfahrungsrückfluss).

Vor dem Hintergrund der Komplexität rechnerbasierter Sicherheitsleittechnik und zur künftigen Vermeidung von Unklarheiten erscheint es sinnvoll, dass sich die einschlägigen Prüfinstitutionen auf einheitliche Prüfstandards verständigen. Weiterhin erscheint es sinnvoll, dass zu rechnerbasierten Leittechniksystemen ein Prüfleitfaden, der die Typprüfung nach KTA 3503 konkretisiert, erstellt wird.

Diese Thematik sollte im Rahmen des Ausschusses Elektrische Einrichtungen behandelt und weiterverfolgt werden.

[11] Zu beachten ist hierbei, dass kein einheitlicher Bewertungsmaßstab existiert, in dem Qualitätsaussagen für Software-Komponenten festgelegt sind. Für Hardware-Komponenten gilt die KTA 3503 als Maßstab.

In Bezug genommene Unterlagen

Kapitel 1

[1.1] RSK-Ausschuss ELEKTRISCHE EINRICHTUNGEN; Positionspapier: „Rechnerbasierte Sicherheitsleittechnik für den Einsatz in der höchsten Sicherheitskategorie in deutschen Kernkraftwerken“; 04.06.2009

Kapitel 2

[2.1] DIN 40 041; Zuverlässigkeit: Begriffe; Dezember 1990

[2.2] VDI-Richtlinie 4001 Blatt 2: Begriffsbestimmungen zum Gebrauch des VDI-Zuverlässigkeitshandbuchs (Teil des VDI-Zuverlässigkeitshandbuchs); Juni 1986

[2.3] NTG- Empfehlung 3004: Zuverlässigkeitsbegriffe im Hinblick auf komplexe Software und Hardware, NTZ, 35(5):428-443, 1982

[2.4] E DIN IEC 61513; Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Allgemeine Systemanforderungen; Entwurf Fassung 2010-04

[2.5] DIN EN 62340: Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Anforderungen zur Beherrschung von Versagen aufgrund gemeinsamer Ursache; Fassung 2010-12

[2.6] VDI/VDE 3528: Regelung und Steuerung von Kernreaktoren; Spezielle Begriffe und Benennungen; 1972

[2.7] DIN EN 61226; Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Kategorisierung leittechnischer Funktionen; Fassung 2010-08

[2.8] DIN EN 60880: Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Softwareaspekte für rechnerbasierte Systeme zur Realisierung von Funktionen der Kategorie A, Fassung 2010-03

Kapitel 5

[5.1] IEC 61513; Nuclear power plants - Instrumentation and control for systems important to safety - General requirements for systems; Fassung 2001-03

[5.2] IAEA Safety Standards Series No. NS-R-1; Safety of Nuclear Power Plants: Design – Requirements; Fassung 2000

[5.3] IAEA Safety Standards Series No. NS-G-1.3; Instrumentation and control systems important to safety in Nuclear Power Plants; Safety Guide; Fassung 2002

[5.4] IEC 61508; Functional safety of electrical/electronic/programmable electronic safety-related systems; Fassungen 1998 und Entwurf 2010

[5.5] EN 50128, prEN 50128:2008; Railway applications - Communications, signalling and processing systems - Software for railway control and protection systems

[5.6] ISO DIS 26262; Road vehicles — Functional safety; Fassung 2009

[5.7] ISO 13849; Safety of machinery — Safety-related parts of control systems; Fassung 2006

[5.8] RTCA DO 178B bzw. ED-12B; Software Considerations in Airborne Systems and Equipment Certification; Fassung 1992

[5.9] ECSS-Q-80-03A; Space product assurance – Methods and techniques to support the assessment of software dependability and safety; Fassung Draft 2006

Kapitel 6

[6.1] E DIN IEC 61513; Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Allgemeine Systemanforderungen; Entwurf Fassung 2010-04

[6.2] DIN EN 62340: Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Anforderungen zur Beherrschung von Versagen aufgrund gemeinsamer Ursache; Fassung 2010-12

Kapitel 7

[7.1] E DIN IEC 61513; Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Allgemeine Systemanforderungen; Entwurf Fassung 2010-04

[7.2] DIN EN 62340: Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Anforderungen zur Beherrschung von Versagen aufgrund gemeinsamer Ursache; Fassung 2010-12

[7.3] U.S. NRC; Duke Energy Carolinas, LLC; Docket No. 50-269; Oconee Nuclear Station, Unit 1; Amendment to renewed facility operating license; 28.01.2010

[7.4] U.S.NRC; Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems; NUREG/CR-7007

Kapitel 9

[9.1] VdTÜV; Stellungnahme des VdTÜV zu den erforderlichen Vorsorgemaßnahmen gegen systematisches Versagen von digitalen leittechnischen Einrichtungen in kerntechnischen Anlagen, die Leittechnikfunktionen der Kategorie 1 ausführen; 22.01.2008

[9.2] Ulrich Waas; Auswirkungen von CCF-Postulaten an der Schnittstelle Leittechnik/Verfahrenstechnik; Textbeitrag vom 10. November 2010

Kapitel 12

[12.1] Weisungsbeschluss 35 der TÜV-Leitstelle Kerntechnik bei der VdTÜV: Prüfung von Serienbauteilen für Kernkraftwerke im Rahmen atomrechtlicher Genehmigungs- und Aufsichtsverfahren, Fassung 03.2004

Anhang

zur Stellungnahme „Rechnerbasierte Sicherheitsleittechnik für den Einsatz in der höchsten Sicherheitskategorie in deutschen Kernkraftwerken“ – Darstellung der Beratungsergebnisse der RSK-Arbeitsgruppe ERL

Beratungsverlauf

Die Arbeitsgruppe hat in insgesamt neun Sitzungen beraten. In der 1. Sitzung am 21.05.2010 /1.1/ nahm die Arbeitsgruppe entsprechend der Aufgabenstellung der RSK (426. Sitzung am 20.05.2010) /1.2/ ihre Arbeit auf und stellte auf Basis des Vorschlags /1.8/ unter Berücksichtigung von /1.3 - 1.7/, der Kommentierung /1.9/ und entsprechender Diskussionen einen Ablaufplan für die weiteren Beratungen auf. In einem Ablaufplan /1.10/ wurden die Aufgabenverteilung an die Arbeitsgruppenmitglieder und weiterer Experten aufgeführt.

In der 2. Sitzung am 21./22.06.2010 /2.1/ stand als Beratungsgegenstand die Darstellung des internationalen Standes zum Einsatz rechnerbasierter Systeme in der Sicherheitsleittechnik in Kernkraftwerken im Vordergrund, aufgeteilt in drei Komplexe:

1. Darstellung unterschiedlicher Sicherheitsphilosophien bzw. -konzepte und die Einordnung von Sicherheitsleittechnikarchitekturen in das Sicherheitskonzept;
2. Diversitätsmerkmale / Unabhängigkeitsmerkmale sowie gerichtetes / ungerichtetes Ausfallverhalten;
3. NUREG CR 7007 unter Bezugnahme von NRC BTP 7-19.

H. Verstegen stellte in seinem Vortrag /2.2/ die aus Sicht des VdTÜV aufzustellenden CCF Postulate für rechnerbasierte leittechnische Einrichtungen und die Gründe, die zu diesen Postulaten führen, dar. Anschließend führte er allgemeine Grundlagen der Auslegung der Sicherheitsleittechnik in US-amerikanischen Kernkraftwerken auf. H. Waas beschrieb in seinem Vortrag /2.3/ die Sicherheitsgrundsätze für die technische Auslegung eines rechnerbasierten Schutzsystems entsprechend den Ereignisklassen und Sicherheitsebenen. Er zeigte Schutzkonzepte gegen übergreifende Einwirkungen und die Folgerungen für die Sicherheitsleittechnik auf.

Unter dem 2. Thema gab Fr. Bühler /2.4/ einen Überblick über Realisierungen in ausländischen Anlagen basierend auf Informationen aus NUREG/CR-7007 /2.5/. Zum Begriffsunterschied von Dissimilarität und Diversität wurde auf die Definition aus /2.6/ hingewiesen. Als Beispiel aus der Praxis berichtete H. Verstegen über 11 ASN/GPR-Anforderungen zum EPR Flamanville 3 /2.7/. Des Weiteren erläuterte Dr. Fischer /2.8, Folie 16 + 17/ das Grundverständnis zur Anlagensicherheit und dem gestaffelten Vorgehen.

Zum 3. Themenkomplex erläuterte die GRS /2.9/ die Anforderungen der NRC an die Diversität als Vorkehrung gegen gemeinsam verursachte Ausfälle rechnerbasierter Sicherheitsleittechnik. Dabei wurde auf die wesentlichen Anforderungen aus BTP 7-19 /2.10/ und DI&C-ISG-02 /2.11/ sowie auf NUREG/CR-6303

/2.12/ eingegangen. Es wurden die Diversitätsaspekte aus NUREG CR 7007 /2.5/ erläutert und mit den Diversitätsaspekten aus /2.12/ verglichen. Als Beispiel für eine Umsetzung der Regeln ging die GRS kurz auf das Genehmigungsverfahren zur Umrüstung der Sicherheitsleittechnik auf Teleperm XS (TXS) im US-amerikanischen Kernkraftwerk in Oconee ein. Eine detaillierte Beschreibung des Oconee-Projekts nahm Dr. Graf vor /2.13/. Er beschrieb zuvor die regulativen Anforderungen, die in den USA an eine rechnerbasierte Leittechnik bzgl. CCF bestehen /2.10, 2.13, 2.14/. Außerdem wurden die Defense-in-Depth. und Diversitäts-Analyse einschließlich der unterstellten CCF-Fehlermodi sowie aus deren Ableitung die geforderte Qualität der Backup-Maßnahmen erläutert.

Auf der Basis der vorgestellten Berichte und unter Verweis auf einen Vortrag /2.15/ sowie auf NUREG/CR 7007 /2.5/, Abschnitt 4, erstellte der Vorsitzende im Nachgang der Sitzung eine systematische Zusammenstellung der verschiedenen Realisierungen mit Gegenüberstellung vergleichbarer Aspekte wie Diversität bzw. Dissimilarität /2.16/.

In der 3. Sitzung am 05./06.07.2010 /3.1/ wurde hinsichtlich bestehender Anforderungen zur Vermeidung / Beherrschung eines CCF ein Überblick über die internationale Normen und Regelwerke gegeben. Diskutiert wurde insbesondere, ob die Anforderungen vollständig sind.

Dr. Riekert erläuterte /3.2/ die Bewertung der digitalen Leittechnik im MDEP-Prozess der OECD NEA und die wesentliche Inhalte der IAEA Reports /3.3 und 4/. Dr. Lindner erläuterte, dass die Standards des SC 45A die Prinzipien der IAEA Safety Guides in technische Regeln implementiert /3.5/. Er gab einen Überblick über die IEC-Arbeiten. Außerdem erläuterte er den CDV (Committee Draft for Voting) IEC 61513 /3.6/ im Hinblick auf die Behandlung eines CCF. Weiterhin wies er hinsichtlich einer Wahrscheinlichkeitsbetrachtung für ein software-basiertes System auf /3.7/ hin. In Großbritannien darf für das Versagen eines softwarebasierten Systems im Anforderungsfall eine Wahrscheinlichkeit nicht kleiner als 10^{-4} belastet werden /3.8/. In der anschließenden Diskussion wurde auf den Vergleich digitaler Leittechnik-Anwendungen in ausländischen Kernkraftwerken /3.7/ verwiesen, bei dem vier Diversität-Auslegungsformen von software-basierter Sicherheitsleittechnik festgestellt wurden. In die Diskussion wurden die Unterlagen /3.9/ und /3.10/ einbezogen.

H. Schröder beschrieb die Berücksichtigung des CCF im IEC-Regelwerk der Serie IEC 61513 und deren untergeordneter Normen /3.11/. Im Zusammenhang mit seiner Ausführung zum Entwurf DIN EN 62340 verwies er auf /3.12/.

H. Faller beschrieb in seinem Vortrag Normen aus anderen Industrien hinsichtlich der Behandlung des CCF /3.13, 3.14/. Neben den IEC-Normen IEC 61508 und IEC 61511 verwies er abschließend auf die Aerospace Analysetechniken /3.15/ und auf die Hazop-Studien /3.16, 3.17/. Außerdem erläuterte er das Stress-Strength-Denkmodell, das in den meisten Industrien zugrunde gelegt ist.

In einem weiteren Vortrag wurde von H. Waas die Schnittstelle Leittechnik / Verfahrenstechnik am Beispiel einer DWR-Anlage dargestellt /3.18/.

Abschließend diskutierte die Arbeitsgruppe über mögliche Leittechnikarchitekturen unter Einbeziehung der bisherigen Diskussionen /2.16, 3.19/.

In der 4. Sitzung am 16./17.08.2010 /4.1/ erfolgte eine vertiefende Betrachtung von Einzelthemen. Dr. Graf beschrieb in seinem Vortrag die Umsetzbarkeit der funktionalen Diversität insbesondere auf Basis der DIN IEC 62340 /4.2/. Dr. Lindner erläuterte die Bedeutung und Wirksamkeit der für TXS vorgesehenen externen Überwachungseinrichtung (ExtÜ), die Bestandteil des VGB-Konzepts ist /4.3/. Partiell wurde in dem Zusammenhang auch das Thema Diversität angesprochen. Herr Waas berichtete über die Konsequenzen von länger anstehenden Fehlansteuerungen abhängig vom Postulat des gerichteten oder des ungerichteten Ausfallverhaltens /4.4/. Anschließend fasste die Arbeitsgruppe, die aus den Vorträgen gewonnenen Ergebnisse zusammen, die in die Stellungnahme einfließen sollten. Auf Basis eines Vorschlags /4.5, 4.6/ legte die Arbeitsgruppe Zielsetzung und Inhaltsschwerpunkte der Stellungnahme fest und stellte einen Zeitplan auf /4.7/.

In der 5. Sitzung am 27.09.2010 /5.1/ begann die Arbeitsgruppe nach einer kurzen Diskussion zu einem aktuellen Security-Thema (Schadsoftware „Stuxnet“) mit der Diskussion zum 1. ENTWURF/Stellungnahme /5.2/. Anhand eines Strukturvorschlags /5.3/ waren Zuarbeiten von den AG-Mitgliedern /5.4 – 5.14/ für einen ersten Entwurf einer Stellungnahme vereinbart worden.

In der 6. Sitzung am 13.10.2010 /6.1/ wurde die Diskussion zum ENTWURF/Stellungnahme /6.2/ fortgesetzt, in den zwischenzeitlich weitere Kommentierungen bzw. Ergänzungen /6.3 – 6.8/ eingefügt wurden. Außerdem lag die Unterlage /6.9/ vor.

In der 7. Sitzung am 08. /09.12.2010 /7.1/ wurde die Arbeitsgruppe von Dr. Haake, TÜV Nord, und Dr. Lindner, ISTec, über die Typprüfung des TXS-Systems informiert /7.2, 7.3/. Anschließend setzte die Arbeitsgruppe seine Diskussion zum zwischenzeitlich von H. Brettner überarbeiteten ENTWURF/Stellungnahme unter Einbeziehung von Beiträgen der Arbeitsgruppenmitglieder fort. Es konnte kein Konsens hinsichtlich des Textes und Umfang erzielt werden /7.15/. Die wesentlichen Aussagen des ENTWURF/Stellungnahme sollen in einer Executive Summary zusammengefasst werden und als gemeinsames Papier der Arbeitsgruppe verabschiedet werden. Die Langfassung des Textes soll nur von einem Teil der Arbeitsgruppe gebilligt und der RSK vorgelegt werden.

In der 8. Sitzung am 09.02.2011 beriet die Arbeitsgruppe kurz zu dem Thema „Redesign von Baugruppen“ /8.2 - 8.4/ und kam zu dem Ergebnis, dass die weiteren Beratungen im Ausschuss ELEKTRISCHE EINRICHTUNGEN erfolgen sollten. Anschließend setzte die Arbeitsgruppe seine Beratung zur Stellungnahme fort. Der in der 7. Sitzung durchgesprochenen Entwurf (im Folgenden „Langfassung“ genannt) /7.15/ wurde zwischenzeitlich überarbeitet /8.5, 8.6/. Die wesentlichen Aussagen sollen in einer Executive Summary zusammengefasst werden und als gemeinsames Papier der AG verabschiedet werden.

Gegenstand der Diskussion war der als Executive Summary (im Folgenden mit „Kurzfassung“ bezeichnet) zusammengefasste Entwurf /8.7, 8.8/. Unter Einbeziehung weitere Unterlagen /8.9 - 8.11/ sowie weiterer Anmerkungen und Ergänzungen überarbeitete die Arbeitsgruppe die Kurzfassung der Stellungnahme /8.12/. Im Nachgang der Sitzung wurde der Entwurf unter Einbeziehung der Absprachen auf der 8. AG ERL

Sitzung und der eingegangen Kommentare und Textüberarbeitungen /8.13/ als Beratungsunterlage für die abschließende 9. Sitzung überarbeitet.

In der 9. Sitzung am 07.09.2011 lagen zusätzlich zur Unterlage /8.13/ Kommentare von Fr. Bühler/H. Verstegen /9.1/, Dr. Riekert /9.2/ und H. Waas/Dr. Graf /9.3/ vor. Nach Diskussion verabschiedete die Arbeitsgruppe die vorliegende Fassung.

Beratungsunterlagen

/1.1/ Kurzprotokoll der RSK-Ad-hoc-Arbeitsgruppe Einsatz Rechnerbasierter Leittechnik (ERL) der 1. Sitzung am 21.05.2010 (EP_AG-ERL1.doc)

/1.2/ M. Brettner, Vorschlag für die Aufgabenstellung für die RSK Ad-hoc-Arbeitsgruppe „Einsatz Rechnerbasierter Sicherheitsleittechnik“ (AG ERL), 426. RSK-Sitzung am 20.05.2010 (Vorschlag Aufgabenstellung AG ERL 100518.doc)

/1.3/ M. Brettner, „RSK AG Einsatz rechnerbasierter Sicherheitsleittechnik der höchsten Sicherheitskategorie: Eingrenzung des Beratungsbedarfs abgeleitet aus einem Abgleich bestehender Anforderungen in RSK LL DWR, Modul 5 und Positionspapier RSK Ausschuss EE“, 11.05.2010, (Eingrenzung Beratungsbedarf 11-5-2010.doc)

/1.4/ BMU, „ Sicherheitskriterien für Kernkraftwerke, REVISION D, APRIL 2009 (modulerevisiond020709.pdf)

/1.5/ RSK-Leitlinien für Druckwasserreaktoren, Ursprungsfassung (3. Ausgabe vom 14. Oktober 1981) mit Änderungen vom 15.11.1996 (RSK_LL96.pdf)

/1.6/ RSK418, Info-7, „Rechnerbasierte Sicherheitsleittechnik für den Einsatz in der höchsten Sicherheitskategorie in deutschen Kernkraftwerken“ - Positionspapier des Ausschusses ELEKTRISCHE EINRICHTUNGEN“ einschließlich 9 Anlagen, (RSK418_Info-7_RSK418 inkl. Anhang 1-9.pdf)

/1.7/ R. Faller, „Ad-hoc AK ERL Einsatz rechnerbasierte Leittechnik, SILT Diskussion“ (AdHoc AK ERL.pdf)

/1.8/ M. Brettner, Vorschlag Beratungsgegenstände (hier nur CCF) für 1. Sitzung der AG ERL am 21.05.2010 (e-mail_Brettner_19.05.2010_Vorschlag_Beratungsgegenstände hier_nur_CCF für 1. Sitzung.pdf)

/1.9/ C. Verstegen, Kommentare /Änderungswünsche zum Vorschlag Beratungsgegenstände für 1. Sitzung der AG ERL am 21.05.2010 (VorschlagBrettnerKomVer-1.doc)

/1.10/ Anhang zum Kurzprotokoll der 1. Sitzung Arbeitsgruppe ERL am 21.05.2010 (Anhang EP_AG-ERL1_Ablaufplan der Beratungen.doc)

/2.1/ Kurzprotokoll der 2. Sitzung der RSK-Ad-hoc-Arbeitsgruppe Einsatz Rechnerbasierter Leittechnik (ERL) am 21./22.06.2010 (EP_AG-ERL2.doc)

/2.2/ C. Verstegen, Fehlerpostulate und Grundlagen der Auslegung in US KKW, 2. Sitzung AG ERL, 21./22.06.2010 (Verstegen, GRS, Fehlerpostulate.ppt)

/2.3/ U. Waas, Einordnung von Sicherheitsleittechnikarchitekturen in das Sicherheitskonzept, Foliensatz ,(RSK-AG_DSILT_20100621-ang.ppt)

/2.4/ Cornelia Bühler, TÜV SÜD Industrie Service GmbH, Vorsorgemaßnahmen gegen CCF, Beispiele zum internationalen Stand basierend auf NUREG/CR-7007, RSK-Arbeitsgruppe ERL 21./22.06.2010, Foliensatz (ERL internationaler Stand.ppt)

/2.5/ US NRC, NUREG/CR 7007, Diversity Strategies für Nuclear Power Plant Instrumentation and Control Systems, published February 2010 (NUREGcr7007.pdf)

/2.6/ Cornelia Bühler, TÜV SÜD Industrie Service GmbH, Digitale Leittechnik im Reaktorschutz Vorsorgemaßnahmen gegen CCF Die Anforderungen der Sachverständigen im VdTÜV, Symposium des TÜV Nord am 29. – 30.09.2009 in Hamburg (09 Bühler_Symposium TÜV Nord 9 2009.pdf)

/2.7/ C. Verstegen, GRS, Forderungen der ASN zur geplanten Architektur der softwarebasierten Leittechnik im französischen EPR Flamanville 3 – „Réacteurs nucléaires à eau sous pression Projet EPR-Flamanville 3 – Architecture générale du contrôle-commande et des plateformes associées“ von der französischen Aufsichtsbehörde (Autorité de Sureté Nucléaire ASN) an die EDF (15.10.2009), 21./22. Juni 2010, Foliensatz (RSK ERL_170610.ppt)

/2.8/ Dr.-Ing. Erwin Fischer, Technische Leitung Kernkraftwerk Isar, Sicherer Langzeitbetrieb von Kernkraftwerken – ein Widerspruch?, 3. VdTUV-Forum Kerntechnik 2010, Berlin 15.-16- Marz 2010 (25_Fischer-Langzeitbetrieb.pdf)

/2.9/ J. Stiller, D. Sommer, C. Verstegen, GRS, Anforderungen der NRC an Diversität als Vorkehrung gegen gemeinsam verursachte Ausfälle softwarebasierter Sicherheitsleittechnik, 2. Sitzung der Ad-hoc-Arbeitsgruppe „Einsatz Rechnerbasierter Leittechnik“ (ERL) der RSK, Foliensatz (GRS-Vortrag Stiller.ppt)

/2.10/ US NRC, BTP 7-19, Branch Technical Position 7-19, Guidance for Evaluation of Diversity and Defense-In-Depth in Digital Computer-Based Instrumentation and Control Systems (BTP19_rev5.pdf)

/2.11/ US NRC, DI&C-ISG-02, Task Working Group #2: Diversity and Defense-in-Depth Issues, Interim Staff Guidance, Revision 2 (TWG #2 ISG R2.pdf)

/2.12/ NUREG/CR-6303, Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems, published Dezember 1994 (NUREGCR-6303.pdf)

/2.13/ Arnold Graf, I&C Architecture Design Authority, AREVA, CCF Behandlung im Genehmigungsverfahren Oconee, 2010-06-14, Foliensatz (Oconee Licensing.ppt)

/2.14/ Answers to questions (Answers to Questions.doc)

/2.15/ Arndt Lindner, Institut für Sicherheitstechnologie (ISTec) GmbH, Anforderungen an rechnerbasierte Sicherheitsleittechnik für den Einsatz in der höchsten Sicherheitskategorie in deutschen Kernkraftwerken, Bonn 18./19.02.2008 (RSK-Workshop "Digitale Leittechnik"), 2 Foliensätze (RSK-Workshop-Vortrag04-Lindner_RSK Workshop_1.ppt, RSK-Workshop-Vortrag04- Lindner_RSK Workshop_2.ppt)

/2.16/ M. Brettner, RSK Ad-Hoc Arbeitsgruppe „Einsatz Rechnerbasierter Leittechnik (AG ERL)" Darstellung möglicher Leittechnikarchitekturen unter Einbeziehung des bisherigen Diskussionsstandes in der AG, Bremen, 30.06.2010 (Strukturierung von Leittechnikarchitekturen_30-6-2010.doc)

/3.1/ Kurzprotokoll der 3. Sitzung der RSK-Ad-hoc-Arbeitsgruppe Einsatz Rechnerbasierter Leittechnik (ERL) am 05./06.07.2010 (EP_AG-ERL3.doc)

/3.2/ Dr. Thomas Riekert, RSK, Überblick über internationale Normen und Regelwerk: MDEP OECD NEA, IAEA, Foliensatz, (Vortrag DrRi.ppt)

/3.3/ IAEA Nuclear Energy Series, No NP-T-1.4, Implementing Digital Instrumentation and Control Systems in the Modernization of Nuclear Power Plants (IAEA_Implementing digital I and C.pdf)

/3.4/ IAEA Nuclear Energy Series, No NP-T-1.5, Protecting against Common Cause Failures in Digital I&C Systems of Nuclear Power Plants (Pub1410_web.pdf)

/3.5/ Dr. Lindner, IEC/SC45A Standards, Tabelle (IEC_SC45A Standards.docx)

/3.6/ Arndt Lindner, Institut für Sicherheitstechnologie (ISTec) GmbH, 3. Sitzung der Ad-hoc-Arbeitsgruppe „Einsatz Rechnerbasierter Leittechnik" (ERL) der RSK, Foliensatz (IEC61513-CCF.pptx)

/3.7/ Arndt Lindner, Institut für Sicherheitstechnologie (ISTec) GmbH, Anforderungen an rechnerbasierte Sicherheitsleittechnik für den Einsatz in der höchsten Sicherheitskategorie in deutschen Kernkraftwerken Bonn 18./19.02.2008, Digitale Sicherheitsleittechnik – Anwendungen in ausländischen Kernkraftwerken (modifiziert für 3. Sitzung der Ad-hoc-Arbeitsgruppe „Einsatz Rechnerbasierter Leittechnik" (ERL) der RSK), Foliensatz (RSK-WS_mod.ppt)

/3.8/ B. Littlewood et. al., Modelling Softwaredesign diversity: a review, (Bev Littlewood et al, Modelling software design diversity.pdf)

/3.9/ Stellungnahme des VdTÜV zu den erforderlichen Vorsorgemaßnahmen gegen systematisches Versagen von digitalen leittechnischen Einrichtungen in kerntechnischen Anlagen, die Leittechnikfunktionen der Kategorie 1 ausführen, 06.03.2008 (Erforderliche_Vorsorgemaßnahmen_digitale_Sicherheitsleittechnik.pdf)

/3.10/ B. Littlewood, The use of proof in diversity arguments, (Diversity_and_logic.pdf)

/3.11/ M. Schröder, Behandlung CCF in DIN IEC 61513, 3. Sitzung der Ad-hoc-Arbeitsgruppe „Einsatz Rechnerbasierter Leittechnik“ (ERL) der RSK am 05./06.07.2010 (100605-ERL-Behandlung_CCF_in_DIN_IEC_61513.ppt)

/3.12/ Anhang 9 des Positionspapiers des Ausschusses ELEKTRISCHE EINRICHTUNGEN 8 EE200_Positionspapier-Anhang9.doc)

/3.13/ R. Faller, Ad-hoc AK ERL Einsatz Rechnerbasierter Leittechnik, (AdHoc AK ERL R2 CCA.ppt),
einschließlich:
P.G. Bishop, Adelard, Review of Software Design Diversity
Bev Littlewood et al, Modelling software design diversity
Susan Brilliant, John Knight, Nancy Leveson, Analysis of Faults in an N-Version Software Experiment

/3.14/ Tabelle zu /3.13/, (Tabelle von AdHoc AK ERL R2 CCA.xls)

/3.15/ Draft ECSS-Q-80-03, Space product assurance Methods and techniques to support the assessment of software dependability and safety, 1 March 2006 (Draft-ECSS-Q-80-03A(1March2006).pdf)

/3.16/ Ministry of Defence, Defence Standard 00-58, HAZOP Studies on Systems Containing Programmable Electronics, Part 1 Requirements, Issue 2 Publication Date 19 May 2000 (DStan 00-58-1-Hazop Teil1.pdf)

/3.17/ Ministry of Defence, Defence Standard 00-58, HAZOP Studies on Systems Containing Programmable Electronics, Part 2 General Application Guidance, Issue 2 Publication Date 19 May 2000 ((DStan 00-58-1-Hazop Teil2.pdf)

/3.18/ U. Waas, Schnittstelle Verfahrenstechnik/Leittechnik am Beispiel einer DWR-Anlage (RSK-AG-ERL_vitale_20100706.PPT)

/3.19/ /2.16/ mit Änderungen aus der 3. Sitzung (Strukturierung von Leittechnikarchitekturen_30-6-2010 Änderung.doc)

/4.1/ Kurzprotokoll der 4. Sitzung der RSK-Ad-hoc-Arbeitsgruppe Einsatz Rechnerbasierter Leittechnik (ERL) am 16./17.08.2010 (EP_AG-ERL4.doc)

/4.2/ Dr. Graf, „Umsetzbarkeit funktionaler Diversität", (Funktionale Diversitaet_fin.pptx)

/4.3/ Arndt Lindner, Institut für Sicherheitstechnologie (ISTec) GmbH, 4. Sitzung der Ad-hoc-Arbeitsgruppe „Einsatz Rechnerbasierter Leittechnik" (ERL) der RSK, Wirksamkeit der externen Überwachungseinrichtung, (ERL_WEUE.pptx)

/4.4/ U. Waas, „Konsequenzen von länger anstehenden Fehlansteuerungen", RSK-AG-ERL, 16.08.2010 (RSK-AG_DSILT_CCF-LT-VT_20100816.ppt)

/4.5/ M. Brettner, „Strukturvorschlag für die Darstellung der Beratungsergebnisse der RSK AG ERL", Bremen, den 16. Juli 2010 (Strukturvorschlag Beratungsergebnisse AG ERL 16-7-2010.doc)

/4.6/ Dr. Riekert, „Vorschlag für eine Gliederung der Empfehlung zur digitalen Sicherheitsleittechnik für den Reaktorschutz", (Riekert_Vorschlag fuer Gliederung_15.07.2010.doc)

/4.7/ Strukturvorschlag für die Darstellung der Beratungsergebnisse der RSK AG ERL, in der 4. Sitzung am 17.08.2010 überarbeitet (Strukturvorschlag Beratungsergebnisse AG ERL 4.Sitzung-17.08.2010.doc)

/5.1/ Kurzprotokoll der 5. Sitzung der RSK-Ad-hoc-Arbeitsgruppe Einsatz Rechnerbasierter Leittechnik (ERL) am 27.09.2010 (EP_AG-ERL5.doc)

/5.2/ RSK-Information Nr. ERL5, ENTWURF/Stellungnahme „Rechnerbasierte Sicherheitsleittechnik für den Einsatz in der höchsten Sicherheitskategorie in deutschen Kernkraftwerken" – Ergebnisse der RSK-Arbeitsgruppe ERL", 27.09.2010 Dr. Graf, „Umsetzbarkeit funktionaler Diversität", (ERL-Stellungnahme_27-09-2010_Sitzung_5)

/5.3/ M. Brettner, „Strukturvorschlag für die Darstellung der Beratungsergebnisse der RSK AG ERL", überarbeitet in 4. Sitzung AG ERL, 17.08.2010 (Strukturvorschlag Beratungsergebnisse AG ERL 4.Sitzung-17.08.2010)

/5.4/ M. Brettner, „Begriffe", Abschnitt 2, (Entwurf zu Abschnitt 2 - Begriffe.doc)

/5.5/ Dr. Lindner, Kommentare zu /2/, Abschnitt 2, (Entwurf zu Abschnitt 2 - Begriffe_Kommentare Lindner.doc)

/5.6/ W. Fischer, „Software basierte Sicherheitsleittechnik –Prinzipielle Vor- und Nachteile – Sicherheitstechnischer Nutzen/Gewinn", 19.09.2010, Abschnitt 4 (Vor u Nachteile softwarebasierter Lettechnik_v02_RSK.doc)

/5.7/ Dr. Riekert, „5. Übergeordnete Anforderungen im bestehenden deutschen Regelwerk und Anpassungsnotwendigkeiten", Kurzfassung, 08.09.2010, Abschnitt 5 (Kapitel 5 DrRi 06092010 Kurzfassung)

/5.8/ Dr. Riekert, „5. Übergeordnete Anforderungen im bestehenden deutschen Regelwerk und Anpassungsnotwendigkeiten", 08.09.2010, (Kapitel 5 DrRi 06092010)

/5.9/ M. Schröder, „6. Übersicht über Ansätze im internationalen Regelwerk zum Lebenszyklus rechnerbasierter Sicherheitsleittechnik, 6.1 Allgemeine Übersicht über Regelungsinhalte im IEC und DIN-IEC-Regelwerk", 20.09.2010, Abschnitt 6.1 (Kapitel_6 1_Regelungsinhalte_IEC_DIN-IEC_05.doc)

/5.10/ Dr. Graf, „Diversität als Maßnahme zur CCF Vermeidung / Beherrschung", 14.09.2010, Abschnitt 7 (Diversität als Massnahme.pdf)

/5.11/ M. Brettner, „Diversitätsentscheidungen und Diversität im Ausfallverhalten", 19.09.2010, Abschnitt 7 (7b_Entwurf zu Abschnitt 7)

/5.12/ H. Faller, „Vorschlag für Ergänzungen der Qualifizierungsanforderungen an Rechner in Cat A Funktionen", 13.09.2010, Abschnitt 8 (RSK ERL R002 V0R2.docx)

/5.13/ U. Waas, „Auswirkungen von CCF-Postulaten an der Schnittstelle Leittechnik/Verfahrenstechnik", 21.09.2010, Abschnitt 9 (RSK-Beratung_SILT_CCF-Postulate_LT-VT_20100918.doc)

/5.14/ M. Brettner, „Abschnitt 10 der Darstellung der Beratungsergebnisse der RSK AG ERL", 15.09.2010, Abschnitt 10 (Entwurf Abschnitt 10 Beratungsergebnisse AG ERL 15-09-2010.doc)

/6.1/ Kurzprotokoll der 6. Sitzung der RSK-Ad-hoc-Arbeitsgruppe Einsatz Rechnerbasierter Leittechnik (ERL) am 13.10.2010, ENTWURF (EEP_AG-ERL6.doc)

/6.2/ RSK-Information Nr. ERL6, ENTWURF/Stellungnahme „Rechnerbasierte Sicherheitsleittechnik für den Einsatz in der höchsten Sicherheitskategorie in

deutschen Kernkraftwerken“ Fassung 12.10.2010 (ERL-Stellungnahme_Sitzung_6_12-10-2010.doc)

/6.3/ Ergänzung zu Abschnitt 10, Dr. Riekert, 27.09.2010 (e-mail_Riekert_27.09.2010_AW AG ERL Unterlagen.pdf)

/6.4/ Ergänzungen und Kommentierungen zu Abschnitt 7a, H. Verstegen, 07.10.2010 (7_Verstegen_07.10.2010_Kap. 7a)

/6.5/ Ergänzungen und Kommentierungen zu Abschnitt 9.1, H. Verstegen, 07.10.2010 (9_Verstegen_07.10.2010_Kap. 9-1.doc)

/6.6/ Ergänzungen und Kommentierungen zu Abschnitt 10, H. Verstegen, 07.10.2010 (10_Verstegen_07.10.2010_Kap. 10.doc), 07.10.2010

/6.7/ Ergänzung zu Abschnitt 6.2, Dr. Riekert, 11.10.2010 (6.2_Riekert_Kapitel 6_2 DrRi 22092010.doc)

/6.8/ Kommentierung Abschnitt 7a, Dr. Graf, 12.10.2010 (7a_Graf_12.10.2010_Kap. 7a_gr.doc)

/6.9/ Kommentierung Abschnitt 9, H. Waas, 12.10.2010 (9_Waas_12.10.2010_Wa_Verstegen_Kap. 9.doc)

/7.1/ Kurzprotokoll der 7. Sitzung der RSK-Ad-hoc-Arbeitsgruppe Einsatz Rechnerbasierter Leittechnik (ERL) am 08./09.12.2010, ENTWURF (EPV_AG-ERL7.doc)

/7.2/ Dr. D. Haake, TÜV-Nord SysTec GmbH & Co. KG, „Aspekte zur Typprüfung TXS“, 8. Dezember 2010 (RSK_DLT_20101208_Haa2)

/7.3/ Dr. Lindner, „Software-Prüfungen“, 08.11.2010 (SW-Pruefungen)

/7.4/ U. Waas, Anmerkungen zu Kapitel 9, 07.11.2010 (Kap. 9_2010-11-10.doc)

/7.5/ RSK-Information „Rechnerbasierte Sicherheitsleittechnik für den Einsatz in der höchsten Sicherheitskategorie in deutschen Kernkraftwerken“ – Darstellung der Beratungsergebnisse der RSK-Arbeitsgruppe ERL (ENTWURF/Stellungnahme), Stand 19.11.2010 (ERL-Stellungnahme_neu_19-11-2010.doc)

/7.6/ R. Faller, Anmerkungen zu „Rechnerbasierte Sicherheitsleittechnik für den Einsatz in der höchsten Sicherheitskategorie in deutschen Kernkraftwerken“ – Darstellung der

Beratungsergebnisse der RSK-Arbeitsgruppe ERL (ENTWURF/Stellungnahme), Stand 19.11.2010 (ERL-Stellungnahme_neu_19-11-2010_RF.doc)

/7.7/ Cornelia Bühler, „Rechnerbasierte Sicherheitsleittechnik für den Einsatz in der höchsten Sicherheitskategorie in deutschen Kernkraftwerken“ – Darstellung der Beratungsergebnisse der RSK-Arbeitsgruppe ERL, Stand: 19.11.2010 - Generelle übergeordnete Kommentare zu den einzelnen Kapiteln, 07.12.2010

/7.8/ C. Bühler, C. Verstegen, Ergänzung zu 10.3, Seite 44, (Textauszug Abschnitt 9.3_Architektur 1bue_ver.doc)

/7.9/ C. Verstegen, Kommentare zu „Rechnerbasierte Sicherheitsleittechnik für den Einsatz in der höchsten Sicherheitskategorie in deutschen Kernkraftwerken“ – Darstellung der Beratungsergebnisse der RSK-Arbeitsgruppe ERL (ENTWURF/Stellungnahme), Stand 19.11.2010, (Verstegen_ERL-Stellungnahme_neu_19-11-2010.doc)

/7.10/ RSK-Information „Rechnerbasierte Sicherheitsleittechnik für den Einsatz in der höchsten Sicherheitskategorie in deutschen Kernkraftwerken“ – Darstellung der Beratungsergebnisse der RSK-Arbeitsgruppe ERL (ENTWURF/Stellungnahme), Stand 06.12.2010 (ERL-Stellungnahme_neu_06-12-2010.doc)

/7.11/ RSK-GS, Waldorf, Anhang zu „Rechnerbasierte Sicherheitsleittechnik für den Einsatz in der höchsten Sicherheitskategorie in deutschen Kernkraftwerken“ – Darstellung der Beratungsergebnisse der RSK-Arbeitsgruppe ERL (ENTWURF/Stellungnahme), Stand 06.12.2010, „3. Beratungsverlauf“ (3_ERL-Stellungnahme_Anhang 3 Beratungsgang.doc)

/7.12/ HSE Health and Safety Executive, “Out of control, Why control systems go wrong and how to prevent failure”, ISBN 978 0 7176 2192 7 (hsg238.pdf)

/7.13/ R. Faller, exida, “Common Cause Analysis for Integrated Circuits with On-Chip Redundancy”, Safetronic 2010 (Safetronic exida IC CCA V3R1.pdf)

/7.14/ Nuclear Engineering International, “USA’s first fully digital station”, November 2010 (Nucl.Eng.Oconee_stuxnet.pdf)

/7.15/ RSK-Information „Rechnerbasierte Sicherheitsleittechnik für den Einsatz in der höchsten Sicherheitskategorie in deutschen Kernkraftwerken“ – Darstellung der Beratungsergebnisse der RSK-Arbeitsgruppe ERL (ENTWURF/Stellungnahme), Stand 06.12.2010 (7.Sitzung ERL-Stellungnahme_09-12-2010.doc)

/8.1/ Kurzprotokoll der 8. Sitzung der RSK-Ad-hoc-Arbeitsgruppe Einsatz Rechnerbasierter Leittechnik (ERL) am 09.02.2011, ENTWURF (EPV_AG-ERL8.doc)

/8.2/ Vereinigte Elektronikwerkstätten GmbH, „REDESIGN, NACHFERTIGUNG, NEUENTWICKLUNG“, Schreiben vom 07.01.2011 an das BMU, H. Fabian (Brief Bundesministerium f. Umwelt Fabian 07.01..doc) einschließlich Prospekt (_Prospekt-VEW-Bremen.pdf), Referenzen (_ausgewaehlte-Referenzen_VEW-Bremen.pdf) und Anzeige aus VGB PowerTech 12/2010, Seite 15

/8.3/ VGB PowerTech 10/2010, Hentschel et al, „Alterungsmanagement der Elektro- und Leittechnik in Kraftwerken der RWE Power“, (_Hentschel_et_al-2010_Alterung-EuLT_VGB-Powertech.pdf)

/8.4/ A: Graf; „Redesigns Programmable Logic Devices”, Foliensatz, (PLD_Redesign.ppt)

/8.5/ RSK-Information ERL7/Info_HP, „Rechnerbasierte Sicherheitsleittechnik für den Einsatz in der höchsten Sicherheitskategorie in deutschen Kernkraftwerken“ - „Zwischen den AG ERL Mitgliedern Brettner, Faller, Fischer, Graf, Riekert, Schröder und Waas abgestimmtes Hintergrundpapier zur gemeinsam getragenen Darstellung der Beratungsergebnisse der RSK-Arbeitsgruppe ERL“”, Entwurf vom 26.01.2011 (7.Sitzung ERL-Langfassung_26-01-2011.doc)

/8.6/ Kommentare von H. Schröder zu /2.2/ vom 07.02.2011 (7.Sitzung ERL-Langfassung_26-01-2011_Anmerkungen_Sch.doc)

/8.7/ RSK-Information ERL7/Info 1, “„Rechnerbasierte Sicherheitsleittechnik für den Einsatz in der höchsten Sicherheitskategorie in deutschen Kernkraftwerken“ Darstellung der Beratungsergebnisse der RSK-Arbeitsgruppe ERL”, Entwurf vom 14.01.2011 (7.Sitzung ERL-Stellungnahme_14-01-2011_Kurzfassung.doc)

/8.8/ RSK-Information ERL7/Info 1, “„Rechnerbasierte Sicherheitsleittechnik für den Einsatz in der höchsten Sicherheitskategorie in deutschen Kernkraftwerken“ Darstellung der Beratungsergebnisse der RSK-Arbeitsgruppe ERL”, Entwurf vom 17.01.2011 (7.Sitzung ERL-Stellungnahme_17-01-2011_Kurzfassung.doc)

/8.9/ C. Bühler, C. Verstegen, „gekürzte Fassung der RSK-Information ERL7/Info 1 vom 14.01.2011“, 21.01.2011 (7 Sitzung ERL-Stellungnahme_14-01-2011_Kurzfassung gekuerzt.doc)

/8.10/ Dr. Riekert, „Anmerkungen zur RSK-Information ERL7/Info 1 vom 17.01.2011“, 06.02.2011 (ERL-Stellungnahme_17-01-2011_Kurzfassung_DrRi.doc)

/8.11/ U. Waas, „Kapitel 14: Zusammenstellung abgeleiteter Anforderungen und Empfehlungen“, 04.02.2011 (7 Sitzung ERL-Stellungnahme_Kap.14_20110204.doc)

/8.12/ RSK-Information ERL8/Info 1, “„Rechnerbasierte Sicherheitsleittechnik für den Einsatz in der höchsten Sicherheitskategorie in deutschen Kernkraftwerken“ Darstellung der Beratungsergebnisse der RSK-Arbeitsgruppe ERL”, Entwurf vom 09.02.2011 (ERL-Stellungnahme_Kurzfassung_09.02.2011.doc)

/8.13/ RSK-Information ERL9/Info 1, “„Rechnerbasierte Sicherheitsleittechnik für den Einsatz in der höchsten Sicherheitskategorie in deutschen Kernkraftwerken“ Darstellung der Beratungsergebnisse der RSK-Arbeitsgruppe ERL”, Entwurf vom 09.02.2011 (ERL-Stellungnahme_Kurzfassung_09.03.2011.doc)

/9.1/ /8.13/ mit Kommentare von Frau Bühler und Herrn Verstegen, 16.08.2011 (ERL-Stellungnahme_16-08-2011_VER_BUE an Brettner.doc)

/9.2/ /9.1/ mit Kommentare von Herrn Dr. Riekert, 03.09.2011 (ERL-Stellungnahme_16-08-2011_VER_BUE Struktur DrRi.doc)

/9.3/ /9.1/ mit Kommentare von Herrn Dr. Riekert, 03.09.2011 (ERL-Stellungnahme_16-08-2011_VER_BUE an Brettner_gr+wa.doc)