Forschungsarbeiten zur Entwicklung einer Bewertungsgrundlage für rechnerbasierte und programmierbare Leittechniksysteme in kerntechnischen Anlagen und Erforschung des Weiterentwicklungsbedarfs der dazugehörigen Anforderungen in der Leittechnik

GRS - 649

Gesellschaft für Anlagen-
und Reaktorsicherheit
(GRS) gGmbH

Forschungsarbeiten zur Entwicklung einer Bewertungsgrundlage für rechnerbasierte und programmierbare Leittechniksysteme in kerntechnischen Anlagen und Erforschung des Weiterentwicklungsbedarfs der dazugehörigen Anforderungen in der Leittechnik

Bewertungsgrundlage für digitale Leittechnik

Christian Müller
Ewgenij Piljugin

September 2021

Anmerkung:

Das diesem Bericht zugrunde liegende Forschungsvorhaben wurde mit Mitteln des Bundesministeriums für für Umwelt, Naturschutz und nukleare Sicherheit (BMU) unter dem Kennzeichen 4718R01530 durchgeführt.

Die Verantwortung für den Inhalt dieser Veröffentlichung liegt bei der GRS.

Der Bericht gibt die Auffassung und Meinung der GRS wieder und muss nicht mit der Meinung des BMU übereinstimmen.

GRS - 649
ISBN 978-3-949088-38-4

Deskriptoren

Bewertungsgrundlage, Digitale Leittechnik, modellbasierte Analyse, PSA

Inhaltsverzeichnis

1 Einleitung

Eine zentrale Aufgabe der GRS ist die Gewinnung wissenschaftlicher Erkenntnisse sowie die Entwicklung von Grundlagen auf dem Gebiet der Reaktorsicherheit, um den hohen Sicherheitsstand deutscher Kernkraftwerke zu erhalten und ggf. zu verbessern sowie um die Ereignisse in ausländischen kerntechnischen Anlagen bewerten zu können. Forschung und Entwicklung gehören zu den Grundvoraussetzungen für die ständige Verbesserung der Sicherheit kerntechnischer Einrichtungen im In- und Ausland. Der sichere Betrieb kerntechnischer Einrichtungen und Kernkraftwerke erfordert deshalb eine kontinuierliche, an sicherheitstechnischen Zielen ausgerichtete, qualitativ hochwertige und effiziente Forschung, die sich an internationalen Maßstäben orientiert und diese umsetzt. Daher gehört zu den grundlegenden Zielen der GRS, den aktuellen Stand von Wissenschaft und Technik nicht nur zu kennen und jederzeit darstellen zu können, sondern auch die Weiterentwicklung des Standes von Wissenschaft und Technik (W&T) aktiv zu betreiben.

In deutschen Kernkraftwerken werden für Leittechnikfunktionen der Sicherheitssysteme (z. B. im Reaktorschutz) vorwiegend analoge leittechnische Einrichtungen eingesetzt. Dennoch wurden bereits einige Einrichtungen der Sicherheitsleittechnik gegen programmierbare oder rechnerbasierte leittechnische Einrichtungen ausgetauscht. Im Ausland werden sicherheitsrelevante Leittechniksysteme in den Kernkraftwerken längst auf der Basis digitaler Leittechnik ausgelegt bzw. modernisiert.

Die generischen Erfahrungen aus anderen Einsatzbereichen digitaler Leittechnik (u. a. Luft- und Raumfahrtindustrie, Energieversorgung) zeigen, dass digitale Leittechnik ein beträchtliches Potenzial für kritische Fehler in der Software und speziell für gemeinsam verursachte Ausfälle (CCFs – Common Cause Failures) von sicherheitsrelevanten Funktionen hat. Die Ursachen von CCFs mit sicherheitsrelevanten Auswirkungen sind breit gefächert: Spezifikationsfehler, Herstellungsmängel, Komplexität der Hardware und Software, unbekannte Alterungsphänomene der Hardware digitaler Einrichtungen, eingeschränkte Prüfbarkeit, fehlerhafte Instandhaltungsmaßnahmen und Softwareupdates.

Zur Vermeidung bzw. Beherrschung der CCFs sollen sowohl bei der Auslegung als auch beim Betrieb digitaler Leittechnik, wirksame Maßnahmen eingesetzt werden. Dabei wird zwischen fehlervermeidenden und fehlerbeherrschenden Maßnahmen unterschieden.

Während es sich bei fehlervermeidenden Maßnahmen im Wesentlichen um konstruktive, analytische und allgemeine Maßnahmen der Qualitätssicherung und des Schutzes gegen unzulässige Zugriffe auf Hard- und Software handelt, orientiert sich die Beherrschung der CCFs generell am Einsatz von Diversität bei der Auslegung sicherheitsrelevanter digitaler Leittechnik. Durch den Einsatz von geeigneten Architekturen der Leittechniksysteme mit konsequenter Diversifizierung der Hard- und Software, wird eine erhöhte Fehlertoleranz gegenüber potenziellen CCFs und eine Verbesserung der Nachweisführung der erforderlichen Zuverlässigkeit sicherheitsrelevanter Leittechnik erwartet.

Eine Bewertung der Zuverlässigkeit digitaler Leittechnik wird auf der Basis deterministischer oder probabilistischer Methoden (z. B. FMEA – Failure Modes and Effects Analysis, FTA – Fault Tree Analysis) durchgeführt. Die meisten Analysen werden modellbasiert durchgeführt und unterscheiden sich u. a. durch die Modellierungsansätze, Annahmen, Zuverlässigkeitskenndaten und methodischen Vorgehensweisen. Damit öffnen sich neue Handlungsfelder sowohl bei der Verifizierung und Validierung der Ergebnisse als auch bei deren Vergleichbarkeit für und Übertragung auf ähnliche Systeme und Einrichtungen. Diese Problemstellung hat die Arbeitsgruppe WGRISK (Working Group on Risk Assessment) der OECD (Organisation for Economic Co-operation and Development) / NEA (Nuclear Energy Agency) im Rahmen der DIGREL (DIGital System RELiability failure mode taxonomy)-Studie im Jahr 2008 veranlasst, eine Leitlinie für die Durchführung modellbasierter FMEAs (Fehlermöglichkeits- und -einflussanalysen) digitaler Leittechnik zu entwickeln. Diese Arbeit wurde 2014 abgeschlossen und in einem Bericht /NEA 15/ dokumentiert.

Die OECD/NEA-Arbeitsgruppe WGRISK hat nach Beendigung der DIGREL-Studie beschlossen, ab 2018 die Arbeiten mit Fokus auf die Modellierung sicherheitsrelevanter digitaler Leittechnik im Rahmen einer neuen Studie („Digital I&C PSA – Comparative Application of Digital I&C Modelling Approaches for PSA (DIGMAP)”) fortzusetzen. Hierzu wurden die Erfahrungen der Experten aus OECD-Mitgliedsländern hinsichtlich Modellierung und Analyse digitaler Leittechnik, Bewertungskriterien und Modellierung von CCFs (Software & Hardware) zusammengeführt und entsprechende Empfehlungen zur Bewertungsmethodologie digitaler Leittechnik erarbeitet sowie wichtige Felder für zukünftige Forschungsarbeiten identifiziert.

Die Mitwirkung in dieser Arbeitsgruppe ermöglichte es der GRS, die eigene fachliche Grundlage für die Bewertung digitaler Leittechnik zu aktualisieren und zu vervollständigen.

2 AP1 Stand von Wissenschaft und Technik

Im AP1 fanden Literatur- bzw. Internetrecherchen sowie Teilnahmen von GRS-Experten an ausgewählten wissenschaftlich-technischen Konferenzen zur Verfolgung des Standes von Wissenschaft und Technik statt. Hierzu zählen auch mehrere Arbeitstreffen der internationalen Arbeitsgruppe WGRISK der OECD/NEA, deren Ergebnisse in den Besprechungsnotizen und den von den Teilnehmern vorgestellten Präsentationsunterlagen dokumentiert wurden. Seit Beginn der Corona-Krise im Jahr 2020 fanden Veranstaltungen nur in virtueller Form (u. a. Telefon- und Videokonferenzen) statt.

Im Dezember 2018 hat die GRS in Dallas (USA) am „11th International Workshop on the Application of FPGAs in NPPs“ teilgenommen. Diese jährlich stattfindende Fachkonferenz zur Anwendung von FPGAs (Field Programmable Gate Arrays) in Kernkraftwerken wird abwechselnd in Europa, den USA, Kanada und Asien durch verschiedene Institutionen ausgerichtet, um führenden internationalen Spezialisten auf dem Gebiet der digitalen Leittechnik den Austausch über die neuesten Fortschritte in der Entwicklung, dem Einsatz und der Bewertung von FPGAs in Kernkraftwerken zu ermöglichen. An der Veranstaltung in Dallas nahmen 67 Vertreter aus 14 Ländern von Betreibern, Zulieferern, Regulierungsbehörden und Forschungseinrichtungen teil (u. a. aus Kanada, China, Frankreich, Deutschland, Ungarn, Japan, Südkorea, Schweden, der Ukraine, Großbritannien und den USA). Der Workshop war in drei Themenbereiche eingeteilt:

- Bewährte Verfahren zur Verifizierung und Validierung von FPGA-Leittechnik,
- praktische Erfahrungen aus FPGA-Projekten und
- Aspekte der Diversifizierung in FPGA-basierten Systemen.

Während der Veranstaltung haben verschiedene Hersteller in einer Ausstellung eigene FPGA-basierte Leittechnikplattformen präsentiert.

In Bezug auf das Vorhaben hat die Teilnahme der GRS an diesem Workshop zur Aktualisierung der Informationen über aktuelle internationale Forschungs- und Entwicklungsaktivitäten beigetragen, insbesondere auf den Gebieten:

- Entwicklung und Aufbau FPGA-basierter Leittechniksysteme,
- Implementierung von Diversität in FPGA-basierter Leittechnik,
- Validierung und Qualifizierung FPGA-basierter Systeme und
- Sicherheitsbewertung und Anwendung von bestehenden Regelwerken auf FPGA-basierte Leittechnik.

Des Weiteren nahm die GRS im Rahmen des Vorhabens im Februar 2020 am „Technical Meeting on the Safety Aspects of Using Smart Digital Devices in Nuclear Systems Important to the Safety of Nuclear Power Plants" der IAEA (International Atomic Energy Agency) in Wien teil. Das Ziel des Meetings war es die Fertigstellung des IAEA-Berichts „Safety Aspects of Using Smart Devices in Nuclear Systems Important to Safety" durch eine Fachdiskussion der internationalen Experten zu intensivieren. Der Berichtsentwurf besteht aus vier Kapiteln:

- Motivation und Herausforderungen in Verbindung mit Smart Devices,
- Betrachtungen der Gesamtarchitektur beim Einsatz von Smart Devices,
- Qualifikation von Smart Devices und
- Lebenszyklus von Smart Devices bei Anwendung in Kernkraftwerken.

Der zukünftige IAEA-Report soll eine Übersicht über den Umgang mit Smart Devices geben und den Mitgliedsstaaten helfen ihre eigenen Regularien im Hinblick auf diese zu entwickeln.

An diesem Meeting beteiligten sich insgesamt 46 Experten aus 20 Staaten, wobei 28 Vorträge zu verschiedenen Aspekten von Auslegung und Fertigung sowie zur Qualifizierung und zum Einsatz von Smart Devices für sicherheitsrelevante Funktionen in kerntechnischen Anlagen gehalten wurden. Die Teilnehmer des Meetings präsentierten hierzu die Positionen von Aufsichtsbehörden, Betreibern der Kernkraftwerke, Zulieferern und Herstellern.

Die Vorträge teilten sich in folgende Themenfelder auf:

- regulatorische Maßnahmen,
- qualifizierende Maßnahmen und
- Einsatz von Smart Devices in Kernkraftwerken.

Im Rahmen des Technical Meetings wurden die regulatorischen Maßnahmen der USA, Südkoreas, Indiens, Brasiliens, Rumäniens, Großbritanniens und Pakistans vorgestellt. Die Repräsentanten stellten in ihren Vorträgen die bisher geltenden nationalen Regelwerke für Smart Devices vor und legten dar, wie die Anforderungen an Smart Devices sich in die allgemeinen Anforderungen an sicherheitsrelevante Systeme einbeziehen lassen. Alle für das Vorhaben relevanten Informationen aus den Veranstaltungen wurden in den Reiseberichten dokumentiert und die Workshopunterlagen (Präsentationsfolien, Vortragstexte, Herstellerprospekte) als Informationsquellen in der GRS gespeichert.

2.1 Arbeitsergebnisse

Für in Betrieb befindliche Kernkraftwerke ebenso wie für Neubauten stehen häufig analoge Leittechniksysteme und -einrichtungen nicht mehr zur Verfügung. Dies stellt nationale und internationale Regulatoren und Betreiber von Kernkraftwerken vor Herausforderungen im Umgang mit digitaler Leittechnik, insbesondere hinsichtlich Zertifizierung, Qualifizierung, sicherheitstechnischer Bewertung von deren Auslegung sowie deren Einsatz. Die wichtigste internationale Organisation, die Sicherheit kerntechnischer Anlagen fördert und überwacht, ist die IAEA. Diese reagierte mit der Überarbeitung bestehender Anforderungen an die Leittechnik in den Anlagen mit Leistungs- und Forschungsreaktoren. Zu den wichtigsten aktuellen Publikationen der IAEA in Bezug auf sicherheitsrelevante Leittechnik (Leittechnikfunktionen der Sicherheitsebenen 2, 3, und 4) gehören:

- Specific Safety Guide SSG-39 „Design of Instrumentation and Control Systems for Nuclear Power Plants“ /IAE 16/,
- Specific Safety Guide SSG-37 “Instrumentation and Control Systems and Software Important to Safety for Research Reactors”, /IAE 15/,
- Factors Engineering in the Design of Nuclear Power Plants”, /IAE 19/. Specific Safety Guide SSG-51 “Human

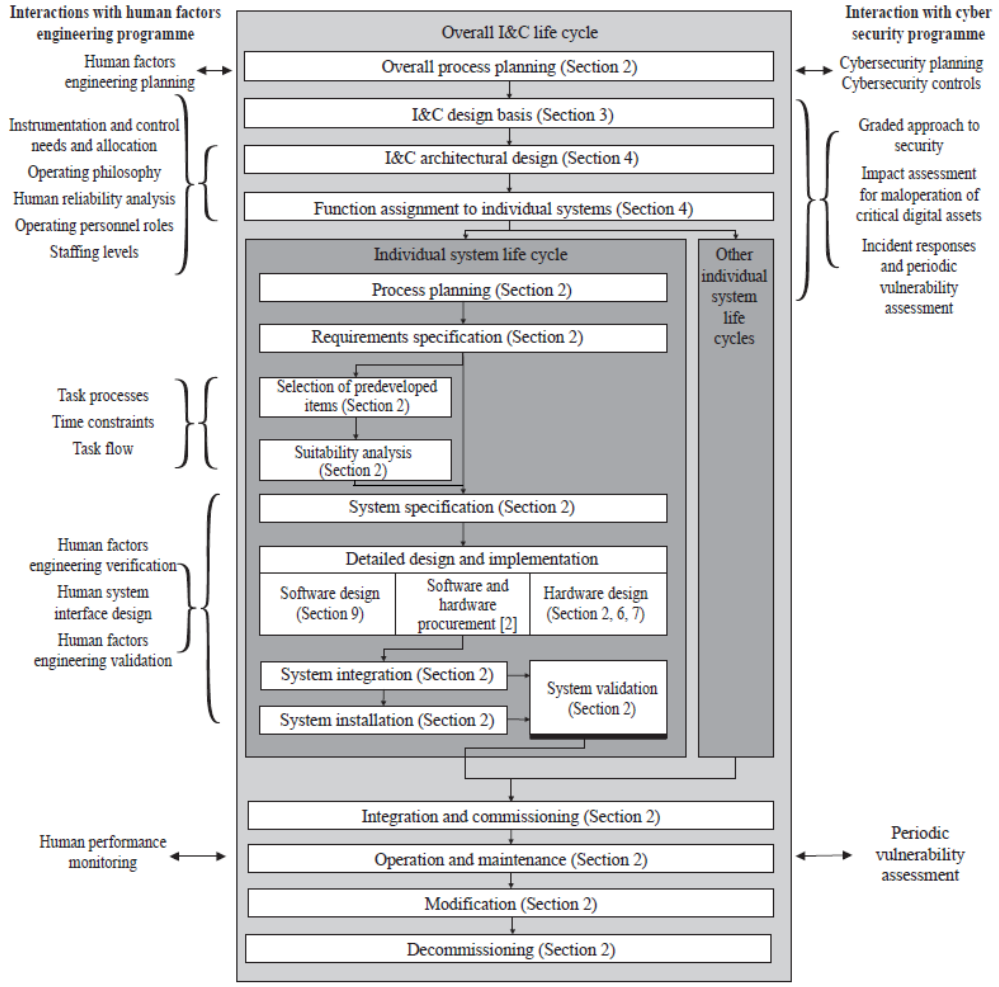

Abb. 2.1 Lebenszyklus eines Leittechniksystems nach /IAE 16/

SSG-39 stellt ein zentrales Dokument dar, in dem Empfehlungen für die einzelnen Phasen des Lebenszyklus eines Leittechniksystems formuliert sind. In Abb. 2.1 wird das Lebenszyklusmodell der Leittechnik in einem Kernkraftwerk vorgestellt und mit den entsprechenden Textabschnitten des SSG-39 verknüpft. In den o. g. IAEA-Leitlinien (Guides) wird ein Zusammenhang zwischen Entwicklung und Betrieb der Hard- und Software der Leittechnik und der zu berücksichtigenden menschlichen Faktoren entsprechend dem Stand von Wissenschaft und Technik hergestellt. Darüber hinaus wird hierbei auf die Bedeutung der IT-Sicherheit hingewiesen.

Des Weiteren hat die IAEA mehrere neue Publikationen (IAEA Nuclear Energy Series, Technical Reports) in Bezug auf den Einsatz digitaler Leittechnik veröffentlicht, bei denen der Austausch wissenschaftlicher und technischer Informationen über die Nutzung digitaler Leittechnik im Fokus steht. Folgende Berichte wurden im Rahmen des Vorhabens hinsichtlich des Kompetenzerhalts der GRS (u. a. Fachgespräche, Ermittlung des Forschungsbedarfs, Methodenentwicklung) ausgewertet:

- Series NP-T-3.19 (2017) Instrumentation and Control Systems for Advanced Small Modular Reactors
- NP-T-2.11 (2018) Approaches for Overall Instrumentation and Control Architectures of Nuclear Power Plants,
- NP-T-3.27 (2018) Dependability Assessment of Software for Safety Instrumentation and Control Systems at Nuclear Power Plants,
- NP-T-3.30 (2020) Computer Security Aspects of Design for Instrumentation and Control Systems at Nuclear Power Plants,
- NP-T-3.31 (2020) Challenges and Approaches for Selecting, Assessing and Qualifying Commercial Industrial Digital Instrumentation and Control Equipment for Use in NPP Applications,
- NP-T-2.12 (2021) Human Factors Engineering Aspects of Instrumentation and Control System Design.

Die Einführung der COTS-Leittechnik (COTS – Commercial-Off-The-Shelf) in Kernkraftwerken hat die Aufmerksamkeit der IAEA auf die sogenannten „Smart Devices“ in sicherheitsrelevanten Leittechnikfunktionen gerichtet. Bisher werden Einrichtungen mit Smart Devices im Ausland nur in Ausnahmefällen für kerntechnische Anwendungen ausgelegt und hergestellt oder nach industriellen Standards (z. B. IEC 61513) für den Einsatz in Kernkraftwerken qualifiziert. Die Qualifizierung der COTS-Leittechnik unterscheidet sich zwischen einzelnen Ländern deutlich, je nach den entwickelten Qualifizierungsprozessen und den regulatorischen Vorgaben.

Nach der IAEA-Definition handelt es sich bei Smart Devices um einfache digitale Einrichtungen, welche Software oder programmierbare Logik besitzen und für sicherheitsrelevante Funktionen verwendet werden. Solche Einrichtungen können nur eine spezifizierte Funktion innerhalb eines Leittechniksystems ausführen, z. B. als Temperaturmessung oder als Antriebssteuerung.

Ein Smart Device kann nach Definition der IAEA durch Anwender nicht programmiert, sondern nur konfiguriert werden und unterscheidet sich damit deutlich von softwarebasierten programmierbaren Einrichtungen.

Die IAEA hat folgende sicherheitstechnische Aspekte der Einführung von Smart Devices identifiziert:

- Regulatorische Maßnahmen
- Qualifizierende Maßnahmen

Die Experten der IAEA-Arbeitsgruppe haben festgestellt, dass weiterhin große Herausforderungen hinsichtlich Nutzung von Smart Devices bestehen:

- Die Definition einer Smart-Device-Einrichtung muss klarer festgelegt werden,
- die Anforderungen an die Qualifizierung von Smart Devices müssen eindeutig festgelegt werden,
- die IT-Sicherheit für Smart Devices muss gewährleistet werden und
- die Anforderungen zum Einsatz von Smart Devices in sicherheitsrelevanten Leittechniksystemen müssen unter Berücksichtigung des Lebenszyklus definiert werden.

Hinsichtlich der Weiterentwicklung von Anforderungen zum Einsatz digitaler Leittechnik in Kernkraftwerken sind die regulatorischen Aktivitäten der U.S. NRC hervorzuheben. Die Lizensierung (Genehmigung) digitaler Leittechnik für den Einsatz in Kernkraftwerken innerhalb der USA erfolgt auf der Grundlage von Regulatory Guides der U.S. NRC (RG 1.152, 1.168, 1.169, 1.170, 1.171, 1.172, 1.173) und des Standard Review Plans (NUREG-0800) der U.S. NRC. Die spezifischen, technologieabhängigen Anforderungen und Empfehlungen an die Auslegung und den Betrieb der Leittechnik sind in weiteren Dokumenten der U.S. NRC unter Einbeziehung einiger nationaler und internationaler Industriestandards enthalten, z. B. BTP 7-19 (Branch Technical Position „Guidance for Evaluation of Defence in Depth and Diversity To Address Common-Cause Failure Due to Latent Design Defects in Digital Safety Systems“) /NRC 20/, DO-254 (Design Assurance), IEEE STD 1012 (V&V), IEEE STD 7-4.3.2 (Safety Digital Systems). Die U.S. NRC empfiehlt nicht generell die Anwendung der Industriestandards, sondern legt ggf. Diskrepanzen in der Position der U.S. NRC und des Standards dar.

Beispielsweise sollte nach Auffassung der U.S. NRC der Software in Kernkraftwerken die Integritätsstufe 4 (SIL-Klassifizierung) zugewiesen werden. Im Industriestandard IEEE 1012 ist das SIL-Klassifizierungsschema für die Software nicht zwingend vorgeschrieben, sondern legt nur die Mindestanforderungen an die Verifizierung und Validierung fest.

Besonders interessant aus der Sicht der Zielstellung des Vorhabens ist die aktuelle Version des Dokuments BTP 7-19 (Standard Review Plans NUREG-0800, Revision 8 soll 2021 veröffentlicht werden). In diesem Dokument werden die Vorgehensweise bei der Sicherheitsbewertung und die Akzeptanzkriterien in Bezug auf Vermeidung und Beherrschung potenzieller CCF-Ausfälle für verschiedene Leittechniksysteme beschrieben. Hierzu werden die Aufgabe und die Auslegungsgrundsätze diversitärer Leittechnik zur Beherrschung von CCF definiert (u. a. Vorrang, Akzeptanzkriterien). Diese Informationen sind wichtig für die Festlegung der Architektur einer Sicherheitsleittechnik in Kernkraftwerken sowie für die Entwicklung geeigneter Analysemethoden.

In Großbritannien befinden sich gegenwärtig einige neue Kernkraftwerke in der Errichtungs- oder Genehmigungsphase (u. a. UK EPR, ABWR, AP1000, UK HPR1000). Die britische Aufsichtsbehörde (ONR – Office for Nuclear Regulation) hat hinsichtlich des Einsatzes digitaler Leittechnik folgende Herausforderungen aus regulatorischer Sicht identifiziert:

- Keine Leittechnik (Technologie) kann alle (oder auch nur die Mehrheit der) Fehler beseitigen/detektieren, obwohl einige Techniken sehr leistungsfähig sind.
- Die Nachweisführung der Fehlerfreiheit durch Tests der Leittechniksysteme/-plattformen wird als nicht ausreichend angesehen, denn selbst in kleinen Systemen können zu viele interne Zustände bzw. Kombinationen von Parametern entstehen, um in einer angemessenen Zeit die Testabdeckung zu erreichen. Die Tests sind allerdings notwendig, um nachzuweisen, dass die funktionalen Anforderungen erfüllt sind.
- Die Nachweisführung auf der Basis von statistischen Tests wird bisher nicht akzeptiert, weil bisher dabei einige Probleme bei der Ermittlung und Validierung der Ausfallwahrscheinlichkeit festgestellt wurden. Bei dieser Methode wird digitale Leittechnik (Hard- und Software) mit einer Vielzahl von Anforderungen getestet, die das Anforderungsprofil für das System widerspiegeln sollen.

Des Weiteren haben die GRS-Recherchen gezeigt, dass eine breite Einführung digitaler Leittechnik unterschiedlicher Hersteller zu grundsätzlichen Problemen im Genehmigungsprozess der einzelnen Länder führen kann. Ein prominentes Beispiel hierfür ist die sicherheitstechnische Klassifizierung (Kategorisierung) leittechnischer Systeme und Funktionen. Obwohl weltweit breite Einigkeit über die Notwendigkeit der Identifikation und der sicherheitstechnischen Klassifizierung aller Funktionen herrscht, die zur Erfüllung der Sicherheitsfunktionen in allen Anlagenzuständen erforderlich sind, unterscheiden sich die Vorgehensweisen in verschiedenen Standards und nationalen Regelwerken deutlich.

Die internationale Arbeitsgemeinschaft WNA (World Nuclear Association) von Herstellern, Lieferanten und Betreibern von Kernkraftwerken hat in einem Bericht /WNA 20/ diese Problematik aktuell dargestellt. Abb. 2.2 verdeutlicht unterschiedliche Klassifizierungssysteme: Häufig bereitet die konsistente Zuordnung von Funktionen und Systemen Probleme und lässt viel Raum für Diskussionen.

Organizations or Countries		Safety Classification of I&C Functions and systems in nuclear plants			
Main international standard organizations					
IAEA Safety Glossary		Items important to safety[6]			Items not important to safety[7]
		Safety systems	Safety-related items[7]		
			Safety features (for DEC)		
IAEA SSG-30	Function	Safety category 1	Safety category 2	Safety category 3	
	System	Safety class 1	Safety class 2	Safety class 3	
IEC 61226		Systems Important to Safety			Systems not Important to Safety
	I&C function	Category A	Category B	Category C	Non-categorized
	I&C system	Class 1	Class 2	Class 3	Non-classified
IEEE		Systems Important to Safety			Non-safety-related
		Safety-related	[9]		
EUR[10]	Safety level of functions / I&C systems	1	2	3	NS (non-safety)
Selected states with nuclear power programs					
Canada		Category 1	Category 2	Category 3	Category 4
China		F1A	F1B	F2	Non-classified
Finland		Class 2	Class 3	EYT/ STUK	EYT (classified non-nuclear)
France		Class 1	Class 2	Class 3	Non-classified
Germany	I&C function	Category 1	Category 2	Category 3	Non-classified
	I&C equipment	E1		E2	
India		IA	IB	IC	NINS
Japan		PS1/MS1	PS2/MS2	PS3/MS3	Non-nuclear safety
Korea		IC-1	IC-2	IC-3	Non-classified
Russia	I&C function	Category A	Category B	Category C	Non-categorized
	I&C system	Class 2		Class 3	Class 4 (Systems not important to safety)
South Africa[11]		Level 1 Direct influence on safety performance	Level 2 Products important to nuclear safety	Level 3 All products of the Nuclear installation	Non safety or availability related
Switzerland		1	2	3	Non-classified
UK		Class 1	Class 2	Class 3	Non-classified
USA		System important to safety			(not specified)
		Safety related[12]	[8]		

Abb. 2.2 Länder- bzw. standardspezifische Klassifizierungssysteme /WNA 20/

Im WNA-Bericht wird im Zusammenhang mit der sicherheitstechnischen Klassifizierung der Leittechnik auf folgende Schwierigkeiten hingewiesen:

- Inkonsistenz zwischen internationalen Standards (z. B. IAEA SSG-30, IEC61226, IEEE) und nationalen Regeln,
- mehrdeutige Anforderungen an die Sicherheitsklassifizierung von Systemen und Funktionen,
- unvollständige Anforderungen für die Kategorisierung von Leittechnikfunktionen und
- inkonsistente Anforderungen an diversitäre Backup-Systeme bzw. Funktionen.

Die IAEA und weitere nationale und internationale Institutionen (u. a. WENRA, IEC, U.S. NRC) plädieren dafür, dass die internationale Zusammenarbeit zur Harmonisierung der Sicherheitsanforderungen an die Leittechnik in kerntechnischen Anlagen fortgesetzt werden sollte, um die schnelle Entwicklung digitaler Technologien und deren Einsatz in Kernkraftwerken sicher zu gestalten.

2.2 Zusammenfassung AP1

Die Recherchen im Rahmen des Vorhabens haben gezeigt, dass weiterhin ein Weiterentwicklungsbedarf für das nationale und internationale kerntechnische Regelwerk hinsichtlich sicherheitstechnischer Anforderungen und der Bewertung digitaler Leittechnik besteht. Dabei wird auch eine größere Bedeutung von Smart Devices in der Leittechnik kerntechnischer Anlagen (z. B. als Sensoren, Antriebstechnik, Kransteuerung) erwartet. Die Einführung dieser Technologien für sicherheitsrelevante Funktionen lässt bisher einige regulatorische und qualifizierende Fragestellungen offen. Die Recherchen zum Stand von Wissenschaft und Technik auf diesem Gebiet sollten daher auch nach Beendigung des aktuellen Vorhabens bei der GRS fortlaufend fortgesetzt werden.

Die Teilnahmen an Konferenzen zum Thema Sicherheit und Zuverlässigkeit digitaler Leittechnik (z. B. im Rahmen von IAEA, OECD, IEC, ANS) bieten die Möglichkeit für einen breiten fachlichen, interdisziplinären Austausch mit Vertretern von Aufsichtsbehörden und deren TSOs (Technical Support Organizations), Herstellern und Entwicklern digitaler Leittechnik und damit zum Kompetenzerhalt der GRS auf diesem Gebiet.

Die Mitarbeit in den technischen Arbeitsgruppen (z. B. OECD/NEA-DIGREL/DIGMAP) ermöglicht eine intensive Einarbeitung in die qualifizierenden Maßnahmen (z. B. Methodenentwicklung zur Validierung und Verifizierung der Sicherheit und Zuverlässigkeit digitaler Leittechnik) und in die regulatorischen Aspekte der Genehmigung neuer Technologien.

Des Weiteren verfügt die GRS über Testsysteme (z. B. AnTeS – das Analyse- und Testsystem) und einige leittechnische Einrichtungen, um aktuelle Fragestellungen zum Einsatz von FPGA-basierten Geräten und Smart Devices zu evaluieren, u. a. FPGA-basierte Baugruppen zur Antriebs- und Vorrangsteuerung, eine TDR-Füllstandsmesssonde (Smart Device nach IAEA-Definition; TDR – Time-Domain Reflectometer) sowie mehrere Druckmessumformer (Smart Devices nach IAEA-Definition).

Im Rahmen avisierter zukünftiger Vorhaben der GRS ist es damit möglich, sowohl die regulatorischen Anforderungen an die Sicherheit (u. a. Diversitätsmerkmale, Testabdeckung) und Qualifizierung derartiger Geräte zu überprüfen als auch eigene V&V-Methoden (V&V – Verification and Validation) und Werkzeuge zu entwickeln.

3 AP2 Entwicklung von Bewertungsgrundlagen für digitale Sicherheitsleittechnik

In diesem Vorhaben wurden die Grundlagen zur Bewertung programmierbarer oder rechnerbasierter Sicherheitsleittechnik („digitale Leittechnik“ – DI&C) unter Berücksichtigung der internationalen Erfahrungen erweitert und überarbeitet. Wesentlich hierfür war die Teilnahme der GRS an der Studie „Digital I&C PSA – Comparative Application of Digital I&C Modelling Approaches for PSA (DIGMAP)“ eines internationalen Expertenteams der Arbeitsgruppe WGRISK der OECD/NEA (siehe Tab. 3.1), welche im nachfolgenden Abschnitt vorgestellt wird.

Tab. 3.1 Teilnehmer der DIGMAP-Studie der Arbeitsgruppe WGRISK der OECD/NEA

Name	Organisation	Land
Hans Brinkman	NRG	Niederlande
Jeanne Demgné	EDF R&D	Frankreich
Léo Granseigne	EDF R&D	Frankreich
Milan Jaros	ÚJV Řež, a. s.	Tschechien
Christian Müller	Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH	Deutschland
Venkat Natarajan	NRG	Niederlande
Paolo Picca	Office for Nuclear Regulation (ONR)	Großbritannien
Ewgenij Piljugin	Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH	Deutschland
Markus Porthin	Paul Scherrer Institut (PSI)	Schweiz
Richard Quatrain	EDF R&D	Frankreich
Jiri Sedlak	ÚJV Řež, a. s.	Tschechien
Sung-Min Shin	Korea Atomic Energy Research Institute (KAERI)	Südkorea
Tero Tyrväinen	VTT Technical Research Centre of Finland Ltd (VTT)	Finnland

Die Qualität des am Ende der Studie gemeinsam erstellten Reports /WGR 21/ wurde durch eine Vielzahl von Rezensenten, ebenfalls internationalen Experten, sichergestellt (siehe Tab. 3.2).

Tab. 3.2 Rezensenten („Reviewer“) des DIGMAP-Reports

Name	Organisation	Land
Geza Baksa	Nuclear Safety Research Institute (NUBIKI)	Ungarn
HAN Bao	Idaho National Laboratory (INL)	USA
Attila Bareith	Nuclear Safety Research Institute (NUBIKI)	Ungarn
Sushil Birla	U.S. Nuclear Regulatory Commission (US NRC)	USA
SungwHAN Cho	Canadian Nuclear Safety Commission (CNSC)	Kanada
Mehdi Reisi Fard	U.S. Nuclear Regulatory Commission (US NRC)	USA
Per Hellström	Swedish Radiation Safety Authority (SSM)	Schweden
Elod Hollo	Nuclear Safety Research Institute (NUBIKI)	Ungarn
Jan-Erik Holmberg	Radiation and Nuclear Safety Authority in Finland (STUK)	Finnland
Hyungook Kang	Rensselaer Polytechnic Institute (RPI)	USA
Yann Morvan	EDF R&D	Frankreich
Joel Robinson	Office for Nuclear Regulation (ONR)	Großbritannien
Marina Röwekamp	Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH	Deutschland
Vincent Sorel	EDF R&D	Frankreich
Andrew White	Office for Nuclear Regulation (ONR)	Großbritannien
Hongbin Zhang	Idaho National Laboratory (INL)	USA

3.1 DIGMAP-Studie

Das Ziel der DIGMAP-Studie war der Vergleich von PSA-Modellierungsansätzen für sicherheitsrelevante DI&C-Systeme eines exemplarischen KKWs (Referenzfall). Sechs der teilnehmenden Organisationen entwickelten hierfür eigene Modelle auf der Grundlage dieses Referenzfalls. Durch den Vergleich der Ansätze und der damit jeweils erlangten Ergebnisse konnten wertvolle Erkenntnisse für die zukünftige Entwicklung von Modellierungsmethoden identifiziert werden.

Die Ergebnisse der DIGMAP-Studie werden als gemeinsamer Report veröffentlicht, dieser ist anschließend im Internet herunterladbar /WGR 21/. Wesentliche Inhalte dieser Studie sind komprimiert in den nachfolgenden Abschnitten dargestellt. Eine Einordnung der Ergebnisse hinsichtlich der Ziele dieses Vorhabens ist in Abschnitt 3.2 zu finden.

3.1.1 Referenzfall

Der Referenzfall der DIGMAP-Studie basiert auf dem Modell eines generischen Siedewasser-Reaktors (BWR - Boiling Water Reactor) der DIGREL-Studie /AUT 13/. Das ursprüngliche Modell wurde für die DIGMAP-Studie dahingehend modifiziert, dass insbesondere wesentliche Merkmale digitaler Leittechnik (DI&C), wie Hard- und Software in der Analyse berücksichtigt werden konnten.

Der Aufbau der verfahrenstechnischen Sicherheitssysteme im Modell der Referenzanlage ist in Abb. 3.1 dargestellt, Abb. 3.2 zeigt das zugehörige Reaktorschutzsystem. Die vollständigen Namen der einzelnen Sicherheitssysteme in Abb. 3.1 sind in Tab. 3.3 aufgeführt. Mit Ausnahme des Reaktorschutzsystems, sind alle Sicherheitssysteme der Referenzanlage nur einfach redundant aufgebaut.

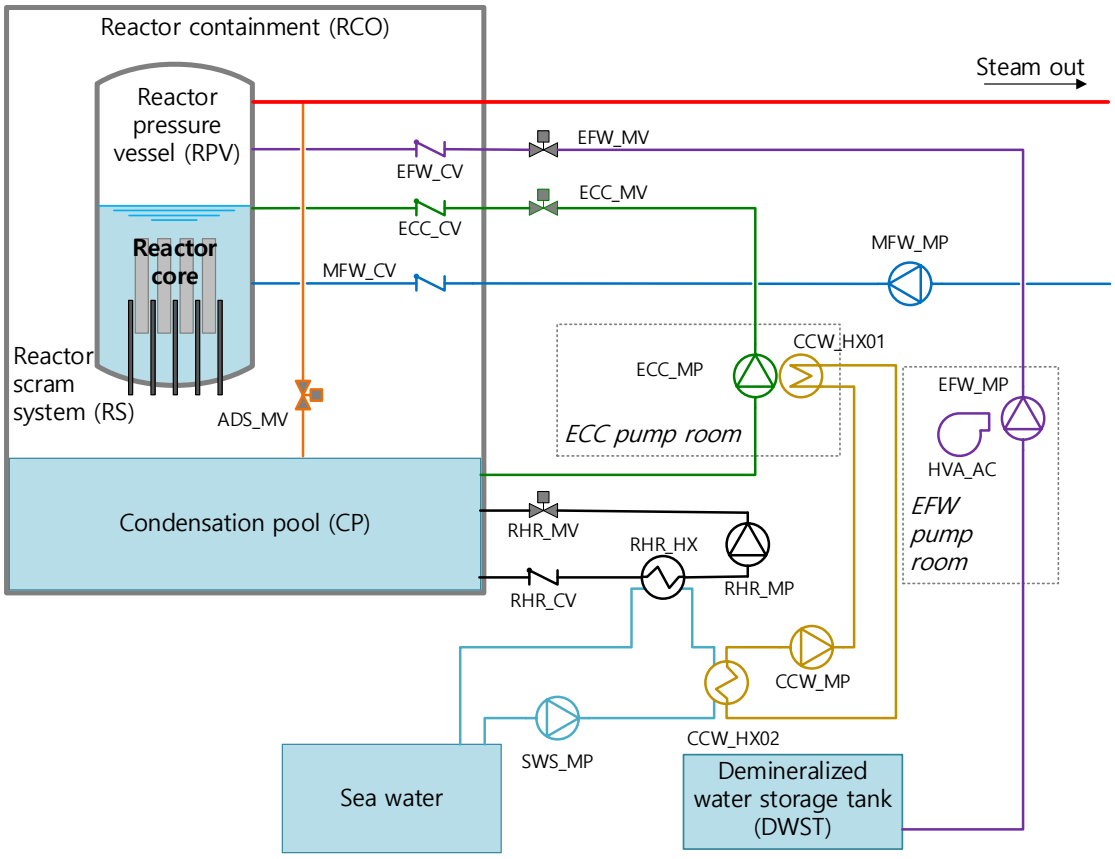

Abb. 3.1 Aufbau der Sicherheitssysteme des Referenzanlagenmodells

Vereinfachtes BWR-Modell

Tab. 3.3 Sicherheitssysteme des betrachteten Referenzfalls

Abkürzung	System
ADS	Automatic Depressurization System
CCW	Component Cooling Water System
ECC	Emergency Core Cooling System
EFW	Emergency Feedwater System
SWS	Service Water System
HVA	Heating, Ventilation and Air Conditioning System
MFW	Main Feedwater System
RHR	Residual Heat Removal System
RPS	Reactor Protection System
RS	Reactor Scram System

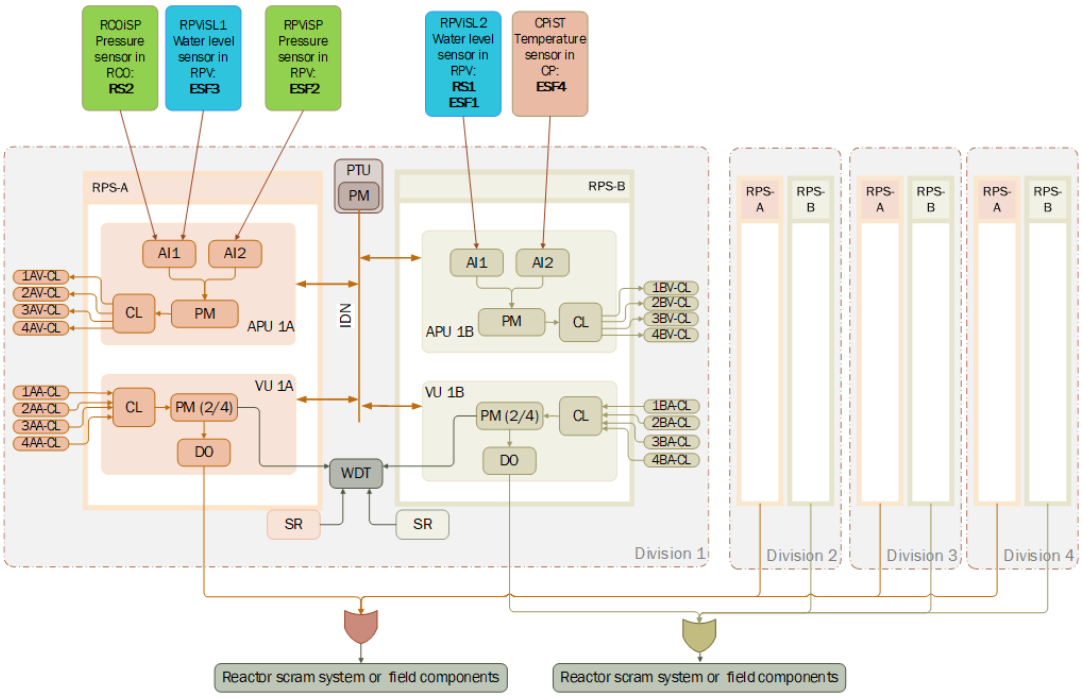

Abb. 3.2 Das Reaktorschutzsystem (RPS) des Referenzfalls

Anmerkung: Der Zusatz „(2/4)“ für die Prozessormodule (PMs) der Voting Units (VUs) soll verdeutlichen, dass eine 2-von-4-Auswahl durchgeführt wird. Die Prozessormodule der APUs und VUs unterscheiden sich hinsichtlich des Aufbaus der Hardware nicht.

Das digitale Reaktorschutzsystem (RPS – Reactor Protection System) des Referenzfalls in Abb. 3.2 besteht aus vier räumlich getrennten Scheiben, die identisch aufgebaut sind.

Jede Scheibe verfügt über eigene Messsensoren und ist in jeweils zwei Subsysteme (RPS-A und RPS-B) aufgeteilt, in denen unterschiedliche Leittechnikfunktionen umgesetzt sind und die als lediglich funktional diversitär angenommen werden (also aus identischen Hard- und Software-Komponenten aufgebaut sind). Jedes dieser Subsysteme besteht wiederum aus einer Erfassungs- und Verarbeitungseinheit (APU – Acquisition and Processing Unit) sowie einer Wertungseinheit (VU – Voting Unit). Die APU und VU jedes Teilsystems in jeder Scheibe sind jeweils gemeinsam in einem Baugruppenträger (Subrack – SR) untergebracht.

In den APUs werden die Messwerte von den zugeordneten Sensoren mit Grenzwerten verglichen und ggfs. Auslösesignale erzeugt. Diese Auslösesignale werden zwischen allen vier Scheiben des jeweiligen Teilsystems (Subsystem A oder B) ausgetauscht. Die VU jedes Teilsystems und jeder Scheibe führt danach eine Wertung der generierten Auslösesignale in Form einer 2-von-4-Auswahl durch. Bei zwei oder mehr anstehenden Signalen erfolgt also die Auslösung der entsprechenden verfahrenstechnischen Sicherheitssysteme. Liegen allerdings nur zwei valide Signale vor (d. h. wurden auf der Ebene der APUs durch das Leittechniksystem selbst Fehler in zwei der vier Signalwege erkannt), so wird die Auswahllogik der VUs auf eine 1-von-2-Auswahl umgeschaltet. Werden auf Ebene der APUs Fehler in drei der vier Signalwege detektiert, so erfolgt vorsorglich eine sicherheitsgerichtete Auslösung der Sicherheitssysteme.

APUs und VUs enthalten jeweils eine Prozessorbaugruppe (PM – Processor Module) und eine Kommunikationsbaugruppe (CL – Communication Link Module). Zusätzlich sind in den APUs analoge Eingangsbaugruppen (AI – Analogue Input Module) für das Einlesen der Sensordaten und in den VUs digitale Ausgangsbaugruppen (DO – Digital Output Module) zur Ausgabe von Auslösesignalen an die Steuerungsebene vorhanden.

Die Prozessorbaugruppen bestehen nicht nur aus Hardware, sondern auch aus Betriebssystem- und Plattformsoftware (OP – Operating System and Platform Software) sowie Anwendungssoftware (AS – Application Software). Die anderen Baugruppen (CL, AI, DO) verfügen ebenfalls über Betriebssystem- und Plattformsoftware (OP), allerdings über keine spezifische Anwendungssoftware. Die Baugruppenträger (SR) sind reine Hardware.

In der DIGMAP-Studie wurden Hardware-Ausfälle innerhalb des Reaktorschutzsystems durch Ausfallraten und Software-Ausfälle durch Failure-On-Demand-Wahrscheinlichkeiten ausgedrückt (siehe Appendix A des DIGMAP-Reports /NEA 21/, der in Kürze auf der Internetseite der WGRISK /WGR 21/ herunterladbar sein wird, für die angenommenen Zuverlässigkeitskenndaten).

Das Reaktorschutzsystem des Referenzfalls verfügt über drei Mechanismen zur Erkennung und Beherrschung von Hardwarefehlern (FTT – Fault Tolerant Techniques):

- A – automatische Tests
    - Werden alle 50 ms von der Anwendungssoftware bestimmter Baugruppen und vom Watchdog (WDT – Watchdog Timer) durchgeführt.
- P – periodische Tests
    - Werden alle 24 Stunden durch die Anwendungssoftware der Prozessorbaugruppen (PM) der PTUs (Periodical Testing Units) durchgeführt, indem über das scheibeninterne Kommunikationsnetzwerk (IDN – Intra-Division Network) Informationen gesammelt werden.
- F – wiederkehrende Prüfungen (Full-Scope Testing)
    - Werden alle sechs Monate (182,5 Tage) vom Personal durchgeführt.

Die Erkennungsabdeckungen der verschiedenen FTTs überschneiden sich teilweise, d. h., dass aufgetretene Fehler teilweise durch mehr als einen Mechanismus entdeckt werden können. Insbesondere wurde in der DIGMAP-Studie auch angenommen, dass mit wiederkehrenden Prüfungen (F) jeder Hardware-Ausfall zuverlässig gefunden wird. Weitere Informationen hierzu können dem DIGMAP-Report /NEA 21/ entnommen werden. Appendix A dieses Reports enthält auch Ausfalldaten von Feldkomponenten (z. B. Instrumentierung) und CCF-Parameter, die in den Modellen verwendet wurden. Es ist zu beachten, dass die in dieser Studie verwendeten Ausfalldaten und weitere Parameter als bekannt vorausgesetzt wurden. Spezifische Methoden, die zur Quantifizierung von Zuverlässigkeitsparametern von Komponenten verwendet werden, waren nicht Teil dieser Studie.

Darüber hinaus haben alle Organisationen, die eigene PSA-Modelle entwickelt haben, einheitlich ein durch EDF entwickeltes Modell (Fehlerbäume) für die verfahrenstechnischen Systeme verwendet, in welchen Schnittstellen für die Signale aus dem Reaktorschutzsystem vorgesehen waren. An diese vorhandenen Schnittstellen wurden die individuellen Fehlerbäume der unterschiedlichen Modelle für das Reaktorschutzsystem angebunden. Hierdurch wurde sichergestellt, dass die Modellierung der verfahrenstechnischen Systeme nicht zu weiteren, für die hier durchgeführten Untersuchungen irrelevanten Unterschieden zwischen den Modellen der Organisationen führten, da diese nicht im Fokus der durchgeführten Studie lagen.

3.1.2 PSA-Modelle

Tab. 3.4 fasst die wichtigsten Merkmale der von den teilnehmenden Organisationen entwickelten PSA-Modelle (PSA - Probabilistische Sicherheitsanalyse) zusammen. Eine kurze Beschreibung der einzelnen Modelle befindet sich in den nachfolgenden Unterabschnitten, noch mehr Details können im Appendix B des DIGMAP-Reports /NEA 21/ nachgelesen werden. Einige grundsätzliche Anmerkungen und Erläuterungen zu PSAs können im Anhang A.1 nachgelesen werden.

Die einzelnen Zeilen der Tab. 3.4 können wie folgt interpretiert werden:

- Verwendete Werkzeuge:
    - Werkzeuge, die für die Modellierung oder Hintergrundberechnungen verwendet wurden.
- Abstraktionslevel (und Gesamtzahl der Basisereignisse):
    - Hoch: Basisereignisse bei der Modellierung waren Subsystem- oder Scheibenausfälle;
    - Mittel: Zwischen hohem und niedrigem Abstraktionsniveau;
    - Niedrig: Für jede Baugruppe wurden Hardware-, OP- und AS-Ausfälle und die Auswirkungen der FTTs explizit modelliert.
    - Anm.: Die Anzahl der Basisereignisse eines Modells liefert unmittelbar einen Hinweis auf den Abstraktionsgrad – je mehr Basisereignisse das Modell berücksichtigt, desto geringer ist der Abstraktionsgrad).

- Detaillierungsgrad CCFs:
    - Voll: Mit Ausnahme der AI-Hardware-CCFs wurden alle Kombinationen der zugehörigen Ausfälle innerhalb von CCF-Gruppen explizit modelliert;
    - Abstrahiert: Im CCF-Modell wird ein Abstraktions- oder Vereinfachungsprozess verwendet. Einige Teilnehmer haben z. B. CCF-Ereignisse mit gleichen Auswirkungen zusammengefasst und im Hintergrund bzw. in einem speziellen Arbeitsschritt die entsprechenden Ausfallwahrscheinlichkeiten berechnet.
- Berücksichtigung geänderter Wertungslogiken in den VUs:
    - Die aktive Änderung der Wertungslogiken (n-von-m) der VUs aufgrund von erkannten Fehlern wurde im Modell berücksichtigt (Ja) oder nicht berücksichtigt (Nein).
- Berücksichtigung von FTT-bezogenen Faktoren:
    - Erstes Ja/Nein: Überlappende Fehlererkennungsabdeckung wurde im Modell berücksichtigt (Ja) oder nicht berücksichtigt (Nein);
    - Zweites Ja/Nein: Prüfintervalle (der FTTs) wurde im Modell explizit berücksichtigt (Ja) oder nicht berücksichtigt (Nein);
    - Drittens Ja/Nein: Die Funktionssicherheit (der FTTs selbst) wurde im Modell berücksichtigt (Ja) oder nicht berücksichtigt (Nein).
- Berücksichtigung von Unverfügbarkeiten während Reparaturen:
    - Unverfügbarkeiten während Reparaturen wurden im Modell berücksichtigt (Ja) oder nicht berücksichtigt (Nein).
- Modellierungsinputs aus Hintergrundberechnungen:
    - Welche Arten von Hintergrundberechnungen wurden durchgeführt?
- Weitere Merkmale:
    - Andere wichtige Merkmale oder Annahmen.

Tab. 3.4 Übersicht über die Modellierungsansätze der teilnehmenden Organisationen

	EDF	GRS	KAERI	NRG	UJV	VTT
Verwendete Werkzeuge	RiskSpectrum[1)], EDF KB3[2)], Tabellenkalkulationen	RiskSpectrum[1)], FMEA[3)]	AIMS-PSA[4)], Tabellenkalkulationen	Risk-Spect-rum[1)]	RiskSpect-rum[1)]	FinPSA[5)] Tabellenkalkulationen
Abstraktionslevel (Gesamtzahl der Basisereignisse)	Hoch (64)	Mittel (460)	Niedrig (2664)	Niedrig (5546)	Niedrig (5857)	Mittel (72)
Detaillierungsgrad CCFs	Abstrahiert	Abstrahiert	Voll	Voll	Voll	Abstrahiert
Berücksichtigung geänderter Wertungslogiken in den VUs	Ja	Ja	Nein	Ja	Ja	Nein
Berücksichtigung von FTT-bezogenen Faktoren	Ja/Ja/Ja	Ja/Ja/Ja	Ja/Ja/Ja	Ja/Ja/Ja	Nein/Ja/Ja	Ja/Ja/Ja
Berücksichtigung von Unverfügbarkeiten während Reparaturen	Ja	Ja	Ja	Ja	Ja	Ja
Modellierungsinputs aus Hintergrundberechnungen	Testverfügbarkeiten, Hardware-Nichtverfügbarkeiten, CCF-Kombinationen und deren Aggregation wurden mit separaten Tabellenkalkulationen berechnet.	Ausfallwahrscheinlichkeiten von zusammengefassten Basisereignissen wurden in separaten Fehlerbäumen berechnet. Für die Ermittlung der relevanten Minimalschnitte wurden FMEAs verwendet.	Das Prüfintervall der FTTs wurde entsprechend der Zuverlässigkeit der einzelnen FTT-Funktionen modifiziert.	-	-	Hardware-Ausfallwahrscheinlichkeiten wurden mit Hilfe von eigenen Fehlerbäumen im Hintergrund berechnet. CCF-Kombinationen und -Wahrscheinlichkeiten wurden mit separaten Tabellenkalkulationen berechnet.

	EDF	GRS	KAERI	NRG	UJV	VTT
Weitere Merkmale	CCFs mit gleichen Auswirkungen auf der Systemebene wurden zusammengefasst, so dass insgesamt nur 5 Arten von makroskopischen I&C-Ereignissen übrig blieben. Signale wurden als Zuverlässigkeitsdiagramme in KB3 modelliert, das basierend darauf Fehlerbäume erzeugt.					

1) RiskSpectrum PSA /RIS 21/ - kommerzielle Software von Lloyd‘s Register

2) KB3^{TM} /EDF 21/ – von der EDF entwickelte Software zum grafischen Erstellen, interaktiven Simulieren und Transformieren von Systemzuverlässigkeitsmodellen in quantitative Modelle (ausgehend von generischen Modellen, die in Bibliotheken verfügbar sind), die anschließend mit RiskSpectrum ausgewertet werden

3) FMEA /IEC 18/ – Fehlermöglichkeits- und -einflussanalysen (bzw. Failure Modes and Effects Analysis)

3) AIMS-PSA /HAN 16/ - vom KAERI entwickelte Software für PSA

5) FinPSA /VTT 13/ - vom VTT entwickelte Software für PSA

3.1.2.1 PSA-Modell der EDF

EDF verwendete einen sehr stark abstrahierten Modellierungsansatz (unter dem Schlagwort "Kompaktmodell"). In diesem Ansatz wurden Signalausfälle mit möglichst wenigen voneinander unabhängigen Basisereignissen modelliert. Diese Basisereignisse fassen systematische Ausfälle, die mehrere redundante Kanäle betreffen zusammen, solange sie die gleiche Auswirkung auf das Gesamtsystem haben. Ziel eines solchen Ansatzes ist es, die Komplexität des finalen Modells so gering und damit leicht interpretierbar wie möglich zu halten, dabei aber trotzdem an den grundlegenden Konzepten für PSA-Analysen festzuhalten.

Für den in der DIGMAP-Studie betrachteten Fall basierten die Leittechnik-Fehlerbäume des EDF-Modells letztlich auf nur fünf Arten von Basisereignissen:

- Messfehler-Basisereignisse
    - fassen die Ausfälle von 3-von-4 redundanten Sensoren zusammen
- 3 spezifische Arten von Verarbeitungs-Basisereignissen
    - fassen Ausfälle zusammen, die nur ein (oder einen begrenzten Satz von) Signal(en) betreffen:
    - Ausfall von AI-Baugruppen
    - Ausfall von auslösender oder überwachender Anwendungssoftware (AS) und
    - Ausfall von (nur) einem RPS-Subsystem
- RPS-Verlust-Basisereignisse
    - fassen alle fatalen Ausfälle zusammen, die durch die gemeinsame Nutzung von Hardware- oder Software-Modulen verursacht werden

Die quantitative Analyse konzentrierte sich auf CCFs, da diese von EDF als die einzigen signifikanten Beiträge zur Nichtverfügbarkeit dieses hochredundanten Systems angesehen werden. Die zugehörigen Wahrscheinlichkeiten wurden durch Berechnungen ermittelt, die die Testeffizienz und -abdeckung (der FTTs) sowie die tatsächliche Wertungslogik (der VUs) unter Berücksichtigung des Fail-Safe-Verhaltens einbezogen und bei großen CCF-Gruppen äußerst komplex sind.

Diese zusätzlichen Berechnungen wurden mit einem Tabellenkalkulationsprogramm durchgeführt, das die Zwischenberechnungen zur Dokumentation und zum Vergleich mit den detaillierteren Modellen der anderen Teilnehmer nachvollziehbar machten.

3.1.2.2 PSA-Modell der GRS

Das PSA-Modell der GRS berücksichtigt Ausfälle der übergeordneten Einheiten (Erfassungseinheiten (AU[1]), Verarbeitungseinheiten (PU), Wertungseinheiten (VU) und Baugruppenträger (SR[2])) als Basisereignisse. Dabei wird zwischen zwei verschiedenen Arten von Ausfällen unterschieden: Selbstmeldende (SF) und nicht-selbstmeldende Ausfälle (NSF). SF unterscheiden sich von NSF dadurch, dass erstere vom Leittechniksystem selbst durch die sogenannten Fault Tolerant Techniques (FTTs) erkannt, gemeldet und ggf. anders verarbeitet werden. Im Gegensatz hierzu können NSF ausschließlich durch Full-Scope-Tests entdeckt werden. Um die Wahrscheinlichkeiten von SF und NSF zu ermitteln, wurden im Vorfeld separate Fehlerbäume für die einzelnen Einheiten erstellt, um aus den in der Systembeschreibung des Referenzfalls angegebenen Zuverlässigkeitskenngrößen der Baugruppen (z. B. Prozessorbaugruppen PM) die entsprechenden Daten zu gewinnen.

Für die Erstellung der Fehlerbäume für das Gesamtsystem wurden die relevanten Fehlerausfallarten (Failure Modes) mit Hilfe von Fehlermöglichkeits- und -einflussanalysen (FMEAs) identifiziert. Hierbei wurden auch die Änderungen der Wertungslogiken berücksichtigt, indem die entsprechenden zugehörigen Kombinationen in die FMEAs aufgenommen wurden. Da im Gesamtmodell nicht zwischen Hardware und Software der Geräte unterschieden wird, wurden CCFs auf der Ebene der Einheiten (AU, PU, VU, SR) unter Berücksichtigung der Fehlerarten (SF, NSF) betrachtet.

---

[1] Im GRS-Modell wird die in /MÜL 18/ verwendete Nomenklatur verwendet. Dort wird lediglich zwischen AU, PU, VU und SR unterschieden. Die VU eines einzelnen Teilsystems einer Scheibe setzt sich beispielsweise einem CL (Communication Link Module), einem PM (Prozessormodul) und einem DO (Digital Output Module) zusammen (vgl. Abb. 3.2). Eine AU besteht entsprechend nur aus einer einzigen Komponente, nämlich einem AI (Analogue Input Module).

[2] Baugruppenträgern (SR – Subracks) sind hier keine rein passiven Bauteile. Neben der Stromversorgung der eingesetzten Baugruppen, sorgen diese über den Rückwandbus teilweise auch für die Kommunikation zwischen den eingesetzten Karten (siehe auch Anhang A.2.1).

3.1.2.3 PSA-Modell des KAERI

Das PSA-Modell des KAERI ist vergleichsweise detailliert, wenn auch etwas geringer detailliert als die Modelle von NRG und UJV. Einschränkungen des Detaillierungsgrads gab es hinsichtlich CCFs der AI-Baugruppen, da CCF-Gruppen[3] (bei Verwendung eines Alpha-Faktor-Modells[4]) mit mehr als acht Elementen in der von KAERI verwendeten Software (AIMS-PSA /HAN 16/) nicht ohne Weiteres berücksichtigt werden können. Weitere Einschränkungen gab es bei der Berücksichtigung der Unverfügbarkeiten der FTTs. Diese wurden indirekt über eine Variation der FTT-Testintervalle modelliert (bei Überschneidungen der Erkennungsabdeckung mehrerer FTTs wurde angenommen, dass die FTT mit dem kürzesten Prüfintervall greift und dessen Modellparameter in Hintergrundberechnungen angepasst).

Darüber hinaus wurde eine Reihe weiterer konservativer Annahmen getroffen:

- Jedes Basisereignis innerhalb einer Baugruppe (durch Hardware-, OP- oder AS-Fehler) verursacht im KAERI-Modell den Ausfall der gesamten Baugruppe.
- Außerdem wurden Änderungen der Wertungslogik der VUs aufgrund erkannter Ausfälle nicht explizit modelliert und auch die Nichtverfügbarkeit aufgrund von Reparaturen nur bei Ausfällen innerhalb der Hardware berücksichtigt.

3.1.2.4 PSA-Modell der NRG

Das PSA-Modell der NRG ist durch eine sehr aufwendige und detaillierte Modellierung des Leittechniksystems gekennzeichnet. Die grundlegende Detailebene, die modelliert wurde, beschreibt die Hard- und die Software jeder Baugruppe separat. Die Hardware der Baugruppen wurde entsprechend der verwendeten FTTs aufgeteilt. Alle Parameter und Testabdeckungen wurden direkt als Basisereignisse in das PSA-Modell eingeführt.

---

[3] CCF-Gruppe meint in diesem Zusammenhang eine Gruppe von Komponenten bzw. Elementen, die aufgrund gleicher Ursache ausfallen können. Häufig werden CCF-Gruppen auch als Common-Cause-Component-Groups (CCCG) bezeichnet.

[4] Siehe hierzu Anhang A.1.

Die aktive Umschaltung der Wertungslogiken der VUs, die Auswahl der jeweils relevanten Sensoren sowie AI-Baugruppen wurden im NRG-Modell durch bedingte Auslöser im Modell berücksichtigt. Eine Einschränkung dieses sehr detaillierten Ansatzes war lediglich die CCF-Modellierung der AI-Einheiten (16 Komponenten), da große CCF-Gruppen (mit mehr als acht Komponenten) nicht ohne Weiteres in der verwendeten Software (RiskSpectrum /RIS 21/) bei Verwendung eines Alpha-Faktor-Modells berücksichtigt werden können.

3.1.2.5 PSA-Modell der UJV

UJV verfolgte wie NRG ebenfalls einen sehr detaillierten Modellierungsansatz. Alle Berechnungen wurden explizit im PSA-Modell selbst modelliert. Im Unterschied zum Modell von NRG wurde jedoch die Überlappung der FTTs nicht explizit modelliert.

3.1.2.6 PSA-Modell des VTT

Der Modellierungsansatz von VTT hatte das Ziel, möglichst einfache Fehlerbäume zu erstellen und komplexe Berechnungen im Hintergrund durchzuführen. Alle RPS-bezogenen Basisereignisse im Modell sind CCFs, die zum Ausfall einer oder mehrerer Sicherheitsfunktionen führen. Die CCFs wurden für verschiedene Baugruppen und für AS, OP und Hardware getrennt modelliert. Für jede Baugruppe gibt es daher nur ein einzelnes Hardware-Basisereignis, welches alle unerkannten und (von FTTs) erkannten Ausfälle kombiniert.

Dementsprechend wurden die FTTs nur in Hintergrundberechnungen berücksichtigt und sind nicht explizit im Modell enthalten. Im Hintergrundmodell gibt es für jede Baugruppe einen Fehlerbaum, der die Gesamtausfallwahrscheinlichkeit der Hardware im Modul bestimmt. In diesen Fehlerbäumen werden Ausfälle, die von verschiedenen FTTs erkannt werden, und Ausfälle der FTTs selbst modelliert. Änderungen in der Wertungslogik (von VUs) wurden nicht modelliert, da der Risikobeitrag der entsprechenden Szenarien in einer früheren Modellversion als vernachlässigbar eingestuft wurde. Hardware-Basisereignisse kombinieren im VTT-Modell erkannte und unerkannte Ausfälle, und die Auswirkungen von erkannten Ausfällen werden konservativ denen von nicht erkannten Ausfällen gleichgesetzt.

CCFs mit den gleichen Auswirkungen wurden zu einem Basisereignis zusammengefasst. Die Wahrscheinlichkeiten der Hardware-CCF-Basisereignisse wurden mit Hilfe von Tabellenkalkulationen berechnet. Zusätzlich zu den normalen Alpha-Faktor-Berechnungen erfordert dies recht komplexe kombinatorische Berechnungen, um die CCF-Kombinationen mit Gruppengrößen von 8 und 16 zu verwalten. Die CCF-Basisereigniswahrscheinlichkeiten wurden konservativ mit 1,1 multipliziert, was durch Expertenurteil auf der Grundlage einiger begrenzter unterstützender Berechnungen entschieden wurde (siehe Anhang B6 im DIGMAP-Report /NEA 21/).

3.1.3 Ergebnisse

Um die unterschiedlichen Modellierungsansätze der teilnehmenden Organisationen zu vergleichen, sind in Abb. 3.3 die mit den Modellen berechneten Kernschadenshäufigkeiten als Balken dargestellt (für das auslösende Ereignis LMFW – Loss of Main FeedWater, also dem Ausfall der Hauptspeisewasserversorgung).

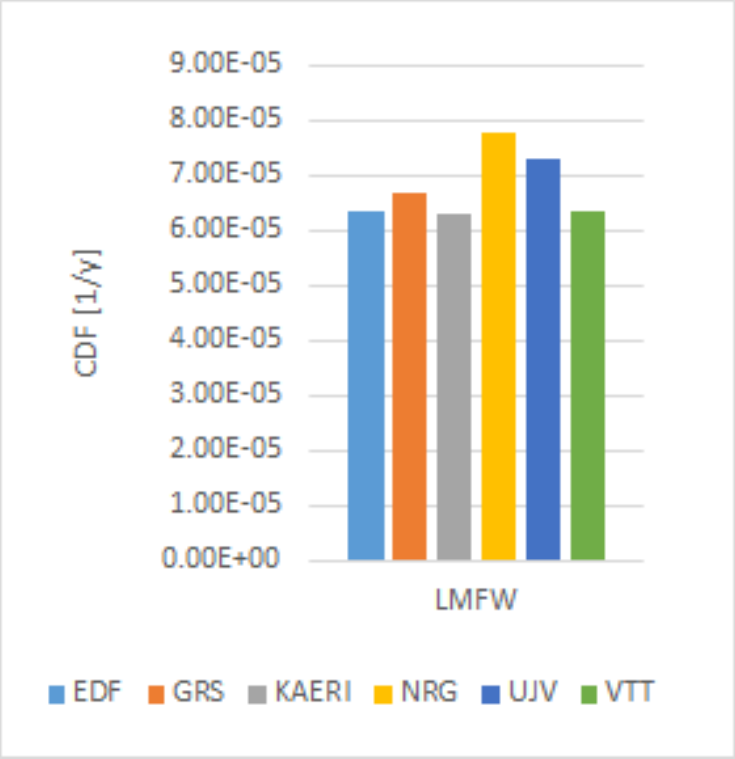

Abb. 3.3 Kernschadenshäufigkeiten für das auslösende Ereignis LMFW

Mit unterschiedlichen Modellen (von EDF, GRS, KAERI, NRG, UJV und VTT) ermittelte Kernschadenshäufigkeiten (CDF – Core Damage Frequency) für das auslösende Ereignis (Loss of Main FeedWater).

Die Ergebnisse aller Modelle liegen vergleichsweise nah beieinander, so zeigt die Kernschadenshäufigkeit (CDF) nur eine relativ geringe Variabilität (maximal um einen Faktor von 1,24). Die dennoch vorhandenen Unterschiede zwischen den einzelnen Modellen können nicht durch deren Detaillierungsgrad erklärt werden. So gehören z. B. sowohl das KAERI-Modell (mit dem niedrigsten Ergebniswert) als auch das NRG-Modell (mit dem höchsten Ergebniswert) zur Gruppe mit niedrigem Abstraktionsgrad und damit hohem Detaillierungsgrad (siehe Tab. 3.4).

Stattdessen konnten die quantitativen Unterschiede durch eine ausführliche Analyse einzelnen Modellierungsentscheidungen zugeordnet werden, die ausdrücklich nicht im Zusammenhang mit dem Abstraktionsgrad des jeweiligen Modells stehen, wie durch Tab. 3.5 verdeutlicht wird.

Tab. 3.5 Auf die Unterschiede der Modellierungsansätze adaptierte Ergebnisse

Hier wurden die Einheiten weggelassen, sämtliche Größen sind in 1/ry angegeben (pro Reaktor und Jahr).

	Einfluss auf CDF	**EDF**	**GRS**	**KAERI**	**NRG**	**UJV**	**VTT**
CDF	**-**	**$6{,}33\cdot10^{-5}$**	**$6{,}68\cdot10^{-5}$**	**$6{,}28\cdot10^{-5}$**	**$7{,}78\cdot10^{-5}$**	**$7{,}30\cdot10^{-5}$**	**$6{,}32\cdot10^{-5}$**
Einschränkungen durch RiskSpectrum hinsichtlich CCF von 16 AI-Baugruppen	$1{,}52\cdot10^{-5}$				$-1{,}52\cdot10^{-5}$	$-1{,}52\cdot10^{-5}$	
Verteilte Softwarefehler	$-5{,}00\cdot10^{-6}$					$5{,}00\cdot10^{-6}$	
Faktor 1,1 für CCF hoher Ordnung	$2{,}80\cdot10^{-7}$						$-2{,}80\cdot10^{-7}$
Allgemeine Rundung	$4{,}00\cdot10^{-7}$	$-4{,}00\cdot10^{-7}$					
Verwendung eines Beta-Faktor-Modells[5] anstatt Alpha-Faktor-Modells für Hardware-CCFs	$1{,}15\cdot10^{-5}$		$-1{,}15\cdot10^{-5}$				
Verwendung eines Beta-Faktor-Modells anstatt Alpha-Faktor-Modells für Software-CCFs	$-7{,}45\cdot10^{-6}$		$7{,}45\cdot10^{-6}$				
Beta-Faktor von 0,9 für OP	$-2{,}50\cdot10^{-7}$				$2{,}50\cdot10^{-7}$		
„Korrigierte“ Ergebnisse	**-**	**$6{,}29\cdot10^{-5}$**	**$6{,}28\cdot10^{-5}$**	**$6{,}28\cdot10^{-5}$**	**$6{,}29\cdot10^{-5}$**	**$6{,}29\cdot10^{-5}$**	**$6{,}29\cdot10^{-5}$**

Die erste Zeile dieser Tabelle (CDF) spiegelt die grundlegenden Ergebnisse der Modelle wider, wie sie auch in Abb. 3.3 dargestellt sind. In den darauffolgenden Zeilen werden die quantitativen Auswirkungen bestimmter Modellierungsentscheidungen aufgeführt. Dabei wird in jeder Zeile die häufigste Modellierungsentscheidung als Referenz herangezogen und die quantitative Auswirkung auf die CDF von alternativen Lösungen durch einen positiven oder negativen Wert dargestellt.

[5] Zum Alpha-Faktor-Modell und Beta-Faktor-Modell: siehe Anhang A.1.

So führt beispielsweise die Verwendung eines Beta-Faktor-Modells für CCF der Hardware im GRS-Modell zu einem $1{,}15 \cdot 10^{-5}$/ry (pro Reaktor (r) und Jahr (y)) größeren Ergebnis als die Verwendung eines Alpha-Faktor-Modells (wie in den anderen Modellen). Korrigiert man die individuellen Ergebnisse der ersten Zeile mit den Einflüssen spezifischer Modellierungsentscheidungen, so erhält man die in der untersten Zeile („korrigierte“ Ergebnisse) angegebenen Werte.

Die genaue Bedeutung der einzelnen Modellierungsentscheidungen kann im DIGMAP-Report /NEA 21/ nachgelesen werden, dort sind auch weitere Erläuterungen zur Berechnung der hier angegebenen Werte vorhanden. Entscheidend an dieser Stelle ist, dass die „korrigierten“ Werte deutlich weniger als 1 % voneinander abweichen. Die Teilnehmer der DIGMAP-Studie sind somit zu der Schlussfolgerung gekommen, dass die organisationsspezifischen Modellierungsannahmen vollständig die Unterschiede der unkorrigierten Ergebnisse erklären und daher die verschiedenen Modellierungsansätze konsistent und miteinander vergleichbar sind, unabhängig vom gewählten Abstraktionsgrad.

Sehr viele weitere Details und Ergebnisse (insbesondere auch von durchgeführten Sensitivitätsanalysen) können dem gemeinsamen DIGMAP-Report /NEA 21/ entnommen werden.

3.2 Bewertungsgrundlagen für digitale Sicherheitsleittechniksysteme

Die Ausführungen in diesem Abschnitt basieren auf den Ergebnissen der DIGMAP-Studie (Abschnitt 3.1) und auf den durch die GRS für diese Studie durchgeführten Arbeiten (siehe Anhang) sowie der Aufbereitung des Standes von Wissenschaft und Technik im Kapitel 2.

3.2.1 Allgemeines

Die Interpretation des Verhaltens eines digitalen Leittechniksystems in verschiedenen Fehlerszenarien ist nicht trivial. Sie erfordert das Verständnis verschiedener Aspekte, u. a. der Systemspezifikationen, des Systemdesigns und des Betriebsverhaltens einschließlich der Wartungs- und Teststrategie. Die hierfür benötigten Informationen liegen dabei nicht unbedingt in einem derart dokumentierten Format vor, dass diese für eine Modellerstellung unmittelbar genutzt werden können.

Während sich beispielsweise die Designdokumentation typischerweise darauf konzentriert, wie das System funktionieren soll, ist der PSA-Spezialist in der Regel mehr daran interessiert zu verstehen, ob und wie seine Funktionalität durch Fehler (sowohl in der Hardware als auch der Software) beeinträchtigt werden könnte.

Dies führte zu einem erheblichen Aufwand innerhalb der Arbeitsgruppe der DIGMAP-Studie. Es waren mehrere Iterationen notwendig, um zu einer gemeinsamen Auffassung und gemeinsamen Annahmen zu gelangen, die widerspiegeln, wie die betrachteten leittechnischen Systeme ausfallen können und sich in verschiedenen Situationen verhalten.

Nach Meinung der Arbeitsgruppe ist dieser Aufwand vergleichbar mit den vorbereitenden Aktivitäten, die ein PSA-Praktiker im Allgemeinen benötigt, wenn er versucht, die Leittechnik-Designdokumentation zu interpretieren. Bei der Modellierung von leittechnischen Systemen, die in kerntechnischen Anlagen installiert sind, sind eingehende Diskussionen mit Leittechnik-Ingenieuren und Betreibern erforderlich, um zu bestätigen, dass die Dokumentation und Betriebsbedingungen korrekt interpretiert und in ein Zuverlässigkeitsmodell übersetzt wurden.

Ein allgemeiner sehr wichtiger Punkt, der in den durchgeführten Arbeiten auftauchte, ist die Notwendigkeit einer klaren Erfassung (und Dokumentation) aller Annahmen, die beim Prozess der Modellierung getroffen wurden, um die Validierung und Überprüfung des PSA-Modells zu unterstützen (z. B. bei der Einschätzung der Genauigkeit des entwickelten Modells mit Hilfe von Leittechnik-Ingenieuren oder bei der Interpretation der Ergebnisse).

3.2.2 Benchmarks

Der Vergleich der innerhalb der DIGMAP-Studie entwickelten Modelle zeigt die Bedeutung eines Benchmarks für die Durchführung von PSAs. Tatsächlich halfen die Iterationen zur Konsolidierung des Testfalls dabei, Probleme in den PSA-Modellen zu identifizieren und diese daraufhin zu verbessern. Obwohl dies nicht spezifisch für die Modellierung eines digitalen Leittechniksystems ist, wird von den Teilnehmern an der DIGMAP-Studie die Bedeutung eines Benchmarks im Fall der PSA von digitalen Leittechniksystemen aufgrund der Komplexität und der Vielzahl der möglichen Ausfallmechanismen von Komponenten und der komplexen und hochredundanten Systemarchitektur besonders hervorgehoben.

In Anbetracht dieser Erkenntnis war sich die Arbeitsgruppe einig, dass es sinnvoll ist, PSA-Modelle zu vergleichen, z. B. bei der Lizenzierung einer neuen Anlage oder zur Unterstützung von Systemänderungen in einer bestehenden Anlage. Dies könnte mittels einer unabhängigen PSA-Modellierung (auch in vereinfachter Form) erfolgen, die z. B. von einer unabhängigen Organisation als Teil einer PSA-Validierung, von der Aufsichtsbehörde oder ihrer technischen Unterstützungsorganisation (TSO – Technical Support Organization) durchgeführt werden kann.

Zusätzlich können die Ergebnisse und Beschreibungen des DIGMAP-Reports /NEA 21/ als Benchmark genutzt werden, um damit die eigenen Modellierungsmethoden zu testen.

3.2.3 Abstraktions- bzw. Detaillierungsgrad von Modellen

Eine wichtige Erkenntnis aus der DIGMAP-Studie ist, dass unabhängig vom Detaillierungsgrad der Modellierung die Ergebnisse der verschiedenen Modelle im Wesentlichen gleich sind, sofern die gleichen Annahmen verwendet werden. Es gilt dabei, dass für jeden Detaillierungsgrad der Modellierung der gleiche Grad an Verständnis des Leittechniksystems und seines Verhaltens bei Ausfällen erforderlich ist. Auf einer niedrigen Abstraktionsebene ist dieses Verständnis für die detaillierte explizite Modellierung jeder Ausfallart jeder Hard- und Softwarekomponente notwendig. In einem hoch abstrakten Modell (bei Verwendung detaillierter Hintergrundberechnungen) wird derselbe Grad an Verständnis benötigt, um die möglichen Vereinfachungen zu definieren und diese in ein Analysemodell zu übersetzen. Dies impliziert, dass die Modellierungsannahmen durch Experteneinschätzungen, detaillierte Zuverlässigkeitsanalysen, Verweise auf den Stand von Wissenschaft und Technik oder, wenn möglich, durch die Nutzung von Betriebserfahrungen hinsichtlich Ausfälle von Leittechnikkomponenten begründet werden sollten.

Vereinfachungen können auf verschiedenen Ebenen vorgenommen werden. Dies kann Zeit bei der Erstellung und Pflege des Modells sparen, allerdings auf Kosten des Detaillierungsgrades der Ergebnisse. Die Entwicklung eines vereinfachten Modells kann hingegen mehrere Iterationen erfordern, da im Vorfeld nicht unbedingt bekannt ist, welche Art von Vereinfachungen vorgenommen werden können. Bei der Entscheidung über das Abstraktionsniveau muss sorgfältig darauf geachtet werden, dass nichts Wichtiges ausgelassen wird. Was wichtig ist, hängt in hohem Maße von der Verwendung des Modells ab. Solange die Modellierung korrekt und für den Zweck der Analyse geeignet ist, ist es eine Frage der Präferenzen des Analysten, ob er Vereinfachungen vornimmt oder nicht.

Der Detaillierungsgrad ist weder universell noch starr festgelegt. Es kann ein pragmatischer Ansatz verfolgt werden, indem Details übersprungen werden, wenn sie sich als vernachlässigbar erweisen. Es kann auch sinnvoll sein, einige Details in Hintergrundanalysen zu modellieren, damit das PSA-Modell selbst weniger komplex wird. In diesem Sinne können die detaillierten Modelle des vorliegenden Testfalls - ein kleiner, aber repräsentativer Teil des RPS - als Hintergrundberechnungen angesehen werden, die zur Untermauerung eines abstrakteren Modells des gesamten RPS verwendet werden können.

Die Modelle können auch heterogen sein: Sowohl Ansätze mit detaillierter Hardware und einfacher Softwaremodellierung (UJV-Modell) als auch vereinfachte Hardware und detailliertere Modellierung der Anwendungssoftware (EDF-Modell) wurden innerhalb der DIGMAP-Studie betrachtet.

Generell spielen bei der Wahl des Detaillierungsgrades bei der Modellierung folgende Aspekte eine Rolle:

- Verwendungszweck des Modells, z. B. zur Sicherheitsbewertung, Design-Evaluierung, im KKW-Betrieb, usw.;
- Pre-Processing-Aufwand bei kompakter Modellierung versus Post-Processing-Aufwand bei detaillierter Modellierung (z. B. zur Darstellung der Ergebnisse);
- Modellierungsaufwand (Zeit und Ressourcen), der für eine detaillierte Modellierung erforderlich ist, gegenüber dem Fachwissen und den Fähigkeiten, die für die Erstellung eines abstrakten Modells benötigt werden (einschließlich F&E-Arbeiten);
- Möglichkeiten zur Wieder-/Weiterverwendung des Modells (z. B. Flexibilität bei einer notwendigen Erhöhung des Detaillierungsgrads);
- Außendarstellung von Ergebnissen: Detaillierte Informationen vs. aggregierte Informationen;
- Verfügbare Daten/Informationen;
- Funktionale Einschränkungen des verwendeten PSA-Werkzeugs;
- Wartungsaufwand des Modells (Implementierung von zukünftigen Systemänderungen und Upgrades).

3.2.4 Wichtige Faktoren

Basierend auf den individuellen Ergebnissen der GRS und den Ergebnissen der DIGMAP-Studie (aus dem Vergleich der unterschiedlichen Modellierungsansätze und zusätzlich durchgeführten Sensitivitätsanalysen), konnten die folgenden Hauptfaktoren, die einen wesentlichen Beitrag zur Zuverlässigkeit digitaler Leittechniksysteme leisten, identifiziert werden:

Software Insbesondere Ausfälle in der Anwendungssoftware (AS), aber auch Ausfälle in der Betriebssystem- und Plattformsoftware (OP), tragen wesentlich zur Ausfallwahrscheinlichkeit von Auslösesignalen bei. Sensitivitätsanalysen belegen, dass deren Beitrag für große (konservative) Werte sogar dominant werden kann. Umgekehrt zeigen die durchgeführten Sensitivitätsanalysen aber auch, dass sich die Auswirkungen von Software-CCFs deutlich verringern können, wenn geringere Abhängigkeiten begründet werden können. Auch aus diesem Grund ist insbesondere die systematische Abbildung aller CCF-Bedingungen (hinsichtlich Software) in einem Modell eine große Herausforderung.

CCF Die Identifikation von CCF-Gruppen und der zugordneten CCF-Parameter sind Schlüsselthemen bei der Modellierung von digitalen Leittechniksystemen, da typischerweise viele identische Hardware- und Softwarekomponenten in redundanten Konfigurationen, in verschiedenen Baugruppen und Teilsystemen digitaler Leittechniksysteme enthalten sind. Unterschiedliche Einschätzungen des Ausmaßes der Unabhängigkeit und Diversität solcher Komponenten können zu sehr unterschiedlichen Ergebnissen führen, was sich während des Benchmark-Prozesses und bei Sensitivitätsanalysen innerhalb der DIGMAP-Studie zeigte. Insbesondere Hardware-CCFs haben einen erheblichen Einfluss auf die Zuverlässigkeit des Reaktorschutzsystems.

FTT Der Prozentsatz der Ausfälle, die durch die unterschiedlichen FTTs (Fault Tolerant Techniques) entdeckt werden kann, hat einen großen Einfluss auf das Ergebnis. So haben in der DIGMAP-Studie beispielsweise nicht-detektierte Ausfälle, die nur durch Full-Scope-Tests entdeckt werden können, einen großen Anteil am Gesamtergebnis, da in der Studie ein Abstand von 4380 Stunden (ein halbes Jahr) zwischen den Tests angenommen wurde (bei einer Reparaturzeit von acht Stunden). Allgemein macht es einen großen Unterschied, ob der Anteil nicht automatisch identifizierbarer Ausfälle z. B. 1 % oder 10 % beträgt.

Einen vergleichsweisen geringen Einfluss auf das Ergebnis haben hingegen die folgenden Faktoren:

Wertungslogiken Aktive Änderungen der Wertungslogiken (n-von-m) innerhalb von VUs (Wertungseinheiten) haben nur einen geringen Einfluss auf die Zuverlässigkeit des Systems. Dies lässt sich dadurch erklären, dass Änderungen der Wertungslogiken nur dann durchgeführt werden, wenn (vom Reaktorschutzsystem selbst) erkannte Ausfälle vorliegen und diese dann ohnehin kurzfristig (innerhalb von acht Stunden in der DIGMAP-Studie) behoben werden. Hierbei muss allerdings angemerkt werden, dass diese Aussagen für ungewollte Auslösungen (Spurious Actuations) nicht unbedingt gültig bleiben, diese wurden im Rahmen der DIGMAP-Studie aber nicht untersucht.

FTT-Ausfälle Ausfälle von leittechnischen Einrichtungen, die der Umsetzung von FTTs dienen (z. B. PTUs), spielen eine geringe Rolle. Insbesondere war deren Einfluss auf das Ergebnis in der DIGMAP-Studie angesichts der angenommenen Erkennungsabdeckung, des Testintervalls für Full-Scope-Tests (4.380 Stunden) und der angenommenen Ausfallwahrscheinlichkeiten nicht signifikant (solange diese nicht eine Größenordnung höher liegen als in der Studie angenommen, selbst dann wäre der Beitrag zur Kernschadenshäufigkeit aber immer noch gering).

Reparaturzeiten Im Rahmen der DIGMAP-Studie wurde eine Reparaturzeit von acht Stunden angenommen (für alle entdeckten Ausfälle). Unverfügbarkeiten während Reparaturen haben keinen signifikanten Einfluss auf das Ergebnis, wie durch den Vergleich unterschiedlicher Modelle sowie Sensitivitätsanalysen belegt werden konnte.

Abschließend konnte bisher weder die Dominanz von Hardware noch von Software auf die Gesamtsystemzuverlässigkeit (eines RPS) nachgewiesen werden. Obwohl die spezifische Gewichtung dieser beiden Elemente zwischen den einzelnen Modellen variierte, ist es nicht möglich, a priori zu bestimmen, ob Software oder Hardware (oder eine Kombination aus beiden) den größten Beitrag zur Gesamtzuverlässigkeit liefert. Dies deutet auf die Wichtigkeit einer ausgewogenen Zuverlässigkeitsmodellierung hin.

3.2.5 Sensitivitätsanalysen

Die für die Modellierung eines digitalen Leittechniksystems notwendigen Daten sind (insbesondere hinsichtlich der Software) mit einer großen Unsicherheit behaftet. Im Rahmen der DIGMAP-Studie wurden zwar die Methoden zu Bestimmung von Zuverlässigkeitskenndaten nicht betrachtet und die verwendeten Ausfalldaten und weitere Parameter als bekannt vorausgesetzt (siehe Abschnitt 3.1.1). Die Diskussionen innerhalb der DIGMAP-Arbeitsgruppe, welche konkreten Zuverlässigkeitskenndaten plausibler Weise verwendet werden sollten, haben aber die Unsicherheit der Daten und die Mehrdeutigkeit ihrer Interpretation hervorgehoben.

Schlüsselparameter, die schwer quantifizierbar sind, gehören zu den folgenden Bereichen:

- Quantifizierung der Software-Zuverlässigkeit,
- Modellierung der Software-CCF,
- Abdeckung von automatischen Tests (FTTs) für die Fehlererkennung.

Für einige Parameter (z. B. zur Software-Zuverlässigkeit und -CCF) gibt es derzeit nur einen begrenzten Konsens darüber, wie diese abzuschätzen sind, und für andere Fälle (z. B. Erkennungsabdeckung von automatischen Tests) sind quantitative Informationen nicht ohne weiteres in den Leittechnikdokumentationen zu finden.

Die Herausforderung liegt teilweise auch darin, wie entsprechende Daten in ein Modell implementiert werden sollen. Beispielsweise, wenn durch Experteneinschätzung oder statistische Tests zwar Werte vorliegen, aber nicht klar ist, wie diese hinsichtlich der Betriebssystem- und Plattformsoftware (OP) sowie der Anwendungssoftware (AS) zu berücksichtigen sind.

Die DIGMAP-Arbeitsgruppe war sich einig, dass es eine gute Praxis ist, Sensitivitätsanalysen zu diesen Parametern durchzuführen, um deren Bedeutung einschätzen zu können und insbesondere die Bereiche zu identifizieren, wo es zu einem „Kippen“ der Ergebnisse kommen könnte.

3.2.6 Große CCF-Gruppen

Eine weitere Herausforderung bei der Modellierung digitaler Leittechnik ist die Berücksichtigung großer CCF-Gruppen (siehe auch Abschnitt 3.2.4). Aktuelle PSA-Werkzeuge (z. B. RiskSpectrum /RIS 21/) können typischerweise vollständige Logiken für CCF-Gruppen aus 8 – 15 Komponenten berechnen. Für noch größere Gruppen ist deren Berechnungsfähigkeit begrenzt, d. h. die Berechnungen werden zu stark vereinfacht und konservativ, sofern sie überhaupt möglich sind. Die Hauptschwierigkeit bei der Berechnung der vollständigen Logik größerer CCF-Gruppen besteht darin, dass der Rechenaufwand für die Schnittmengengenerierung drastisch ansteigt und somit der Rechenaufwand insgesamt drastisch ansteigt.

Der Vergleich der unterschiedlichen Modelle der DIGMAP-Studie zeigt eine Reihe alternativer Vorgehensweisen auf:

- Die genaueste Option besteht darin, die CCF-Kombinationen und ihre Wahrscheinlichkeiten im Hintergrund zu berechnen (z. B. mithilfe von Tabellenkalkulationen) und Makro-Komponenten im PSA-Modell zu verwenden.
- Das Verschmelzen ähnlicher CCF-Ereignisse zu einem gemeinsamen Ereignis lieferte in der DIGMAP-Studie ähnliche Ergebnisse wie mit der genaueren Option. Allerdings kann dieser Ansatz das Risiko je nach Fall und Komponentengruppierung auch unterschätzen (d. h. es sind bei diesem Ansatz genaue Betrachtungen erforderlich, um zu überprüfen, ob diese Verschmelzungen zulässig sind).

- Bei Verwendung von RiskSpectrum als PSA-Werkzeug: Für den Fall, dass die Gruppengröße das Maximum übersteigt, das RiskSpectrum vollständig verarbeiten kann, werden automatisch Basisereignisse erzeugt, welche Mehrfachausfälle kombinieren. Im Allgemeinen liefert dieser Ansatz akzeptable Ergebnisse. Im Referenzfall der DIGMAP-Studie ist das Ergebnis jedoch übermäßig konservativ. Wenn es sich z. B. um eine CCF-Gruppe von 16 Komponenten handelt, generiert RiskSpectrum in der aktuellen Version nur CCF-Ereignisse von bis zu drei Komponenten-Kombinationsausfällen und ein Basisereignis, das alle anderen Kombinationen von vier oder mehr Ausfällen kombiniert. Da ein CCF von vier Baugruppen im Referenzfall der DIGMAP-Studie jedoch keinen Ausfall der Leittechnik bedeutet (ein sechsfacher Ausfall ist erforderlich), ist das Ergebnis in diesem speziellen Fall also übermäßig konservativ.

Die DIGMAP-Arbeitsgruppe kam zu folgenden gemeinsamen Aussagen überein:

- PSA-Analytiker sollten sich der Einschränkungen des jeweils verwendeten PSA-Softwarewerkzeugs bewusst sein und Workarounds sorgfältig bewerten, bevor sie diese anwenden.
- Es wäre wertvoll, wenn (z. B. auch Hersteller von PSA-Werkzeugen) sich künftige Forschung auf die Entwicklung eines praktikablen CCF-Modells und auf die Ermittlung von Daten ausrichtet, um mehr als 16 Komponenten realistisch berücksichtigen zu können.
- Die CCF-Theorie ist nicht ausgereift genug, um alle spezifischen Merkmale von digitalen Leittechniksystemen sicher abzudecken.
- Es gibt einen Mangel an Daten für große CCF-Gruppen.

3.3 Zusammenfassung AP2

Im Rahmen der Teilnahme an der DIGMAP-Studie (siehe Abschnitt 3.1) hat die GRS basierend auf den in /MÜL 18/ entwickelten Methoden ein eigenes PSA-Modell entwickelt (siehe Anhang). Ein wesentlicher Aspekt der Arbeiten war die Verwendung von Benchmarks (bzw. die Erstellung möglichst eines zweiten, unabhängigen Modells – siehe Abschnitt 3.2.2) bei PSAs.

Neben allgemeinen Erkenntnissen zu den Herausforderungen bei der Modellierung von digitaler Leittechnik, wurden durch das Benchmark und zusätzlich durch Sensitivitätsanalysen im Rahmen der DIGMAP-Studie die wichtigsten und weniger wichtigen Faktoren/Parameter bei der Modellerstellung identifiziert.

So lagen die Ergebnisse der unterschiedlichen Modelle der DIGMAP-Studie nach der ersten Iteration (also beim ersten Treffen der DIGMAP-Arbeitsgruppe) noch deutlich weiter auseinander als dies am Ende der Studie der Fall war. Die Gründe hierfür waren hauptsächlich unterschiedliche Interpretationen der bewerteten Leittechnik, hier insbesondere der Diversität der Teilsysteme. Allgemein ist die Berücksichtigung großer CCF-Gruppen besonders herausfordernd bei der Durchführung von PSAs.

Eine wichtige Erkenntnis der Untersuchungen ist, dass der Detaillierungsgrad eines PSA-Modells quasi keine Rolle hinsichtlich der Ergebnisse spielt (dieser sollte nach anderen Gesichtspunkten, z. B. dem Verwendungszweck des Modells oder gemäß den vorhandenen Ressourcen, gewählt werden). Wichtiger bei der Modellierung ist die korrekte Interpretation der vorhandenen Informationen (beispielsweise in den Systembeschreibungen realer Anlagen; im Fall der DIGMAP-Studie die Beschreibung des Referenzfalls) sowie die Verfügbarkeit von Zuverlässigkeitskenngrößen.

Darüber hinaus sind auch die vorhandenen und im Rahmen dieses Vorhabens weiterentwickelten Methoden der GRS durch den Vergleich mit den anderen Modellen der DIGMAP-Studie validiert worden.

4 Zusammenfassung und Ausblick

In diesem Bericht werden Forschungsarbeiten zur Entwicklung von Bewertungsgrundlagen für digitale Leittechniksysteme in kerntechnischen Anlagen vorgestellt. Die Basis dieser Forschungsarbeiten bildeten Recherchen zum Stand von Wissenschaft und Technik, Teilnahmen an einschlägigen Veranstaltungen (siehe Kapitel 2) sowie die Beteiligung der GRS an der DIGMAP-Studie (/NEA 21/) (siehe Kapitel 3).

Die Recherchen zum Stand von Wissenschaft und Technik zeigen, dass immer noch ein Weiterentwicklungsbedarf für das nationale und internationale kerntechnische Regelwerk hinsichtlich digitaler Leittechniksysteme besteht. Insbesondere spielen Smart Devices in der Leittechnik kerntechnischer Anlagen (z. B. als Sensoren oder in der Antriebstechnik) eine zunehmende Rolle, entsprechende regulatorische Fragestellungen sind aber noch völlig offen. Die Recherchen zum Stand von Wissenschaft und Technik auf diesem Gebiet sollten daher auch nach Beendigung des aktuellen Vorhabens bei der GRS fortlaufend fortgesetzt werden.

Im Rahmen der Mitarbeit an der DIGMAP-Studie war die GRS u. a. an der Entwicklung eines Referenzanlagenmodells sowie der an der Erstellung der Beschreibung des Referenzfalls beteiligt. Anschließend wurde von der GRS auch eines der sechs in der DIGMAP-Studie betrachteten PSA-Modelle erstellt und beim Vergleich dieser Modelle wesentliche Beiträge geleistet.

Der Vergleich der unterschiedlichen Modelle und verwendeten Ansätze im Rahmen der DIGMAP-Studie hat wirkungsvoll dazu beigetragen, dass einige wichtige Erkenntnisse zu PSA-Modellen für die Leittechnik erlangt wurden:

- Allgemeine Herausforderungen und wichtige Gesichtspunkte bei modellbasierten Analysen und der Bewertung digitaler Leittechnik;
- Bewertung des Einflusses des Detaillierungsgrads bei der Modellierung digitaler Leittechnik für Zuverlässigkeits- und Sicherheitsanalysen;
- Bestimmung wesentlicher Faktoren/Parameter modellbasierter Zuverlässigkeitsanalysen digitaler Leitechnik;
- Bedeutung von Benchmarks und Sensitivitätsanalysen für die Modellerstellung.

Des Weiteren wurden durch die Teilnehmer an dieser Studie eine Reihe potenzieller Bereiche für zukünftige Forschungsarbeiten identifiziert:

- Fortsetzung der DIGMAP-Studie für einen realitätsnäheren Fall zur Bestätigung der Erkenntnisse aus der DIGMAP-Studie unter realistischeren Bedingungen, d. h. idealerweise Modellierung eines konkreten in einem KKW installierten leittechnischen Systems.
- Entwicklung von Leitfäden
  - zur Modellentwicklung einschließlich Verifikation und Validierung (V&V),
  - zur Sammlung und Auswertung von Eingangsdaten für Fehlerbaumanalysen,
  - zur Modellierung der Techniken zur Fehlererkennung und Fehlervermeidung (FTT – Fault Tolerant Techniques),
  - zur Modellierung von CCFs (CCF – Common Cause Failure) in der Hard- und Software sowie allgemein
  - zu Sensitivitäts- und Unsicherheitsanalysen.
- Bestimmung quantitativer Werte für Schlüsselparameter hinsichtlich der Software bei der Modellierung digitaler Leittechniksysteme.

Die Bestimmung von quantitativen Werten für Schlüsselparameter der Software in der Leittechnik stellt nach heutigem Stand eine enorme Herausforderung dar, die insbesondere die Beteiligung weiterer Stakeholder (u. a. Hersteller und Betreiber von leittechnischen Systemen) erfordern würde, ohne deren Beteiligung eine Umsetzung nicht möglich ist. Die Entwicklung von Leitfäden wird von der Arbeitsgruppe derzeit als langfristiges Ziel betrachtet. Daher haben die Teilnehmer an der DIGMAP-Studie beschlossen, die DIGMAP-Studie für einen realitätsnäheren Fall in einem Nachfolgeprojekt fortzusetzen. Hierbei sollen bei den Forschungsarbeiten u. a. die folgenden zusätzlichen Schwerpunkte gelegt werden:

- Berücksichtigung der betrieblichen Leittechnik und deren Anbindung über Prioritätsmodule,
- Wechselwirkungen zwischen Reaktorschutzsystem und ESFAS-Signalen (ESFAS – Engineered Safety Features Actuation System; Steuerung der Sicherheitssysteme),

- Wechselwirkungen zwischen manuellen und automatischen Auslösungen von Sicherheitsfunktionen,
- Einfluss der Mensch-Maschine-Schnittstellen (HMI – Human-Machine-Interface),
- Berücksichtigung weiterer denkbarer Störquellen (z. B. durch die Stromversorgung, Hilfssysteme, etc.).

Die GRS plant sich an den nachfolgenden Forschungsarbeiten der OECD/NEA-Arbeitsgruppe WGRISK zu beteiligen und ggf. die Führung des Nachfolgeprojekts zu übernehmen.

Unabhängig von den Erkenntnissen der Arbeitsgruppe hat die GRS im Rahmen dieses Vorhabens weitere wichtige Fragestellungen mit hoher sicherheitstechnischer Relevanz identifiziert, beispielsweise zu den Bewertungsgrundlagen beim Einsatz FPGA-basierter Geräte und Smart Devices in der Kerntechnik. Zu diesen Fragestellungen könnte die GRS einen wesentlichen Beitrag leisten, da bei der GRS die Smart Devices verschiedener Hersteller vorhanden sind.

Die Erkenntnisse bestätigen auch die im Vorhaben 4718R01314 („Forschungsarbeiten zur Weiterentwicklung der Methode der Sensitivitätsanalyse zur Bewertung von Fehlerauswirkungen auf ein Leittechnik-Testsystem“) identifizierten angestrebten zukünftigen Betätigungsfelder der GRS:

- Inbetriebnahme einer Betriebsleittechnik (BELT) und deren Kopplung mit der Sicherheitsleittechnik (SILT) des Analyse- und Testsystems AnTeS der GRS über digitale Einrichtungen der Vorrangebene moderner Leittechniksysteme;
    - Untersuchungen zu verschiedenen Automatisierungssystemen und -einrichtungen (z. B. SILT und BELT) von Kränen und Hebezeugen, Forschungsreaktoren und Systemen im Nachbetrieb (z. B. BE-Becken).

Referenzen

/AUT 13/ Authén, S., Holmberg, J.: *Guidelines for reliability analysis of digital systems in PSA context - Phase 3 Status Report*, NKS-277, Nordic nuclear safety research (NKS), Roskilde, Dänemark, 2013.

/BFS 05/ Bundesamt für Strahlenschutz: *Methoden zur probabilistischen Sicherheitsanalyse für Kernkraftwerke*, BfS-SCHR-37/05, Wirtschaftsverlag NW, Salzgitter, Deutschland, 2005.

/EDF 21/ *Design Code KB3* [online], verfügbar unter: https://www.edf.fr/en/the-edf-group/inventing-the-future-of-energy/r-d-global-expertise/our-offers/simulation-softwares/kb3, zuletzt abgefragt am 02.06.2021.

/HAN 16/ Han, S., Lim, H., Jang, S. and Yang, J.: *AIMS-PSA: A Software for Integrated PSA*, 13th International Conference on Probabilistic Safety Assessment and Management (PSAM 13), Seoul, Südkorea, 2016.

/IAE 15/ Specific Safety Guide SSG-37: *Instrumentation and Control Systems and Software Important to Safety for Research Reactors*, International Atomic Energy Agency (IAEA), Wien, Österreich, 2015.

/IAE 16/ Specific Safety Guide SSG-39: *Design of Instrumentation and Control Systems for Nuclear Power Plants*, International Atomic Energy Agency (IAEA), Wien, Österreich, 2016.

/IAE 19/ Specific Safety Guide SSG-51: *Human Factors Engineering in the Design of Nuclear Power Plants*, International Atomic Energy Agency (IAEA), Wien, Österreich, 2019.

/IEC 18/ IEC 60812:2018: *Failure Modes and Effects Analysis (FMEA and FMECA)*, VDE Verlag GmbH, Berlin, Deutschland, 2018.

/MÜL 18/ Müller, C., Peschke, J. and Piljugin, E.: *Entwicklung und Erprobung eines Werkzeugs zur Sensitivitätsanalyse der Fehlerauswirkungen in der sicherheitsrelevanten digitalen Leittechnik*, GRS-494, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH, Köln, Deutschland, 2018.

/NEA 15/ NEA/CSNI: *Failure Modes Taxonomy for Reliability Assessment of Digital I&C Systems for PRA*, NEA/CSNI/R(2014)16, OECD Nuclear Energy Agency (NEA/CSNI), Paris, Frankreich, 2015.

/NEA 21/ NEA/CSNI: *Digital I&C PSA – Comparative Application of Digital I&C Modelling Approaches for PSA*, Bezeichnung ausstehend, OECD Nuclear Energy Agency (NEA/CSNI), Paris, Frankreich, 2021.

/NRC 20/ NUREG-0800: *Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems*, Branch Technical Position BTP 7-19, U.S. Nuclear Regulatory Commission (NRC), Rockville, USA, 2020.

/RIS 21/ *RiskSpectrum™: Risk and Reliability Software* [online], verfügbar unter https://www.lr.org/en/riskspectrum/, zuletzt abgefragt am 02.06.2021.

/RIS 21a/ *RiskSpectrum Analysis Tools: Theory Manual*, Version 3.4.2, Lloyd's Register Consulting – Energy AB, London, England
Wird in elektronischer Form mit der jeweiligen RiskSpectrum-Version ausgeliefert.

/VTT 13/ *Probabilistic Risk Analysis and Decision Making with FinPSA* [online], verfügbar unter https://cris.vtt.fi/en/publications/probabilistic-risk-analysis-and-decision-making-with-finpsa, zuletzt abgefragt am 02.06.2021. Demoversion verfügbar unter https://www.simulationstore.com/finpsa, zuletzt abgefragt am 02.06.2021.

/WNA 20/ *Safety Classification for I&C Systems in Nuclear Power Plants – Current Status and Difficulties*, World Nuclear Association, Report No. 2020/001, London, Großbritannien, 2020.

/WGR 21/ *Working Group on Risk Assessment (WGRISK)* [online], verfügbar unter https://www.oecd-nea.org/jcms/pl_25617/working-group-on-risk-assessment-wgrisk, zuletzt abgefragt am 28.07.2021.

/WIK 21/ Wikipedia: *Probabilistische Sicherheitsanalyse* [online], verfügbar unter https://de.wikipedia.org/wiki/Probabilistische_Sicherheitsanalyse, zuletzt abgefragt am 18.08.2021.

Tabellenverzeichnis

Abbildungsverzeichnis

Abkürzungen

A	Automatic Test
ADS	Automatic Depressurization System
AI	Analogue Input (Module)
ANS	American Nuclear Society
AnTeS	Analyse- und Testsystem (der GRS)
APU	Acquisition and Processing Unit
AS	Application Software
AU	Acquisition Unit
BE	Brennelement
BELT	Betriebsleittechnik
BTP	Branch Technical Position (der U.S. NRC)
BWR	Boiling Water Reactor
CCF	Common Cause Failure
CCW	Component Cooling Water System
CDF	Core Damage Frequency
CL	Communication Link (Module)
COTS	Commercial-Off-The-Shelf
DI&C	Digital I&C (Instrumentation and Control)
DIGMAP	Digital I&C PSA – Comparative Application of Digital I&C Modelling Approaches for PSA
DIGREL	Digital System Reliability Failure Mode Taxonomy
DO	Digital Output (Module)
ECC	Emergency Core Cooling System
EFW	Emergency Feedwater System
ESFAS	Engineered Safety Features Actuation System
F	Full-Scope Test
FMEA	Failure Mode and Effects Analysis
FoD	Failure on Demand
FPGA	Field Programmable Gate Array
FTA	Fault Tree Analysis
FTT	Fault Tolerant Techniques
HMI	Human-Machine-Interface
HVA	Heating, Ventilation and Air Conditioning System
HW	Hardware
IAEA	International Atomic Energy Agency

IDN	Intra-Division Network
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronic Engineers
IEEE STD	IEEE Standard
KKW	Kernkraftwerk
MFW	Main Feedwater System
NEA	Nuclear Energy Agency (der OECD)
NSF	Non-Self-signaling Failure
OECD	Organisation for Economic Co-operation and Development
OP	Operation System and Platform Software
P	Periodical Test
PM	Processor Module
PSA	Probabilistic Safety Analysis
PTU	Periodical Testing Unit
PU	Processing Unit
RG	Regulatory Guide (der U.S. NRC)
RHR	Residual Heat Removal System
RPS	Reactor Protection System
RS	Reactor Scram System
SF	Self-Signaling Failure
SILT	Sicherheitsleittechnik
SR	Subrack
SSG	Specific Safety Guide (der IAEA)
SW	Software
SWS	Service Water System
TDR	Time-Domain Reflectometer
TSO	Technical Support Organization
U.S. NRC	U.S. Nuclear Regulatory Commission
V&V	Verification and Validation
VU	Voting Unit
W&T	Wissenschaft und Technik
WDT	Watchdog Timer
WENRA	Western European Nuclear Regulators Association
WGRISK	Working Group on Risk Assessment (der OECD/NEA)
WNA	World Nuclear Association

A Anhang

A.1 Grundsätzliches zur Probabilistischen Sicherheitsanalyse – PSA

Die Probabilistische Sicherheitsanalyse (PSA) untersucht die Risiken von Industrieanlagen (in der DIGMAP-Studie eines Referenzkraftwerks) mittels der Methoden der Wahrscheinlichkeitsrechnung und Systemanalyse /WIK 21/. Die Durchführung einer PSA speziell für kerntechnische Anlagen wird beispielsweise ausführlich in /BFS 05/ beschrieben. Demnach werden allgemein bei der Durchführung einer PSA nacheinander die folgenden Schritte durchlaufen:

- Identifikation der Gefahrenpotentiale, die in einer Anlage enthalten sind
- Beschreibung der Sicherheitstechnik, der Maßnahmen und Barrieren, die den Gefahrenpotentialen entgegenwirken
- Bestimmung der Störfälle, die zu einer Freisetzung der Gefahrenpotentiale führen können (störfallauslösende Ereignisse, engl. „Initiating Events“).
- Festlegung des Spektrums der störfallauslösenden Ereignisse.
- Analyse der Störfallabläufe und der Wirkungsweise der Systemtechnik unter den Störfallbedingungen sowie Umsetzung der Störfallabläufe in Ereignis- und Fehlerbäume (sie bilden das probabilistische Modell in der PSA, das mit den Methoden der Wahrscheinlichkeitsrechnung quantifiziert werden kann).
- Ermittlung der Eingangsgrößen in das probabilistische Modell, den Zuverlässigkeitskenndaten, HF-, CCF-Daten (Wahrscheinlichkeitsgrößen) und den Instandsetzungszeiten und Prüfintervallen (Zustandsänderungsgrößen) der Komponenten des Systems.
- Quantifizierung des probabilistischen Modells.
- Bewertung der Risikoergebnisse, Feststellung der führenden Risikobeiträge (Systemschwachstellen) und der möglichen risikosenkenden Maßnahmen.

  Für die Durchführung einer PSA ist also die Erstellung von Fehlerbäumen essentiell, aus denen sich das quantifizierbare probabilistische Modell ergibt. Ausführliche Erläuterungen zu Fehlerbäumen können beispielsweise in /BFS 05/ (Abschnitt 3.2.3 – „Der Fehlerbaum“) nachgelesen werden.

Für das Verständnis der in diesem Bericht beschriebenen, durchgeführten PSAs werden an dieser Stelle nachfolgend einige wichtige Begrifflichkeiten erläutert, die nicht unmittelbar in /BFS 05/ zu finden sind.

CCF-Modellierung

Die Modellierung von CCFs (z. B. in der Software RiskSpectrum) lässt sich am besten anhand eines Beispiels erläutern (aus /RIS 21a/). Angenommen, es sollen CCFs für die vier Komponenten A, B, C und D modelliert werden. Dann werden zunächst die einzelnen Ausfälle der vier Komponenten durch vier Basisereignisse im Fehlerbaum dargestellt. Wenn diese Basisereignisse (der Einfachheit halber auch A, B, C und D genannt) vorhanden sind, können diese einer sogenannten CCF-Gruppe zugeordnet werden. Anschließend wird das zu verwendende CCF-Modell (z. B. Beta-Faktor oder Alpha-Faktor – siehe hierzu weiter unten) und die entsprechenden Parameter des CCF-Modells festgelegt.

Wenn die Bearbeitung der CCF-Gruppe abgeschlossen ist, erstellt das Programm RiskSpectrum automatisch die folgenden CCF-Ereignisse als Basisereignisse (AB bedeutet einen CCF mit den Komponenten A und B): AB, AC, AD, BC, BD, CD, ABC, ABD, ACD, BCD, ABCD. In diesem Beispiel werden also insgesamt 11 neue Basisereignisse automatisch erstellt und in den Fehlerbaum integriert. Anstatt allein durch einen Einzelausfall, kann dann beispielsweise die Komponente A durch die folgenden Basisereignisse ausfallen:

- A – Einzelausfall von A
- AB – gemeinsamer Ausfall von A und B
- AC – gemeinsamer Ausfall von A und C
- AD – gemeinsamer Ausfall von A und D
- ABC – gemeinsamer Ausfall von A, B und C
- ABD – gemeinsamer Ausfall von A, B und D
- ACD – gemeinsamer Ausfall von A, C und D
- ABCD – gemeinsamer Ausfall von A, B, C und D

Welche (automatisch berechneten) Zuverlässigkeitskenndaten den einzelnen Basisereignissen zugeordnet werden, hängt dabei von der Auswahl des zu verwendenden CCF-Modells ab.

Alpha-Faktor-Modell

Bei der Verwendung des Alpha-Faktor-Modells (bezogen auf das Beispiel oben) für die Modellierung von CCFs werden Faktoren (Alpha-Faktoren) für den Ausfall von zwei, drei und vier Komponenten festgelegt, mit deren Hilfe aus den ursprünglichen Einzelausfallwahrscheinlichkeiten die Zuverlässigkeitskenndaten für die einzelnen CCF-Basisereignisse berechnet werden. Details hierzu können in /RIS 21a/ nachgelesen werden.

Beta-Faktor-Modell

Bei Verwendung des Beta-Faktor-Modells wird davon ausgegangen, dass jeder CCF grundsätzlich den Ausfall aller Komponenten verursacht. Im Beispiel oben bedeutet das, dass den Ausfallkombinationen AB, AC, AD, BC, BD, CD, ABC, ABD, ACD und BCD formal die Wahrscheinlichkeit 0 zugeordnet wird. Die Zuverlässigkeitskenndaten für das einzig verbleibende CCF-Basisereignis ABCD wird aus dem sogenannten Beta-Faktor berechnet. Beträgt dieser beispielsweise 0,05 (5 %), so tritt mit 5 % Wahrscheinlichkeit anstatt eines Einzelfehlers ein CCF auf. Genauere Details können /RIS 21a/ entnommen werden.

A.2 PSA-Modell der GRS

Das von der GRS entwickelte PSA-Modell im Rahmen der DIGMAP-Studie wurde mit RiskSpectrum /RIS 21/ auf der Grundlage von vorab durchgeführten Fehlermöglichkeits- und -einflussanalysen (FMEAs) erstellt. Wie in Abb. A 1 dargestellt, sind die kleinsten Einheiten, die dabei berücksichtigt wurden, die Erfassungseinheiten (AUs – Acquisition Units), die Verarbeitungseinheiten (PUs – Processing Units), die Bewertungseinheiten (VUs – Voting Units) und die Baugruppenträger (SRs – Subracks) der beiden Teilsysteme RPS-A und RPS-B. Bei den Ausfallarten wurde zwischen selbstmeldenden (SF – Self-signalling Failure) und nicht-selbstmeldenden (NSF – Non-Self-signalling Failure) Ausfällen unterschieden. Diese Vorgehensweise entspricht einer von der GRS entwickelten Methode und ist in /MÜL 18/ beschrieben.

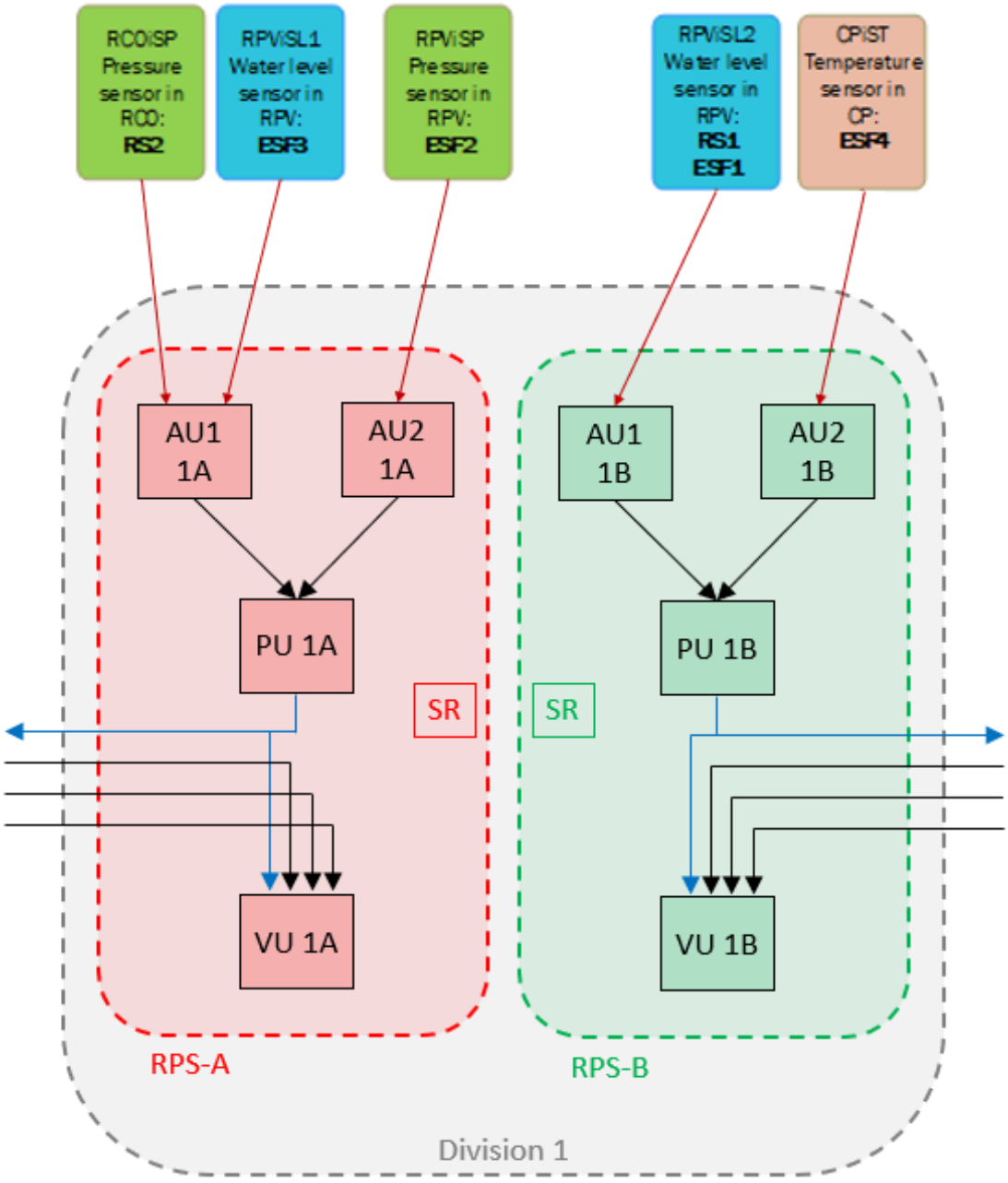

Abb. A.1 Leittechniksystem in der GRS-Modellierung

Hier nur für Scheibe 1 dargestellt, die abgehenden und ankommenden Pfeile rechts und links deuten die Kommunikation mit den anderen Scheiben an.

Für die Umsetzung wurden zunächst für die AUs, PUs, VUs und SRs eigene Fehlerbäume erstellt, um deren Ausfallwahrscheinlichkeiten (für SF und NSF) zu ermitteln. An dieser Stelle wurden bereits die Techniken zur Fehlervermeidung und Fehlererkennung (FTTs – Fault Tolerant Techniques) berücksichtigt, die einen direkten Einfluss auf die Auftretenswahrscheinlichkeit der betrachteten Fehler haben.

Anschließend wurden die Ergebnisse dieser Fehlerbäume verwendet, um die Reaktorschutzsignale (RPS-Signale) in weiteren Fehlerbäumen zu beschreiben, nachdem die relevanten Fehlermodi mit Fehlermöglichkeits- und -einflussanalysen (FMEAs) identifiziert wurden.

A.2.1 Fehlerbäume für die APUs (AUs und PUs), VUs und SRs

Die Fehlerbäume für die einzelnen Einheiten (APU - AU und PU, VU, SR) wurden auf analoge Weise erstellt. Im Folgenden wird stellvertretend die Erstellung der Fehlerbäume für die Bewertungseinheiten (VUs – Voting Units) näher erläutert, für die übrigen Einheiten werden dann nur einige wenige grundlegende Informationen zusätzlich angegeben.

VUs – Voting Units

1AV (Scheibe 1, Teilsystem A, Bewertungseinheit VU) steht stellvertretend für alle VUs im Modellierungsansatz der GRS, d. h., die Ergebnisse für 1AV können direkt auf alle anderen VUs übertragen werden, nämlich: 2AV, 3AV, 4AV, 1BV, 2BV, 3BV, 4BV.

Software-Ausfälle (Betriebs- und Plattformsoftware OP und Anwendungssoftware AS) werden durch Ausfallwahrscheinlichkeiten bei Anforderung (Failure on Demand) beschrieben und werden in der Regel nicht erkannt (siehe Appendix A des DIGMAP-Reports /NEA 21/). Für 1AV können die entsprechenden Basisereignisse daher direkt definiert werden:

- 1AV-DOOP
  - Ausfall der Betriebs- und Plattformsoftware (OP) der digitalen Ausgabebaugruppe (DO) der VU im Teilsystem RPS-A, Scheibe 1
  - RiskSpectrum-Zuverlässigkeitsmodell: Mission Time (24 h)
  - Fehlerrate: $4{,}17 \cdot 10^{-7}$ /h (= $1 \cdot 10^{-5}$ /d)*)

- 1AV-PMOP
  - Ausfall der Betriebs- und Plattformsoftware (OP) der Prozessorbaugruppe (PM) der VU im Teilsystem RPS-A, Scheibe 1
  - RiskSpectrum-Zuverlässigkeitsmodell: Mission Time (24 h)
  - Fehlerrate: $4{,}17 \cdot 10^{-7}$ /h (= $1 \cdot 10^{-5}$ /d)*)
- 1AV-CLOP
  - Ausfall der Betriebs- und Plattformsoftware (OP) der Kommunikationsbaugruppe (CL) der VU im Teilsystem RPS-A, Scheibe 1
  - RiskSpectrum-Zuverlässigkeitsmodell: Einsatzzeit (24 h)
  - Fehlerrate: $4{,}17 \cdot 10^{-7}$ /h (= $1 \cdot 10^{-5}$ /d)*)
- 1AV-PMAS
  - Ausfall der Anwendungssoftware (AS) der Prozessorbaugruppe (PM) der VU im Teilsystem RPS-A, Scheibe 1
  - RiskSpectrum-Zuverlässigkeitsmodell: Mission Time (24 h)
  - Ausfallrate: $4{,}17 \cdot 10^{-6}$ /h (= $1 \cdot 10^{-4}$ /d)*)

*) die konkreten verwendeten Zahlenwerte an dieser Stelle und auch alle weiteren Werte im nachfolgenden Text entstammen der Beschreibung des Referenzfalls der DIGMAP-Studie /NEA 21/.

Hardware(HW)-Ausfälle können nicht durch einzelne Basisereignisse beschrieben werden. Dies liegt an den im Leittechnik-Modell eingesetzten Techniken zur Fehlervermeidung und Fehlererkennung (FTTs). Je nachdem, welche FTT einen Ausfall erkennt, muss z. B. von unterschiedlichen Testintervallen ausgegangen werden (je nachdem, wie viel Zeit zwischen zwei aufeinanderfolgenden Tests vergeht, beispielsweise 24 Stunden zwischen automatischen Tests durch die PTUs oder einem halben Jahr für Full-Scope-Tests).

Betrachtet man z. B. HW-Ausfälle von 1AV-DO, so müssen diese durch zwei unterschiedliche Ereignisse beschrieben werden. Zum einen gibt es 20 % der Ausfälle, die nur durch Full-Scope-Testing (F) erkannt werden können und weitere 80 % der Ausfälle, die sowohl durch Full-Scope-Testing als auch durch periodisches Testen (FP, siehe Appendix A des DIGMAP-Reports /NEA 21/) erkannt werden. Die kombinierte Ausfallwahrscheinlichkeit für beide Arten von Ausfällen beträgt $2 \cdot 10^{-6}$ /h. Welche der beiden Erkennungsoptionen (F oder P für FP) für die Ereignisse zum Tragen kommt, die durch die Vollprüfung (F) oder die periodische Prüfung (P) erkannt werden können, wird dadurch entschieden, ob die entsprechende periodische Prüfeinheit (1PTU) verfügbar ist oder nicht. Für die vollständige Beschreibung von HW-Ausfällen des 1AV-DO sind also drei Basisereignisse erforderlich.

Im Allgemeinen werden die meisten HW-Ausfälle mit dem RiskSpectrum-Zuverlässigkeitsmodell "tested" beschrieben. Diese werden durch eine Ausfallrate, eine Reparaturzeit und ein Testintervall bestimmt. Je nach Verfügbarkeit des FTT müssen für jede Untereinheit mehrere Basisereignisse definiert werden (die sich oft nur durch das Testintervall unterscheiden). Ist das Testintervall extrem klein (z. B. 50 ms beim automatischen Test mit dem Watchdog), wird dies als sofortige Erkennung betrachtet und das Zuverlässigkeitsmodell "repairable" verwendet.

Die Beschreibung von HW-Ausfällen (als Beispiel) für die Prozessorbaugruppe (PM) von 1AV erfordert daher folgende Basisereignisse:

- 1AV-PMHW_F
  - Ausfälle, die nur durch F erkannt werden können
  - Zuverlässigkeitsmodell: „tested" (Testintervall: 6 Monate)
- 1AV-PMHW_FA_A
  - Ausfälle, die von F und A erkannt werden können
  - Erkannt von A (kein Ausfall des Watchdogs)
  - Zuverlässigkeitsmodell: „repairable"

- 1AV-PM_FA_F
  - Ausfälle, die von F und A erkannt werden können
  - Erkannt von F (Ausfall des Watchdogs)
  - Zuverlässigkeitsmodell: „tested" (Testintervall: 6 Monate)
- 1AV-PMHW_FP_P
  - Ausfälle, die von F und P erkannt werden können
  - Erkannt durch P (kein Ausfall von 1PTU)
  - Zuverlässigkeitsmodell: „tested " (Testintervall: 24 Stunden)
- 1AV-PMHW_FP_F
  - Ausfälle, die von F und P erkannt werden können
  - Erkannt durch F (Ausfall von 1PTU)
  - Zuverlässigkeitsmodell: „tested " (Testintervall: 6 Monate)
- 1AV-PMHW_FPA_A
  - Ausfälle, die von F und P und A erkannt werden können
  - Erkannt von A (kein Ausfall des Watchdogs)
  - Zuverlässigkeitsmodell: „repairable "
- 1AV-PMHW_FPA_P
  - Ausfälle, die von F und P und A erkannt werden können
  - Erkannt von P (Ausfall des Watchdogs, aber kein Ausfall von 1PTU)
  - Zuverlässigkeitsmodell: tested" (Testintervall: 24 Stunden)
- 1AV-PMHW_FPA_F
  - Ausfälle, die von F und P und A erkannt werden können
  - Erkannt durch F (Ausfall des Watchdogs und Ausfall von 1PTU)
  - Zuverlässigkeitsmodell: „tested" (Testintervall: 6 Monate)

Um das in /MÜL 18/ beschriebene Verfahren anzuwenden, wurden mit den Basisereignissen zwei verschiedene Fehlerbäume erstellt, die zwischen den beiden möglichen Fehlertypen SF (selbstmeldende Fehler - erkannt durch A) und NSF (nicht-selbstmeldende Fehler - erkannt durch P oder F) unterscheiden.

Abb. A 2 zeigt den Fehlerbaum für NSF von 1AV. Diese VU gilt als ausgefallen (NSF), wenn eine ihrer drei Untereinheiten (1AV-DO, 1AV-PM, 1AV-CL) ausgefallen ist. Die Ursache für den Ausfall jeder Untereinheit kann ihre Hardware (HW), ihr Betriebssystem (OP) oder (falls zutreffend) ihre Anwendungssoftware (AS) sein. Diese Ausfälle werden durch Basisereignisse und zusätzliche Zweige des Fehlerbaums beschrieben, die in Abb. A 3 bis Abb. A 5 dargestellt sind.

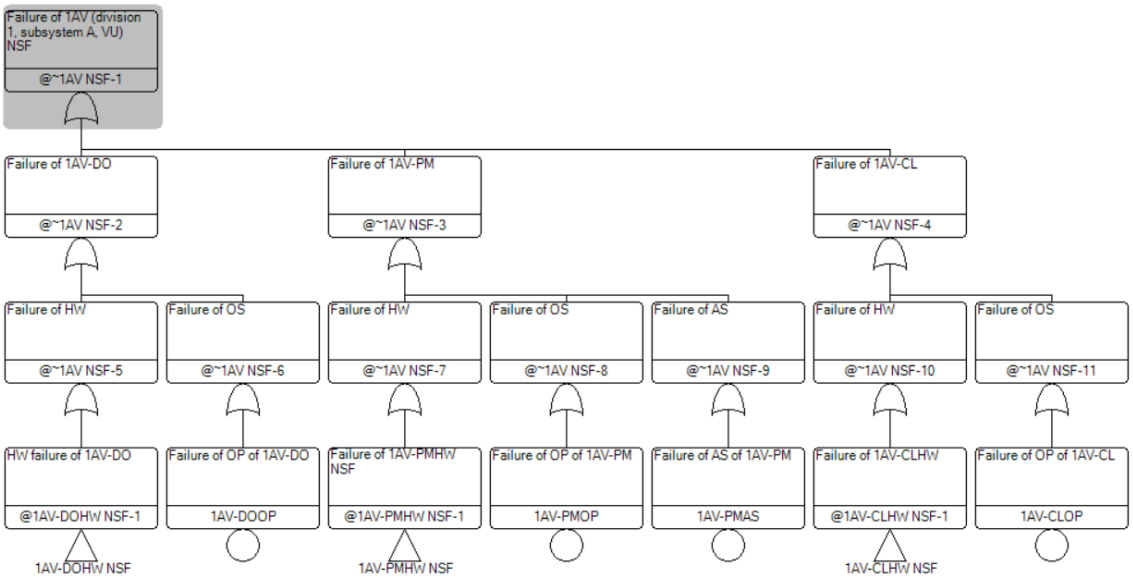

Abb. A.2 Fehlerbaum für NSF von 1AV

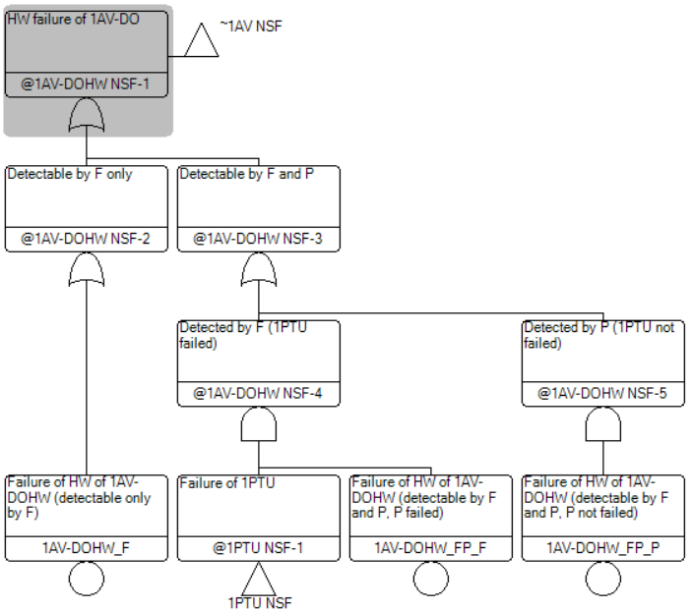

Abb. A.3 Zweig des Fehlerbaums für NSF von 1AV, der NSF von 1AV-DOHW beschreibt

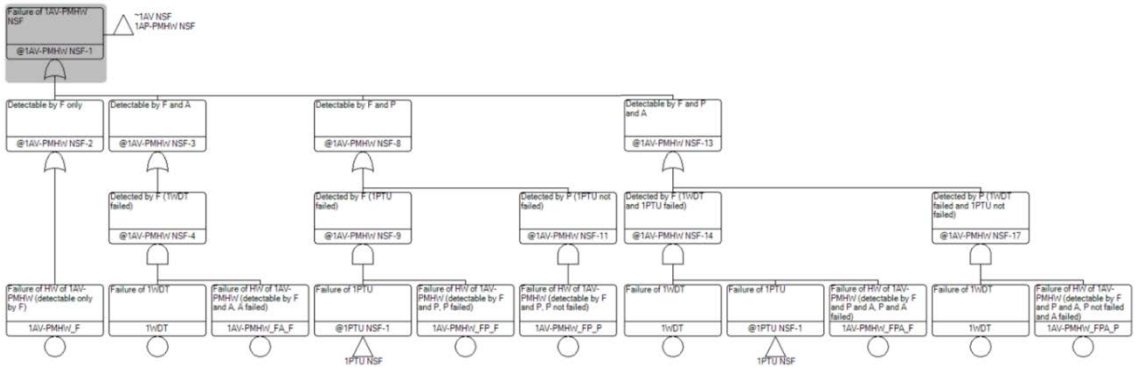

Abb. A.4 Zweig des Fehlerbaums für NSF von 1AV, der NSF von 1AV-PMHW beschreibt

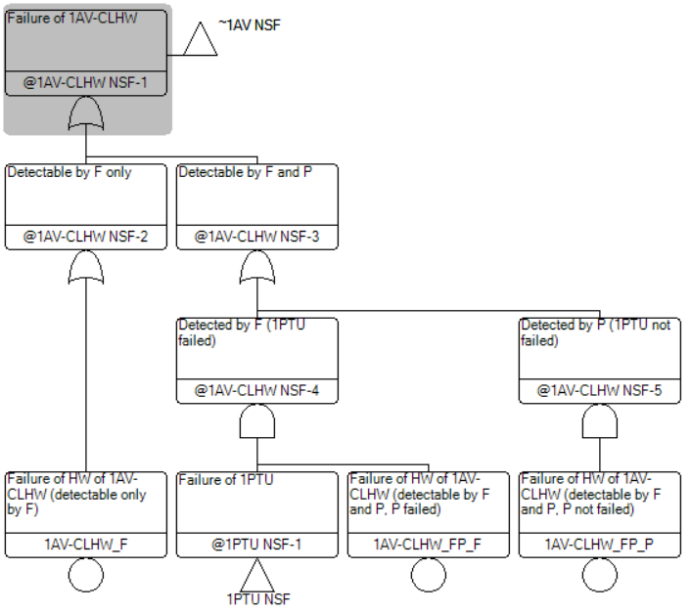

Abb. A.5 Zweig des Fehlerbaums für NSF von 1AV, der NSF von 1AV-CLHW beschreibt

Der Fehlerbaum für SF von 1AV ist in Abb. A 6 dargestellt. SF von 1AV können nur durch Hardware-Fehler von 1AV-PM verursacht werden und diese werden dann durch die FTT A erkannt (siehe zusätzlichen Zweig für diesen Teil des Fehlerbaums in Abb. A 7).

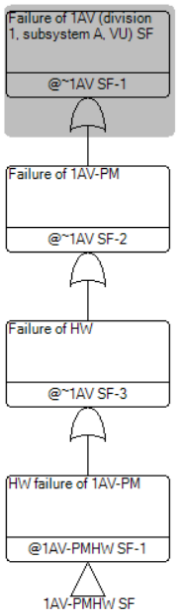

Abb. A.6 Fehlerbaum für SF von 1AV

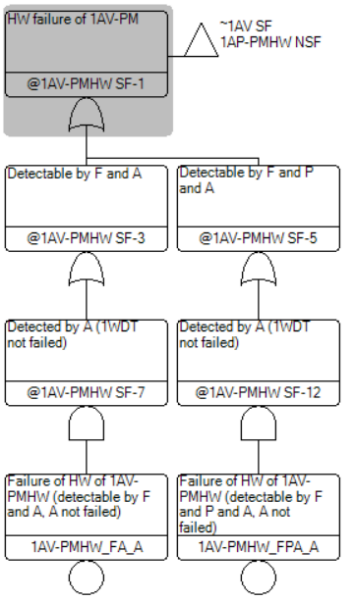

Abb. A.7 Zweig des Fehlerbaums für SF von 1AV-PM

APUs – Acquisition and Processing Units

Bei den APUs ist es etwas komplizierter, da diese jeweils zwei AI-Baugruppen (Analog Input Modules) enthalten. Allerdings wird nur eine davon für die Erzeugung eines einzelnen bestimmten Ansteuersignals verwendet. Daher ist es sinnvoll, die APUs in zwei einzelne AIs und eine PU aufzuteilen (vgl. Abb. A 1). Um in der vorgegebenen Nomenklatur allgemein zu bleiben, bilden die beiden AIs dann jeweils eine eigene AU (z. B. 1AA1 und 1AA2 für die Scheibe 1 des Subsystems A). Als repräsentative AU wurde die 1AA1 (Scheibe 1, Subsystem A, AU1) modelliert, die Ergebnisse wurden anschließend auf alle anderen AUs übertragen. Grundsätzlich ist die Vorgehensweise für AUs analog zu der obigen Beschreibung für die VUs, gleiches gilt auch für die PUs.

Man beachte, dass in einigen Modellen der anderen Teilnehmer der DIGMAP-Studie die beiden AI-Baugruppen jeder Scheibe und jedes Subsystems als eine einzige kombinierte AU behandelt wurden. Aus Gründen der Vergleichbarkeit wurde daher überprüft, ob dies einen signifikanten Einfluss auf die Ergebnisse im GRS-Modell hat oder nicht. Dazu wurden die separaten AUs testweise in einer CCF-Zweiergruppe mit einem Beta-Faktor von 1 kombiniert, dabei wurden aber keine signifikante Auswirkung festgestellt.

SRs – Subracks

Jeder Baugruppenträger (SR – Subrack) stellt die Infrastruktur (u. a. den Rückwandbus) für jeweils ein Subsystem einer Scheibe zur Verfügung. Gemäß Systembeschreibung (siehe Appendix A des DIGMAP-Reports /NEA 21/) werden SRs als reine Hardware betrachtet. Ausfälle von SRs können über die FTTs F, A (über den jeweiligen Watchdog WDT) oder P (über die jeweilig PTU) erkannt werden. Entsprechende Fehlerbäume sind für ein repräsentatives SR erstellt worden.

Zwischenergebnisse

Als erstes Zwischenergebnis wurden mit den zuvor beschriebenen Fehlerbäumen für die Einheiten (AU1s, AU2s, PUs, VUs und SRs) die nachfolgenden Wahrscheinlichkeiten für Ausfälle bei Anforderung bestimmt (Tab. A 1).

Tab. A.1 Ausfallwahrscheinlichkeiten bei Anforderung für jeden Typ von Einheit (AU1, AU2, PU, VU, SR) und Ausfallart (SF, NSF)

Einheit	Wahrscheinlichkeit
AU1 xy NSF	$9{,}03 \cdot 10^{-4}$
AU1 xy SF	$9{,}60 \cdot 10^{-6}$
AU2 xy NSF	$9{,}03 \cdot 10^{-4}$
AU2 xy SF	$9{,}60 \cdot 10^{-6}$
PU xy NSF	$2{,}90 \cdot 10^{-3}$
PU xy SF	$1{,}28 \cdot 10^{-5}$
SR xy NSF	$8{,}92 \cdot 10^{-6}$
SR xy SF	$1{,}44 \cdot 10^{-5}$
VU xy NSF	$3{,}84 \cdot 10^{-3}$
VU xy SF	$1{,}28 \cdot 10^{-5}$
x = 1, 2, 3, 4 (Scheibe) y = A, B (Subsystem) SF – selbstmeldender Ausfall NSF – nicht-selbstmeldender Ausfall	

A.2.2 Fehlermöglichkeits- und -einflussanalysen

Für die Erstellung der Fehlerbäume für das Gesamtsystem (siehe Abb. A 1) wurden die relevanten Ausfallarten mit Hilfe von modellbasierten Fehlermöglichkeits- und -einflussanalysen (FMEAs) ermittelt. Dabei wurden auch gleich die Änderungen der Wertungslogiken der VUs berücksichtigt (siehe hierzu FMEA-Tabelle für die APUs in Abschnitt A.3 in diesem Anhang).

Weitere Details zu diesem Verfahren können in /MÜL 18/ nachgelesen werden. Die vollständigen FMEA-Tabellen sind in Abschnitt A.3 zu finden.

A.2.3 Fehlerbäume für die Auslösesignale

Für das Reaktorschutzsystem des in der DIGMAP-Studie betrachteten Referenzfalls (siehe Abschnitt 3.1.1) wurde eine Reihe von Maßnahmen definiert, die durch unterschiedliche Auslösesignale angesprochen werden können (jeweils eine ODER-Verknüpfung von ein, zwei oder drei funktional diversen Auslösesignalen für eine Maßnahme). Details hierzu können im gemeinsamen DIGMAP-Report /NEA 21/ nachgelesen werden.

Dort findet man darüber hinaus auch den Ereignisbaum (Event Tree), der das im Referenzfall betrachtete Ereignis (Verlust der Hauptspeisewasserversorgung, LMFW – Loss of Main FeedWater) beschreibt.

Die Fehlerbäume für die einzelnen Auslösesignale sind grundsätzlich sehr ähnlich aufgebaut. Stellvertretend soll daher im Folgenden der Fehlerbaum für das Signal RS1 beschrieben werden.

Anm.: RS1 (erzeugt durch Subsystem RPS-B) und das funktional diversitär erzeugte Signal RS2 (erzeugt durch Subsystem RPS-A) bilden zusammen das Signal RS (ODER-Verknüpfung). RS (RS1 oder RS2) löst als Maßnahme eine Reaktorschnellabschaltung aus.

Ursachen für einen Ausfall bei Anforderung (FoD – Failure on Demand) von RS1 können Ausfälle der Baugruppenträger (SRs), der Wertungseinheiten (VUs) oder der Erfassungs- und Verarbeitungseinheiten (APUs) des Subsystem RPS-B sein (Abb. A 8).

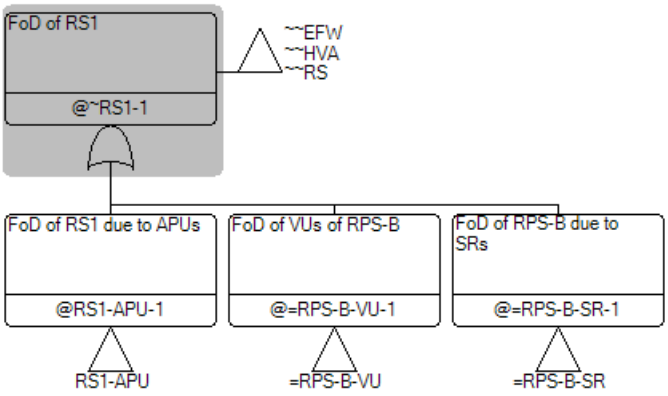

Abb. A.8 Ausfall bei Anforderung (FoD – Failure on Demand) für das Reaktorschutzsignal RS1

Stellvertretend ist in Abb. A 9 der Fehlerbaum für den Ausfall der VUs von RPS-B dargestellt (Zweig des Fehlerbaums in Abb. A 8).

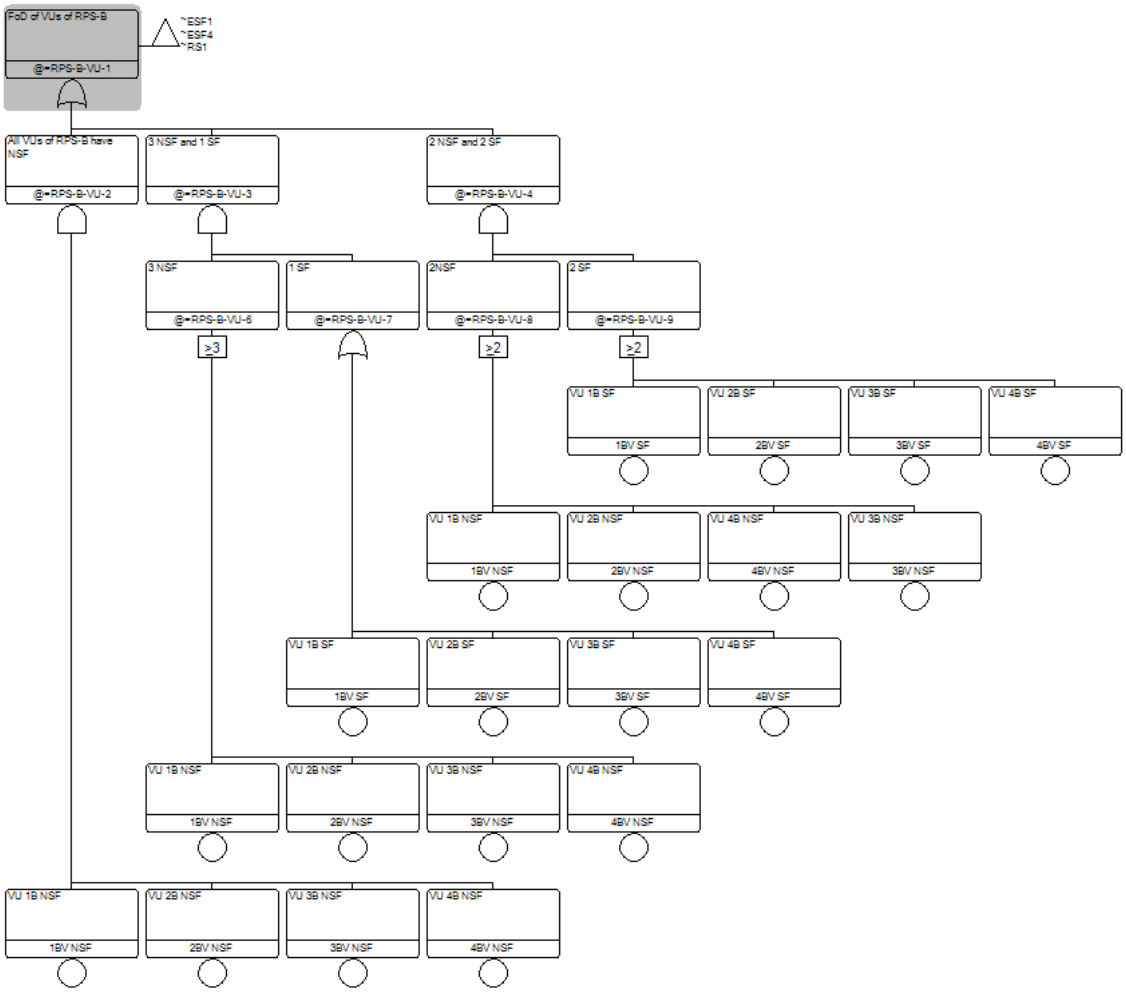

Abb. A.9 Ausfall bei Anforderung (FoD – Failure on Demand) von VUs des Subsystems RPS-B im GRS-Modell

Die unterschiedlichen Ausfallkombinationen in diesem Zweig des Fehlerbaums wurden durch eine FMEA bestimmt (siehe Abschnitt A.3.2).

Anm.: Die Umsetzung in diesem Fehlerbaum stellt eine Vereinfachung dar. Z. B. wird ein gleichzeitiger nicht-selbstmeldender Ausfall (NSF) von VU 1B (VU von Subsystem B in Scheibe 1) und VU 2B (VU von Subsystem B in Scheibe 2) zusammen mit gleichzeitigen selbstmeldenden Ausfällen (SF) von VU 1B und VU 2B insgesamt als 2 NSF und 2 SF gewertet, was nicht der tatsächlichen Intention entspricht (NSFs in zwei VUs und SFs in den anderen beiden VUs). Der Einfluss dieser (konservativen) Vereinfachung ist jedoch nicht signifikant, wie ein alternativ erzeugter Fehlerbaum zeigte (nicht dargestellt), der nur die wirklich relevanten Kombinationen enthielt.

Für alle Auslösesignale wurden Fehlerbäume in der oben beschriebenen Weise erstellt. Die mit diesen Fehlerbäumen erzielten Ergebnisse werden im folgenden Abschnitt (A.2) näher beschrieben.

A.3 Individuelle Ergebnisse des GRS-Modells

Die Fehlerbäume für die Frontline-System (verfahrenstechnische Systeme des Referenzfalls) wurden von EDF erstellt und von allen DIGMAP-Teilnehmern gleichermaßen verwendet, die eigene PSA-Modelle erstellt haben. Dies hat den Vorteil, dass das Verhalten der Frontline-Systeme in allen individuellen PSA-Modellen der DIGMAP-Teilnehmer identisch war und nicht zu vermeidbaren zusätzlichen Unterschieden in den Ergebnissen geführt hat (da diese nicht im Fokus der DIGMAP-Studie waren).

Im von EDF gelieferten Modell für die Frontline-Systeme waren „Dummy"-Basisereignisse für die Auslösesignale vorhanden, welche durch die im vorherigen Abschnitt beschriebenen Fehlerbäume ersetzt wurden.

Der Vergleich der ersten PSA-Modelle der sechs teilnehmenden Organisationen, die jeweils eigene Modelle erstellt haben, hat gezeigt, dass die Auffassung zum Diversitätsgrad zwischen den Subsystemen RPS-A und RPS-B in den unterschiedlichen Modellen verschieden war. In einigen Modellen waren die Subsysteme als vollständig diversitär angenommen worden, während in den anderen Modellen lediglich von einer funktionalen Diversität ausgegangen worden war (also Unterschiede hauptsächlich in der jeweiligen Anwendungssoftware (AS) angenommen wurden).

Aus diesem Grund wurden zwei unterschiedliche Testfälle („volle Diversität" und „funktionale Diversität") definiert, welche beide anschließend von allen sechs Organisationen modelliert wurden. An dieser Stelle werden nur die Ergebnisse des (relevanteren) Testfalls „volle Diversität" für das GRS-Modell wiedergegeben. Die vollständigen Ergebnisse des anderen Testfalls für das GRS-Modell können im Appendix B2 des DIGMAP-Reports /NEA 21/ nachgelesen werden.

Nimmt man an, dass keine vollständige Unabhängigkeit zwischen den Subsystemen RPS-A und RPS-B besteht, so können die CCF-Gruppen wie folgt definiert werden:

- XYA1 NSF
  - CCF von xyA1 NSF (x=1, 2, 3, 4; y=A, B)
  - alle AU1s von RPS-A und RPS-B
- XYA1 SF
  - CCF von xyA1 SF (x=1, 2, 3, 4, y=A, B)
  - alle AU1s von RPS-A und RPS-B
- XYA2 NSF
  - CCF von xyA2 NSF (x=1, 2, 3, 4, y=A, B)
  - alle AU2s von RPS-A und RPS-B
- XYA2 SF
  - CCF von xyA2 SF (x=1, 2, 3, 4, y=A, B)
  - alle AU2s von RPS-A und RPS-B
- XYP NSF
  - CCF von xyP NSF (x=1, 2, 3, 4, y=A, B)
  - alle PUs von RPS-A und RPS-B
- XYP SF
  - CCF von xyP SF (x=1, 2, 3, 4, y=A, B)
  - alle PUs von RPS-A und RPS-B
- XYS NSF
  - CCF von xyS SF (x=1, 2, 3, 4, y=A, B)
  - alle SRs von RPS-A und RPS-B
- XYS SF
  - CCF von xyS SF (x=1, 2, 3, 4, y=A, B)
  - alle SRs von RPS-A und RPS-B

- XYV NSF
  - CCF von xyV NSF (x=1, 2, 3, 4, y=A, B)
  - alle VUs von RPS-A und RPS-B
- XYV SF
  - CCF von xyV NSF (x=1, 2, 3, 4, y=A, B)
  - alle VUs von RPS-A und RPS-B
- XCPIST
  - CCF von xCPiST (x=1, 2, 3, 4)
  - alle CPiST-Sensoren
  - Details zu den Sensoren: siehe /NEA 21/
- XRCOISP
  - CCF von xRCOiSP (x=1, 2, 3, 4)
  - alle RCOiSP-Sensoren
  - Details zu den Sensoren: siehe /NEA 21/
- XRPVISL1
  - CCF von xRPViSL1 (x=1, 2, 3, 4)
  - alle RPViSL1-Sensoren
  - Details zu den Sensoren: siehe /NEA 21/
- XRPVISL2
  - CCF von XRPViSL2 (x=1, 2, 3, 4)
  - alle RPViSL2-Sensoren
  - Details zu den Sensoren: siehe /NEA 21/
- XRPVISP
  - CCF von xRPViSP (x=1, 2, 3, 4)
  - alle RPViSP-Sensoren
  - Details zu den Sensoren: siehe /NEA 21/

Für die Sensoren wurden jeweils das RiskSpectrum-Modell „Alpha-4-Factor“ gewählt (mit Alpha-Faktoren entsprechend der dritten Zeile in Appendix 1 der Systembeschreibung in Appendix A von /NEA 21/ (CCG # 4; Failed # 2, 3, 4). Alle anderen CCFs wurden mit dem RiskSpectrum-Modell „Beta-Factor“ modelliert. Als Beta-Faktor wurde der in Appendix 1 der Systembeschreibung in Appendix A angegebene Alpha-Wert für zwei Ausfälle einer CCF-Gruppe von 8 gewählt (CCG # 8, Failed # 2).

Die Analyse der Ergebnisse, insbesondere der Vergleich zwischen den verschiedenen Testfällen und Modellen, wird im DIGMAP-Report /NEA 21/ durchgeführt. An dieser Stelle werden daher nur unkommentiert die Ergebnisse für die Kernschadenshäufigkeit für den Testfall „volle Diversität“ in Form der ersten 100 Minimalschnitte wiedergegeben.

Tab. A.2 Ergebnisse zu Kernschadenshäufigkeit für Testfall „volle Diversität“

Die ersten 100 Minimalschnitte für das auslösende Ereignis LMFW (Loss of Main FeedWater) im Testfall „volle Diversität“ (die Kernschadenshäufigkeit (CDF - Core Damage Frequency) für diesen Fall beträgt $6{,}68 \cdot 10^{-5}$ /Jahr).

Nr.	Beitrag zur CDF [1/Jahr]	Ereignis 1	Ereignis 2	Ereignis 3
1	2,40E-05	LMFW	RHR_MP_FR	
2	2,40E-05	LMFW	SWS_MP_FR	
3	8,06E-06	LMFW	XYV NSF-ALL	
4	6,09E-06	LMFW	XYP NSF-ALL	
5	1,90E-06	LMFW	XYA1 NSF-ALL	
6	1,20E-06	LMFW	RHR_HX_FR	
7	5,00E-07	LMFW	RHR_MP_FS	
8	5,00E-07	LMFW	RHR_MV_FO	
9	5,00E-07	LMFW	SWS_MP_FS	
10	5,00E-08	LMFW	RHR_CV_FO	
11	1,87E-08	LMFW	XYS NSF-ALL	
12	1,15E-08	LMFW	ECC_MP_FR	EFW_MP_FR
13	1,15E-08	LMFW	CCW_MP_FR	EFW_MP_FR
14	5,00E-09	LMFW	CPO_TK_FS	
15	1,15E-09	LMFW	ECC_MP_FR	HVA_AC_FR
16	1,15E-09	LMFW	CCW_MP_FR	HVA_AC_FR
17	9,10E-10	LMFW	EFW_MP_FR	XYA2 NSF-ALL
18	5,76E-10	LMFW	CCW_HX1_FR	EFW_MP_FR
19	5,76E-10	LMFW	CCW_HX2_FR	EFW_MP_FR
20	4,80E-10	LMFW	ADS_MV_FO	EFW_MP_FR
21	2,40E-10	LMFW	ECC_MP_FR	EFW_MP_FS
22	2,40E-10	LMFW	CCW_MP_FR	EFW_MP_FS
23	2,40E-10	LMFW	ECC_MP_FR	EFW_MV_FO
24	2,40E-10	LMFW	CCW_MP_FR	EFW_MV_FO
25	2,40E-10	LMFW	ECC_MV_FO	EFW_MP_FR
26	2,40E-10	LMFW	CCW_MP_FS	EFW_MP_FR
27	2,40E-10	LMFW	ECC_MP_FS	EFW_MP_FR
28	1,07E-10	LMFW	ECC_MP_FR	XRPVISL2-3AB
29	1,07E-10	LMFW	ECC_MP_FR	XRPVISL2-3AC
30	1,07E-10	LMFW	CCW_MP_FR	XRPVISL2-3AB
31	1,07E-10	LMFW	EFW_MP_FR	XRPVISL1-3AC
32	1,07E-10	LMFW	CCW_MP_FR	XRPVISL2-3AD
33	1,07E-10	LMFW	ECC_MP_FR	XRPVISL2-3AA

Nr.	Beitrag zur CDF [1/Jahr]	Ereignis 1	Ereignis 2	Ereignis 3
34	1,07E-10	LMFW	EFW_MP_FR	XRPVISL1-3AA
35	1,07E-10	LMFW	EFW_MP_FR	XRPVISP-3AC
36	1,07E-10	LMFW	CCW_MP_FR	XRPVISL2-3AA
37	1,07E-10	LMFW	EFW_MP_FR	XRPVISP-3AA
38	1,07E-10	LMFW	EFW_MP_FR	XRPVISL1-3AB
39	1,07E-10	LMFW	EFW_MP_FR	XRPVISL1-3AD
40	1,07E-10	LMFW	CCW_MP_FR	XRPVISL2-3AC
41	1,07E-10	LMFW	ECC_MP_FR	XRPVISL2-3AD
42	1,07E-10	LMFW	EFW_MP_FR	XRPVISP-3AB
43	1,07E-10	LMFW	EFW_MP_FR	XRPVISP-3AD
45	9,88E-11	LMFW	ECC_MP_FR	XRPVISL2-ALL
46	9,88E-11	LMFW	EFW_MP_FR	XRPVISL1-ALL
47	9,88E-11	LMFW	CCW_MP_FR	XRPVISL2-ALL
48	9,10E-11	LMFW	HVA_AC_FR	XYA2 NSF-ALL
49	5,76E-11	LMFW	CCW_HX2_FR	HVA_AC_FR
50	5,76E-11	LMFW	CCW_HX1_FR	HVA_AC_FR
51	4,80E-11	LMFW	ADS_MV_FO	HVA_AC_FR
52	2,40E-11	LMFW	CCW_MP_FS	HVA_AC_FR
53	2,40E-11	LMFW	ECC_MP_FS	HVA_AC_FR
54	2,40E-11	LMFW	ECC_MV_FO	HVA_AC_FR
55	2,40E-11	LMFW	CCW_MP_FR	EFW_DWST_FS
56	2,40E-11	LMFW	ECC_MP_FR	HVA_AC_FS
57	2,40E-11	LMFW	CCW_MP_FR	HVA_AC_FS
58	2,40E-11	LMFW	CCW_MP_FR	EFW_CV_FO
59	2,40E-11	LMFW	ECC_MP_FR	EFW_CV_FO
60	2,40E-11	LMFW	ECC_MP_FR	EFW_DWST_FS
61	2,40E-11	LMFW	ECC_CV_FO	EFW_MP_FR
62	1,90E-11	LMFW	EFW_MV_FO	XYA2 NSF-ALL
63	1,90E-11	LMFW	EFW_MP_FS	XYA2 NSF-ALL
64	1,20E-11	LMFW	CCW_HX1_FR	EFW_MP_FS
65	1,20E-11	LMFW	CCW_HX2_FR	EFW_MV_FO
66	1,20E-11	LMFW	CCW_HX2_FR	EFW_MP_FS
67	1,20E-11	LMFW	CCW_HX1_FR	EFW_MV_FO
68	1,07E-11	LMFW	HVA_AC_FR	XRPVISL1-3AC
69	1,07E-11	LMFW	HVA_AC_FR	XRPVISL1-3AD
70	1,07E-11	LMFW	HVA_AC_FR	XRPVISP-3AA
71	1,07E-11	LMFW	HVA_AC_FR	XRPVISL1-3AB

Nr.	Beitrag zur CDF [1/Jahr]	Ereignis 1	Ereignis 2	Ereignis 3
72	1,07E-11	LMFW	HVA_AC_FR	XRPVISP-3AC
73	1,07E-11	LMFW	HVA_AC_FR	XRPVISP-3AB
74	1,07E-11	LMFW	HVA_AC_FR	XRPVISL1-3AA
75	1,07E-11	LMFW	HVA_AC_FR	XRPVISP-3AD
76	1,00E-11	LMFW	ADS_MV_FO	EFW_MV_FO
77	1,00E-11	LMFW	ADS_MV_FO	EFW_MP_FS
78	9,89E-12	LMFW	HVA_AC_FR	XRPVISP-ALL
79	9,89E-12	LMFW	HVA_AC_FR	XRPVISL1-ALL
80	8,44E-12	LMFW	XRCOISP-3AC	XYA2 NSF-ALL
81	8,44E-12	LMFW	XRPVISL2-3AB	XYA2 NSF-ALL
82	8,44E-12	LMFW	XRCOISP-3AB	XYA2 NSF-ALL
83	8,44E-12	LMFW	XRCOISP-3AD	XYA2 NSF-ALL
84	8,44E-12	LMFW	XRPVISL2-3AC	XYA2 NSF-ALL
85	8,44E-12	LMFW	XRPVISL2-3AD	XYA2 NSF-ALL
86	8,44E-12	LMFW	XRCOISP-3AA	XYA2 NSF-ALL
87	8,44E-12	LMFW	XRPVISL2-3AA	XYA2 NSF-ALL
88	7,81E-12	LMFW	XRPVISL2-ALL	XYA2 NSF-ALL
89	7,81E-12	LMFW	XRCOISP-ALL	XYA2 NSF-ALL
90	5,34E-12	LMFW	CCW_HX1_FR	XRPVISL2-3AA
91	5,34E-12	LMFW	CCW_HX2_FR	XRPVISL2-3AC
92	5,34E-12	LMFW	CCW_HX1_FR	XRPVISL2-3AC
93	5,34E-12	LMFW	CCW_HX2_FR	XRPVISL2-3AA
94	5,34E-12	LMFW	CCW_HX1_FR	XRPVISL2-3AB
95	5,34E-12	LMFW	CCW_HX2_FR	XRPVISL2-3AD
96	5,34E-12	LMFW	CCW_HX2_FR	XRPVISL2-3AB
97	5,34E-12	LMFW	CCW_HX1_FR	XRPVISL2-3AD
98	5,00E-12	LMFW	ECC_MP_FS	EFW_MP_FS
99	5,00E-1	LMFW	ECC_MV_FO	EFW_MV_FO
100	5,00E-12	LMFW	CCW_MP_FS	EFW_MP_FS

Legende:

ADS_…	Ausfälle im Automatic Depressurization System (Frontline-Systeme)
CCW_…	*Ausfälle im Component Cooling Water System (Frontline-Systeme)*
ECC_…	Ausfälle im Emergency Core Cooling System (Frontline-Systeme)
EFW_…	Ausfälle im Emergency Feedwater System (Frontline-Systeme)
SWS_…	Ausfälle im Service Water System (Frontline-Systeme)
HVA_…	Ausfälle im Heating, Vent. and Air Cond. System (Frontline-Systeme)
RHR_…	Ausfälle im Residual Heat Removal System (Frontline-Systeme)
XRP…_ …	Sensorausfälle
XYA1/XYA2_ …	Ausfälle von AU1s/AU2s (RPS)
XYP_ …	Ausfälle von PUs (RPS)
XYV_ …	Ausfälle von VUs (RPS)
XYS_ …	Ausfälle von SRs (RPS)

Suffixe:

… -ALL	CCF aller entspr. Komponenten (Beta- oder Alpha-Faktor-Modell)
…-3…	CCF von 3 Komponenten einer 4er-Gruppe (Alpha-Faktor-Modell)
	Die angehängten Buchstaben hinter diesem Suffix stammen von RiskSpectrum und beschreiben die beteiligten Komponenten. (Details können der Online-Hilfe von RiskSpectrum entnommen werden)

A.4 FMEA-Tabellen zum GRS-Modell

Dieser Abschnitt enthält die unkommentierten FMEA-Tabellen des GRS-Modells. Genauere Details zu deren Interpretation findet man in /MÜL 18/.

A.4.1 Subracks (SRs)

1yS (y = A, B)	2yS (y = A, B)	3yS (y = A, B)	4yS (y = A, B)	RPS-Signal (1oo4)	FT	Remarks
Quality	Quality	Quality	Quality			
0 Failures						
OK	OK	OK	OK	yes		
1 Failure						
SF	OK	OK	OK	yes		
OK	SF	OK	OK	yes		
OK	OK	SF	OK	yes		
OK	OK	OK	SF	yes		
NSF	OK	OK	OK	yes		
OK	NSF	OK	OK	yes		
OK	OK	NSF	OK	yes		
OK	OK	OK	NSF	yes		
2 Failures						
SF	SF	OK	OK	yes		
SF	OK	SF	OK	yes		
SF	OK	OK	SF	yes		
OK	SF	SF	OK	yes		
OK	SF	OK	SF	yes		
OK	OK	SF	SF	yes		
NSF	NSF	OK	OK	yes		
NSF	OK	NSF	OK	yes		
NSF	OK	OK	NSF	yes		
OK	NSF	NSF	OK	yes		
OK	NSF	OK	NSF	yes		
OK	OK	NSF	NSF	yes		
SF	NSF	OK	OK	yes		
NSF	SF	OK	OK	yes		
SF	OK	NSF	OK	yes		
NSF	OK	SF	OK	yes		
SF	OK	OK	NSF	yes		
NSF	OK	OK	SF	yes		
OK	SF	NSF	OK	yes		
OK	NSF	SF	OK	yes		
OK	SF	OK	NSF	yes		

1yS (y = A, B)	2yS (y = A, B)	3yS (y = A, B)	4yS (y = A, B)	RPS-Signal (1oo4)	FT	Remarks
Quality	Quality	Quality	Quality			
OK	NSF	OK	SF	yes		
OK	OK	SF	NSF	yes		
OK	OK	NSF	SF	yes		
3 Failures						
SF	SF	SF	OK	yes		safe shutdown
SF	SF	OK	SF	yes		safe shutdown
SF	OK	SF	SF	yes		safe shutdown
OK	SF	SF	SF	yes		safe shutdown
NSF	NSF	NSF	OK	yes		
NSF	NSF	OK	NSF	yes		
NSF	OK	NSF	NSF	yes		
OK	NSF	NSF	NSF	yes		
NSF	NSF	SF	OK	yes		
NSF	NSF	OK	SF	yes		
NSF	SF	NSF	OK	yes		
NSF	OK	NSF	SF	yes		
NSF	SF	OK	NSF	yes		
NSF	OK	SF	NSF	yes		
SF	NSF	NSF	OK	yes		
OK	NSF	NSF	SF	yes		
SF	NSF	OK	NSF	yes		
OK	NSF	SF	NSF	yes		
SF	OK	NSF	NSF	yes		
OK	SF	NSF	NSF	yes		
SF	SF	NSF	1	yes		
SF	SF	1	NSF	yes		
SF	NSF	SF	1	yes		
SF	1	SF	NSF	yes		
SF	NSF	1	SF	yes		
SF	1	NSF	SF	yes		
NSF	SF	SF	1	yes		
1	SF	SF	NSF	yes		
NSF	SF	1	SF	yes		
1	SF	NSF	SF	yes		
NSF	1	SF	SF	yes		
1	NSF	SF	SF	yes		
4 Failures						
NSF	NSF	NSF	NSF	no	4 NSF	4 NSF
NSF	NSF	NSF	SF	no	3 NSF and 1 SF	3 NSF and 1 SF
NSF	NSF	SF	NSF	no	3 NSF and 1 SF	
NSF	SF	NSF	NSF	no	3 NSF and 1 SF	

1yS (y = A, B)	2yS (y = A, B)	3yS (y = A, B)	4yS (y = A, B)	RPS-Signal (1oo4)	FT	Remarks
Quality	Quality	Quality	Quality			
SF	NSF	NSF	NSF	no	3 NSF and 1 SF	
NSF	NSF	SF	SF	no	2 NSF and 2 SF	2 NSF and 2 SF
NSF	SF	NSF	SF	no	2 NSF and 2 SF	
NSF	SF	SF	NSF	no	2 NSF and 2 SF	
SF	NSF	NSF	SF	no	2 NSF and 2 SF	
SF	NSF	SF	NSF	no	2 NSF and 2 SF	
SF	SF	NSF	NSF	no	2 NSF and 2 SF	
NSF	SF	SF	SF	~	1 NSF and 3 SF	safe shutdown
SF	NSF	SF	SF	~	1 NSF and 3 SF	
SF	SF	NSF	SF	~	1 NSF and 3 SF	
SF	SF	SF	NSF	~	1 NSF and 3 SF	
SF	SF	SF	SF	~	4 SF	safe shutdown

A.4.2 Voting Units (VUs)

1yV (y = A, B)	2yV (y = A, B)	3yV (y = A, B)	4yV (y = A, B)	RPS-Signal (1oo4)	FT	Remarks
Quality	Quality	Quality	Quality			
0 Failures						
OK	OK	OK	OK	yes		
1 Failure						
SF	OK	OK	OK	yes		
OK	SF	OK	OK	yes		
OK	OK	SF	OK	yes		
OK	OK	OK	SF	yes		
NSF	OK	OK	OK	yes		
OK	NSF	OK	OK	yes		
OK	OK	NSF	OK	yes		
OK	OK	OK	NSF	yes		
2 Failures						
SF	SF	OK	OK	yes		
SF	OK	SF	OK	yes		
SF	OK	OK	SF	yes		
OK	SF	SF	OK	yes		
OK	SF	OK	SF	yes		
OK	OK	SF	SF	yes		
NSF	NSF	OK	OK	yes		
NSF	OK	NSF	OK	yes		
NSF	OK	OK	NSF	yes		

1yV (y = A, B)	2yV (y = A, B)	3yV (y = A, B)	4yV (y = A, B)	RPS-Signal (1oo4)	FT	Remarks
Quality	Quality	Quality	Quality			
OK	NSF	NSF	OK	yes		
OK	NSF	OK	NSF	yes		
OK	OK	NSF	NSF	yes		
SF	NSF	OK	OK	yes		
NSF	SF	OK	OK	yes		
SF	OK	NSF	OK	yes		
NSF	OK	SF	OK	yes		
SF	OK	OK	NSF	yes		
NSF	OK	OK	SF	yes		
OK	SF	NSF	OK	yes		
OK	NSF	SF	OK	yes		
OK	SF	OK	NSF	yes		
OK	NSF	OK	SF	yes		
OK	OK	SF	NSF	yes		
OK	OK	NSF	SF	yes		
3 Failures						
SF	SF	SF	OK	yes		safe shutdown
SF	SF	OK	SF	yes		safe shutdown
SF	OK	SF	SF	yes		safe shutdown
OK	SF	SF	SF	yes		safe shutdown
NSF	NSF	NSF	OK	yes		
NSF	NSF	OK	NSF	yes		
NSF	OK	NSF	NSF	yes		
OK	NSF	NSF	NSF	yes		
NSF	NSF	SF	OK	yes		
NSF	NSF	OK	SF	yes		
NSF	SF	NSF	OK	yes		
NSF	OK	NSF	SF	yes		
NSF	SF	OK	NSF	yes		
NSF	OK	SF	NSF	yes		
SF	NSF	NSF	OK	yes		
OK	NSF	NSF	SF	yes		
SF	NSF	OK	NSF	yes		
OK	NSF	SF	NSF	yes		
SF	OK	NSF	NSF	yes		
OK	SF	NSF	NSF	yes		
SF	SF	NSF	1	yes		
SF	SF	1	NSF	yes		
SF	NSF	SF	1	yes		
SF	1	SF	NSF	yes		
SF	NSF	1	SF	yes		

1yV (y = A, B)	2yV (y = A, B)	3yV (y = A, B)	4yV (y = A, B)	RPS-Signal (1oo4)	FT	Remarks
Quality	Quality	Quality	Quality			
SF	1	NSF	SF	yes		
NSF	SF	SF	1	yes		
1	SF	SF	NSF	yes		
NSF	SF	1	SF	yes		
1	SF	NSF	SF	yes		
NSF	1	SF	SF	yes		
1	NSF	SF	SF	yes		
4 Failures						
NSF	NSF	NSF	NSF	no	4 NSF	4 NSF
NSF	NSF	NSF	SF	no	3 NSF and 1 SF	3 NSF and 1 SF
NSF	NSF	SF	NSF	no	3 NSF and 1 SF	
NSF	SF	NSF	NSF	no	3 NSF and 1 SF	
SF	NSF	NSF	NSF	no	3 NSF and 1 SF	
NSF	NSF	SF	SF	no	2 NSF and 2 SF	2 NSF and 2 SF
NSF	SF	NSF	SF	no	2 NSF and 2 SF	
NSF	SF	SF	NSF	no	2 NSF and 2 SF	
SF	NSF	NSF	SF	no	2 NSF and 2 SF	
SF	NSF	SF	NSF	no	2 NSF and 2 SF	
SF	SF	NSF	NSF	no	2 NSF and 2 SF	
NSF	SF	SF	SF	~	1 NSF and 3 SF	safe shutdown
SF	NSF	SF	SF	~	1 NSF and 3 SF	
SF	SF	NSF	SF	~	1 NSF and 3 SF	
SF	SF	SF	NSF	~	1 NSF and 3 SF	
SF	SF	SF	SF	~	4 SF	safe shutdown

A.4.4 Acquisition and Processing Units (APUs)

1yz (y = A, B) (z = A, P)		2yz (y = A, B) (z = A, P)		3yz (y = A, B) (z = A, P)		4yz (y = A, B) (z = A, P)		xAV (x = 1, 2, 3, 4)			FT	Remarks
Output	Er	Output	Er	Output	Er	Output	Er	Valid Input Signals (Er 0)	Voting Type	Output		
0 Failures												
1	0	1	0	1	0	1	0	1; 1; 1; 1	2oo4	1		
1 Failure												
~	1	1	0	1	0	1	0	1; 1; 1	2oo3	1		
1	0	~	1	1	0	1	0	1; 1; 1	2oo3	1		
1	0	1	0	~	1	1	0	1; 1; 1	2oo3	1		
1	0	1	0	1	0	~	1	1; 1; 1	2oo3	1		
0	0	1	0	1	0	1	0	0; 1; 1; 1	2oo4	1		
1	0	0	0	1	0	1	0	1; 0; 1; 1	2oo4	1		
1	0	1	0	0	0	1	0	1; 1; 0; 1	2oo4	1		
1	0	1	0	1	0	0	0	1; 1; 1; 0	2oo4	1		
2 Failures												
~	1	~	1	1	0	1	0	1; 1	1oo2	1		
~	1	1	0	~	1	1	0	1; 1	1oo2	1		
~	1	1	0	1	0	~	1	1; 1	1oo2	1		
1	0	~	1	~	1	1	0	1; 1	1oo2	1		
1	0	~	1	1	0	~	1	1; 1	1oo2	1		
1	0	1	0	~	1	~	1	1; 1	1oo2	1		
0	0	0	0	1	0	1	0	0; 0; 1; 1	2oo4	1		
0	0	1	0	0	0	1	0	0; 1; 0; 1	2oo4	1		
0	0	1	0	1	0	0	0	0; 1; 1; 0	2oo4	1		
1	0	0	0	0	0	1	0	1; 0; 0; 1	2oo4	1		
1	0	0	0	1	0	0	0	1; 0; 1; 0	2oo4	1		
1	0	1	0	0	0	0	0	1; 1; 0; 0	2oo4	1		
~	1	0	0	1	0	1	0	0; 1; 1	2oo3	1		
0	0	~	1	1	0	1	0	0; 1; 1	2oo3	1		
~	1	1	0	0	0	1	0	1; 0; 1	2oo3	1		
0	0	1	0	~	1	1	0	0; 1; 1	2oo3	1		
~	1	1	0	1	0	0	0	1; 1; 0	2oo3	1		
0	0	1	0	1	0	~	1	0; 1; 1	2oo3	1		
1	0	~	1	0	0	1	0	1; 0; 1	2oo3	1		
1	0	0	0	~	1	1	0	1; 0; 1	2oo3	1		
1	0	~	1	1	0	0	0	1; 1; 0	2oo3	1		
1	0	0	0	1	0	~	1	1; 0; 1	2oo3	1		
1	0	1	0	~	1	0	0	1; 1; 0	2oo3	1		

1yz (y = A, B) (z = A, P)		2yz (y = A, B) (z = A, P)		3yz (y = A, B) (z = A, P)		4yz (y = A, B) (z = A, P)		xAV (x = 1, 2, 3, 4)			FT	Remarks
Output	Er	Output	Er	Output	Er	Output	Er	Valid Input Signals (Er 0)	Voting Type	Output		
1	0	1	0	0	0	~	1	1; 1; 0	2oo3	1		
3 Failures												
~	1	~	1	~	1	1	0	1	act.	~	sd	
~	1	~	1	1	0	~	1	1	act.	~	sd	
~	1	1	0	~	1	~	1	1	act.	~	sd	
1	0	~	1	~	1	~	1	1	act.	~	sd	
0	0	0	0	0	0	1	0	0; 0; 0; 1	2oo4	0	3 NSF	3 NSF (AU or PU or Sensor)
0	0	0	0	1	0	0	0	0; 0; 1; 0	2oo4	0		
0	0	1	0	0	0	0	0	0; 1; 0; 0	2oo4	0		
1	0	0	0	0	0	0	0	1; 0; 0; 0	2oo4	0		
0	0	0	0	~	1	1	0	0; 0; 1	2oo3	0	2 NSF and 1 SF	2 NSF and 1 SF (AU or PU or Sensor)
0	0	0	0	1	0	~	1	0; 0; 1	2oo3	0		
0	0	~	1	0	0	1	0	0; 0; 1	2oo3	0		
0	0	1	0	0	0	~	1	0; 1; 0	2oo3	0		
0	0	~	1	1	0	0	0	0; 1; 0	2oo3	0		
0	0	1	0	~	1	0	0	0; 1; 0	2oo3	0		
~	1	0	0	0	0	1	0	0; 0; 1	2oo3	0		
1	0	0	0	0	0	~	1	1; 0; 0	2oo3	0		
~	1	0	0	1	0	0	0	0; 1; 0	2oo3	0		
1	0	0	0	~	1	0	0	1; 0; 0	2oo3	0		
~	1	1	0	0	0	0	0	1; 0; 0	2oo3	0		
1	0	~	1	0	0	0	0	1; 0; 0	2oo3	0		
~	1	~	1	0	0	1	0	0; 1	1oo2	1		
~	1	~	1	1	0	0	0	1; 0	1oo2	1		
~	1	0	0	~	1	1	0	0; 1	1oo2	1		
~	1	1	0	~	1	0	0	1; 0	1oo2	1		
~	1	0	0	1	0	~	1	0; 1	1oo2	1		
~	1	1	0	0	0	~	1	1; 0	1oo2	1		
0	0	~	1	~	1	1	0	0; 1	1oo2	1		
1	0	~	1	~	1	0	0	1; 0	1oo2	1		
0	0	~	1	1	0	~	1	0; 1	1oo2	1		
1	0	~	1	0	0	~	1	1; 0	1oo2	1		
0	0	1	0	~	1	~	1	0; 1	1oo2	1		
1	0	0	0	~	1	~	1	1; 0	1oo2	1		
4 Failures												
0	0	0	0	0	0	0	0	0; 0; 0; 0	2oo4	0	4 NSF	== 3 NSF
0	0	0	0	0	0	~	1	0; 0; 0	2oo3	0	3 NSF	== 3 NSF

1yz (y = A, B) (z = A, P)		2yz (y = A, B) (z = A, P)		3yz (y = A, B) (z = A, P)		4yz (y = A, B) (z = A, P)		xAV (x = 1, 2, 3, 4)			FT	Remarks
Output	Er	Output	Er	Output	Er	Output	Er	Valid Input Signals (Er 0)	Voting Type	Output		
0	0	0	0	~	1	0	0	0; 0; 0	2oo3	0	and 1 SF	== 3 NSF
0	0	~	1	0	0	0	0	0; 0; 0	2oo3	0		== 3 NSF
~	1	0	0	0	0	0	0	0; 0; 0	2oo3	0		== 3 NSF
0	0	0	0	~	1	~	1	0; 0	1oo2	0	2 NSF and 2 SF	== 2N, 1 S
0	0	~	1	0	0	~	1	0; 0	1oo2	0		== 2N, 1 S
0	0	~	1	~	1	0	0	0; 0	1oo2	0		== 2N, 1 S
~	1	0	0	0	0	~	1	0; 0	1oo2	0		== 2N, 1 S
~	1	0	0	~	1	0	0	0; 0	1oo2	0		== 2N, 1 S
~	1	~	1	0	0	0	0	0; 0	1oo2	0		== 2N, 1 S
0	0	~	1	~	1	~	1	0	act.	~	sd	
~	1	0	0	~	1	~	1	0	act.	~	sd	
~	1	~	1	0	0	~	1	0	act.	~	sd	
~	1	~	1	~	1	0	0	0	act.	~	sd	
~	1	~	1	~	1	~	1	~	act.	~	sd	

Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH

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

Forschungszentrum
Boltzmannstraße 14
85748 Garching b. München
Telefon +49 89 32004-0
Telefax +49 89 32004-300

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

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

www.grs.de

ISBN 978-3-949088-38-4