Eine Bewertungs-grundlage für Leittechnikkonzepte neuer Reaktoranlagen im Ausland

GRS - 807

Gesellschaft für Anlagen-
und Reaktorsicherheit
(GRS) gGmbH

Eine Bewertungsgrundlage für Leittechnikkonzepte neuer Reaktoranlagen im Ausland

Eigenständige Analyse der GRS mit Beiträgen zur internationalen Vergleichsstudie DIGMORE der OECD/NEA

Christian Müller
Ewgenij Piljugin

Juni 2025

Anmerkung:

Das diesem Bericht zugrunde liegende Eigenforschungsvorhaben wurde mit Mitteln des Bundesministeriums für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV) unter dem Förderkennzeichen 4723R01430 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 BMUV übereinstimmen.

GRS - 807
ISBN 978-3-911727-00-6

Deskriptoren

Bewertung von Leittechnikkonzepten, digitale und analoge Systeme, Diversität, internationale Vergleichsstudien, Leittechnik, Monte-Carlo-Simulationen, OECD-NEA, probabilistische Sicherheitsanalysen (PSA), Redundanz

Kurzfassung

Im Rahmen dieses Vorhabens wurden Leittechnikkonzepte moderner Reaktoranlagen umfassend analysiert, um eine Bewertungsgrundlage zu entwickeln. Ziel war es, eine systematische Methode bereitzustellen, mit der die sicherheitstechnischen Eigenschaften und Risiken moderner Leittechnikarchitekturen objektiv bewertet werden können. Die Untersuchungen basierten auf einem repräsentativen und realitätsnahen Referenzfall, der die Leittechnikarchitektur eines generischen Siedewasserreaktors modelliert. Dieser Referenzfall wurde durch umfangreiche Recherchen zu bestehenden Leittechnikkonzepten beeinflusst und im Rahmen des internationalen Projekts DIGMORE der OECD/NEA in Zusammenarbeit mit internationalen Experten entwickelt. Die Analysen umfassten die Modellierung und Validierung verschiedener Leittechnikarchitekturen und -systeme, die sich durch unterschiedliche Komplexität und Technologien (z. B. digitale und analoge Signalübertragung) auszeichnen. Monte-Carlo-Simulationen sowie der Vergleich mit Analysen anderer Organisationen (im Rahmen des Projekts DIGMORE der OECD/NEA) dienten der Validierung der Bewertungsgrundlage und deren Anpassung an unterschiedliche Szenarien.

Abstract

In this project, instrumentation and control (I&C) concepts for modern nuclear power plants were comprehensively analyzed in order to provide a basis for safety evaluations. The goal was to provide a systematic methodology for objectively evaluating the safety characteristics and risks of modern I&C architectures. The investigations were based on a representative and realistic reference case modeling the I&C architecture of a generic boiling water reactor. This reference case was informed by extensive research on existing I&C concepts and developed in collaboration with international experts as part of the OECD/NEA DIGMORE project. The analyses included the modeling and validation of various I&C architectures and systems, characterized by different complexities and technologies (e.g., digital and analog signal transmission). Monte Carlo simulations and comparisons with analyses conducted by other organizations (within the framework of the OECD/NEA DIGMORE project) were used to validate the evaluation framework and adapt it to different scenarios.

Inhaltsverzeichnis

1 Einleitung

Leittechnikarchitekturen und -systeme spielen eine zentrale Rolle für die Sicherheit, Zuverlässigkeit und Effizienz von Kernkraftwerken. Diese Leittechnikarchitekturen und -systeme gewährleisten die Überwachung sicherheitskritischer Funktionen, erkennen frühzeitig potenzielle Störungen und leiten bei Bedarf Schutzmaßnahmen ein. Mit der zunehmenden Digitalisierung und Automatisierung haben sich die technischen Anforderungen an Leittechniksysteme erheblich verändert, was nicht nur neue Möglichkeiten, sondern auch spezifische Herausforderungen mit sich bringt.

Ein wesentliches Merkmal neuerer Leittechniksysteme ist ihre zunehmende Komplexität durch den vielfältigen Einsatz digitaler Komponenten, das sich in der Vernetzung redundanter Komponenten, in diversitären Systemansätzen und in der Verarbeitung großer Datenmengen widerspiegelt. Diese Systeme bieten zahlreiche Vorteile, wie eine gesteigerte Flexibilität, verbesserte Selbstüberwachungsmechanismen und eine optimierte Mensch-Maschine-Schnittstelle. Gleichzeitig bestehen Risiken, insbesondere im Hinblick auf latente Fehler in Hard- und Software digitaler Systeme, die zu Ausfällen aufgrund gemeinsamer Ursachen (GVA) führen können. Daher ist es von entscheidender Bedeutung, dass diese immer komplexer werdenden Systeme auch sicherheitstechnisch umfassend bewertet werden können.

Die systematische Analyse und Bewertung von Leittechnikarchitekturen und -systemen erfordert eine methodisch fundierte Herangehensweise, die es ermöglicht, die Sicherheit und Zuverlässigkeit solcher Systeme objektiv zu beurteilen. Eine solche Grundlage ist auch für die Bewertung durch regulatorische Behörden und Sachverständige von entscheidender Bedeutung, da sie die Basis für die Genehmigung und Überwachung neuer Anlagenkonzepte bildet.

Der Schwerpunkt dieses Vorhabens lag daher auf der Entwicklung einer Bewertungsgrundlage für Leittechnikarchitekturen und -systeme neuer Reaktoranlagen. Die hierfür durchgeführten Arbeiten basierten auf einem repräsentativen und realitätsnahen Referenzfall, der die Leittechnik eines generischen Siedewasserreaktors abbildet. Dieser Referenzfall wurde so gestaltet, dass er eine plausible Grundlage für die Analyse moderner Leittechnikkonzepte bietet. Durch die Modellierung verschiedener Architekturen und die Validierung der Ergebnisse mithilfe von Monte-Carlo-Simulationen sowie durch den Ver-

gleich mit internationalen Analysen im Rahmen des Projekts DIGMORE[1] wurde eine Bewertungsgrundlage geschaffen, die sowohl wissenschaftlich fundiert als auch praxisorientiert ist.

Die vorliegende Arbeit liefert eine wichtige Weiterentwicklung zur Bewertung von Leittechniksystemen auf Grundlage eines vertieften internationalen wissenschaftlichen Austauschs und die Etablierung einheitlicher Standards der partizipierten Staaten. Dabei steht die Unterstützung bewertender Institutionen im Fokus, um die Sicherheit neuer Reaktoranlagen nachhaltig zu fördern und das Vertrauen in moderne Leittechnikkonzepte zu stärken.

[1] Beim Projekt DIGMORE („DIGMORE – A Realistic Comparative Application of DI&C Modelling Approaches for PSA“) /DIG 25/ handelt es sich um einen Task der Working Group on Risk Assessment (WGRISK) im Rahmen der Nuclear Energy Agency (NEA) der Organisation for Economic Co-operation and Development (OECD). Die GRS hat die Führung von DIGMORE übernommen, das Projekt läuft voraussichtlich noch bitte Mitte 2026. Der in diesem Vorhaben verwendete Referenzfall und eine der untersuchten Leittechnikarchitekturen wurden im Rahmen von DIGMORE entworfen.

2 Stand von W&T

Die folgenden Ausführungen basieren auf umfassenden Recherchen, die unter anderem unter Einbeziehung von Quellen der International Atomic Energy Agency (IAEA), der öffentlich zugänglichen Dokumentendatenbank NRC ADAMS der US-amerikanischen Nuclear Regulatory Commission (NRC) sowie des britischen Office for Nuclear Regulation (ONR) durchgeführt wurden. Dabei handelt es sich nicht um direkte, wörtliche Zitate dieser Quellen. Vielmehr stellt der Text eine durch die GRS vorgenommene Interpretation und Zusammenfassung der recherchierten Inhalte dar, die im Kontext des vorliegenden Projekts analysiert und aufbereitet wurden. Darüber hinaus hat die GRS auf eigene Datenbanken sowie Erkenntnisse aus in der Vergangenheit durchgeführten Projekten zurückgegriffen, um eine fundierte und umfassende Darstellung der aktuellen Entwicklungen zu gewährleisten.

2.1 Neue Reaktoranlagen in der Design- bzw. Errichtungsphase

Zu Beginn des 21. Jahrhunderts erfolgte eine Konsolidierung der bekannten und etablierten Hersteller von Reaktoranlagen auf dem globalen Markt der nuklearen Energieerzeugung. Abb. 2.1 gibt eine Übersicht über die wichtigsten Anbieter, Zusammenschlüsse und Wechselbeziehungen in der weltweiten Nuklearindustrie sowie deren bedeutendste Reaktormodelle auf Basis der im Rahmen dieses Projekts durchgeführten Recherchen, bei denen unter anderem Informationen von Herstellerseiten ausgewertet wurden. Sie erweitert und aktualisiert wesentlich die in /HEI 10/ enthaltenen Informationen zu neuen Reaktoranlagen und deren Hauptausrüstern.

Einige westliche Hersteller bieten sowohl eigenständig als auch im Rahmen von Konsortien Reaktoranlagen unterschiedlicher Leistung sowie Ausrüstungen und Dienstleistungen zur Modernisierung bestehender Anlagen auf dem internationalen Markt an. Gleichzeitig gewinnen Industrienationen aus dem asiatischen Wirtschaftsraum – insbesondere China, Indien und Südkorea – sowie Russland zunehmend an Bedeutung. Diese Hersteller haben eigene Reaktormodelle entwickelt und versuchen, exportfähige Anlagen der neuesten Generation im internationalen Wettbewerb zu etablieren. Ein herausragendes Beispiel ist der südkoreanische Konzern KEPCO mit dem Reaktorkonzept APR-1400, dessen Hauptausrüstungen von Doosan Heavy Industries & Construction

gefertigt werden. Kernkraftwerke dieses Typs wurden bereits nicht nur in Südkorea, sondern auch international errichtet, darunter das Kernkraftwerk Barakah (Blöcke 1-4) in den Vereinigten Arabischen Emiraten.

Moderne Reaktoranlagen der Generation III/III+ (darunter EPR, AP1000, APR-1400 und WWER-1200) zeichnen sich durch ein gestaffeltes Sicherheitskonzept (Defense-in-Depth), einen erweiterten Einsatz passiver Sicherheitseinrichtungen (z. B. passive Wärmesenken) sowie einen hohen Automatisierungsgrad aus. Im Bereich der Leittechnik bestehen erhebliche Unterschiede zwischen den sicherheitstechnischen Konzepten verschiedener Hersteller, insbesondere hinsichtlich der verwendeten Technologien und der Architektur der Leittechniksysteme.

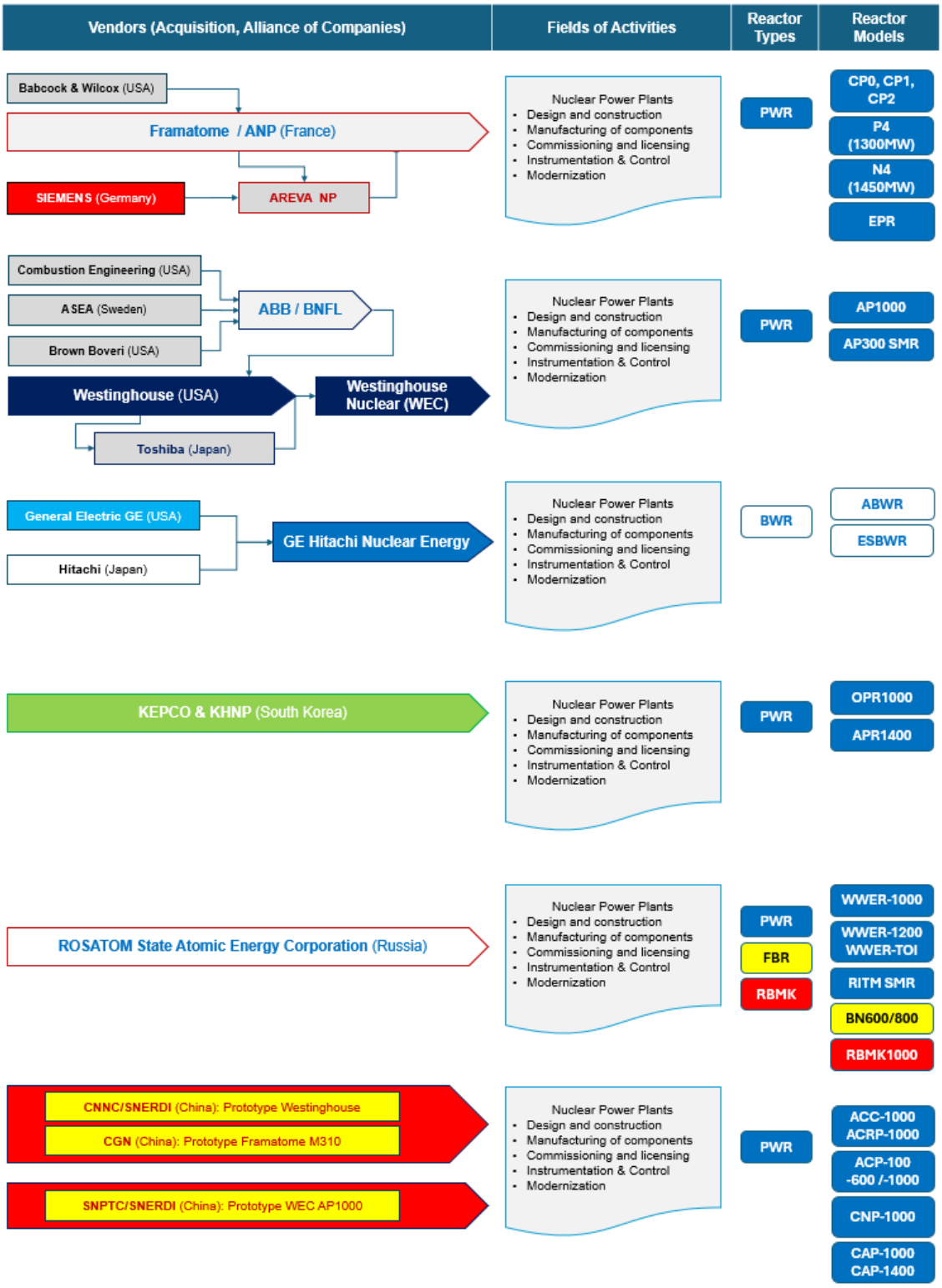


Abb. 2.1 Wichtige Anbieter und Reaktormodelle der globalen Nuklearindustrie

Diese Übersicht zeigt die wichtigsten Anbieter, Unternehmenszusammenschlüsse und Wechselbeziehungen in der globalen Nuklearindustrie sowie deren Reaktormodelle.

Die GRS hat bereits 2010 in /HEI 10/ die Kernkraftwerke mit Leichtwasserreaktoren der Generation III/III+ erfasst, die sich damals in der Errichtungsphase befanden. Im Rahmen des vorliegenden Projekts wurden zusätzlich neue Kernkraftwerke berücksichtigt, die sich seit 2011 in unterschiedlichen Stadien der Fertigstellung befanden.

Tab. 2.1 bietet eine Übersicht über diese Reaktoranlagen. Die Zusammenstellung basiert im Wesentlichen auf Informationen aus /IAE 24/ und erhebt keinen Anspruch auf Vollständigkeit. Vielmehr soll die Übersicht einen allgemeinen Einblick geben, welche Reaktortypen in welchen Ländern errichtet werden.

Tab. 2.1 Übersicht neuer Kernkraftwerke (Stand 2024), Anlagen in der Errichtungsphase sind gelb markiert

Country	Reactor Name	Type	Model	Cap. [MW]	Const.	Grid
Argentina	ATUCHA-2	PHWR	PHWR KWU	693	1981	2014
Belarus	BELARUSIAN-1/2	PWR	WWER-1200/W-491	1110	2013-2014	2020-2023
Brazil	ANGRA-3	PWR	DWR-1300	1340	2010	2028
China	LING AO-4	PWR	CPR-1000	1007	2006	2011
China	QINSHAN 2-4	PWR	CNP-600	623	2007	2011
China	FUQING-1/2/3/4	PWR	CNP-1000	1000	2008-2012	2014-2017
China	FUQING-5/6	PWR	HPR1000	1075	2015	2020-2022
China	FANGJIASHAN-1/2	PWR	CPR-1000	1012	2008-2009	2014-2015
China	HONGYANHE-3/4	PWR	CPR-1000	1061	2009	2015-2016
China	SANMEN-1/2	PWR	AP-1000	1157	2009	2018
China	HAIYANG-1/2	PWR	AP-1000	1170	2009-2010	2018
China	TAISHAN-1/2	PWR	EPR-1750	1660	2009-2010	2018-2019
China	NINGDE-1/2/3/4	PWR	CPR-1000	1018	2008	2012-2016
China	CHANGJIANG-1/2	PWR	CNP-600	601	2010	2015-2016
China	FANGCHENGGANG-1/2	PWR	CPR-1000	1000	2010	2015-2016
China	FANGCHENGGANG-3/4	PWR	HPR1000	1000	2015-2016	2023-2024

Country	Reactor Name	Type	Model	Cap. [MW]	Const.	Grid
China	YANGJIANG-1/2/3/4	PWR	CPR-1000	1000	2008-2012	2013-2017
China	SHIDAO BAY-1	HTGR	HTR-PM	150	2012	2021
China	YANGJIANG-5/6	PWR	ACPR-1000	1000	2013	2018-2019
China	HONGYANHE-1/2	PWR	CPR-1000	1061	2007-2008	2013
China	HONGYANHE-5/6	PWR	ACPR-1000	1061	2015	2021-2022
China	TIANWAN-3/4	PWR	WWER-1000/W-428	1060	2012-2013	2017-2018
China	TIANWAN-5/6	PWR	CNP-1000	1060	2015-2016	2020-2021
China	TIANWAN-7/8	PWR	WWER-1200/W-491T	1171	2021-2022	2026-2027
Finland	OLKILUOTO-3	PWR	EPR	1600	2005	2022-2023
France	FLAMANVILLE-3	PWR	EPR	1630	2007	2024
England	HINKLEY POINT C-1/2	PWR	EPR-1750	1630	2018-2019	2028+
India	KAIGA-4	PHWR	PHWR-200	202	2002	2011
India	KUDANKULAM-1/2	PWR	WWER-1000/W-412	932	2002	2013
India	KAKRAPAR-3/4	PHWR	PHWR-700	630	2010	2021-2024
Iran	BUSHEHR-1	PWR	WWER-1000/W-446	915	1975	2011
Korea	SHIN-KORI-1/2	PWR	OPR-1000	996	2006-2007	2010-2012
Korea	SHIN-WOLSONG-1/2	PWR	OPR-1000	996	2007-2008	2012-2015
Korea	SAEUL-1/2	PWR	APR-1400	1416	2008-2009	2016-2019
Korea	SHIN-HANUL-1/2	PWR	APR-1400	1414	2012-2013	2022-2023
Pakistan	CHASNUPP-2	PWR	CNP-300	300	2005	2011
Pakistan	CHASNUPP-3/4	PWR	CNP-300	315	2011	2016-2017
Pakistan	KANUPP-2/3	PWR	ACP-1000	1017	2015-2016	2021-2022
Russia	Akademik Lomonossow-1/2	PWR	KLT-40S 'Floating'	2*32	2007	2019
Russia	SEVERSK	FBR	BREST-OD-300	300	2021	2026
Russia	NOVOVORONEZH 2-1/2	PWR	WWER-1200/W-392M	1100	2008-2009	2016-2019

Country	Reactor Name	Type	Model	Cap. [MW]	Const.	Grid
Russia	LENINGRAD 2-1/2	PWR	WWER-1200/W-491	1100	2008-2010	2018-2020
Russia	KALININ-4	PWR	WWER-1000/W-320	950	1986	2011
Russia	KURSK 2-1/2	PWR	WWER-1300/W-510	1200	2018-2019	2025-2027
Russia	ROSTOV-3/4	PWR	WWER-1000/W-320	950	2009-2010	2014-2018
Slovakia	MOCHOVCE-3/4	PWR	WWER-440/W-213	440	1987	2023-2024
Turkey	AKKUYU-1/2/3/4	PWR	WWER-1200/W-509	1200	2018-2020	2026-2030
UAE	BARAKAH-1/2/3/4	PWR	APR-1400	1337	2012-2014	2020-2024
USA	WATTS BAR-2	PWR	WH 4LP	1164	1973	2016
USA	VOGTLE-3/4	PWR	AP-1000	1117	2013	2023-2024

Die Informationen aus Tab. 2.1 und Abb. 2.1 ermöglichen ein besseres Verständnis davon, welche Hersteller und Hauptausrüster an der Entwicklung moderner Reaktoranlagen beteiligt sind. Dies betrifft insbesondere auch die Ausstattung von Kernkraftwerken mit moderner Leittechnik, etwa von Unternehmen wie Framatome, Westinghouse und Rosatom.

Die verfahrens- und sicherheitstechnischen Konzepte neuer Reaktoranlagentypen der Generation III+ (z. B. EPR, AP1000, WWER-1200) basieren auf einer konsequenten Weiterentwicklung bewährter Technologien der nuklearen Energieerzeugung, insbesondere von Druck- und Siedewasserreaktoren. Ein wesentlicher technologischer Wandel zeigt sich im Bereich der Automatisierungstechnik (Leittechnik): Während in älteren Anlagen noch analoge Systeme zum Einsatz kamen, basiert die Leittechnik neuerer Reaktoren weitgehend auf digitalen, also prozessor- und softwarebasierten, Systemen. Diese digitale Leittechnik bietet zahlreiche Vorteile, darunter eine höhere Flexibilität bei der Anpassung an die Verfahrenstechnik, einen reduzierten Energieverbrauch und Platzbedarf sowie erweiterte Funktionalitäten zur Selbstüberwachung und verbesserte Mensch-Maschine-Schnittstellen. Gleichzeitig birgt sie jedoch ein erhöhtes Potenzial für latente Fehler in Hard- und Software. Nach aktuellem Stand von Wissenschaft und Technik können diese Fehler durch Qualitätssicherungsprozesse (Verifikation und Validierung) nicht vollständig ausgeschlossen werden. Um die Auswirkungen latenter Fehler – insbesondere Ausfälle aufgrund gemeinsamer Ursache (GVA) – zu minimieren, wurden in neuen

Reaktoranlagen verschiedene Sicherheitskonzepte entwickelt, darunter der Einsatz diversitärer Sicherheitsleittechnik sowie automatische und manuelle Backup-Funktionen.

Wie bereits bei früheren Reaktortypen bieten die Hersteller neuer Anlagen in der Regel ein in sich geschlossenes, bereits in der Designphase aufeinander abgestimmtes Konzept für die Verfahrens- und Leittechnik. Die sicherheitsrelevante Leittechnik sowie die zugehörige Hard- und Software werden entweder von spezialisierten Tochterunternehmen des Reaktoranlagenherstellers entwickelt und produziert oder nach dessen Vorgaben von qualifizierten Leittechnik-Herstellern gefertigt und geliefert.

Eine Ausnahme stellt die Entwicklung und der Einsatz digitaler Leittechnik bei in neuen WWER-Reaktoranlagen aus Russland dar. Der Reaktortyp WWER-1000/W-413 (AES-91) wurde zu Beginn des 21. Jahrhunderts vom Entwicklungsbüro AEP St. Petersburg (Rosatom) auf Basis des WWER-1000/W-320 ausgelegt. Nach diesem Design wurden unter anderem die ersten beiden Blöcke des Kernkraftwerks Tianwan (Blöcke 1 und 2) in China errichtet. Die Weiterentwicklung dieses Reaktortyps erfolgte im Rahmen der Projekte WWER-1000/W-446 (AES-92) durch die Rosatom-Tochter AEP Moskau, Gidropress und das Kurchatov-Institut für den Einsatz in Kernkraftwerken in Indien und Bulgarien.

Für diese sicherheitstechnisch optimierten WWER-1000-Reaktoren kamen bewährte und qualifizierte Leittechnik-Systeme westlicher Hersteller wie Framatome und Siemens zum Einsatz. Diese Systeme waren bereits zuvor bei der Modernisierung älterer WWER-Reaktoranlagen erprobt worden, beispielsweise in den Kernkraftwerken der Baulinie WWER-440 an den Standorten Kola (Russland) und Paks (Ungarn).

Der neu entwickelte russische Anlagentyp WWER-1200 (AES-2006) wurde konzipiert, um die Sicherheitsanforderungen der Reaktorgeneration III+ zu erfüllen. Sie stellt eine Weiterentwicklung der Typen AES-91 und AES-92 dar. Die Komponenten für den WWER-1200 sollten vorrangig von russischen Unternehmen geliefert werden, einschließlich der Elektro- und Leittechnik. Allerdings wurden einige leittechnische Systeme und Einrichtungen im Rahmen von Joint Ventures mit westlichen Unternehmen entwickelt und produziert, darunter beispielsweise die TPTS-Leittechnik des Rosatom-Konzerns mit Beteiligung von Siemens.

Tab. 2.2 bietet eine Übersicht der verwendeten Leittechnikplattformen unterschiedlicher neuer Anlagentypen, wie sie sich nach Recherchen innerhalb dieses Projekts darstellen. Da einzelne Anlagen eines Typs von den Angaben in Tab. 2.2 im Detail abweichen können, sind diese Angaben nicht als allgemeingültig anzusehen und erheben auch nicht den Anspruch der Vollständigkeit.

Tab. 2.2 Leittechniksysteme neuer Reaktoranlagentypen

Typ	Hersteller/Lieferant	Funktionen	Leittechnikplattformen
AP1000	Westinghouse	Reaktorschutz RESA / ESFAS	Common Q (digital)
		Begrenzungen	Common Q (digital)
		Betriebsleittechnik	Ovation (digital)
		Backup	ALS (analog)
APR-1400	KEPCO/KHNP	Reaktorschutz RESA / ESFAS	Common Q (digital) KNICS (digital)
		Begrenzungen	Common Q (digital) KNICS (digital)
		Betriebsleittechnik	Ovation (digital) Doosan DCS (digital)
		Backup	Diverse Plattformen: PLC/FPGA-basierte Leittechnik
APWR	Mitsubishi Heavy Industries	Reaktorschutz RESA / ESFAS	MELTAC (digital)
		Begrenzungen	MELTAC (digital)
		Betriebsleittechnik	MELTAC-N (digital)
		Backup	Zusätzliche analoge Backup-Systeme
EPR	Framatome	Reaktorschutz RESA / ESFAS	Teleperm XS (digital)
		Begrenzungen	Teleperm XS (digital)
		Betriebsleittechnik	Siemens SPPA-T2000 (digital) COMBINE (digital)
		Backup	Siemens SPPA-T2000 (digital) UNICORN (analog) Hardline (analog)
ESBWR	General Electric Hitachi	Reaktorschutz RESA / ESFAS	NUMAC (digital)
		Begrenzungen	NUMAC (digital)
		Betriebsleittechnik	Nicht-1E Leittechnik von DRS (digital) Mark VIe (digital)
		Backup	Mark VIe (digital) TRICON (digital)
WWER-1000 WWER-1200, WWER-1300 (WWER-TOI)	Rosatom	Reaktorschutz RESA / ESFAS	Teleperm XS (digital) TPTS-SB (digital)
		Begrenzungen	Teleperm XS (digital) TPTS-SB (digital)
		Betriebsleittechnik	Siemens SPPA-T2000 (digital) TPTS-NT (digital)
		Backup	Analoge Backup-Systeme vergleichbar mit UNICORN
RESA – Reaktorschnellabschaltung ESFAS – Engineered Safety Features Actuation System DCS – Digital Control System			

2.2 Leittechnikkonzept von AP1000-Anlagen

Das Leittechnikkonzept des AP1000 der Firma Westinghouse Electric sieht grundsätzlich folgende Leittechniksysteme vor (siehe Abb. 2.2)[2]:

- Betriebliche digitale Leittechnik mit Leittechnikfunktionen zum Normalbetrieb der Anlage und zum gestörten Betrieb der Anlage (Nicht-1E-Funktionen),
- Common Q, eine softwarebasierte Sicherheitsleittechnik zur Störfallbeherrschung (1E-Funktionen),
- Eine FPGA-basierte Sicherheitsleittechnik als zweites Reaktorschutzsystem/ Backup-System (Nicht-1E-Funktionen).

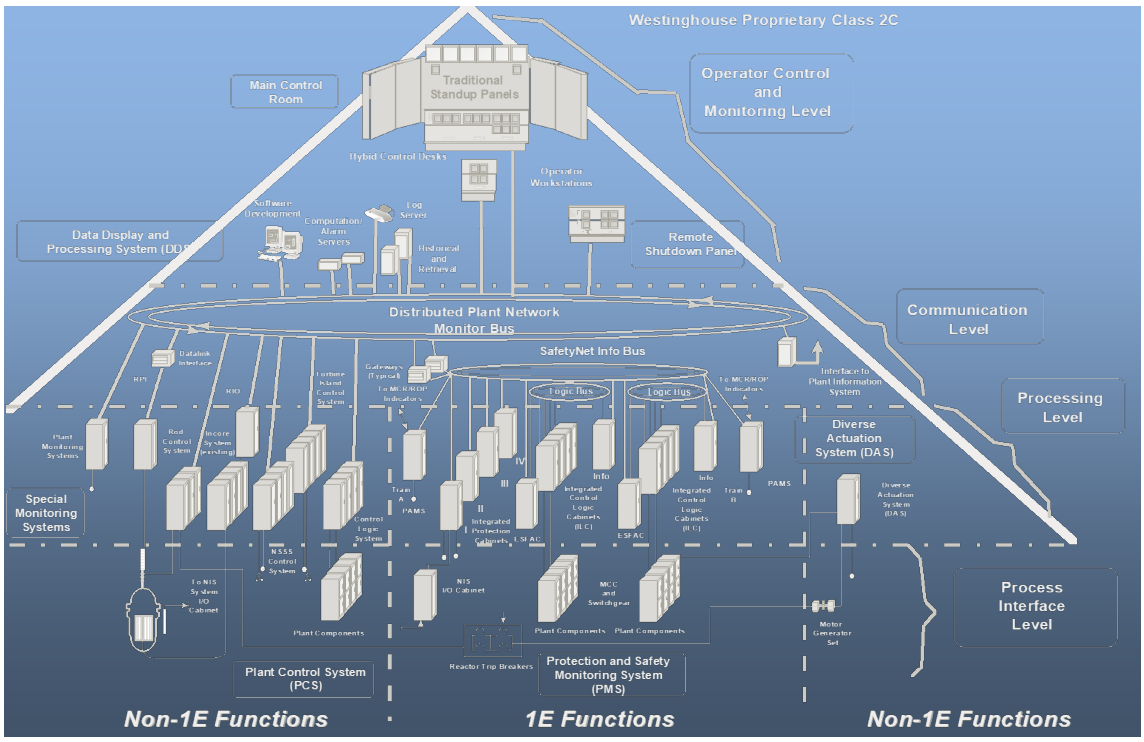


Abb. 2.2 Übersicht der Leittechnik der AP1000-Reaktoranlage /BRO 07/

Die Unabhängigkeit dieser Leittechnikfunktionen und -systeme soll durch den Einsatz unabhängiger Parameter, Auslösepfade und durch unterschiedliche Technologien sichergestellt werden. Des Weiteren erfolgt die Entwicklung und die Herstellung der Hard-

[2] Anmerkung: Die Kategorisierung der 1E- und Nicht-1E-Leittechnikfunktionen erfolgt nach dem Qualifizierungsstandard IEEE-323 /IEE 08/

und Software der Leittechniksysteme durch verschiedene Hersteller mit völlig unterschiedlichen Entwicklungswerkzeugen (Engineering Tools and Environments).

Die Sicherheitsleittechnik PMS (Protection and Safety Monitoring System) des AP-1000 erkennt Überschreitungen der Grenzwerte des bestimmungsgemäßen Betriebs und löst die entsprechenden Sicherheitsfunktionen aus. Wichtige sicherheitsrelevante Untersysteme des PMS (1E-Funktionen) sind

- die nukleare Instrumentierung,
- das Reaktorschutzsystem,
- das Netzwerksystem.

PMS basiert auf der Leittechnikplattform Common Q der Firma Westinghouse. Common Q wurde bereits in konventionellen Kraftwerken und bei der Modernisierung der Betriebsleittechnik in KKW erprobt und in den koreanischen Kernkraftwerken Ulchin-5 und -6 als Sicherheitsleittechnik eingesetzt. Das Reaktorschutzsystem des PMS besteht aus einem System zur Reaktorschnellabschaltung (RT – Reactor Trip) und einem ESFAS (ESFAS – Engineered Safety Features Actuation System) zur Steuerung der Sicherheitssysteme und -einrichtungen. Die Signalverarbeitung des RT- und ESFAS ist in Abb. 2.3 vereinfacht für einen Strang dargestellt.

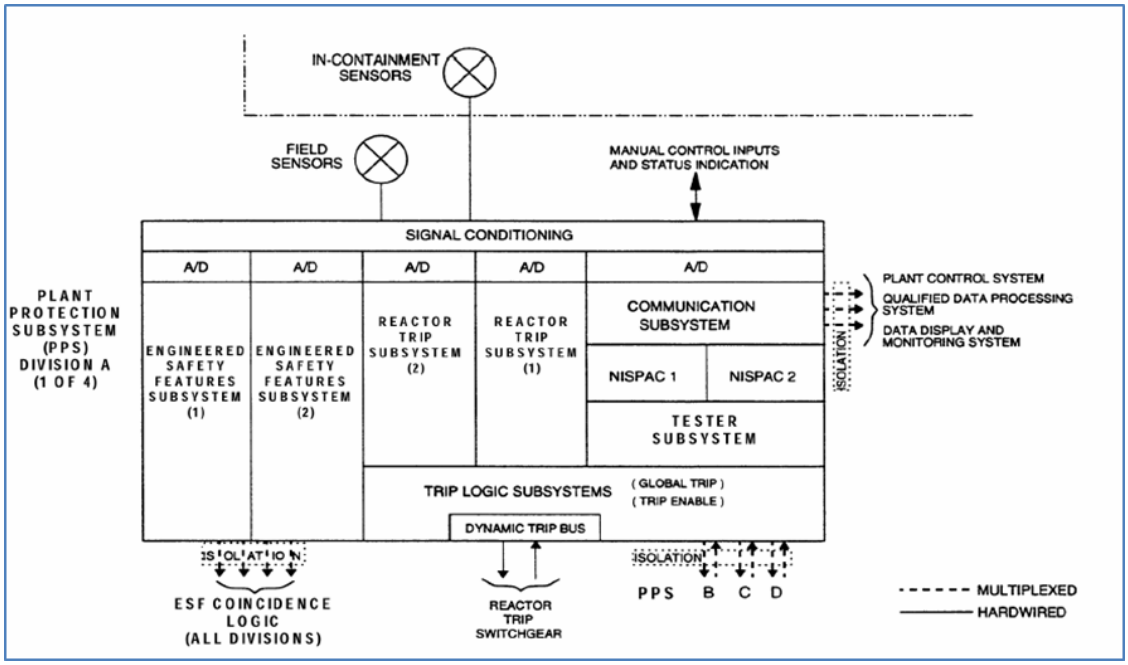


Abb. 2.3 Funktionsdiagramm des Reaktorschutzsystems (RT/ESFAS) /NRC 11/

Das RT-System (Reactor Trip System) übernimmt die Abschaltung des Reaktors (im Bild Reactor Trip), ESFAS (Engineered Safety Functions Actuation System) die Anregung der weiteren Sicherheitssysteme.

Der AP1000 ist konzeptionell mit einer sogenannten kompakten rechnerbasierten Warte ausgestattet (siehe Abb. 2.4).

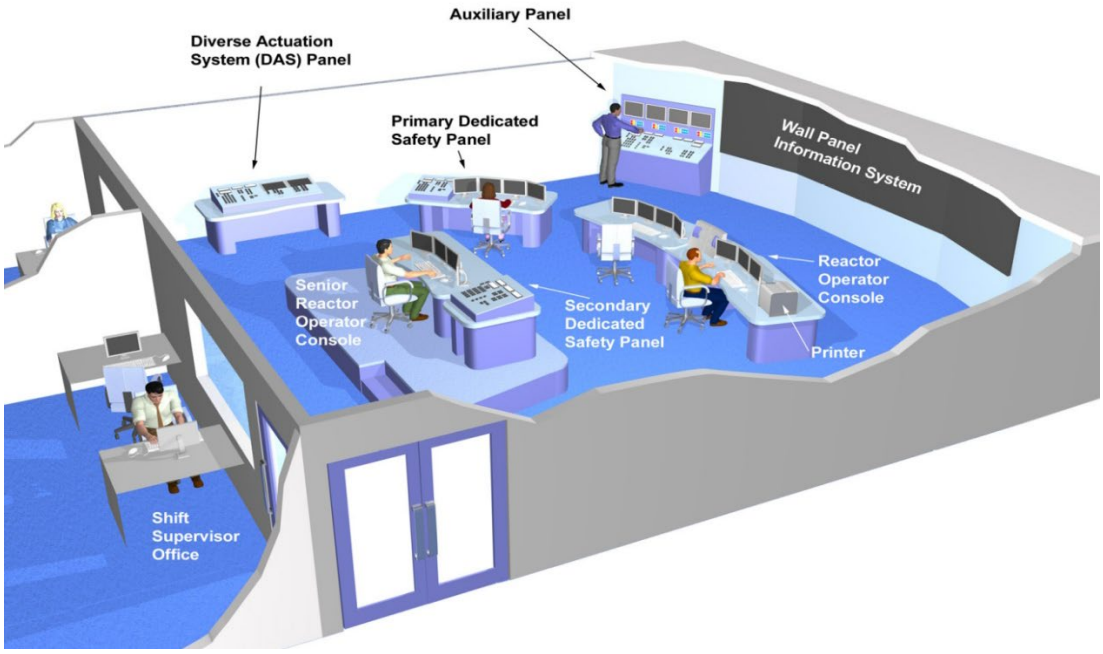


Abb. 2.4 Gestaltung der Warte des AP1000 /BRO 07/

Zur Beherrschung potenzieller GVA in der digitalen Sicherheitsleittechnik des AP1000 wurde eine alternative, diversitäre Leittechnik durch die Firma CS-Innovations entwickelt, die Sicherheitsleittechnik ALS (Advanced Logic System). Diese wurde als logikbasierte, nicht-mikroprozessorgestützte Plattform für den Austausch der Sicherheitsleittechnik in US-amerikanischen Kernkraftwerken konzipiert. Im Sommer 2009 wurde die Firma CS-Innovations durch die Firma Westinghouse übernommen /BER 10/.

ALS beinhaltet Funktions- und Steuerungsbaugruppen, Ein- und Ausgabebaugruppen, eine Kommunikationsbaugruppe zum Signalaustausch sowie Baugruppen zur Erweiterung des Systems (siehe Abb. 2.5).

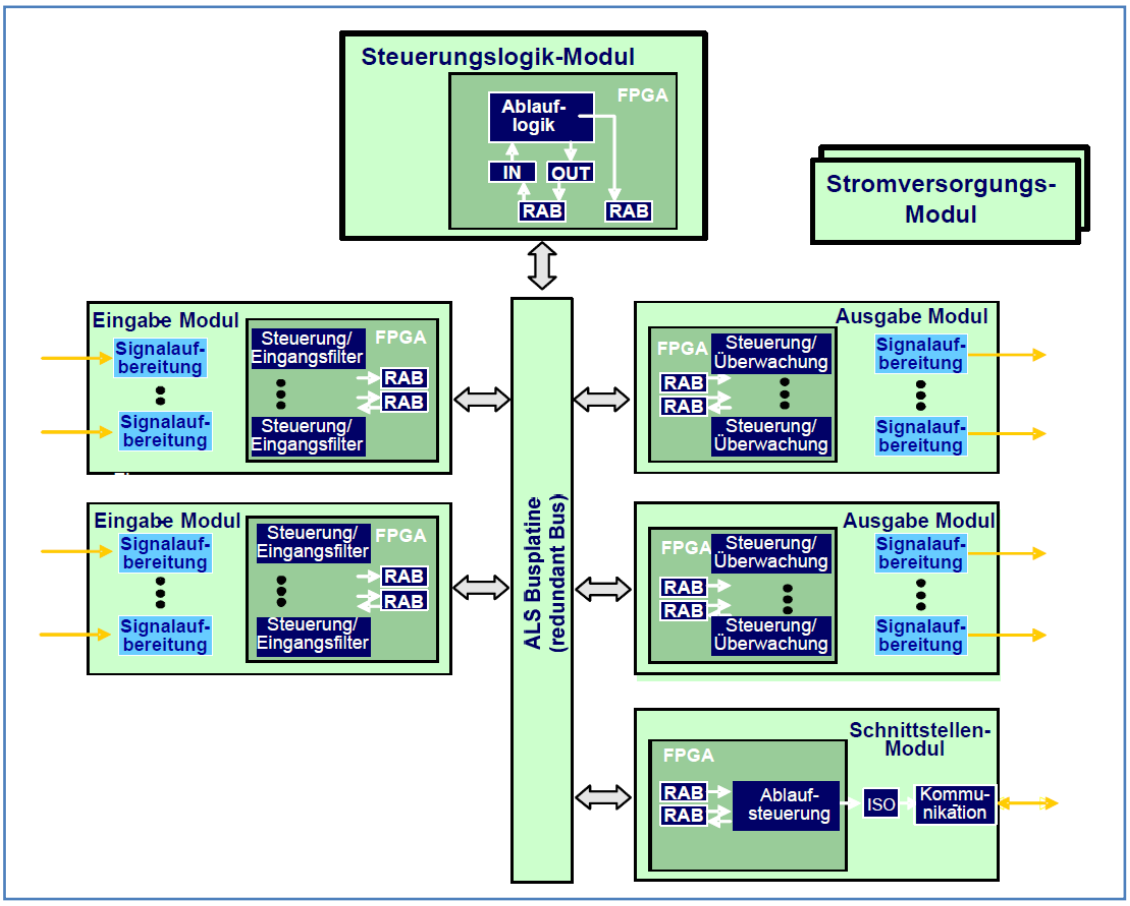


Abb. 2.5 Diagramm der Signalverarbeitung des ALS /BER 10/

ALS ist seit Herbst 2009 im KKW Wolf Creek Generation Station (USA) im Einsatz. Darüber hinaus wird ALS für neue Kernkraftwerke der Firma Westinghouse des Typs AP1000 als DAS (Diverse Actuation System), d. h. als Backup-System für das Reaktorschutzsystem eingesetzt (u. a. im KKW Vogtle-3 und -4, USA).

2.3 Leittechnikkonzept von APR-1400-Anlagen

Die ersten acht KKW in Südkorea (1977-1988) basieren auf Konzepten von Westinghouse und Framatome, zwei weitere auf der Technologie von Combustion Engineering (wurde später durch Westinghouse übernommen). Diese Konzepte wurden durch koreanische Firmen weiterentwickelt und so entstand das koreanische Standard-Kernkraftwerk vom Typ KSNP/KSNP+. Im Jahr 2005 wurde das KSNP/KSNP+ in OPR-1000 (Optimized Power Reactor) umbenannt, offenbar für die asiatischen Märkte, insbesondere Indonesien und Vietnam. Zehn in Betrieb befindliche Anlagen tragen nun die Bezeichnung OPR-1000.

Durch Zusammenführung der Institutionen der Nuklearindustrie (u. a. KEPCO – Operation & Maintenance; Doosan Heavy Industries & Construction – Equipment Design & Manufacturing; Hyundai – Construction, KOPEC – System Design, KNF – Fuel Design & Manufacturing, KAERI – Research) entstand Korea Hydro & Nuclear Power (KHNP/KEPCO) mit einer Bündelung der Kapazitäten und Fähigkeiten zur Herstellung und Betrieb von Reaktoranlagen, die hinsichtlich Kapazität und Sicherheitskonzept (Generation III/OPR1000, Generation III+/APR1400) unterschiedlich ausgelegt werden können /KEP 25/.

Die südkoreanische Nuklearindustrie befindet sich seit einigen Jahren international auf Expansionskurs. Als Exportvariante bietet der KHNP-Konzern die APR-1400-Anlage (APR – Advanced Power Reactor) der Generation III+ (z. B. KKW Barakah, Vereinigte Arabische Emirate) an. Diese Reaktoranlage ist mit softwarebasierter Sicherheitsleittechnik ausgerüstet. Die Entwicklung der Leittechnik in den südkoreanischen Kernkraftwerken ist in Abb. 2.6 dargestellt.

Systems / Plants	Reactor Trip System	ESFAS Systems	Protection Process	NSSS Control	PCS	Turbine Control	Main Control Board
Kori No. 1	Relay Logic (W/H)	Relay Logic (W/H)	Foxboro H-line	Foxboro H-line	Foxboro H-line	DCS	Conventional
Kori No. 1 (Upgraded in 1998)	Relay Logic (W/H)	Relay Logic (W/H)	Spec200 Spec200m (Foxboro)	Spec200 Spec200m (Foxboro)	Spec200 Spec200m (Foxboro)	DCS	Conventional
Kori No. 2,3,4 YGN No. 1,2	SSPS Relay Logic (W/H)	SSPS Relay Logic (W/H)	7300 Analog	7300 Analog	7300 Analog	Mark V (GE)	Conventional
YGN No. 3,4	Relay Logic (ABB-CE)	Relay Logic (ABB-CE)	Analog (ABB-CE)	Spec200 Spec200m (Foxboro)	ILS (Forney)	Mark V (GE)	Conventional
Ulchin No. 3,4	Relay Logic (ABB-CE)	Relay Logic (ABB-CE)	Analog (ABB-CE)	Spec200 Spec200m (Foxboro)	PCS (Eaton)	Mark V (GE)	Hybrid
Wolsong No. 1,2,3,4	Relay Logic (AECL)	Relay Logic (AECL)	Analog/PDC (AECL)	DCC X/Y Computers Control	Analog/Relay (AECL)	Mark V (GE)	Hybrid
YGN No. 5,6	Relay Logic (ABB-CE)	Relay Logic (ABB-CE)	Analog (ABB-CE)	PLC (OMRON)	PCS (Eaton)	Mark V (GE)	Hybrid
Ulchin No. 5,6	PLC (W/H)	PLC (W/H)	Analog (W/H)	PLC (OMRON)	PCS (HFC)	Mark V (GE)	Hybrid
Shin Kori No. 1,2 Shin Wolsong No.1,2	PLC (W/H)	PLC (W/H)	Analog (W/H)	PLC (OMRON) Ovation (W/H)	Teleperm XP (Siemens)	Mark VI (GE)	Hybrid
Shin Kori No. 3,4 (APR-1400)	PLC (W/H)	PLC (W/H)	Analog/PLC (W/H)	Ovation (W/H)	PLC (W/H)	Mark VI (GE)	Compact Workstation

Abb. 2.6 Übersicht zum Einsatz der Leittechnik in den südkoreanischen Kernkraftwerken /HAN 05/

Die Leittechnikarchitektur des APR1400 beinhaltet Sicherheitsleittechnik, Betriebsleittechnik und ein diversitäres Backup-System, eine generische Übersicht bietet Abb. 2.7.

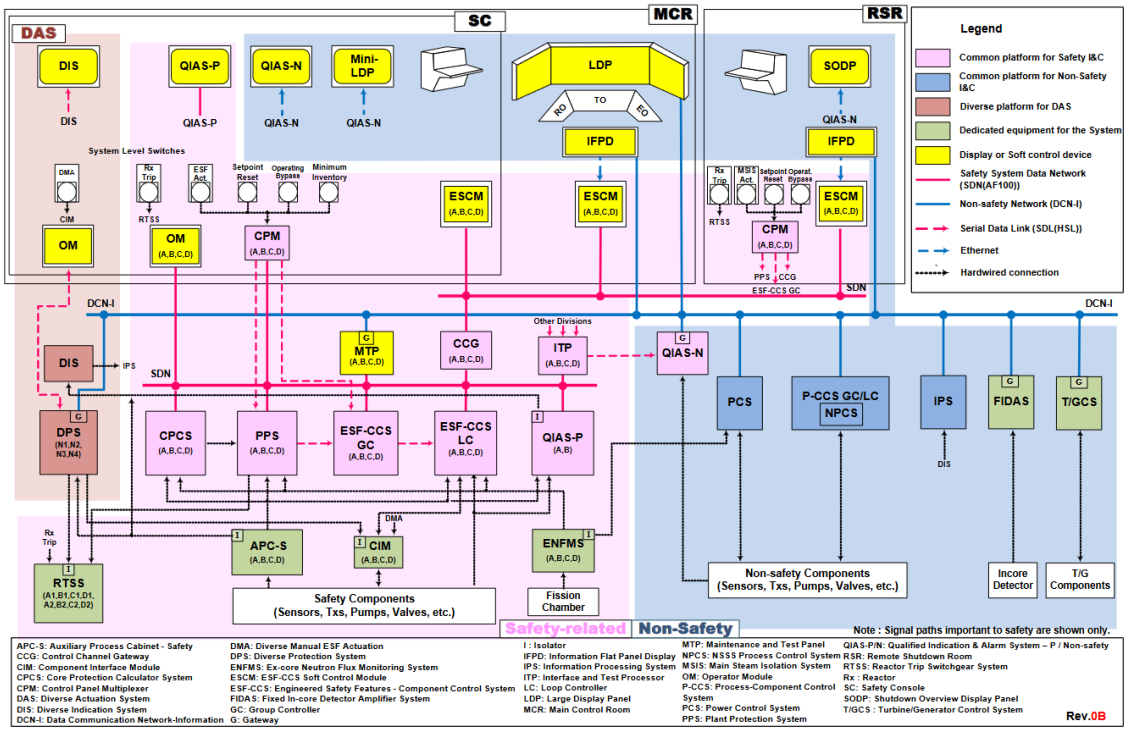


Abb. 2.7 Leittechnikarchitektur einer generischen APR-1400+ Reaktoranlage /NEA 18/

Südkorea entwickelt die eigene Leittechnikplattform KNICS (Korea Nuclear Instrumentation and Control System) /KOR 25/. Es handelt sich dabei um ein nationales Projekt Südkoreas, das darauf abzielt, eigene Technologien für die Instrumentierung und Steuerung von Kernkraftwerken zu entwickeln und zu implementieren. Dieses Vorhaben wurde ins Leben gerufen, um die Abhängigkeit von ausländischen Technologien zu reduzieren und die Sicherheit sowie Effizienz der südkoreanischen Kernkraftwerke zu erhöhen.

2.4 Leittechnikkonzept von APWR-Anlagen

Der japanische Konzern Mitsubishi Heavy Industries (MHI) hat bereits langjährige Erfahrungen beim Errichten von Kernkraftwerken in Japan und beabsichtigt Druckwasserreaktoren des neuentwickelten Typs APWR (Advanced Pressurized Water Reactor) zu exportieren. Als wichtiger Markt für APWR-Anlagen werden die USA angesehen. APWR-Anlagen sollen mit der digitalen, prozessorbasierten MELTAC[3]-Sicherheitsleittechnik der Firma Mitsubishi ausgerüstet werden.

Die generische Leittechnikarchitektur einer APWR-Anlage ist in Abb. 2.8 dargestellt. Diese hat die folgenden Eigenschaften /MHI 07/:

- Eine 4-fach redundante Struktur der Sicherheitsleittechnik,
- eine redundante Struktur der Betriebsleittechnik,
- zweifach redundante Kommunikation zwischen lokalen leittechnischen Einrichtungen und der Warte,
- eine gemeinsame Leittechnikplattform für Sicherheitsleittechnik und Betriebsleittechnik,
- den Einsatz eines diversitären Leittechniksystems,
- computerbasierte Mensch-Maschine-Schnittstelle in der Warte.

Die Entwicklung der Hard- und Software von MELTAC erfolgte speziell für kerntechnische Anwendungen. MHI hat auf einer Präsentation des US-APWR-Reaktors in den

[3] MELTAC – Mitsubishi Electric Total Advanced Controller

USA /MHI 07/ betont, dass die Verfügbarkeit der MELTAC-Plattform für 30 Jahre garantiert wird und die Plattform damit nur einmal während des 60-jährigen Lebenszyklus der APWR-Reaktoranlage ausgetauscht werden müsse.

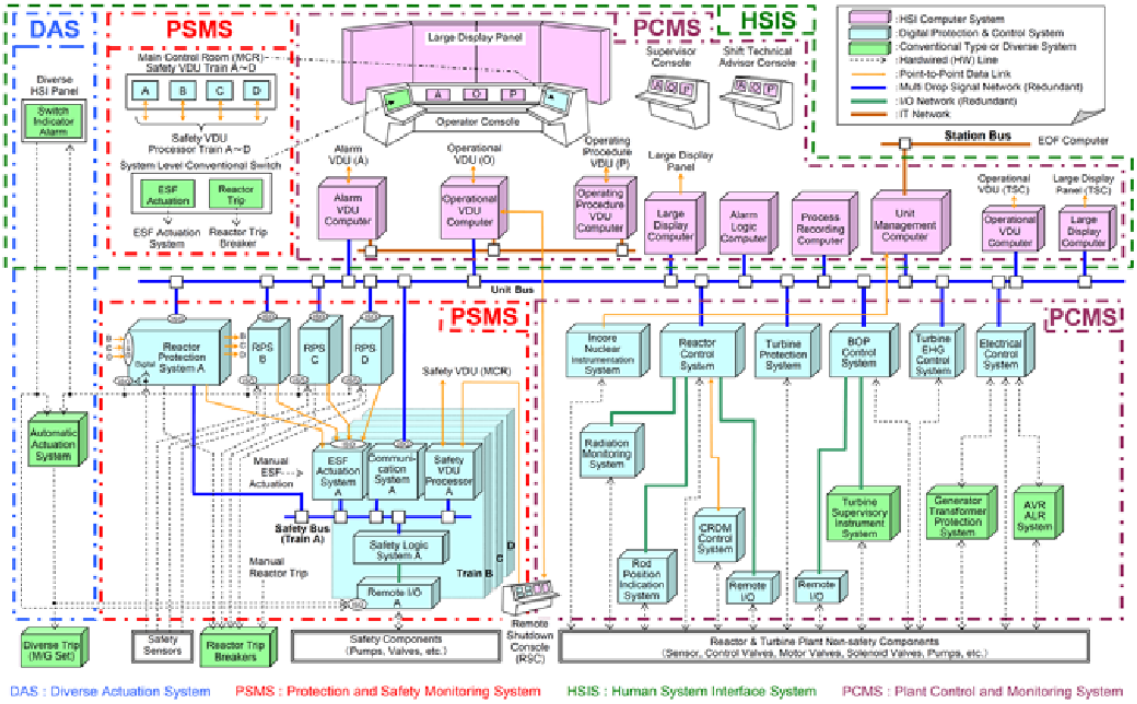


Abb. 2.8 Leittechnikarchitektur einer generischen APWR-Anlage /IAE 13/

Die Signalverarbeitung vom Eingangssignal bis zur Ansteuerung erfolgt in jeder Redundanz durch zwei Prozessoren. Dabei wird funktionelle Diversität der Signalverarbeitung (u. a. unterschiedliche Parameter, unterschiedliche Logik) in den zwei Prozessoren umgesetzt. Diese Strategie unterstützt die Möglichkeit der Instandhaltung dieser Systeme während des Betriebs der Reaktoranlage.

Die rechnerbasierte Warte des APWR soll nach einem sogenannten Kompaktdesignkonzept realisiert werden (siehe Abb. 2.9).

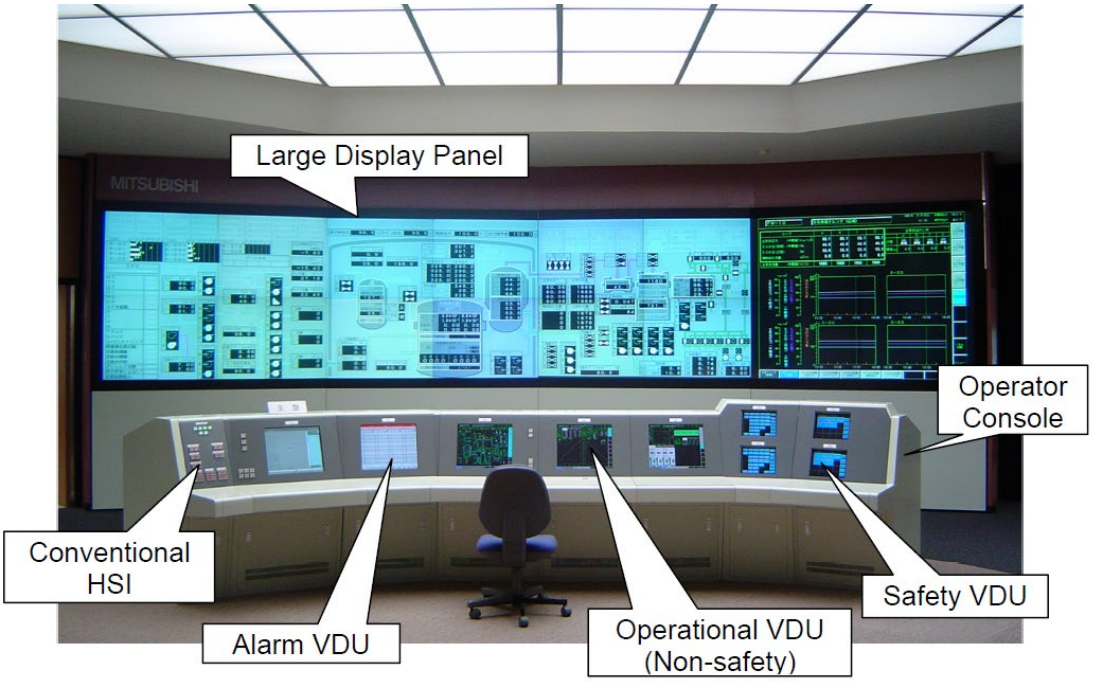


Abb. 2.9 Rechnerbasierte Warte des APWR /IAE 13/

In der Warte kann der Operator über einem Touchscreen sowohl betriebliche als auch sicherheitsrelevante Komponenten betätigen. Für einige sicherheitsrelevante Komponenten sind konventionelle Betätigungselemente (Tasten) vorgesehen.

Die MELTAC-Plattform wird bereits in folgenden Kernkraftwerken in Japan eingesetzt:

- Tomari-3 (Erstinbetriebnahme 2009),
- Ikata-1, -2 (Modernisierung der Leittechnik 2009),
- Takahama-1, -2, -3, -4 (Modernisierung der Leittechnik 2009-2012),
- Ohi-1, -2, -3, -4 (Modernisierung der Leittechnik 2009-2013).

2.5 Leittechnikkonzept von EPR-Anlagen

Der EPR ist eine Baureihe von Druckwasserreaktoren, die gemeinsam von den französischen Unternehmen Framatome und Électricité de France (EDF) sowie der deutschen Siemens AG entwickelt wurde. Framatome gehörte zwischen 2001 und 2017 zum Areva-Konzern, während Siemens seine Nuklearsparte seit 2001 in eine Partnerschaft mit Framatome eingebracht hat. Areva wurde später in verschiedene Konzerne aufgeteilt, wobei Framatome die Reaktorbausparte übernahm. Ursprünglich stand die Abkürzung EPR

für "European Pressurized Reactor" oder "European Pressurized Water Reactor" (Europäischer Druckwasserreaktor). Im internationalen Markt wurde die Technologie auch als "Evolutionary Power Reactor" vermarktet. Heutzutage wird die Abkürzung EPR meist als eigenständiger Markenname verwendet, während die vollständigen Bezeichnungen kaum noch gebräuchlich sind /WIK 25/. Mittlerweile wurde bereits eine neuere Generation (EPR-1750) entwickelt und in China (KKW Taishan-1/2) auch in Betrieb genommen.

Bereits in der EPR-Konzeptphase wurde der Einsatz digitaler Leittechnik auf allen Sicherheitsebenen vorgesehen. Aus diesem Grund wurde für die sicherheitsrelevanten Leittechnikfunktionen des EPR die digitale Leittechnikplattform Teleperm XS (TXS) entwickelt, deren Software und Hardware der höchsten Anforderungskategorie (Kategorie A, /DIN 22/) genügen. Allgemein wurde hierbei TXS auch für andere neue Reaktoranlagen sowie zur Ertüchtigung und Modernisierung bestehender Anlagen konzipiert. Seit der ersten Inbetriebnahme vor mehr als 30 Jahren wird TXS in vielen Kernkraftwerken für unterschiedliche Leittechnikfunktionen weltweit eingesetzt.

Bei der Auslegung von TXS wurden folgende Hauptmerkmale festgelegt:

- Systemplattform der Hard- und Software des TXS wird entwickelt für sicherheitstechnische Anwendungen in Kernkraftwerken.
- Systemeigenschaften des TXS stellen deterministisches Verhalten sicher, einschließlich erforderlicher Robustheit und Zuverlässigkeit, insbesondere durch folgende Merkmale:
  - Zyklischer Betrieb (Rechner, Netzwerke) der Signalverarbeitung,
  - Trennung von System- und Anwendungssoftware,
  - Funktionsweise der Systemsoftware unabhängig vom Anlagenzustand,
  - Entwicklung und Qualifizierung der Systemsoftware-Komponenten nach der höchsten Anforderungskategorie.

Wesentliches Element der Auslegung der Sicherheitsleittechnik bezüglich Fehlerbeherrschung sind die internen Überwachungsmechanismen. Folgende interne Überwachungsmechanismen des TXS stehen hierfür zur Verfügung:

- Zyklische Selbsttests der Verarbeitungseinheiten und der Ein- und Ausgabebaugruppen (E/A-Baugruppen) prüfen Prozessoren und Speicherbausteine,

- ein Hardware-Watchdog (Überwachungseinrichtung) auf jeder Verarbeitungseinheit und auf jeder E/A-Baugruppe überwacht den zyklischen Betrieb,
- jede Verarbeitungseinheit und jede E/A-Baugruppe überwacht ihre Kommunikationspartner anhand der Integrität der gelieferten Daten und der regelmäßigen Datenaktualisierung,
- bei erkannten Ausfällen von Verarbeitungseinheiten werden die angeschlossenen Ausgangsbaugruppen stromlos geschaltet.

Das Leittechnikkonzept einer generischen EPR-Reaktoranlage (siehe Abb. 2.10) basiert neben TXS für Sicherheitsfunktionen auch auf der Leittechnikplattform SPPA-T2000[4] für betriebliche Funktionen /NRC 04/. Die Gesamtleittechnikarchitektur umfasst hierbei ein primäres Sicherheitssystem, ein digitales Backup-System mit reduziertem Umfang der Sicherheitsleittechnikfunktionen und ein festverdrahtetes Backup-System, das im Wesentlichen auf FPGA-Bausteinen[5] basiert. Die Realisierung des Backup-Funktionen kann in verschiedenen EPR-Anlagen auch unterschiedlich realisiert werden, so z. B. mit einem analogen und/oder digitalen Backup-System. Die Reaktorschnellabschaltfunktion und andere Schutzaktionen sind im Reaktorschutzsystem (Protection System PS in Abb. 2.10) realisiert.

In jeder Redundanz des Reaktorschutzsystems sind zwei funktional diversitäre Teilsysteme A und B vorhanden, die auf unterschiedliche Anlagenparameter zugreifen. Jede Redundanz besitzt fünf Erfassungs- und Verarbeitungseinheiten (APU), die jeweils dem Teilsystem A oder dem Teilsystem B zugeordnet sind. Über Glasfaserverbindungen (LWL – Lichtwellenleiter) werden die gebildeten Auslösesignale der APUs in einem Teilsystem an die korrespondierenden Teilsysteme in den anderen drei Redundanzen übertragen. Jedem Teilsystem innerhalb einer Redundanz sind zwei Logikeinheiten (Actuator Logic Units) zugeordnet, die redundant eine 2-von-4-Auswahl vornehmen. Innerhalb der Logik für die Auslösung von Schutzaktionen sind diese Voter mit einem logischen ODER

---

[4] Ehemals Teleperm XP (TXP), eine Leittechnikplattform der Siemens AG. Aktuell wird die Plattform SPPA-T2000 von Siemens Energy weiterentwickelt und vertrieben.

[5] Ein FPGA (Field Programmable Gate Array) ist ein frei programmierbarer, digitaler Schaltkreis, der logische Funktionen flexibel in Hardware abbilden kann. Auf einem FPGA läuft keine Software im klassischen Sinne – stattdessen wird die Hardware selbst durch eine konfigurierbare Logikschaltung programmiert. FPGAs führen demnach keine Befehle wie Prozessoren aus, sondern arbeiten auf Basis von Hardwarebeschreibungen (z. B. in VHDL – VHSIC: Hardware Description Language, wobei VHSIC für Very High Speed Integrated Circuit steht), die festlegen, wie die internen logischen Schaltungen miteinander verbunden werden. Siehe z. B. /ROD 15/.

verknüpft, um auch dann eine Schutzaktion auslösen zu können, wenn ein Voter versagt. Im Fall der Logik für die Auslösung einer Reaktorschnellabschaltung (RESA) sind die Voter mit einem logischen UND verknüpft, um Fehlanregungen von RESAs zu vermeiden (Verfügbarkeit). Die RESA-Auslösesignale der einzelnen Redundanzen öffnen unterschiedliche Leistungsschalter in der Energieversorgung der Steuerstäbe.

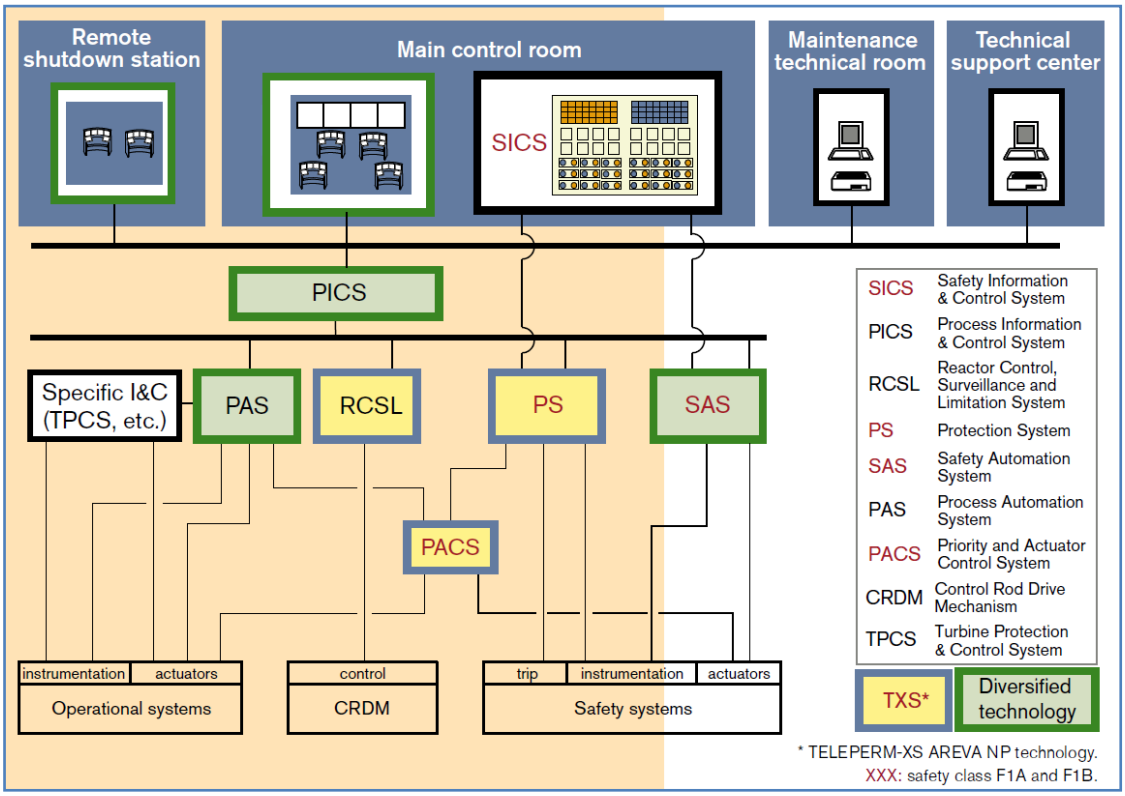


Abb. 2.10 Funktionsdiagramm der Leittechnik einer generischen EPR-Anlage /IAE 18/

Die leittechnischen Einrichtungen der Betriebsleittechnik, die keine direkte Sicherheitsfunktion erfüllen, nutzen die SPPA-T2000-Plattform. Innerhalb dieser Leittechnik dient das zweifach redundant ausgeführte Safety Automation System (SAS) als Backup des Reaktorschutzsystems (bzw. PS für „Protection System“ in der Abbildung) für die Auslösung von Schutzaktionen bei ausgewählten auslösenden Ereignissen.

Für EPR-Anlagen existieren zusätzlich weitere unterschiedliche Konzepte zur Risikominimierung. Hierfür sind sowohl automatische als auch Handmaßnahmen für die Durchführung von erforderlichen Funktionen vorgesehen, die in einem speziellen Backup-System realisiert werden. Framatome hat dafür verschiedene Konzepte entwickelt, die Anforderungen zur Beherrschung potenzieller systematischer Fehler in der software-basierten Leittechnik berücksichtigen. Einige Backup-Funktionen wurden auf der Basis der

speziellen nicht software-basierten Baugruppen der TXS-Plattform realisiert. Für die komplexen Anforderungen wurden die analogen Leittechniksysteme Unicorn und Hardline entwickelt.

2.6 Leittechnikkonzept von ESBWR-Anlagen

Der Economic Simplified Boiling Water Reactor (ESBWR) ist ein Reaktordesign der Generation III+ mit teilweise passiven Sicherheitsfunktionen (d. h. Funktionen, die keine externe Energieversorgung benötigen), das auf seinen Vorgängern, dem Simplified Boiling Water Reactor (SBWR) sowie dem Advanced Boiling Water Reactor (ABWR), basiert. Alle diese Designs stammen aus der Kooperation von General Electric (GE) und Hitachi Nuclear Energy (GEH).

Das Konzept der Sicherheitsleittechnik des ESBWR wurde u. a. auf Basis des Vorgängers ABWR entwickelt, wobei die digitale Leittechnik-Plattform NUMAC (Nuclear Measurement Analysis and Control) zum Einsatz kommt (siehe Abb. 2.11). Die Leittechnikarchitektur ist wie folgt aufgebaut und beinhaltet

- vier Redundanzen zur Reaktorschnellabschaltung,
- vier Redundanzen des ESFAS-Systems,
- vier Redundanzen der alternativen Reaktorschnellabschaltung,
- eine dreifach redundante Struktur der Prozessorlogik der diversitären Leittechnik,
- eine dreifach redundante Struktur der wichtigsten Reaktorregelungen,
- eine dreifach redundante Struktur der Verfügbarkeits-Leittechnik.

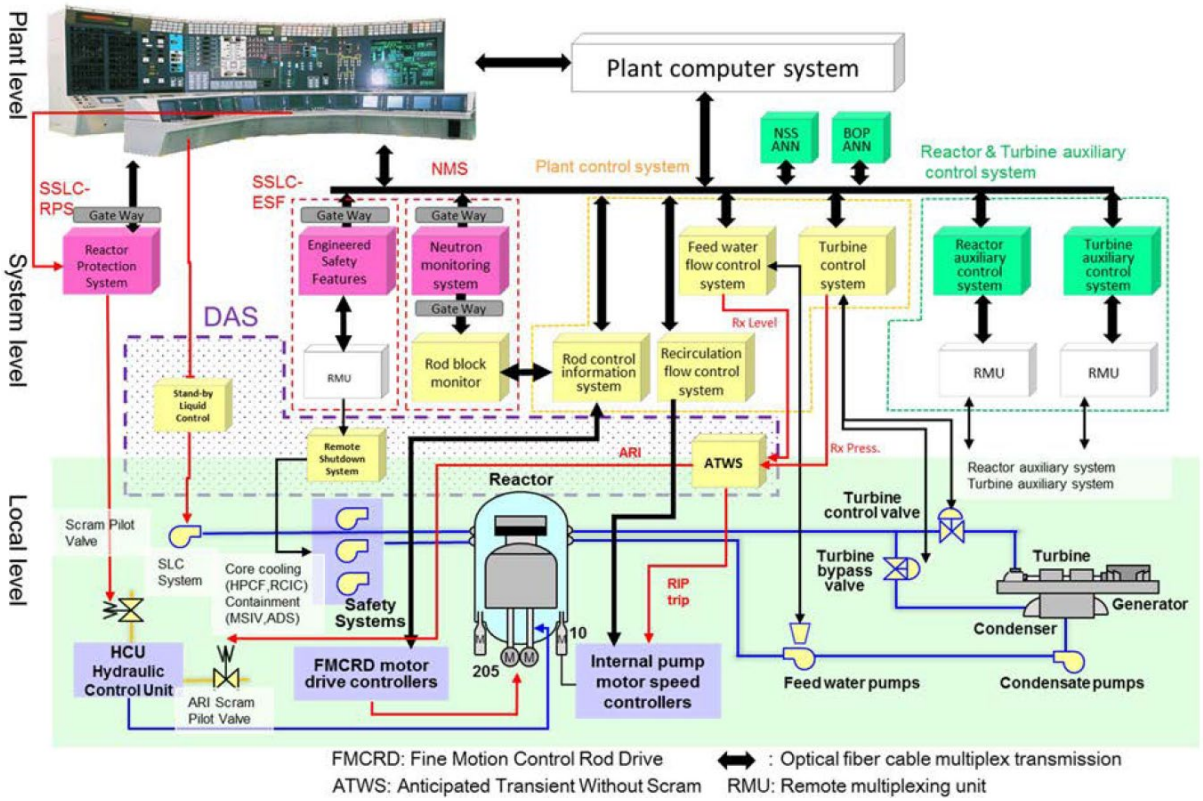


Abb. 2.11 Leittechnikarchitektur einer generischen ABWR-Anlage /IAE 18/

Die Reaktorschnellabschaltung (RESA) des ESBWR hat folgende Merkmale:

- jede RESA-Anregung in jeder Redundanz des Reaktorschutzsystems erfolgt durch eine 2-von-4-Auswahl der redundanten Signale, wobei die Redundanzen miteinander über Kommunikationslinks (LWL-Kabel) kommunizieren,
- konsequente Anwendung des Fail-Safe-Prinzips für die Anregung der Reaktorschellabschaltung,
- definiertes Ausfallverhalten.

Zur Beherrschung von GVA in der Hard- und Software der Sicherheitsleittechnik wird eine funktional und strukturell gestaffelte Diversifizierung der Leittechnik angewendet (Abb. 2.12).

Safety category	*Safety-related DCIS (Q-DCIS)*		*Non-safety-related DCIS (N-DCIS)*		
System families	RPS/NMS	SSLC/ESF	DPS	Nuclear control systems, BOP, DCIS	Plant computer
Architecture families	*Divisional*		*Triple modular redundant*		*Work station*
	NUMAC	Triconex	GE-Mark VIe		

Notes: RPS: Reactor Protection System; SSLC: Safety System Logic and Control; DCIS: Distributed Control and Information System; BOP: Balance of Plant; NMS: Neutron Monitoring System; ESF: Engineered Safety Features; DPS: Diverse Protection System.

Abb. 2.12 Defense-in-Depth-Konzept der Leittechnik des ESBWR /IBR 14/

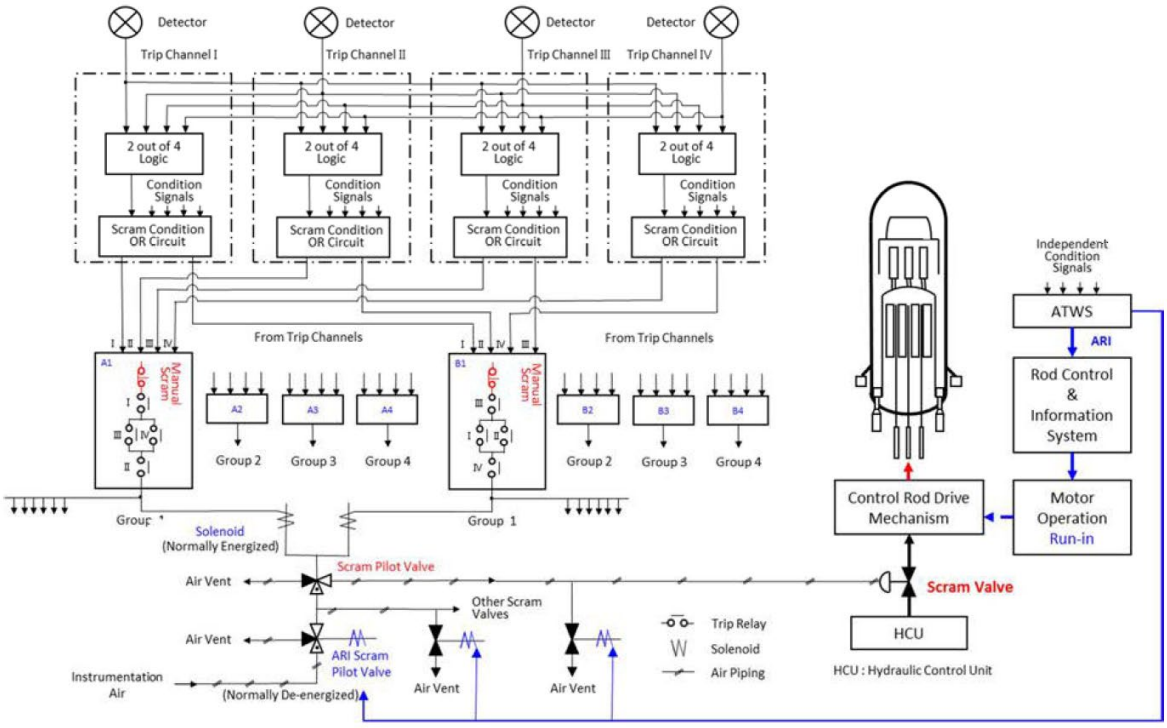


Abb. 2.13 Struktur der RPS-Leittechnik der Reaktorschnellabschaltung /GEH 09/

Die Auslösung der RESA und die Containment-Isolationsfunktion wurden mit der NUMAC-Plattform von GE (General Electric) realisiert. Das System ist vierfach redundant aufgebaut. In jeder Redundanz werden die erfassten Messdaten von Remote Multiplexing Units an sogenannte Digital Trip Modules übertragen, wo die Signalverarbeitung erfolgt. Die gegebenenfalls gebildeten Auslösesignale werden an die Trip Logic Units in allen Redundanzen übermittelt, welche je eine 2-von-4-Auswahl vornehmen.

Das ESFAS beinhaltet weitere Sicherheitsfunktionen, u. a. Funktionen zur Kernkühlung. Das System besteht aus vier Redundanzen für die Auslösung von Sicherheitsfunktionen (siehe Abb. 2.14) sowie einem weiteren Kanal für die Anforderung zusätzlicher Notstromdiesel. Die vier ESFAS-Redundanzen kommunizieren über Glasfaserverbindungen mit dem Reaktorschutzsystem sowie auch untereinander. Die Schutzaktionen werden nach einer 2-von-4-Auswahl ausgelöst. Die ESFAS-Leittechnik basiert auf einem Mikroprozessor-basierten System von DRS Technologies[6] /DRS 25/.

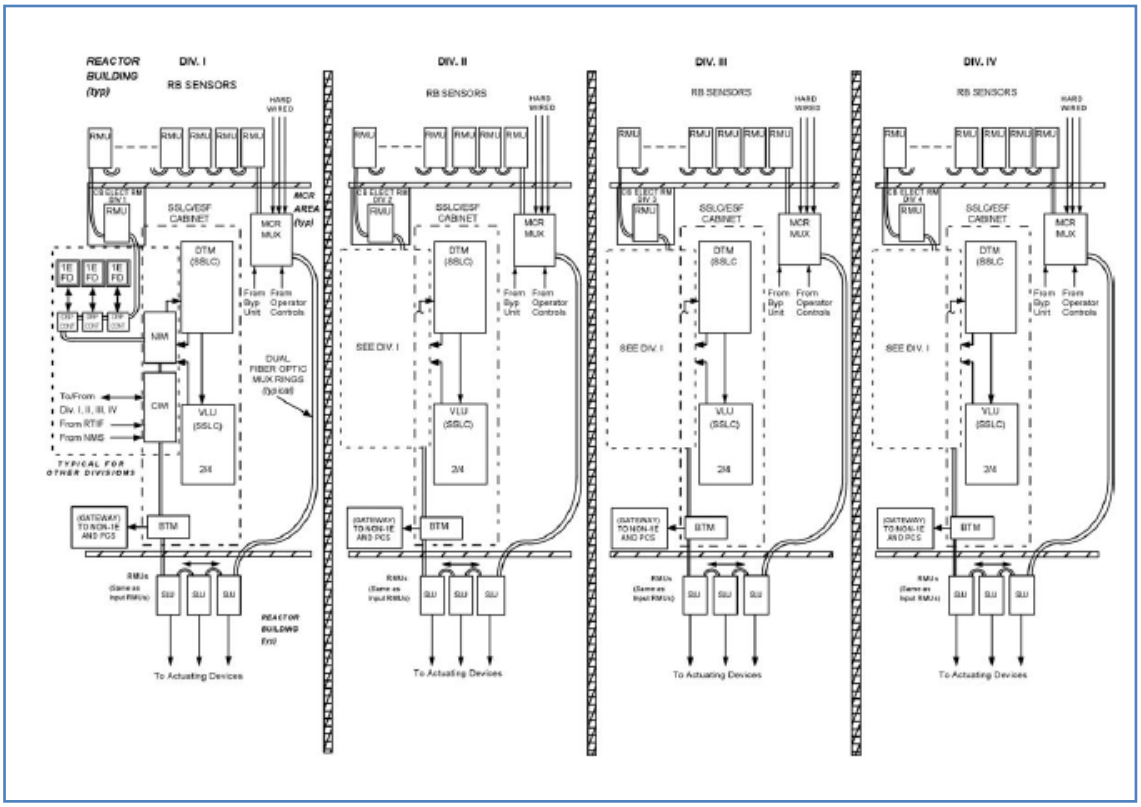


Abb. 2.14 Struktur des ESFAS des ESBWR /GEH 09/

Das gestaffelte Sicherheitskonzept des ESBWR sieht ein zusätzliches Backup-System für ATWS[7]-Ereignisse vor, welches im Anforderungsfall die Schnellabschalt- und Sicherheitsfunktionen übernehmen kann (siehe Abb. 2.15). Die entsprechende Leittechnik hierfür soll in Schränken zur Reaktorschnellabschaltung bzw. ESFAS-Sicherheitsleittechnik untergebracht werden, wobei deren Signalverarbeitung keine Gemeinsamkeiten mit der

[6] Der aktuelle Name lautet Leonardo DRS.

[7] ATWS – Anticipated Transient Without SCRAM, d. h. eine Störung der Wärmeabfuhr bei gleichzeitigem Versagen der Reaktorschnellabschaltung.

anderen Sicherheitsleittechnik hinsichtlich Hardware, Software und Instrumentierung hat.

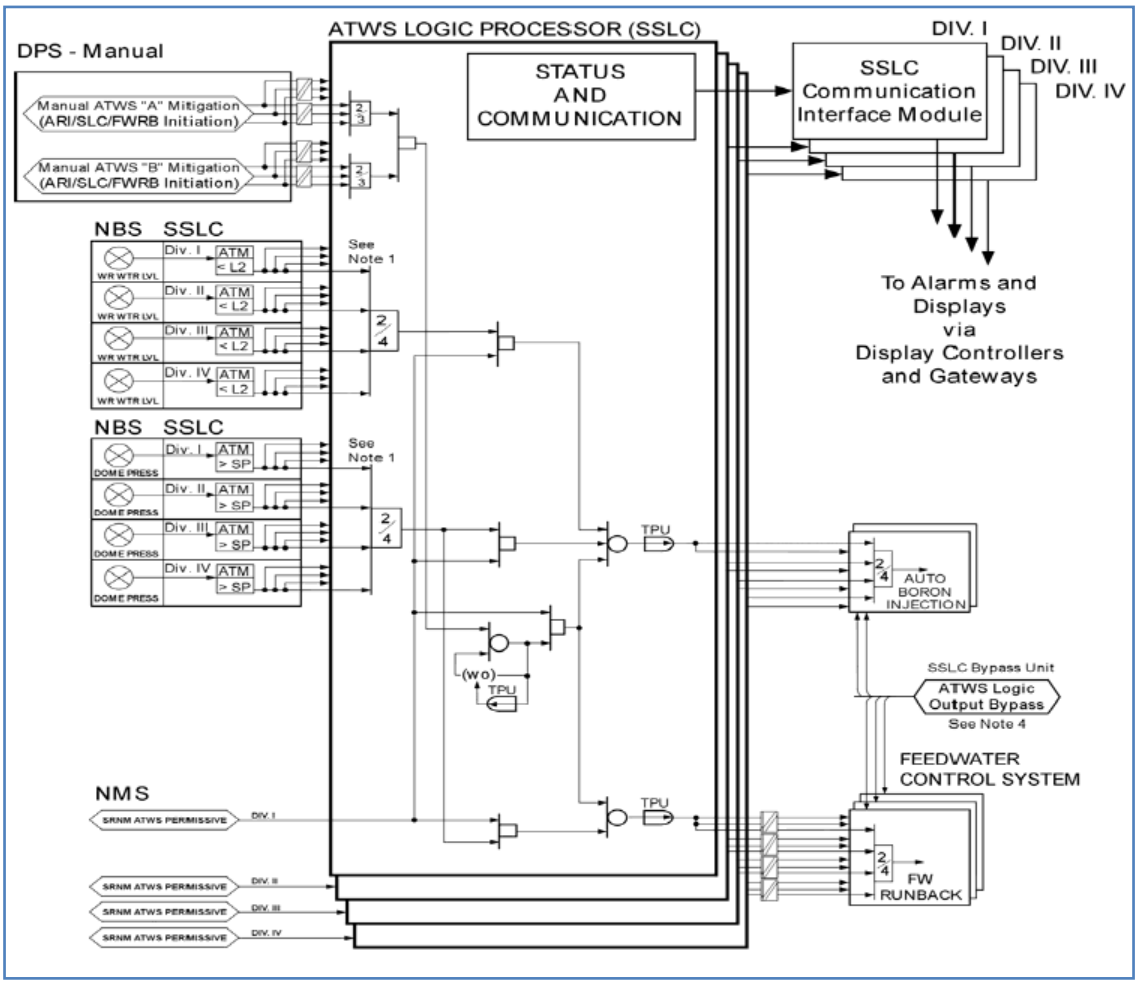


Abb. 2.15 Signalverarbeitung für ATWS des ESBWR /GEH 09/

Die ATWS-Logik des ESBWR ist auf der Basis der TRICON-Leittechnikplattform aufgebaut. Die Entwicklung von TRICON durch die Firma Foxboro begann im Jahr 1986. Foxboro wurde später, wie auch einige weitere Firmen, durch den Konzern Invensys übernommen. 2014 wurde Invensys von Schneider Electric übernommen. Schneider Electric liefert auf Basis der TRICONEX-Systemplattform Produkte, Systeme und Services zur Sicherheit moderner Produktionsanlagen, zur Verarbeitung und Überwachung kritischer Regelungen sowie für Anwendungen im Turbinenbereich. TRICONEX ist für industrielle Anwendungen konzipiert und bis Sicherheitsstufe SIL-3 gemäß Standard IEC 61508 /IEC 98/ zertifiziert.

Tab. 2.3 enthält eine Übersicht über die TRICON-Hardware, die in den USA für den Einsatz in KKW qualifiziert wurde /NRC 01/.

Tab. 2.3 Übersicht TRICON-Hardware

Module	Type Model	Description
Chassis	8110N	Main Chassis
	8111N	Expansion Chassis
	8112N	Remote Expansion Chassis
Main Processor	3006N	Enhanced Main Processor 11, V9, 2 Mb
Remote Extender	4210N	Remote Extender Module (Primary)
	4211N	Remote Extender Module (Remote)
Communication	4119AN	Enhanced Intelligent Communications Module (EICM) V9, isolated
	4329N	Network Communications Module (NCM), V9
	4609N	Advanced Communications Module (ACM)
Analog Input	3700AN	Analog Input (AI) Module, 0/5 Vdc, 6% Overrange
	3701N	AI Module, 0/10 Vdc
	3703EN	Enhanced Isolated Analog Input (EAI) Module
	3704EN	High-Density Analog Input (HDAI) Module, 0-5/0-10 Vdc
Analog Output	3805EN	Analog Output Module, 4/20 mA
Digital Input	3501TN	Enhanced Digital Input (EDI) Module, 115V ac/dc
	3502EN	EDI Module, 48V ac/dc
	3503EN	EDI Module, 24V ac/dc
	3504EN	High-Density Digital Input (HDDI) Module, 24/48 Vdc
	3505EN	EDI Module, 24 Vdc, Low-Threshold
Digital Output	3601TN	Enhanced Digital Output (EDO) Module, 115 Vac
	3603TN	EDO Module, 120 Vdc
	3604EN	EDO Module, 24 Vdc
	3607EN	EDO Module, 48 Vdc
	3623TN	Supervised Digital Output (SDO) Module, 120 Vdc
	3624N	SDO Module, 24 Vdc
Pulse Input	3510N	Pulse Input Module
Thermocouple Input	3706AN	Non-Isolated Thermocouple (NITC) Input Module
	3708EN	Isolated Thermocouple (ITC) Input Module
Relay Output	3636TN	Enhanced Relay Output (ERO) Module, Simplex
Power Supply	8310N	120 Vac/DC Power Supply
	8311N	24 Vdc Power Supply

TRICON[8] soll sowohl bei auftretenden Hardwarefehlern der Komponenten als auch bei externen Störungen eine fehlerfreie, unterbrechungsfreie Steuerung ermöglichen. Ein TRICON-System setzt sich aus einem Hauptgehäuse und bis zu 14 lokalen oder dezentralen Erweiterungsgehäusen zusammen. Die maximale Systemgröße besteht aus 15

[8] TRICONEX bezeichnet die gesamte Produktfamilie sicherheitsgerichteter Steuerungssysteme von Schneider Electric. Innerhalb dieser Familie ist TRICON das klassische TMR-System, welches auch NRC-qualifiziert ist.

Gehäusen sowie insgesamt 118 E/A- und Kommunikationsmodulen (letztere als Schnittstellen zu Fremdsystemen).

TRICON ermöglicht die Kommunikation durch Master- und Slave-Module (MODBUS-Netzwerk) mit externen Prozessleitsystemen, mit externen Hostrechnern über Ethernet-Netzwerke sowie mit anderen TRICON-Geräten über ein Peer-to-Peer-Netzwerk. Die Leittechnikfunktionen eines TRICON-Systems werden mittels systemeigener Werkzeuge in ein Zielsystem implementiert.

Die TriStation 1131 Developer's Workbench ist ein integriertes Werkzeug zur Entwicklung, Prüfung und Dokumentation der sicherheitsgerichteten und kritischen Leittechnikanwendungen für die speicherprogrammierbaren Steuerungen TRICON und Trident.

Die TRICON-Leittechnik basiert auf einer Architektur mit dreifacher Modulredundanz (Triple-Modular Redundancy, TMR). Bei dieser TMR-Architektur sind drei galvanisch getrennte, parallel arbeitende Steuerungssysteme und umfangreiche Diagnosefunktionen zu einem System integriert (siehe Abb. 2.16). Das System verwendet eine 2-von-3-Auswahlschaltung und ermöglicht eine Signalverarbeitung, bei der auch mehrere Einzelfehler in der Hardware zu keinem Gesamtausfall führen können /NRC 01/.

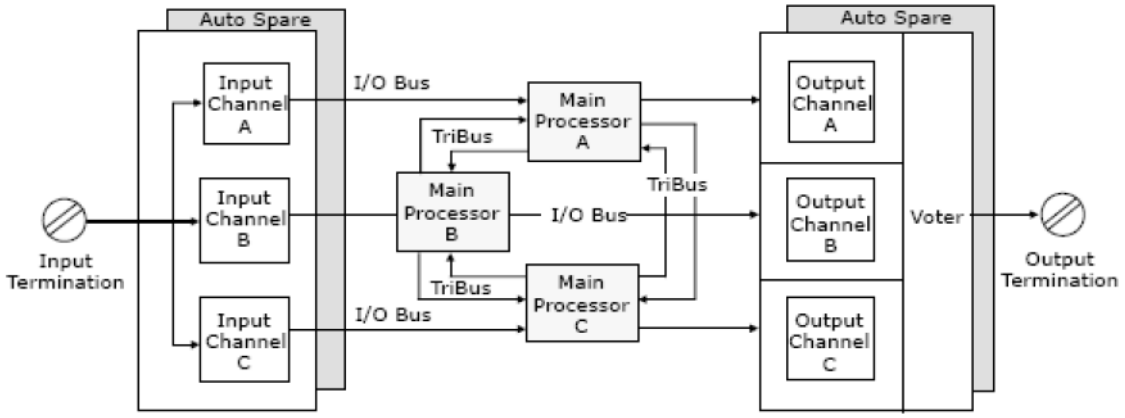


Abb. 2.16 TMR-Architektur der TRICON-Leittechnik /TRI 11/

Leistungsmerkmale des TMR-Konzepts sind /NRC 01/:

- Kein Ausfall durch Einzelfehler einer TMR-Komponente – die Störung einzelner Komponenten beeinträchtigt nicht die Funktion des TRICON-Systems.

- Hochgeschwindigkeits-Verarbeitung – in TRICON (V9.6) arbeiten zwei Prozessoren vom Typ Motorola MPC860.
- Flexibilität im Design – das TRICON-System kann nach den jeweiligen Anforderungen konfiguriert werden.
- Hohe Sicherheitsintegrität – dank seiner TMR-Architektur und den umfangreichen Diagnosefunktionen erreicht das TRICON-System die Sicherheitsstufe SIL-3. TRICON-Systeme wurden durch den TÜV (TÜV-Rheinland, 2001) für den sicherheitsgerichteten Einsatz in Anwendungen der Anforderungsklassen AK 5 und 6 nach IEC61508 /IEC 98/ zertifiziert.
- Hohe Verfügbarkeit – das TRICON-TMR-System lässt sich mit einem, zwei oder drei funktionalen Hauptprozessoren betreiben. Fehlerhafte Module lassen sich bei laufendem System austauschen und gewährleisten so eine unterbrechungsfreie Steuerung.
- Einfache Programmierung – die Windows-Programmiersoftware von TRICONEX erlaubt die Programmierung über Funktionsblöcke, Ablaufpläne oder Kontaktplanlogik. Das garantiert eine schnelle und einfache Konfiguration sowie Emulation der Programme.
- Umfassende Diagnosen – TRICON-TMR-Systeme bieten Online-Diagnosefunktionen ohne zusätzliche Hardware oder spezielle Anwendungsprogrammierung.

Die Ausgangssignale (Datensätze) der TRICON-Steuerungslogik werden in den Ausgangsmodulen nach 2-von-3-Auswahl (siehe Abb. 2.17) ausgewertet und das Ergebnis über die Ausgangsbaugruppen an die Feldgeräte (z. B. Antriebe, Relais usw.) übermittelt.

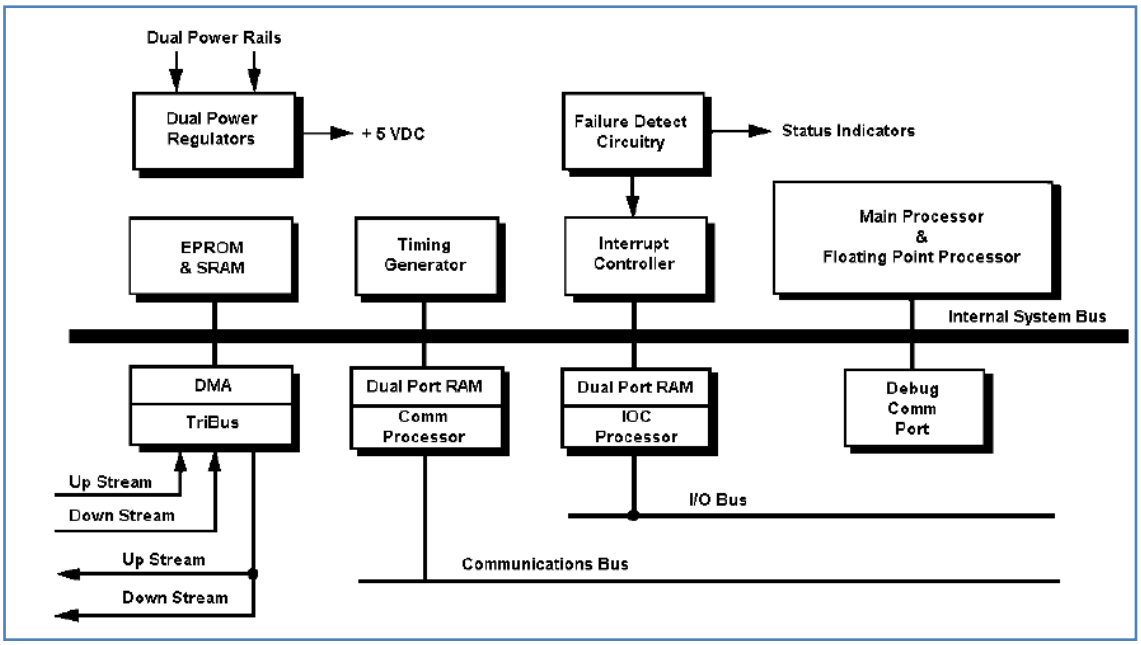


Abb. 2.17 Architektur des Hauptprozessors /TRI 11/

Das TRICON-Leittechniksystem nutzt generell drei Typen von Software:

- Systemsoftware (sicherheitsrelevant, qualifiziert),
- Anwendungssoftware (funktionsspezifische, sicherheitsrelevante Software),
- Entwicklungs-Software (TriStation 1131) für die Anwender-Software.

Die Systemsoftware befindet sich im EEPROM-Speicher der Prozessorbaugruppen, der Ein- bzw. Ausgangssignalbaugruppen und der Kommunikationsbaugruppen. Jedes TRICONEX System besteht aus drei Prozessorbaugruppen mit identischer Software. Jeder Hauptprozessor führt folgende Diagnose, bzw. Selbsttestfunktionen aus (siehe Abb. 2.18):

- Systemstartcheck, Speicher-, Taktgeber- und Kommunikationstest,
- Hintergrunddiagnose: u. a. Prozessorcheck, Interface und Speichertest, Kontrollsummentest (CRC) usw.,
- Überwachung der Signalverarbeitung.

Type	Identification	Ver.	Used in
Main Micro Processors	TSX	5211	3006N Enhanced main processor II
	IOC	5212	3006N Enhanced main processor II
	COM	5206	3006N Enhanced main processor II
Communication	ICM	4930	4119AN EICM, V9, Isolated 4329N Network Communication Module 4609N Advanced Communication Module
	ACMX	5203	4609N Advanced Communication Module
	NCMX	5028	4329N Network Communication Module
	IICX	5276	4119AN EICM, V9, Isolated
	RXM	3310	4210N Remote Extender Module, Primary 4211N Remote Extender Module, Remote
Input/Output	AI/NITC	4873	3700AN AI Module, 0-5 Vdc, 6% Overrange 3701N AI Module, 0-10 Vdc 3706AN NITC Input Module
	EIAI/ITC	5491	3703EN EAI Module, Isolated 3708EN ITC Thermocouple Input Module
	PI	4559	3510N Pulse Input Module
	EDI	5490	3501TN EDI Module, 115V ac/dc 3502EN EDI Module, 48V ac/dc 3503EN EDI Module, 24V ac/dc 3505EN EDI Module, 24 Vdc, Low Threshold
	HDI	5499	3704EN HDDI Module, 24/48 Vdc 3504EN HDAI Module, 0-5/0-10 Vdc
	EAO	5595	3805EN Analog Output Module, 4-20 mA
	EDO	5488	3601TN EDO Module, 115 Vac 3604EN EDO Module, 24 Vdc 3607EN EDO Module, 48 Vdc
	ERO	5497	3636TN ERO Module, N.O., Simplex
	TSDO	5502	3603TN EDO Module, 120 Vdc 3623N SDO Module, 120 Vdc 3624N SDO Module, 24 Vdc

Abb. 2.18 TRICON-Baugruppen /NRC 01/

Die TRICON-Software wird als Endlosschleife im Zielsystem ohne Zeitbezug ausgeführt. Die Interrupts werden nur für spezielle Funktionen verwendet, u. a. Watchdog-Funktionen, Fehlerdiagnoseprozeduren.

Die Entwicklungssoftware TriStation 1131 wird in einer Windows-Umgebung ausgeführt. Diese Software generiert die Anwendungssoftware (Leittechnikfunktionen) eines TRICON-Leittechniksystems. Die Rechner mit der TriStation-Software sind nicht mit dem TRICON-System beim Betrieb der Reaktoranlage verbunden und werden nur während Instandhaltung bzw. Reparatur mit dem Zielsystem verbunden.

Beim ESBWR werden außerdem einige sicherheitsrelevante Leittechnikfunktionen auf der Basis der Mark-Vle-Leittechnikplattform implementiert (siehe Abb. 2.19), diese ermöglichen:

- Automatisches Anfahren der Reaktoranlage aus dem „kalten Zustand“,
- Leistungsbetrieb der Reaktoranlage,
- Abfahren der Reaktoranlage,
- weitere nicht-sicherheitsrelevante Funktionen wie Monitoring, Regelungen usw.

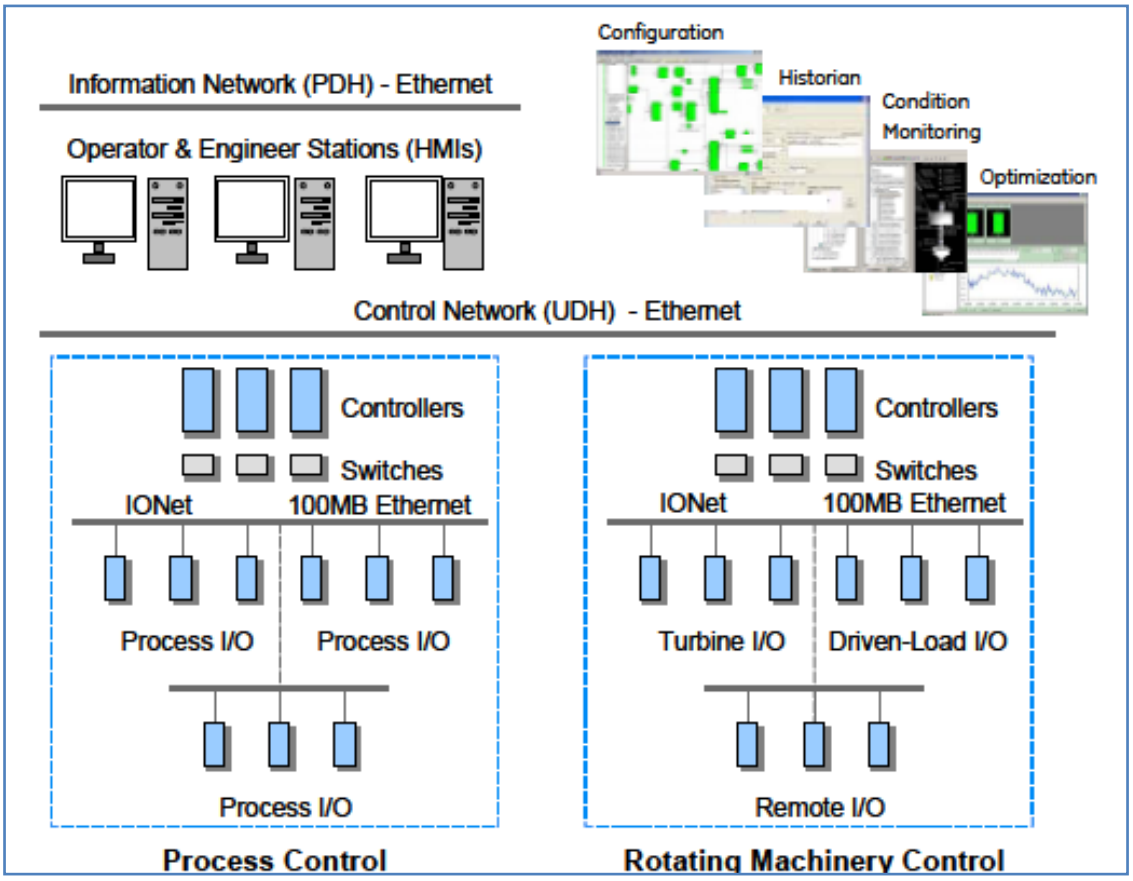


Abb. 2.19 Typische Struktur des Mark-VIe-Systems /GEH 09/

Die Mark-Vle-Leittechnik der Firma General Electric unterscheidet sich wesentlich in der Hard- und Software von der TRICON-Leittechnik. Die Mark-Vle-Leittechnik ist betriebsbewährt und ist bereits in den Anlagen älterer Generationen und in konventionellen Kraftwerken als Automatisierungssystem im Einsatz.

Wichtige Leistungsmerkmale der Mark-Vle-Leittechnik sind:

- 32-bit Prozessor auf dem VME-Board,
- QNX-Betriebssystem,
- Ethernet-Netzwerk-Kommunikation,
- Instandhaltungssoftware Toolbox ST,
- graphische Mensch-Maschine-Schnittstelle CIMPLICITY® auf Basis von Windows,
- Möglichkeiten zum Aufbau einer redundanten Struktur der Leittechnik bis max. dreifacher Redundanz.

2.7 Leittechnikkonzepte aktueller WWER-Anlagen

Die Produktion der TPTS-NT-Leittechnik für WWER-Anlagen begann im Jahr 2011. Sie wurde auf Basis der Teleperm-ME-Leittechnikplattform entwickelt, die unter Lizenz der Firma Siemens steht. Die Verbesserungen der neuen Generation der TPTS-NT-Leittechnik gegenüber dem Vorgänger TPTS-EM /VNI 17/ betreffen u. a.:

- 32-bit-Mikroprozessor 256 MHz,
- verbesserte Reaktionszeiten des Systems,
- verbesserte Ergonomie der Leittechnikschränke,
- Nutzung von Standardprotokollen der Netzwerkkommunikation: RS-485, Ethernet, CAN-Bus, PROFIBUS, PROFINET,
- Flexibilität der Leittechnikkonfiguration: u. a. 2-fach redundante Stromversorgung (z. B. AC 176 – 242 V) der Leittechnikschränke, wahlweise entweder Wechsel- oder Gleichstromversorgung.

Abb. 2.20 zeigt eine Übersicht zur Entwicklung der TPTS-Leittechnik (Hersteller VNIIA /VNI 25/) und deren Einsatz in den verschiedenen WWER-Anlagen. Einige der darin angegebenen Projekte wurden allerdings verspätet (KKW Nowoworonesch und Leningrad) oder gar nicht realisiert (u. a. KKW Kaliningrad). Aktuell sind die Entwickler und Hersteller der Leittechniksysteme für Kernkraftwerke in Russland unter dem Dachverband

RASU zusammengeschlossen worden. Alle russischen Reaktoranlagen sollen leittechnische und elektrotechnische Komponenten aus eigener Herstellung erhalten, um mögliche Auswirkungen von Sanktionen zu vermeiden.

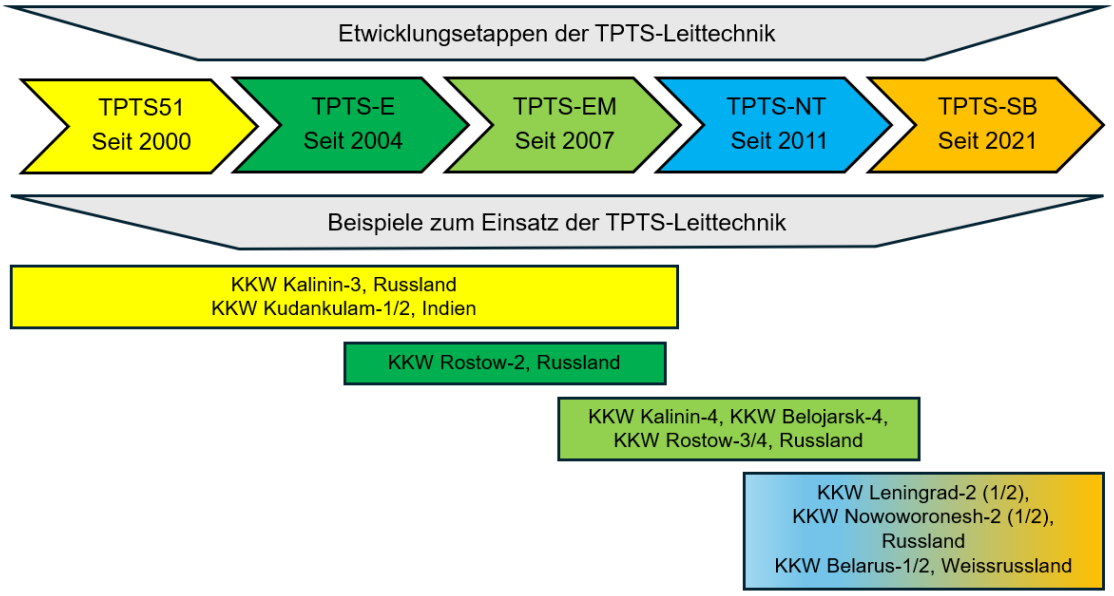


Abb. 2.20 Entwicklung der TPTS-Leittechnik für WWER-Reaktoranlagen (basierend auf /GRS 20/)

Die auf TPTS-NT basierende Plattform für Sicherheitsleittechnik TPTS-SB wurde 2021 in Russland für den Einsatz in den Kernkraftwerken lizensiert /RAS 21/. Dabei wurden wesentliche Verbesserungen der Hard- und Software umgesetzt, um die wachsenden Anforderungen an die Sicherheit und Zuverlässigkeit der Reaktoranlagen zu erfüllen /GRS 20/:

- Embedded-Software für die diversitären Teilsysteme wurde von zwei unabhängigen Entwicklerteams entwickelt,
- es wird kein Betriebssystem in den Rechnern der Signalverarbeitung eingesetzt,
- es wird kein Echtzeitbetrieb und keine Zeitsynchronisation innerhalb der Signalverarbeitung verwendet,
- alle Bestandteile der Hardware werden von einem russischen Hersteller (VNIIA) hergestellt, damit soll die Abhängigkeit von Lieferanten vermieden werden,
- ausschließliche Nutzung von Point-to-Point-Netzwerkkommunikation innerhalb der Signalverarbeitung,

- One-Way-Kommunikation zu den externen Netzwerken (nur Daten- und Informationsausgabe),
- Einschränkung der Nutzerrechte hinsichtlich Konfigurationsmöglichkeiten des Systems und dessen Komponenten.

Im neuen TPTS-SB-System wurde das Prinzip des „gerichteten“ Ausfalls, ähnlich wie beim TXS (Framatome), implementiert. Wichtige Eigenschaften dieses Prinzips sind:

- Bei einem erkannten Ausfall innerhalb des Systems werden alle Ausgangssignale von Baugruppen auf einen definierten „0“-Wert gesetzt.
- Ein fehlerhaftes Prozessormodul wird nach der Erkennung des Ausfalls blockiert und alle betroffenen Signale werden als ungültig markiert und im System nicht weiterverarbeitet.

In Abb. 2.21 ist die generische Architektur der TPTS-SB-Plattform dargestellt.

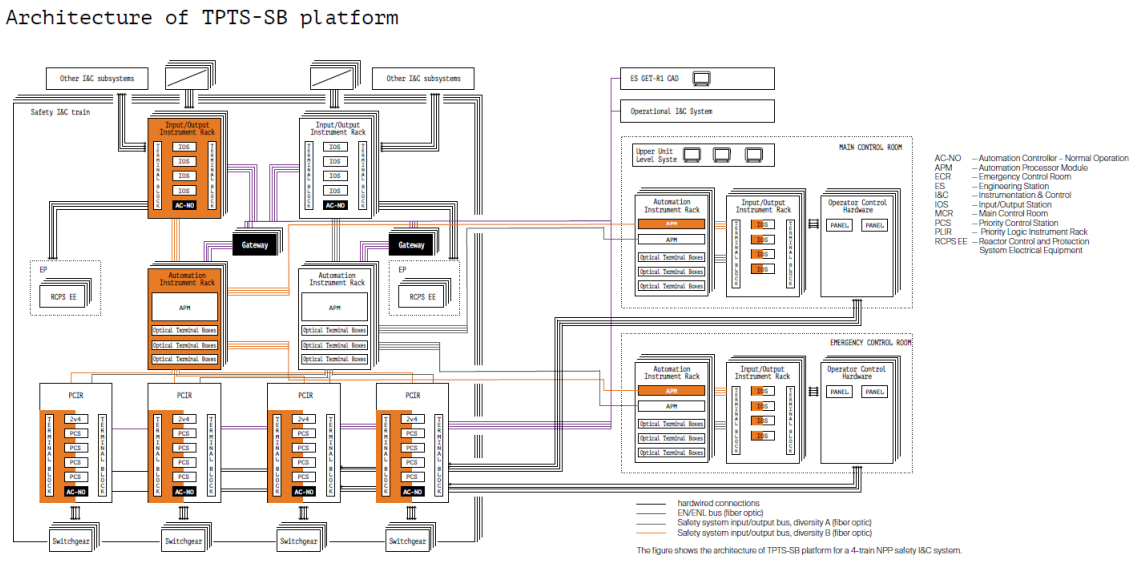


Abb. 2.21 Generische Architektur der TPTS-SB-Plattform /RAS 21/

Als Vorkehrung gegen systematische Ausfälle in der TPTS-SB-Sicherheitsleittechnik wurden die wichtigsten Komponenten des Systems diversifiziert (Abb. 2.22):

- Diversität A
    - Prozessorbaugruppen mit Freescale-/Power-PC400-Prozessoren (basiert auf den Motorola Prozessoren der 68000-Serie)

- FPGA-Bausteine der Firma Altera (ab Werk konfiguriert und können danach nicht mehr verändert werden)

- Diversität B
  - Prozessorbaugruppen des Typs ARM9/400 (System-on-a-Chip-Design: SoC)
  - FPGA-Bausteine der Firma Xilinx (ab Werk konfiguriert und können danach nicht mehr verändert werden)

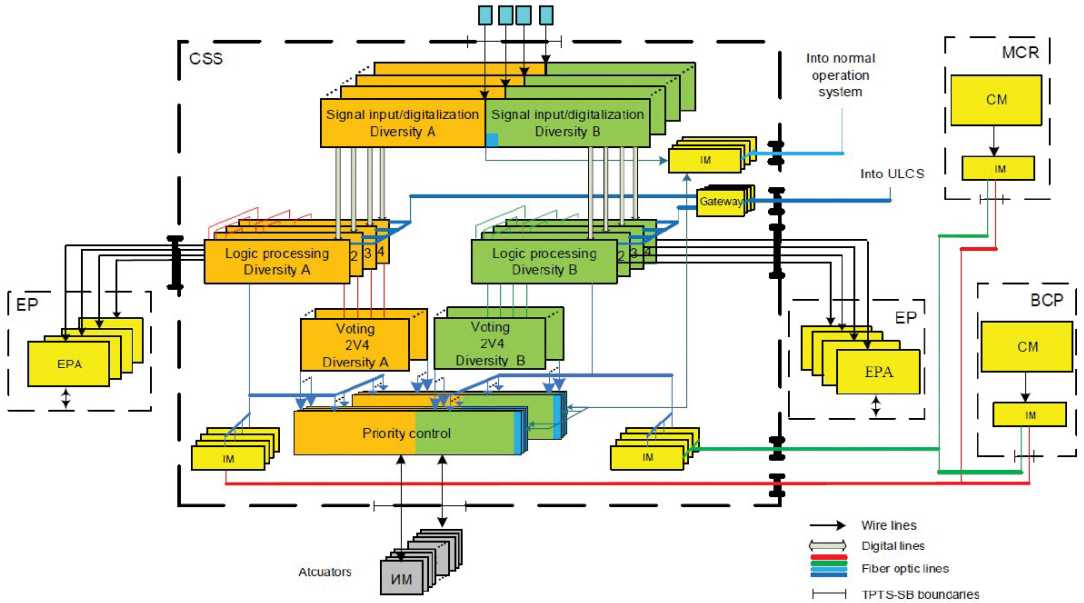
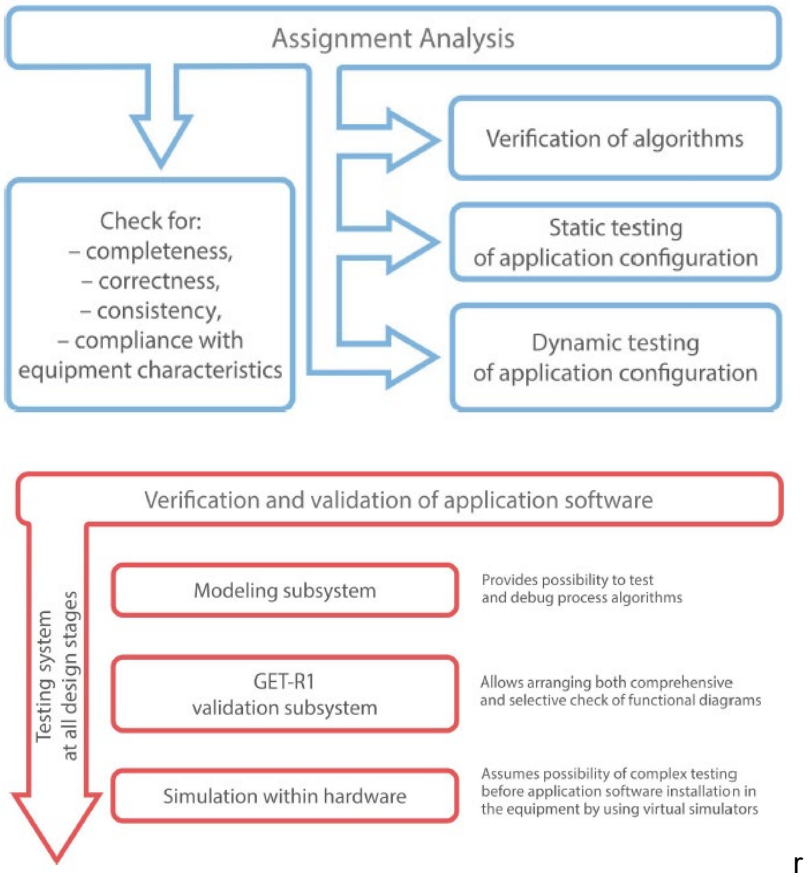


Figure 1. Integrated TPTS-SB-based CSS: EP – emergency protection; MCR – main control room; BCP – backup control panel; ULCS – upper level control system; CSS – control safety system; EPA – emergency protection automatics; IM – interface module; CM – communication module.

Abb. 2.22 Diversifizierung innerhalb der TPTS-SB-Sicherheitsleittechnik /BEL 18/

Die Entwicklung, Dokumentation und Implementierung von Leittechnikfunktionen eines Kernkraftwerks mit TPTS erfolgt mit der Engineering-Umgebung GET-R1 (unter Linux), die Verifizierung und Validierung des entwickelten Leittechniksystems wird durch automatisierte Werkzeuge realisiert /VNI 17/ (Abb. 2.23).



r

Abb. 2.23 Verifizierung und Validierung der Software und Konfiguration eines TPTS-Leittechniksystems /VNI 17/

Die Weiterentwicklung der WWER-Anlagen hinsichtlich Erhöhung der Sicherheit und der Effizienz erfolgte im Rahmen des Projekts AES-2006 (WWER-1200). Die ersten Reaktoranlagen dieser Art sind bereits in Betrieb: Nowoworonesch-2, Leningrad-2 und Belarus-1.

Obwohl die o. g. Anlagen einige standort- oder ausführungsspezifische Unterschiede haben, ist deren funktionelle Struktur der Betriebs- und Sicherheitsleittechnik ähnlich gestaltet (siehe Abb. 2.24), wesentliche Unterschiede bestehen z. B. nur hinsichtlich der Vorrangsteuerung der Funktionen, den Mensch-Maschine-Schnittstellen sowie der Netzwerkkommunikation.

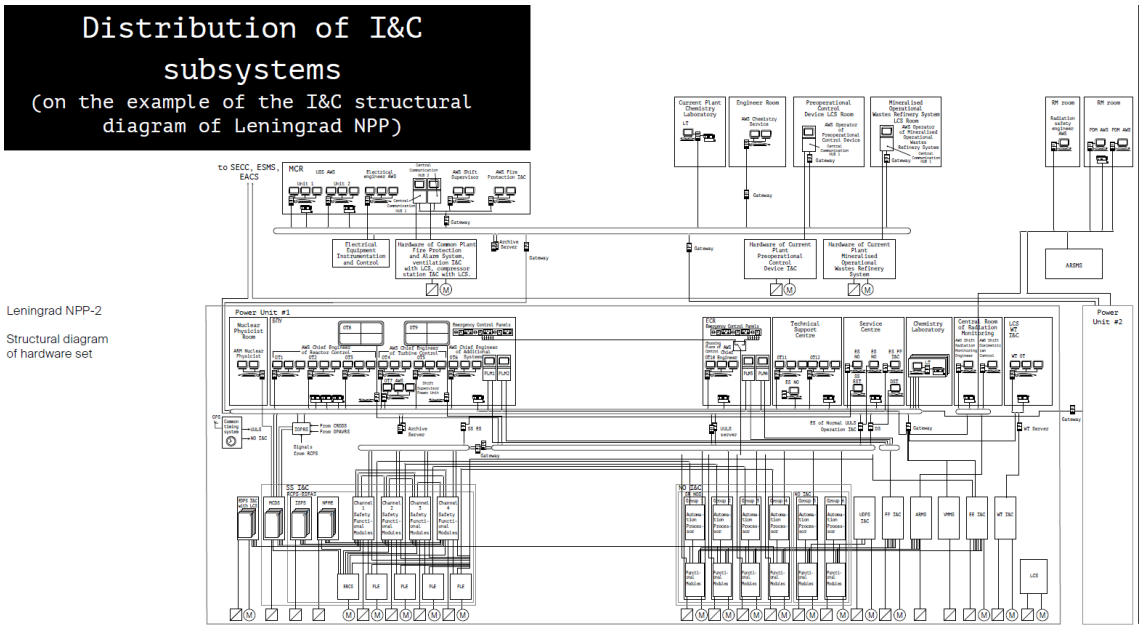


Abb. 2.24 Leittechnik-Architektur des Kernkraftwerks Leningrad-2 /RAS 21/

Die Sicherheitsleittechnik der AES-2006-Reaktoranlagen ist 4-fach redundant aufgebaut. Die Redundanzen der Sicherheitssysteme einschließlich der Sicherheitsleittechnik sind räumlich getrennt (siehe Abb. 2.25), wobei die vier Redundanzen farblich unterschiedlich markiert sind.

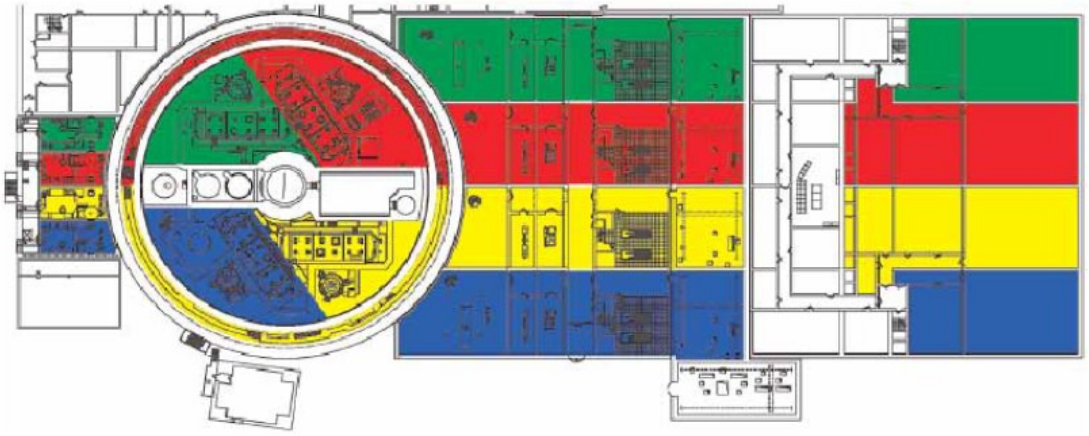


Abb. 2.25 Redundanztrennung der Sicherheitssysteme einschließlich Sicherheitsleittechnik (unterschiedliche Farben für Red. 1 – 4) /GRS 20/

Die Sicherheitsleittechnik der ersten AES-2006-Reaktoranlagen (Nowoworonesch-2 und Leningrad-2) basiert auf TXS und TPTS-SB.

Für die Anlage Nowoworonesch-2 („first of a kind reactor“, Typ WWER-1200, V-392M) wurde eine Leittechnikarchitektur entwickelt, die aus zwei dreifach redundanten Teilsystemen besteht und außerdem jeweils ein diversitäres Backup-Leittechniksystem enthält (siehe Abb. 2.26).

Die Sicherheitsleittechnik der Reaktorschnellabschaltung und zur Steuerung der Sicherheitssysteme (ESFAS) wurde auf der Basis der Soft- und Hardware der TXS-Plattform realisiert. Die Backup-Leittechnik ist dreifach redundant auf Basis von festprogrammierter Logik (FPGA-Baugruppen, russische Hersteller) ausgeführt /GRS 20/.

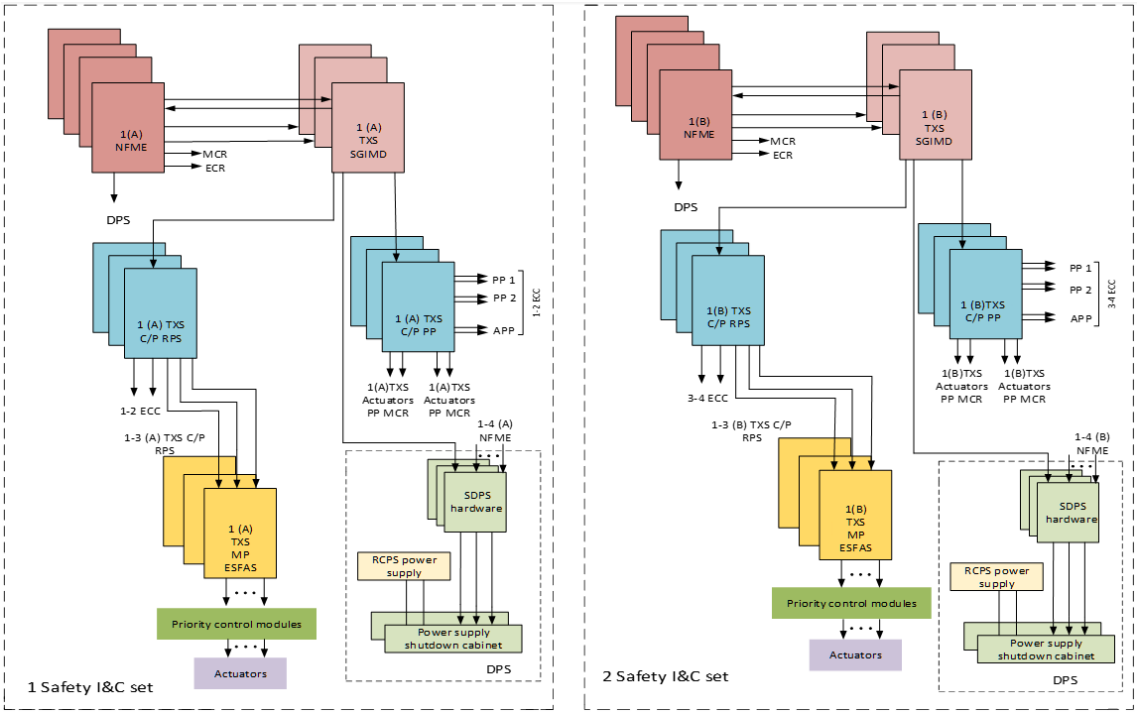


Abb. 2.26 Architektur der Sicherheitsleittechnik im KKW Nowoworonesch-2 /GRS 20/

In den KKW Leningrad-2 und Nowoworonesch-2 sind die Betriebsleittechniksysteme auf Basis der TPTS-NT-Plattform und die Sicherheitsleittechniksysteme auf Basis der TXS-Plattform realisiert worden. Außerdem ist im Kernkraftwerk Leningrad-2 (Typ WWER-1200/491) die diversitäre Leittechnik nur in einem Teilsystem installiert und Netzwerkverbindungen zur betrieblichen Leittechnik sind nicht in jedem Teilsystem, sondern durch eine gemeinsame Netzverbindung (Interserver Exchange Network) umgesetzt (siehe Abb. 2.27).

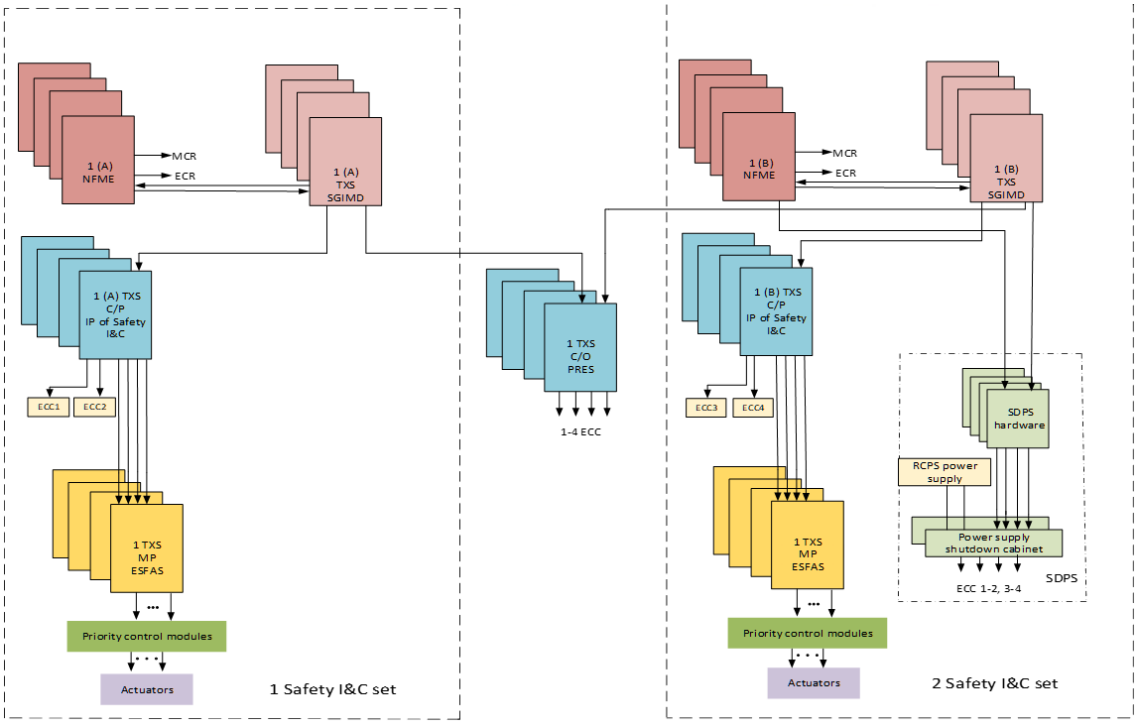


Abb. 2.27 Architektur der Sicherheitsleittechnik im KKW Leningrad-2 /GRS 20/

Die Sicherheitsleittechnik im KKW Belarus-1 wurde ausschließlich auf der Basis der TPTS-SB-Plattform aufgebaut. Hierzu wurde das Defense-in-Depth-Konzept der Pilot-Anlage im KKW Nowoworonesch-2 weiter verbessert, wobei die Hardware-Diversität für Reaktorschutzsysteme umgesetzt wurde (siehe Abb. 2.27, Abb. 2.28). Die Teilsysteme A und B in diesem Konzept sollen zur Beherrschung potenzieller GVA in der Hard- und Software beitragen, wobei in den beiden Teilsystemen jeweils unterschiedliche Hardware eingesetzt wird. Des Weiteren sollen dadurch potenzielle Fehler in der Betriebs- und Anwendersoftware eines softwarebasierten Teilsystems beherrscht werden.

Die Leittechnik-Systeme sind in diesem gestaffelten Schutzkonzept wie folgt gegliedert:

- BLT: Betriebsleittechnik für Normalbetrieb,
- BLT+: Betriebsleittechnik mit Begrenzungsfunktionen (z. B. Reaktorleistungsbegrenzung),
- BLT Schutz Verr: Betriebsleittechnik mit Verriegelungen und Aggregateschutz-Funktionen,
- RS: Reaktorschutz (Reaktorschnellabschaltung & ESFAS),
- BDA: Leittechnik für auslegungsüberschreitende Ereignisse.

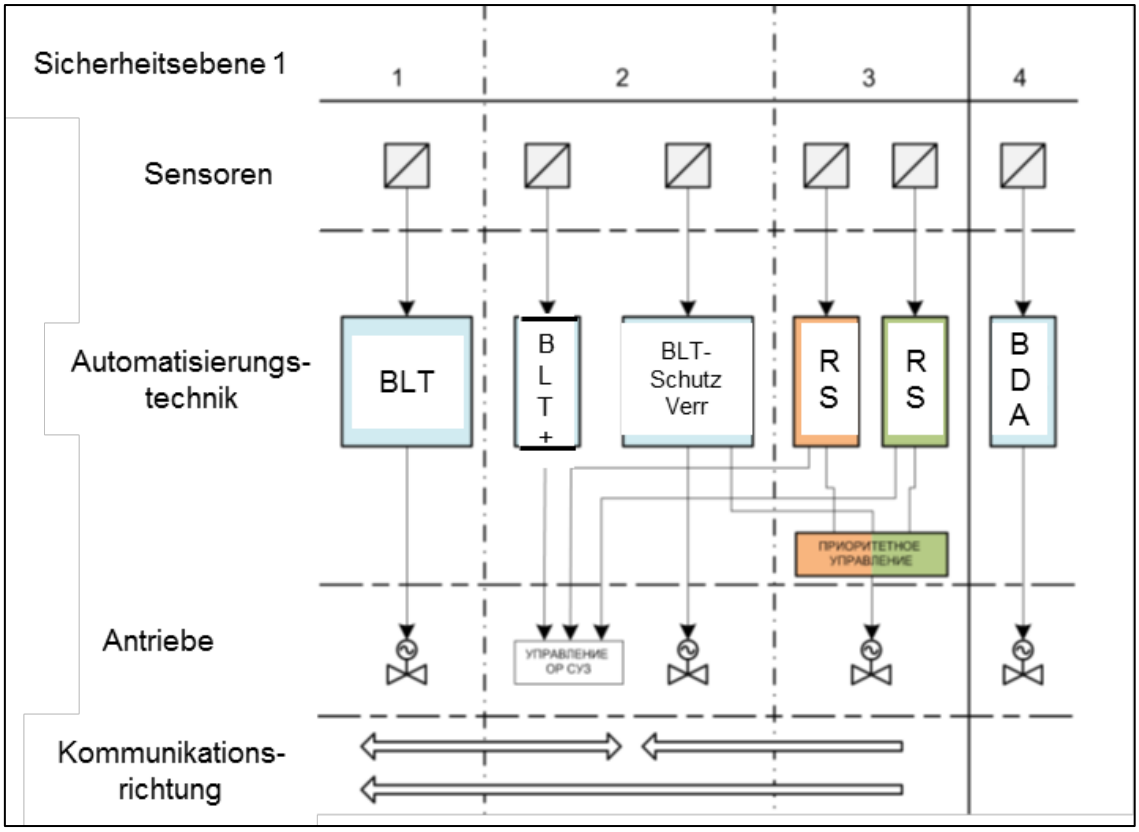


Abb. 2.28 Defense-in-Depth-Konzept der Leittechnik der AES-2006 /GRS 20/

Die Weiterentwicklung der WWER-Reaktoranlagen und deren Leittechnik erfolgt im Rahmen des WWER-TOI[9]-Projekts, wobei die erste Anlage dieses Typs im KKW Kursk-II (zwei Blöcke Kursk-II-1 und Kursk-II-2) realisiert werden soll.

2.8 Leittechnikkonzepte mit SPINLINE

Die mikroprozessorbasierte SPINLINE-Plattform wurde ursprünglich von Rolls-Royce in Zusammenarbeit mit Areva (heute Framatome), Électricité de France (EDF) und Data Systems & Solutions (DS&S) entwickelt /ARI 15/. Heutzutage erfolgt die Herstellung und der Support von SPINLINE durch Framatome.

Während die ältere P4-SPIN-Leittechnik noch 8-bit-Mikroprozessoren und deren Nachfolger N4-SPIN 16-bit-Mikroprozessoren verwendete, kommen seit der Entwicklung von

[9] TOI – Typical, Optimized, with enhanced Information

SPILINE-3 32-bit-Mikroprozessoren zum Einsatz. Die Entwicklung der SPINLINE-Plattform ist schematisch in Abb. 2.29 dargestellt.

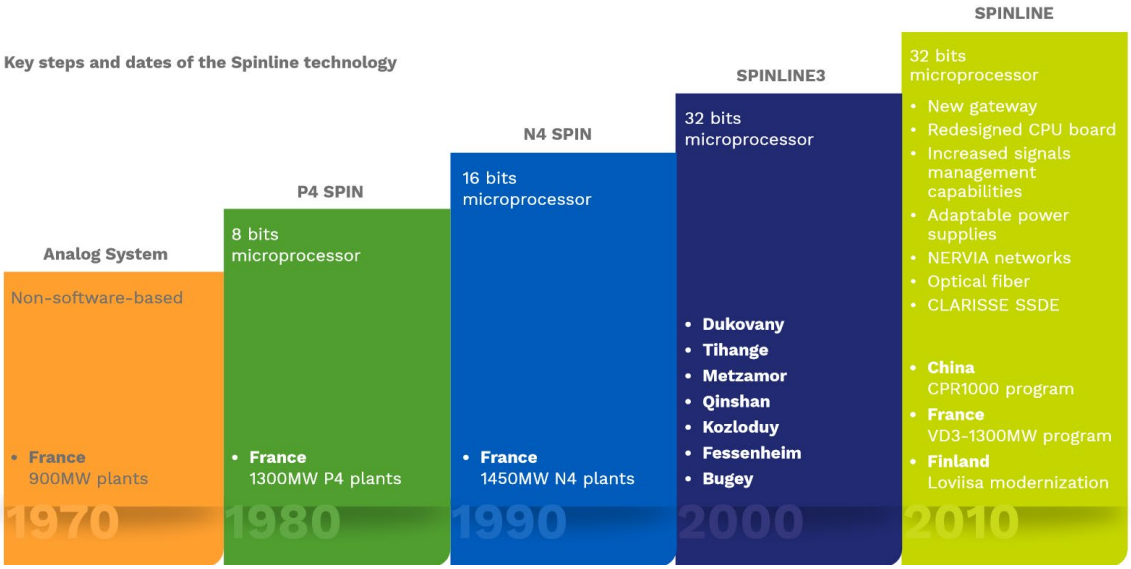


Abb. 2.29 Entwicklung der SPINLINE-Technologie /FRA 22/

SPINLINE-3 wurde bereits vielfach in verschiedenen Anlagen für unterschiedliche, sicherheitsrelevante Funktionen eingesetzt, z. B. zur

- Reaktorschnellabschaltung (Reactor Trip System – RTS),
- Steuerung der Sicherheitseinrichtungen (ESFAS),
- Kerninstrumentierung (Nuclear Instrumentation System – NIS).

Insbesondere wurde SPINLINE-3 auch in einigen WWER-Anlagen im Rahmen von Modernisierungsprojekten eingesetzt (u. a. in den KKW Dukovany (WWER-440) und Kozloduy (WWER-1000)). Beispielhaft ist eine generische Leittechnikarchitektur für den Reaktorschutz in Abb. 2.30 dargestellt.

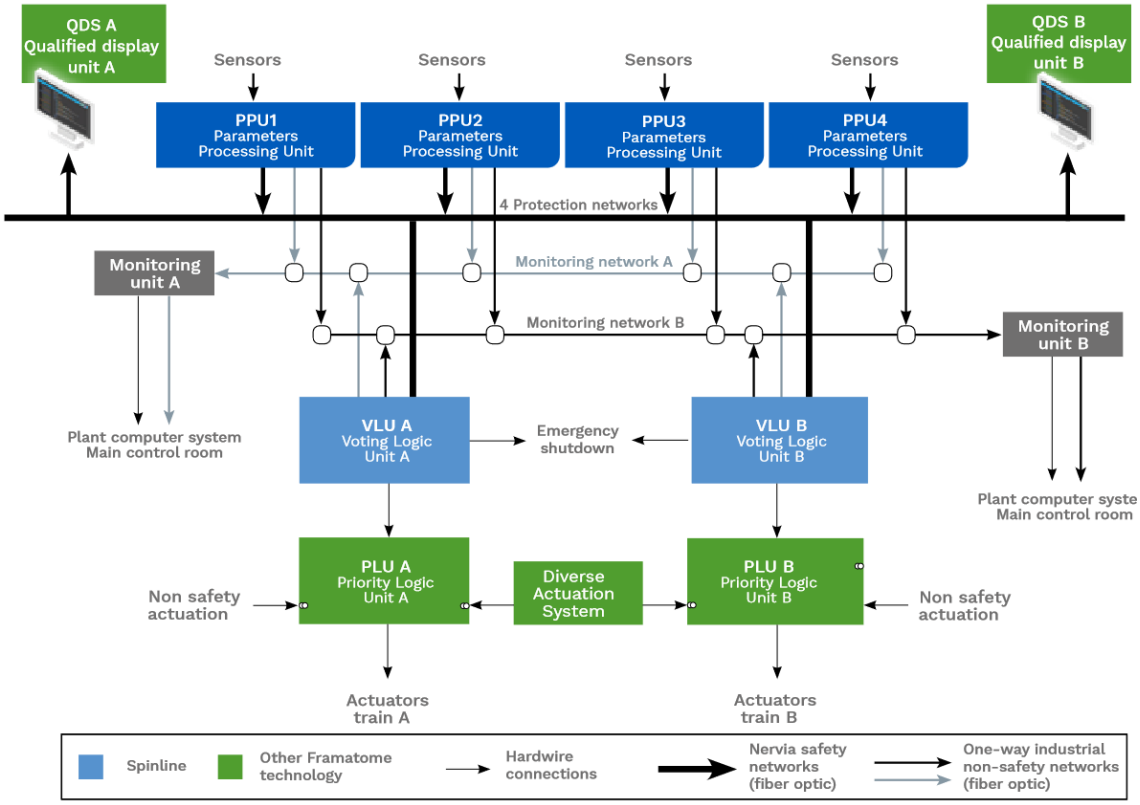


Abb. 2.30 Beispiel einer generischen SPINLINE-Architektur für den Reaktorschutz /FRA 22/

Die Hardware der SPINLINE-3-Plattform besteht im Wesentlichen aus den folgenden Komponenten:

- Leittechnikschränke, Einschübe, usw.,
- Stromversorgungsmodule, Verteiler, Überwachung,
- Module digitaler Signalverarbeitung,
- Kommunikationsmodule (Netzwerk),
- Eingabe- und Ausgabemodule,
- Analogsignalanpassungsmodule,
- Anschlusstechnik, Kabel, usw.,
- Lüftungsmodule für die Hardware-Kühlung.

Die SPINLINE-3-Software besteht aus (vergleiche auch Abb. 2.31):

- Betriebssystem-Software (Qualifiziert Class 1E), diese

  - implementiert für jeden Prozessor die Initialisierung, Selbstüberwachung und Kommunikation mit den Ein- und Ausgabemodulen und mit dem Netzwerk und hat folgende
  - charakteristische Eigenschaften: niedrige Komplexität, zyklische Verarbeitung, keine Interrupts, keine dynamische Verwaltung der Speicher,
  - Konfigurationsmanagement.
- Programmbibliothek für Anwendungssoftware.
- Anwendungssoftware (Qualifiziert Class 1E)
  - wird zyklisch ausgeführt (siehe Abb. 2.31),
  - spezifisch für jedes Kernkraftwerk auf der Basis der Spezifikation,
  - erstellt auf der Basis des SCADE Editors,
  - ausführbarer Code wird mit der CLARISSE Software generiert,
  - Lebenszyklus der Software entspricht IEEE 7-4.3.2 /IEE 16/ und BTP 7-14 /NRC 15/.
- Werkzeuge: CLARISSE System, Software-Entwicklungsumgebung und SCADE Editor
  - zur Erstellung der SPINLINE-3-Leittechnikstruktur (u. a. Prozessormodule, Netzwerk, Eingabe- und Ausgabesignale),
  - zur Erstellung der Leittechnikfunktionen auf der Basis von Funktionsdiagrammen mit dem SCADE Editor,
  - automatisches generieren des ausführbaren Codes,
  - Unterstützung des V&V-Prozesses (Validierung und Verifizierung),
  - Erstellung der Dokumentation für Hard- und Software,
  - Konfigurationsmanagement des Leittechniksystems und der Software.

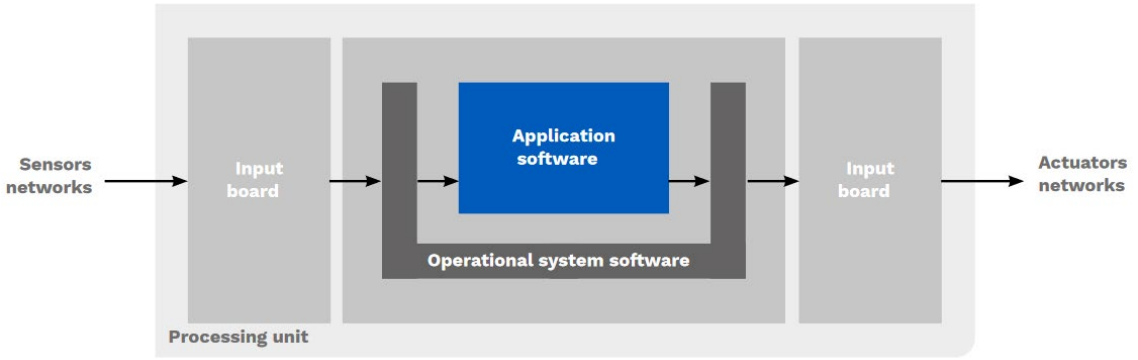


Abb. 2.31 Struktur der SPINLINE-Software /FRA 22/

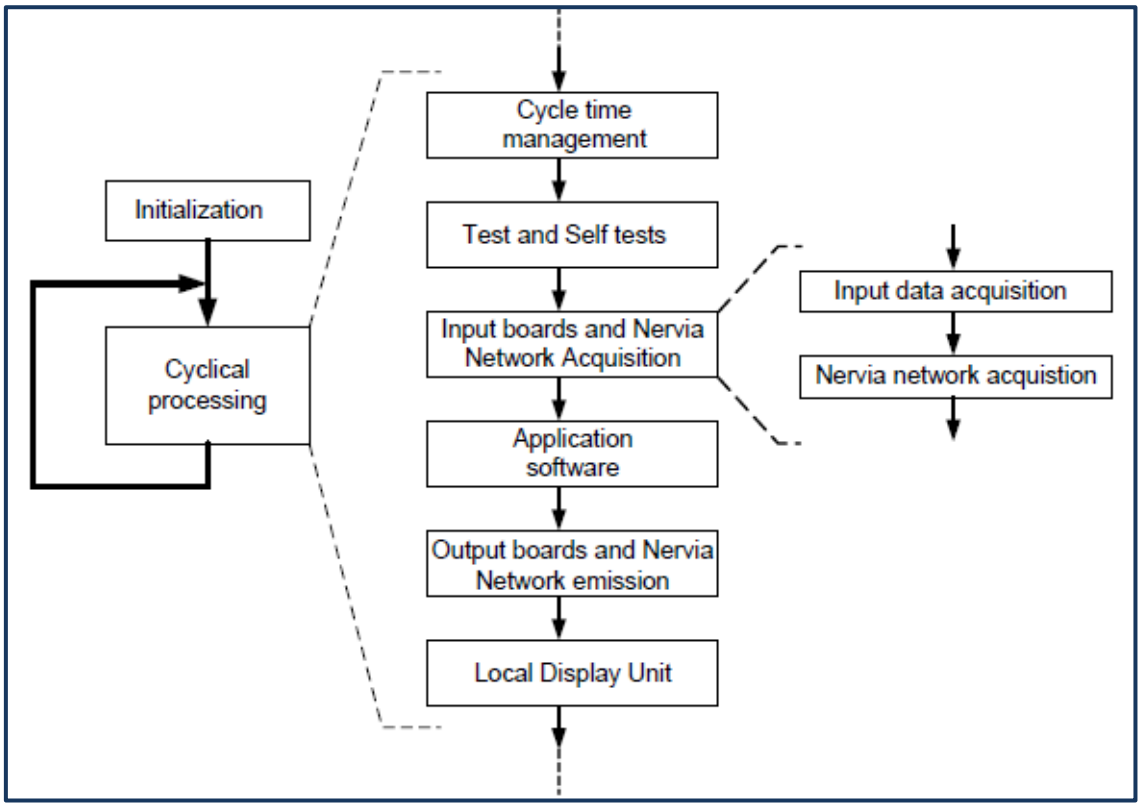


Abb. 2.32 Zyklische Ausführung der Software in SPINLINE /ROL 10/

Die SPINLINE-Leittechnikplattform nutzt NERVIA[10]-Netzwerke als integrale Bestandteile. Dabei handelt es sich um redundante Kommunikationsnetzwerke, die verschiedene Module und Komponenten des Leittechniksystems miteinander verbinden. NERVIA-Netzwerke zeichnen sich durch hohe Zuverlässigkeit und Fehlertoleranz aus. Im Falle eines Ausfalls eines elektronischen Bauteils kann das Netzwerk schnell und

[10] Nuclear Emergency Response and Vital Instrumentation Architecture (digitales Kommunikationsnetzwerk)

effizient wiederhergestellt werden, sodass die Betriebsbereitschaft des Gesamtsystems erhalten bleibt /ROL 10/.

NERVIA ist ein 1E-klassifiziertes Netzwerk für die Kommunikation sicherheitskritischer Leittechnik. Die zugehörige NERVIA-Software entspricht den Anforderungen des IEC-60880-Standards /ROL 10/. Das Netzwerk basiert auf dem NERVIA-Protokoll, das folgende Eigenschaften aufweist:

- Zeitbasiertes Token-Bus-Protokoll: Das Token bzw. die Nachricht wird über das gesamte Netzwerk gesendet und von allen Stationen empfangen.
- Deterministische Übertragung: Die Übertragungszeit ist für jede Station fest definiert und konstant, wobei stets nur eine Station zur gleichen Zeit senden darf.
- Festgelegte Kommunikationszyklen: Der Zyklus der Netzwerkkommunikation ist durch die Konfiguration vordefiniert und bleibt konstant.
- Datenübertragung gemäß Ethernet-Standard: Die Übertragung erfolgt mit 10 Mbit/s auf Ethernet-Layer.

Wichtige Eigenschaften des NERVIA-Netzwerks:

- Physische Trennung und Entkopplung:
  - Glasfaser-Netzwerk und abgeschirmte Leitungen sorgen für eine sichere Signalübertragung.
  - One-Way-Kommunikation über isolierte Verbindungen zu Nicht-1E-Systemen, wobei die Daten des NERVIA-Netzwerks ausschließlich gelesen werden dürfen.
- Fehlertoleranz und Selbstdiagnose:
  - Automatische Fehlererkennung und -isolierung zur Erhöhung der Systemsicherheit.
- Deterministische Funktionsweise:
  - Präzise physikalische und logische Fehlerlokalisierung.
  - Keine Vergabe von statischen oder dynamischen Rechten, um unautorisierte Änderungen zu verhindern.

- Cybersecurity:
  - Mechanismen zur Verhinderung der Ausbreitung von Cyberangriffen (z. B. Viren) innerhalb des Netzwerks.
- Serielle Struktur: die Verarbeitungseinheiten sind in einem NERVIA-Netzwerk seriell verbunden:
  - die erste Verarbeitungseinheit sammelt die Eingangssignale von Sensoren und sendet Parameter zum Netzwerk;
  - die nachfolgende Verarbeitungseinheit empfängt die Daten, verarbeitet sie und sendet die Steuerungsbefehle zu den Antrieben oder zum Netzwerk;
  - die serielle Struktur wird normalerweise für die Signalverarbeitung in einer Redundanz eingesetzt.
- Parallele Struktur: die Verarbeitungseinheiten sind in einem NERVIA-Netzwerk parallel verbunden:
  - die Daten von einer Verarbeitungseinheit werden gleichzeitig via NERVIA-Netzwerk an mehrere weitere Verarbeitungseinheiten gesendet und dort verarbeitet;
  - die parallelen Strukturen werden typischerweise zur Signalverarbeitung mehrerer Redundanzen eingesetzt, wie z. B. Auswahllogik, Prioritätssteuerung.
- Aktuelle Leittechniksysteme kombinieren serielle und parallele Strukturen.

3 Referenzfall

Die in diesem Projekt entwickelte Bewertungsgrundlage basiert auf Methoden der GRS und verfolgt einen modellbasierten Ansatz (zu den GRS-Methoden siehe beispielsweise /MUE 21/). Zur Entwicklung dieser Bewertungsgrundlage wurden die Rechercheergebnisse zu neuen Reaktoranlagen (siehe Kapitel 2) insbesondere ins Projekt DIGMORE der OECD/NEA /DIG 25/ eingebracht, um in diesem gemeinsam mit internationalen Experten einen Referenzfall zu definieren. Die weiterentwickelte Vorgehensweise zur Analyse dieses Referenzfalls durch die GRS im Rahmen dieses Vorhabens ist die Bewertungsgrundlage neuer Leittechnikkonzepte für Reaktoranlagen im Ausland.

Im Projekt DIGMORE wird dieser Referenzfall von unterschiedlichen internationalen Organisationen in individuellen probabilistischen Sicherheitsanalysen (PSA) untersucht, um aus dem Vergleich der Vorgehensweisen und Ergebnisse grundsätzliche Erkenntnisse zur Untersuchung von Leittechniksystemen in unterschiedlichen Leittechnikarchitekturen zu gewinnen (PSA-Vergleichsstudie).

Bei der im Referenzfall des Projekts DIGMORE beschriebenen Referenzanlage handelt es sich um einen vereinfachten, generischen Siedewasserreaktor[11]. Dieser wird in einem eigens hierfür erstellten Dokument der DIGMORE-Task-Group nach Abschluss des Projekts als Teil des entsprechenden Abschlussberichts veröffentlicht /DIG 25/. An dieser Stelle wird der Referenzfall, zum Verständnis der im nachfolgenden Kapitel beschriebenen Untersuchungen mit den Methoden der GRS, in verkürzter Form wiedergegeben.

3.1 Sicherheitssysteme der Referenzanlage

In der Referenzanlage kommen mehrere sicherheitskritische Systeme (und deren Versorgungssystem) zum Einsatz (Abb. 3.1), die im Falle von Störungen, Störfällen und Unfällen bestimmte Schutzmaßnahmen einleiten:

[11] Sowohl in diesem Vorhaben als auch im Projekt DIGMORE liegt der Fokus auf der Leittechnik, die verfahrenstechnischen Sicherheitssysteme spielen eine untergeordnete Roll. Die leittechnischen Einrichtungen sind im Referenzfall deutlich detaillierter beschrieben als die verfahrenstechnischen Systeme. Die Verwendung eines Siedewasserreaktors im Referenzfall geht auf die Vorgängerprojekte zu DIGMORE /DIG 15/, /DIG 24/ zurück.

- Automatisches Druckentlastungssystem **ADS** (Automatic Depressurization System): Ermöglicht eine schnelle Druckreduzierung im Reaktordruckbehälter (RPV – Reactor Pressure Vessel), beispielsweise, um mit anderen Systemen einspeisen zu können.

- Zwischenkühlsystem **CCW** (Component Cooling Water): Dieses Zwischenkühlsystem führt Wärme aus wichtigen Komponenten des ECC-Systems ab, diese wird ans SWS-System abgegeben.

- Notkernkühlsystem **ECC** (Emergency Core Cooling): Dieses System sorgt im Falle eines Notfalls für eine ausreichende Kühlung des Reaktorkerns und verhindert so eine Kernschmelze.

- Not-Speisewassersystem **EFW** (Emergency Feedwater System): Dieses System stellt sicher, dass der Reaktor kontinuierlich mit Kühlwasser versorgt wird, insbesondere im Falle eines Ausfalls der Hauptspeisewasserzufuhr.

- Heiz-, Lüftungs- und Klimatisierungssystem **HVA** (Heating, Ventilation and Air-Conditioning): Das HVA-System gewährleistet die Klimatisierung und Belüftung wichtiger Betriebsräume, im Referenzfall ist es für den korrekten Betrieb des Notspeisewassersystems EFW erforderlich.

- Hauptspeisewassersystem **MFW** (Main Feedwater): Das Hauptspeisewassersystem versorgt den Reaktordruckbehälter kontinuierlich mit Wasser, um die Dampferzeugung zu ermöglichen und die Reaktorkühlung im normalen Betrieb sicherzustellen. Im Referenzfall stellt der Ausfall dieses Systems das Auslöseereignis dar.

- Nachwärmeabfuhrsystem **RHR** (Residual Heat Removal): Nach einem Reaktorstillstand muss die Nachwärme im Kern abgeführt werden. Dieses System spielt eine entscheidende Rolle, um Überhitzung und damit verbundene Gefahren zu verhindern.

- Reaktorschnellabschaltsystem **RS** (Reactor SCRAM): Das Reaktorschnellabschaltsystem ist das zentrale Abschaltsystem des Reaktors. Es sorgt u. a. bei Störfällen dafür, dass die Steuerstäbe automatisch in den Reaktor eingefahren werden, um die Kettenreaktion zu unterbrechen und den Reaktor schnell in einen sicheren Zustand zu überführen.

- Nebenkühlwassersystem **SWS** (Service Water System): Dieses System ist verantwortlich für die Ableitung von Wärme aus dem ECC- und dem RHR-System an die Umgebung.

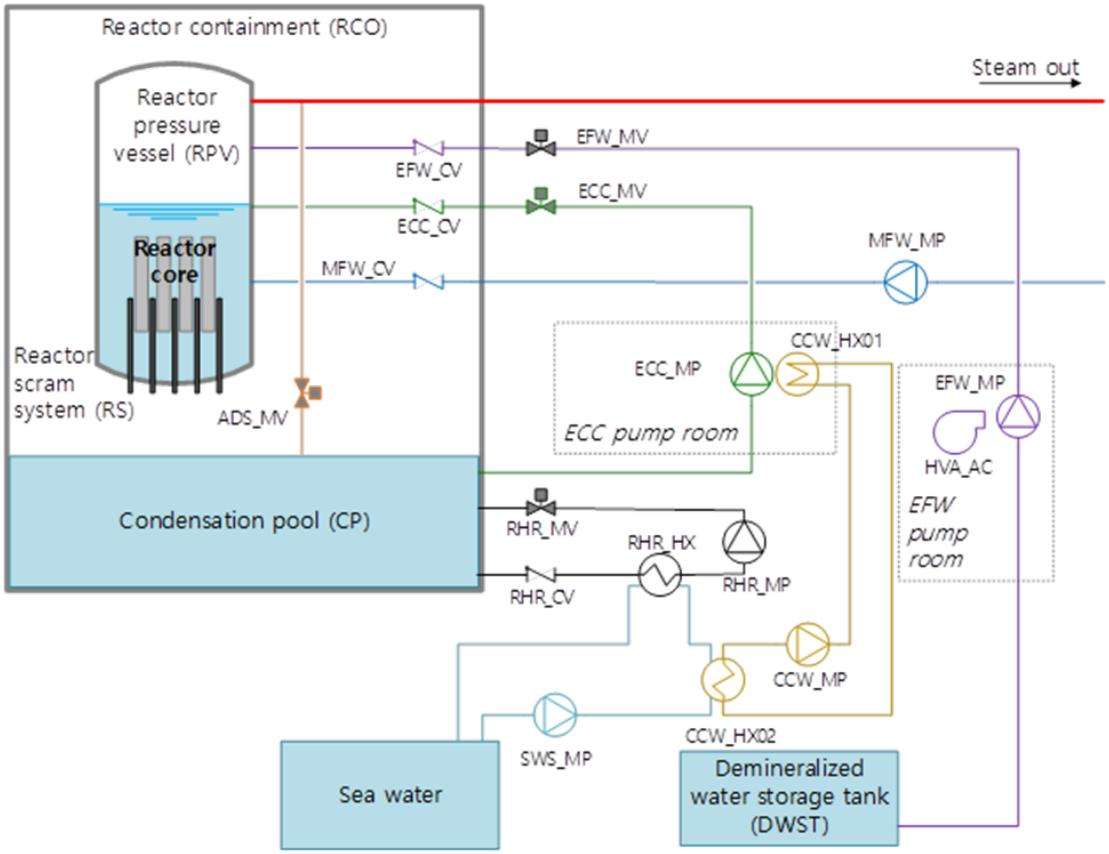


Abb. 3.1 Sicherheitssysteme der Referenzanlage /DIG 24/

Jedes dieser Systeme kann durch verschiedene (ggf. auch mehrere) digitale oder analoge Leittechniksysteme überwacht und gesteuert werden. Hierfür werden im Referenzfall und insbesondere im Rahmen des hier beschriebenen Vorhabens unterschiedliche Leittechnikarchitekturen betrachtet (siehe nachfolgenden Abschnitt).

Im Rahmen des Referenzfalls wurde eine bewusste Vereinfachung bei der Modellierung der verfahrenstechnischen Sicherheitssysteme vorgenommen. Diese Systeme sind in der Referenzanlage lediglich einfach (d. h. ohne Redundanzen) ausgeführt, da der Fokus der Untersuchung der Leittechniksysteme lag. Im Gegensatz dazu weisen die Leittechniksysteme, wie das primäre und das diversitäre Reaktorschutzsystem (PRPS und DRPS), eine mehrfache Redundanz in Form von unabhängigen Scheiben („Divisions“) auf. Die daraus resultierende Diskrepanz zwischen der vereinfachten Darstellung der verfahrenstechnischen Systeme und der hohen Redundanz der Leittechnik wird durch

ein definiertes Erfolgskriterium kompensiert: Für die Aktivierung eines Sicherheitssystems müssen mindestens zwei von vier Priorisierungseinheiten (PAC) ein Auslösesignal generieren.

3.2 Leittechnikarchitekturen und -systeme

Im Rahmen des Referenzfalls werden unterschiedliche Leittechnikarchitekturen betrachtet, die sich in ihrer Komplexität und z. B. teilweise in der Art der Signalübertragung unterscheiden. Diese sind wie folgt festgelegt:

- Architektur I: Diese Architektur umfasst das primäre Reaktorschutzsystem (PRPS), das diversitäre Reaktorschutzsystem (DRPS), das betriebliche Leittechniksystem (OIC) sowie das festverdrahtete Backup-System (HWBS). Zusätzlich werden pro angesteuertes System jeweils zweimal zwei zueinander diversitäre Priorisierungsmodule (PAC) verwendet. In dieser Konfiguration werden sowohl digitale als auch analoge Signalübertragungen genutzt.
- Architektur II: Diese Architektur enthält dieselben Systeme wie Architektur I, allerdings wird ausschließlich analoge Signalübertragung genutzt.
- Architektur III und nachfolgende: Diese Architekturen werden aktuell von der DIGMORE-Task-Group noch entwickelt. Voraussichtlich werden hier Konfigurationen ohne Diversifizierung der PAC sowie mit einer reduzierten Anzahl von Leittechniksysteme (z. B. ohne HWBS) betrachtet.

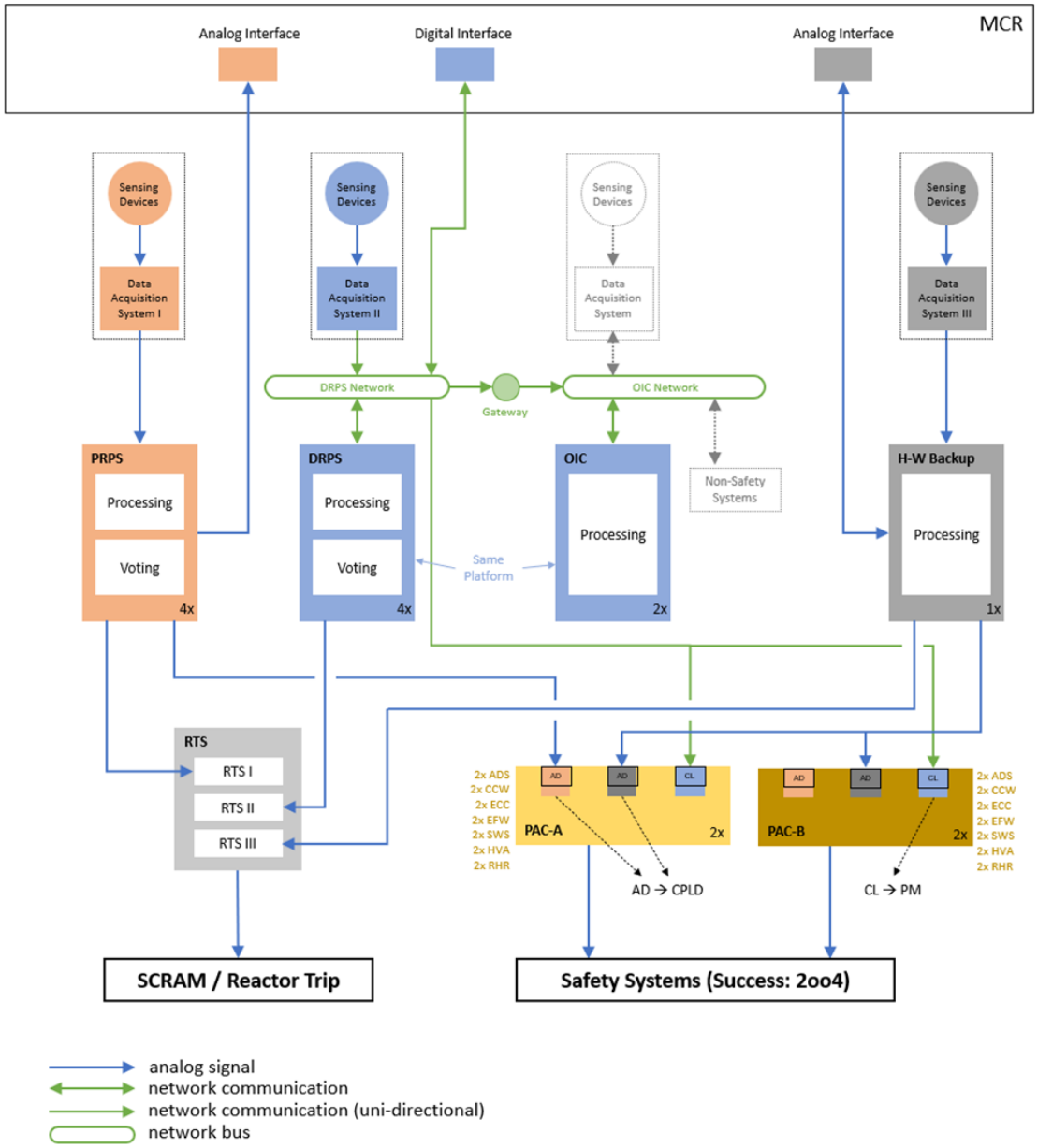


Abb. 3.2 Leittechnikarchitektur I der Referenzanlage

In diesem Vorhaben wurde einerseits die Architektur I, anderseits drei weitere Leittechnikarchitekturen (GII, GIII, GIV)[12] untersucht, um auf diese Weise in diesem Vorhaben eine Bewertungsgrundlage von Leittechnikarchitekturen neuer Reaktoranlagen im Aus-

[12] Der zusätzliche Buchstabe „G“ der drei Leittechnikarchitekturen GII, GIII und GIV steht für „GRS (only)“. Hiermit werden die Leittechnikarchitekturen gekennzeichnet, die (zumindest bisher) ausschließlich für dieses Vorhaben betrachtet wurden und nicht im Rahmen des Projekts DIGMORE.

land zu entwickeln und validieren. Die in diesem Vorhaben betrachteten Leittechnikarchitekturen beinhalten (neben jeweils dem betrieblichen Leittechniksystem OIC) folgende Systeme:

- Architektur I:
  - PRPS (vierfach redundant)
  - DRPS (vierfach redundant)
  - HWBS (einfach redundant)
- Architektur GII:
  - PRPS (vierfach redundant)
  - DRPS (vierfach redundant)
- Architektur GIII:
  - PRPS (vierfach redundant)
  - HWBS (einfach redundant)
- Architektur GIV
  - PRPS (vierfach redundant)

Die einzelnen Leittechniksysteme (PRPS, DRPS, HWBS, OIC), das Reaktorschnellabschaltsystem (RTS) und die Priorisierungsmodule (PAC) werden in den nachfolgenden Abschnitten genauer beschrieben.

3.2.1 Primäres Reaktorschutzsystem (PRPS)

Das primäre Reaktorschutzsystem (Primary Reactor Protection System, PRPS) in Abb. 3.3 überwacht kontinuierlich die wichtigsten Parameter des Reaktors, darunter Druck, Temperatur und Wasserstand im Reaktordruckbehälter. Es besteht aus vier physisch getrennten, aber funktional identischen Redundanzen (in der Abbildung „Divisions“), die in zwei zueinander funktional diversitären Teilsystemen (A und B) sogenannte Erfassungs- und Verarbeitungseinheiten (Acquisition and Processing Units, APU) sowie Bewertungseinheiten (Voting Units, VU) enthalten.

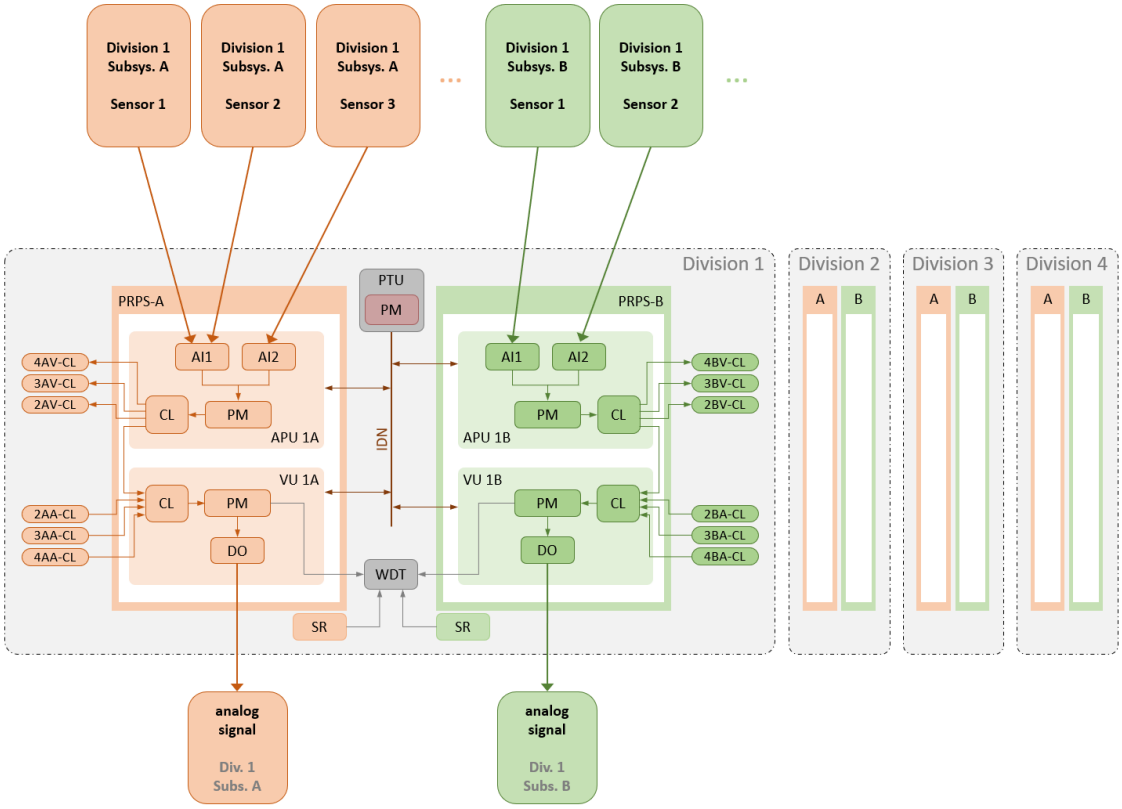


Abb. 3.3 Primäres Reaktorschutzsystem (PRPS) der Referenzanlage

AI – Analog Input (Module)
CL – Communication Link (Module)
DO – Digital Out (Module)
IDN – Intra-Division Network
PM – Processor Module
PTU – Periodical Testing Unit
SR – Subrack
WDT – Watchdog Timer

Die in Abb. 3.3 dargestellten Module und Komponenten bilden diejenige Detailebene ab, die im Referenzfall und bei der Modellierung berücksichtigt wurde. Eine weitergehende Auflösung auf kleinere funktionale Einheiten erfolgte bewusst nicht, um eine praxisgerechte Balance zwischen Detailtiefe und Modellierbarkeit zu gewährleisten.

Die APU erfassen die Messwerte von Sensoren und verarbeiten sie, um mögliche Störfälle zu erkennen und dann entsprechende Signale zu generieren. Die Bewertungseinheiten (Voting Units, VU) bewerten diese Signale und lösen Schutzmaßnahmen aus, wenn bestimmte Kriterien erfüllt sind. Dabei wird in jeder VU durch eine 2-von-4-Auswahl

nur dann ein Schutzsignal ausgelöst, wenn mindestens zwei von vier APU (eines Teilsystems, A oder B) einen kritischen Zustand melden. Dies erhöht die Zuverlässigkeit und reduziert die Wahrscheinlichkeit von Fehlauslösungen.

3.2.2 Diversitäres Reaktorschutzsystem (DRPS)

Das diversitäre Reaktorschutzsystem (Diverse Reactor Protection System, DRPS) dient als Backup-System zum PRPS. Es ist etwas einfacher aufgebaut als das PRPS, verwendet als Basis eine andere Leittechnikplattform als dieses und ist ebenfalls vierfach redundant aufgebaut. Im Gegensatz zum PRPS nutzt das DRPS digitale Netzwerke, um Sensordaten zu empfangen und zu verarbeiten (siehe Abb. 3.4).

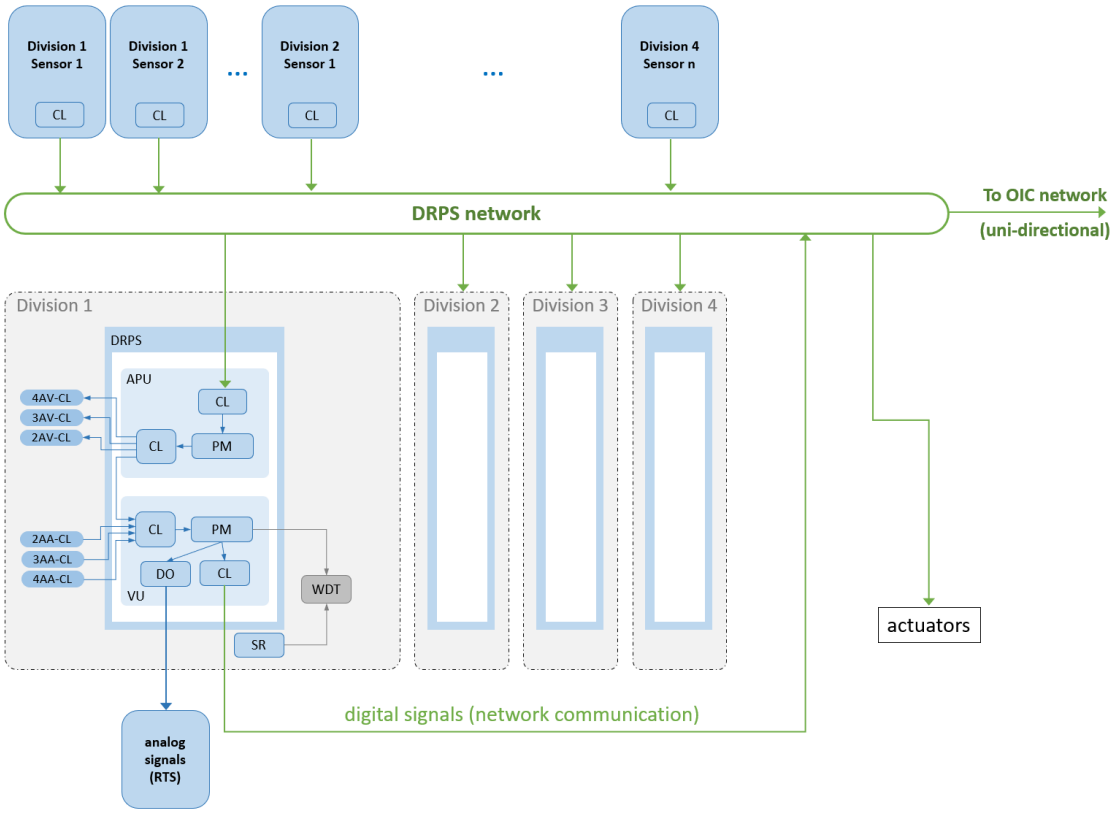


Abb. 3.4 Diversitäres Reaktorschutzsystem (DRPS) der Referenzanlage

Das DRPS wird im Referenzfall (von DIGMORE) in zwei unterschiedlichen Varianten beschrieben. Diese unterscheiden sich im Wesentlichen durch die Kommunikation mit den angesteuerten Sicherheitssystemen. Die hier gezeigte Variante kommuniziert bis auf mit dem Reaktorschnellabschaltsystem (Reactor Trip System, RTS) über digitale Netzwerkkommunikation mit den Aktuatoren. Die Abkürzungen der Module (z. B. PM) entsprechen den Bezeichnungen für das PRPS (siehe Bilderläuterung zu Abb. 3.3).

3.2.3 Betriebliches Leittechniksystem (OIC)

Das zweifach redundante betriebliche Leittechniksystem (Operational Instrumentation and Control, OIC) in Abb. 3.5 überwacht die Betriebsparameter der Anlage und stellt sicher, dass die Anlage innerhalb sicherer Betriebsgrenzen bleibt. Es erhält unidirektional Informationen vom DRPS, um beispielsweise sicherheitsrelevante Informationen im Kontrollraum anzuzeigen. Im Gegensatz zu PRPS und DRPS steuert das OIC keine Sicherheitssysteme, sondern dient lediglich der Unterstützung des Bedienpersonals insbesondere im bestimmungsgemäßen Betrieb.

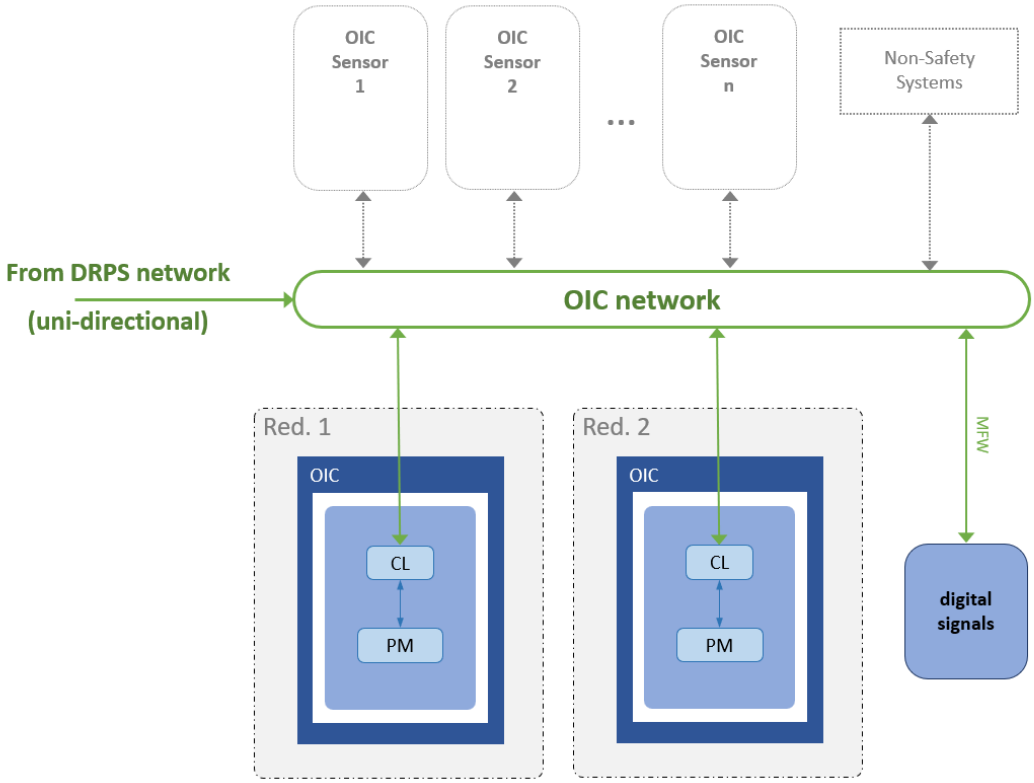


Abb. 3.5 Betriebliches Leittechniksystem (OIC) der Referenzanlage

Im Rahmen des Referenzfalls kann das OIC allerdings Quelle von Fehlauslösungen („Spurious Actuations“) von Sicherheitssystemen sein, wenn beispielsweise aufgrund fehlerhafter Informationen vom DRPS das Hauptspeisewassersystem (Main Feedwater, MFW) abgeschaltet wird (Loss of Main Feedwater, LMFW).

3.2.4 Festverdrahtetes Backup-System (HWBS)

Das festverdrahtete Backup-System (Hard-Wired Backup System, HWBS) in Abb. 3.6 ist eine rein analoge Backup-Option, die im Falle eines Ausfalls der digitalen Systeme verwendet werden kann. Es ermöglicht dem Bedienpersonal in Notfällen manuelle Eingriffe vorzunehmen, um sicherheitskritische Systeme zu steuern. In der Referenzanlage werden keine automatischen Aktionen durch das HWBS ausgelöst. Das HWBS verfügt über eigene Sensoren und Aktoren und ist insbesondere unabhängig von den digitalen Netzwerken der anderen Systeme.

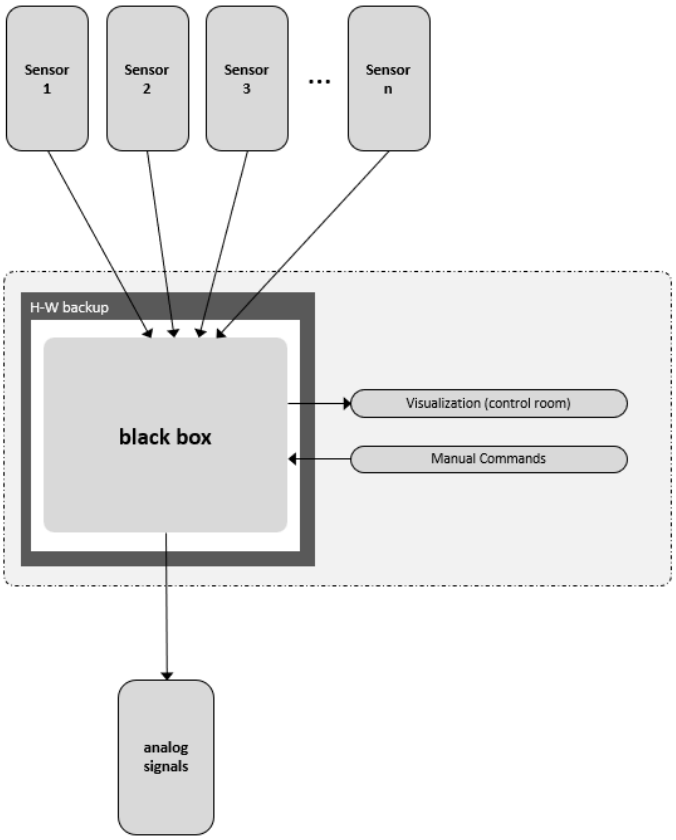


Abb. 3.6 Festverdrahtetes Backup-System (HWBS) der Referenzanlage

Im Rahmen des Referenzfalls wird das HWBS als (einfach redundante) Blackbox behandelt.

3.3 Priorisierungsmodule (PAC)

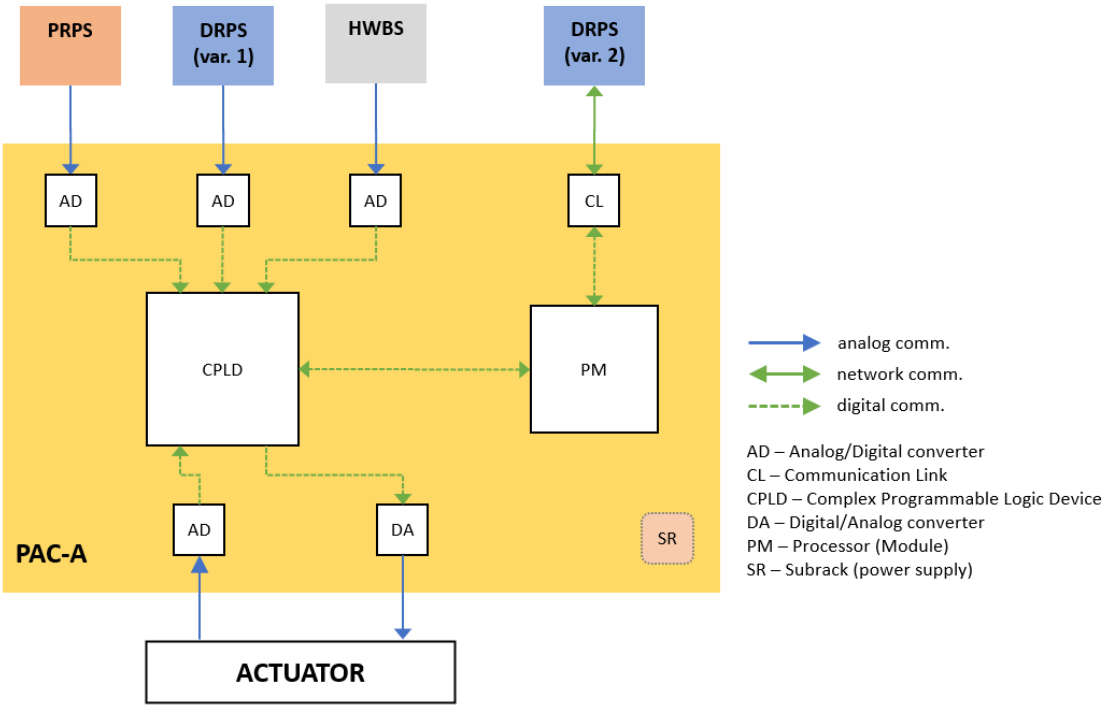


Abb. 3.7 Priorisierungsmodul PAC-A (schematisch)

Dargestellt ist PAC-A, das Priorisierungsmodul PAC-B ist gleichartig aufgebaut, kommt jedoch von einem anderen Hersteller und wird im Rahmen des Referenzfalls als diversitär zu PAC-B betrachtet.

Die Priorisierungsmodule (Priority and Actuation Control, PAC) dienen in der Referenzanlage zur unmittelbaren Ansteuerung sicherheitskritischer Aktoren und zur Priorisierung von Steuerbefehlen, die von den verschiedenen Leittechniksystemen (PRPS, DRPS und HWBS) kommen. Jedes PAC basiert auf einem CPLD (Complex Programmable Logic Device)[13] und enthält zusätzlich einen Prozessor, um bestimmte Kommunikations- und Überwachungsfunktionen zu übernehmen (vergleiche Abb. 3.7). Die PAC werden von verschiedenen Herstellern geliefert (PAC-A und PAC-B) und sind im Referenzfall diversitär zueinander, um das Risiko von gemeinsamen Fehlerursachen zu minimieren. Die Referenzanlage verfügt jeweils über vier PAC pro angesteuertes Sys-

[13] CPLD sind integrierte digitale Schaltkreise, die komplexe Logikfunktionen flexibel und effizient umsetzen. Ein Vorteil von CPLD gegenüber Mikroprozessoren ist ihre deterministische Verarbeitung: Sie reagieren auf Eingaben ohne zusätzliche Verzögerung durch Betriebssysteme oder Softwareprozesse, was sie besonders zuverlässig und vorhersehbar in sicherheitskritischen Anwendungen macht /BRO 96/.

tem (ADS, CCW, ECC, EFW, HVA, RHR, SWS). Für jedes angesteuerte System kommen hierfür jeweils zwei zueinander diversitäre PAC zum Einsatz (2 x PAC-A und 2 x PAC-B)[14], insgesamt verfügt die Referenzanlage also über 56 PAC.

Der CPLD innerhalb eines PAC übernimmt sämtliche sicherheitskritischen Funktionen, darunter die Priorisierung der eingehenden Signale sowie ggf. die Generierung des Auslösebefehls an den verbundenen Aktuator. Die Priorisierungslogik ist einfach gehalten: Befehle vom PRPS haben die höchste Priorität, gefolgt von DRPS-Befehlen und schließlich HWBS-Befehlen.

Der Prozessor (PM – Processor Module) hat unterstützende Aufgaben. Er verarbeitet das digitale Eingangssignal vom DRPS[15] und bereitet dieses für den CPLD auf. Zudem übernimmt der Prozessor die Selbstüberwachung des PAC.

3.4 Reaktorschnellabschaltsystem (RTS)

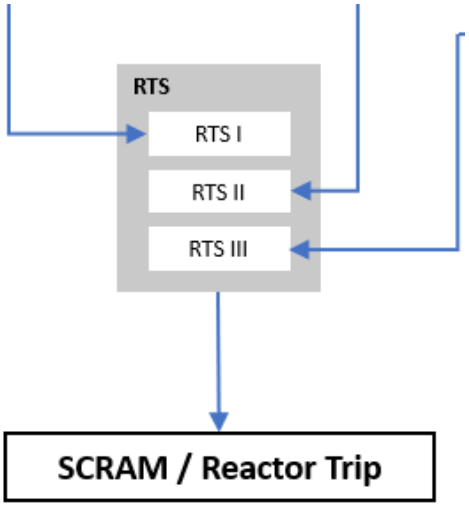


Abb. 3.8 Reaktorschnellabschaltsystem der Referenzanlage

[14] Anmerkung: Dies gilt insbesondere für die Architekturen I und II im Rahmen des Projekts DIGMORE, die derzeit noch in der Entwicklung befindlichen Architekturen (III, …) verfügen teilweise stattdessen über vier gleichartige PAC pro angesteuertes System. Im Rahmen dieses Vorhabens ist dies jedoch für alle betrachteten Architekturen (I, GII, GIII, GIV) der Fall.

[15] Im Referenzfall wird zwischen zwei DRPS-Varianten unterschieden (u. a. mit digitaler bzw. analoger Signalübertragung an die PAC, vergleiche Abb. 3.7). Im Rahmen dieses Vorhabens werden ausschließlich Fälle betrachtet, indem die Kommunikation des DRPS mit den PAC digital stattfindet („var. 2“).

Das Reaktorschnellabschaltsystem (Reactor Trip System, RTS) kann vom primären Reaktorschutzsystem (PRPS), vom diversitären Reaktorschutzsystem (DRPS) und, falls manuelle Eingriffe erforderlich und möglich sind, auch vom festverdrahteten Backup-System (HWBS) ausgelöst werden. Im Rahmen des Referenzfalls wird das Reaktorschnellabschaltsystem als Blackbox betrachtet. Eine Reaktorabschaltung wird eingeleitet, sobald ein entsprechendes Signal von einem der angeschlossenen Leittechniksysteme empfangen wird. Formal betrachtet handelt es sich dabei also um eine logische ODER-Verknüpfung (von RTS I, RTS II und RTS III in Abb. 3.8).

Explizite Ausfälle des RTS selbst werden im Referenzfall nicht berücksichtigt. Solche Ausfälle gelten zum einen als sehr unwahrscheinlich und sind zum anderen bereits durch die Ausfallwahrscheinlichkeiten der Eingangssignale (RTS I, II, III) abgedeckt bzw. können als Teil des ebenfalls im Referenzfall berücksichtigten Versagens der Steuerstäbe (beim Einfahren) betrachtet werden.

3.5 Auslösende Ereignisse und Unfallszenarien

Das zentrale auslösende Ereignis (Initiating Event, IE) im Referenzfall ist der Verlust der Hauptspeisewasserzufuhr (Loss of Main Feedwater, LMFW). Dieser Initiator kann im Referenzfall durch verschiedene Ursachen ausgelöst werden, darunter z. B. Hardwareausfälle im Hauptspeisewassersystem, aber auch Fehlfunktionen im OIC[16].

Im Falle eines LMFW muss der Reaktor sicher abgeschaltet werden, um eine Kernschmelze zu verhindern. In Abhängigkeit des Gelingens oder Versagens der weiteren Sicherheitssysteme (ADS, ECC, EFW, RHR) kommt es dann entweder zu einer Kernschädigung (Core Damage, CD) oder einer erfolgreichen Beherrschung des Störfalls (OK). Die entsprechenden Zusammenhänge sind im Ereignisbaum (Event Tree, ET) in Abb. 3.9 dargestellt.

[16] Das OIC kann somit im Referenzfall Ursache sogenannter Spurious Actuations sein, siehe Abschnitt 3.2.3.

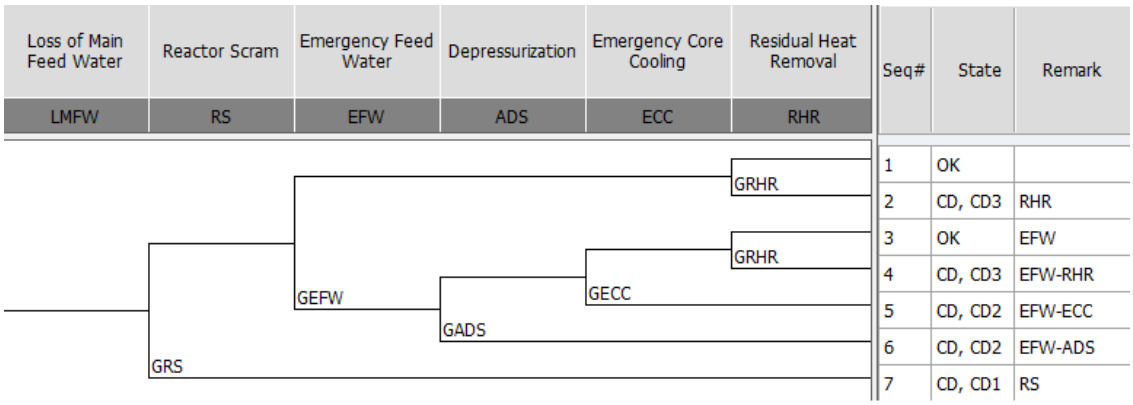


Abb. 3.9 Ereignisbaum für LMFW

3.6 Zuverlässigkeitskenndaten

Um die Zuverlässigkeit der verschiedenen Systeme zu bewerten, werden generische Ausfallwahrscheinlichkeiten angenommen. Diese Wahrscheinlichkeiten basieren auf historischen Daten sowie Erfahrungswerten aus ähnlichen Anlagen und wurden gemeinsam von den Experten, die am Projekt DIGMORE beteiligt sind, festgelegt. Die konkreten Werte können dem Abschlussbericht des Projekts DIGMORE /DIG 25/ entnommen werden, sobald dieser veröffentlicht wurde. Für das PRPS entsprechen die Werte denen im Projekt DIGMAP und können daher bereits vor Abschluss des Projekts DIGMORE im entsprechenden Abschlussbericht von DIGMAP eingesehen werden /DIG 24/.

Beispiele für Ausfallwahrscheinlichkeiten[17] im Projekt DIGMORE sind:

- CCW-Wärmetauscher fällt aus: $1{,}0 \cdot 10^{-6}$ pro Tag.
- Ein bestimmter Sensor des PRPS versagt: $2{,}0 \cdot 10^{-7}$ pro Stunde.
- Ein bestimmtes Prozessormodul des PRPS versagt: $2{,}0 \cdot 10^{-6}$ pro Stunde.

Für die Komponenten der Leittechniksysteme werden im Referenzfall darüber hinaus auch relative Anteile dieser Fehler angegeben, die nur durch bestimmte fehlertolerante Techniken (Fault Tolerant Techniques, FTT) gefunden werden können. So sind beispielsweise 10 % der Ausfälle von Prozessormodulen des PRPS ausschließlich durch

[17] Die hier dargestellten Beispiele decken nur einen verschwindend geringen Teil der verwendeten Zuverlässigkeitskenndaten ab. An dieser Stelle dienen die Werte ausschließlich dazu, einen Eindruck von den Größenordnungen zu vermitteln. In jedem Fall sind alle verwendeten Daten zwar realitätsnah, aber dennoch generisch und dürfen nicht für reale Anwendungen unkritisch übernommen werden.

Full-Scope-Tests (F) (also Wiederkehrende Prüfungen, WKP) zu entdecken, 70 % der Ausfälle können durch (F) oder automatische Selbsttests (A) (innerhalb des Prozessormoduls) entdeckt werden, 10 % der Ausfälle können durch (F) oder periodische Tests (P) (durch die PTU – siehe Abb. 3.3) entdeckt werden und die restlichen 10 % der Ausfälle können durch alle FTT (A, F und P) detektiert werden.

Darüber hinaus werden im Referenzfall auch Angaben zu GVA gemacht, beispielsweise sind GVA-Parameter für die Verwendung von Alpha-Faktoren tabellarisch wiedergegeben. Die konkrete Berücksichtigung von GVA obliegt in DIGMORE jedoch den jeweils modellierenden Organisationen.

Die GRS verwendete bei den in diesem Bericht vorgestellten Modellen entweder jeweils bis zu einer GVA-Gruppengröße von acht Komponenten Alpha-Faktor-Modelle (mit den im Referenzfall angegebenen Faktoren), für noch größere GVA-Gruppen wurde Beta-Faktor-Modelle verwendet (in diesem Fall wurde jeweils der Alpha-Faktor für den gleichzeitigen Ausfall zweier Komponenten als Beta-Faktor verwendet)[18].

[18] Genauere Details können dem Abschlussbericht von DIGMORE /DIG 25/ entnommen werden, sobald dieser veröffentlicht wurde. Eine gleichartige Vorgehensweise wurde von der GRS auch schon im Vorgängerprojekt DIGMAP gewählt, Details können daher auch im entsprechenden Abschlussbericht /DIG 24/ nachgelesen werden.

4 Analysen

4.1 Modellierung Referenzfall

Aufgrund der Erfahrungen im Vorgängerprojekt DIGMAP /DIG 24/ zu DIGMORE /DIG 25/ wurden für die Modellierung des Referenzfalls durch die GRS die folgenden Aspekte zugrunde gelegt:

- Ausfälle fehlertoleranter Techniken (FTT – Fault Tolerant Techniques) haben keinen nennenswerten Einfluss auf das Ergebnis der Analysen,
  - FTT haben jedoch einen Einfluss auf die Ausfälle der überwachten Komponenten (d.h. auf deren Zuverlässigkeitskenndaten).
  - Ausfälle von FTT werden daher im GRS-Modell nicht explizit berücksichtigt.
- Die explizite Berücksichtigung von Änderungen der Auswahllogik in den VU[19] (bei erkannten fehlerhaften Eingangssignalen in die VU) haben keinen nennenswerten Einfluss auf das Ergebnis.
  - Änderungen der Auswahllogik in den VU werden daher im GRS-Modell nicht explizit berücksichtigt.
- Die Zuverlässigkeit von Systemen (z. B. PRPS) wird von GVA dominiert.
  - Bei der Modellierung können (für mehrfach redundante Systeme) Einzelfehler ohne allzu große Ungenauigkeit weggelassen werden und der Fokus stattdessen auf GVA gelegt werden.
  - Dies wurde im Verlauf der Arbeiten explizit validiert und entspricht im Grundsatz auch einer Annahme des sogenannten Kompaktmodells von EDF (siehe hierzu z. B. die Beschreibung des EDF-Modells in DIGMAP /DIG 24/).
  - Einzelfehler wurden daher im GRS-Modell nur für maximal zweifach redundante Systeme (beispielsweise PAC-A, PAC-B) explizit berücksichtigt.
- Die Fehlerbäume der verfahrenstechnischen Sicherheitssysteme wurden von EDF erstellt und von allen an DIGMORE beteiligten Organisationen übernommen.

[19] So kann beispielsweise eine 2-von-4-Auswahl, wenn eines der vier Eingangssignale als fehlerhaft identifiziert wurde, innerhalb der VU automatisch in eine 2-von-3-Auswahl geändert werden.

- Hierdurch wird sichergestellt, dass bei der Betrachtung der Leittechnik nicht unnötige Unterschiede in den Modellen (aller Organisationen) aufgrund der verfahrenstechnischen Systeme entstehen – der Fokus in DIGMORE und in diesem Vorhaben liegt auf der Leittechnik.

Im Rahmen der Entwicklung der Bewertungsgrundlage für Leittechnikkonzepte neuer Reaktoranlagen im Ausland innerhalb dieses Vorhabens[20], wurde insbesondere zunächst die Architektur I (Abb. 3.2) modelliert und untersucht. Das dabei angenommene Auslöseereignis ist ein Ausfall der Hauptspeisewasserversorgung (LMFW – Loss of Main Feedwater). Unabhängig von den weiteren Architekturen in DIGMORE (siehe Abschnitt 3.2) wurden darüber hinaus drei weitere Leittechnikarchitekturen innerhalb dieses Vorhabens definiert und untersucht (siehe Abschnitt 3.2).

Abb. 4.1 zeigt das PRPS mit allen relevanten Sensoren und Ausgangssignalen für eine Redundanz („Division X“)[21] im Falle eines LMFW. Aus den erfassten Anlagenparametern durch entsprechende Sensoren, z. B. P_RPViSP[22] zur Messung des Drucks im Reaktordruckbehälter (Reactor Pressure Vessel, RPV), werden von den Teilsystemen (A, B) entsprechende Auslösesignale (z. B. P_ESF2) generiert und an die PAC der Sicherheitssysteme geschickt (siehe Abb. 4.4).

Das entsprechende DRPS-Modell (repräsentativ für eine Redundanz) für LMFW ist in Abb. 4.2 zu sehen. In diesem kommunizieren die Sensoren mit dem Leittechniksystem digital über das DRPS-Netzwerk. Ebenso werden die ggf. generierten Auslösesignale ebenfalls digital über das DRPS-Netzwerk an die PAC der angesteuerten Sicherheitssysteme gesendet[23].

---

[20] Und damit auch gleichzeitig die erste Modellierung des Referenzfalls für die Vergleichsstudie DIGMORE.

[21] Im GRS-Modell des Referenzfalls sind alle vier Redundanzen inklusive GVA berücksichtigt.

[22] Die entsprechenden Sensoren sind jeweils ebenfalls vierfach redundant vorhanden, d. h. jede Redundanz des PRPS verfügt über eigene Sensoren.

[23] Eine Ausnahme hierzu sind die beiden Signale D_RS1 und D_RS2 („D“ für DRPS). Diese werden nicht nur digital an die PAC der angesteuerten Sicherheitssysteme gesendet, sondern auch analog ans Reaktorschnellabschaltsystem (blauer Pfeil in der Abbildung).

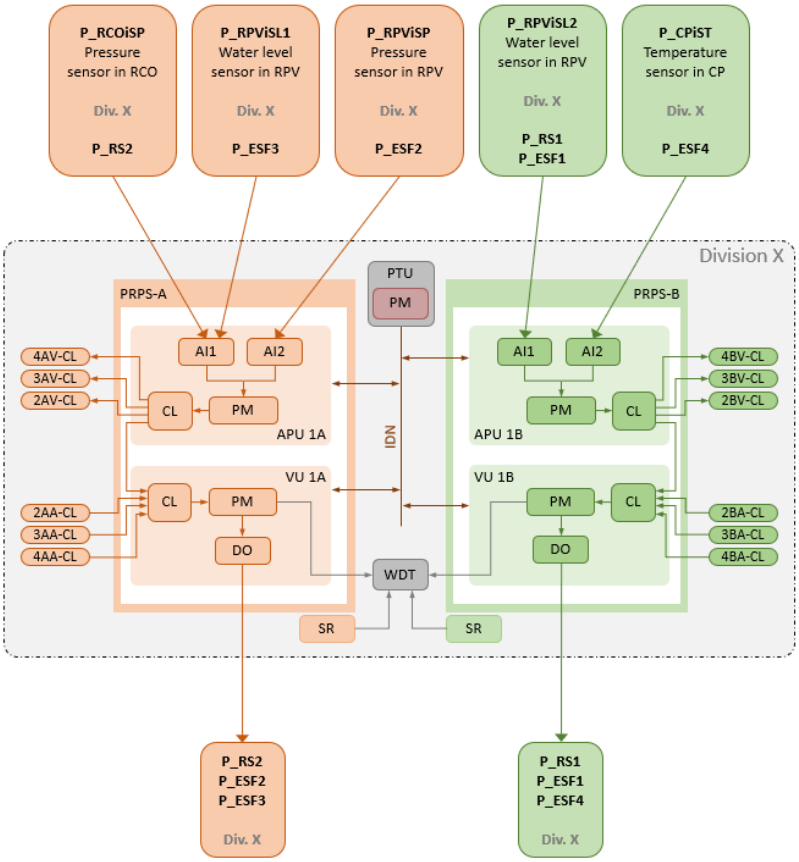


Abb. 4.1 PRPS-Modell einer von vier Redundanzen („Division“) für LMFW

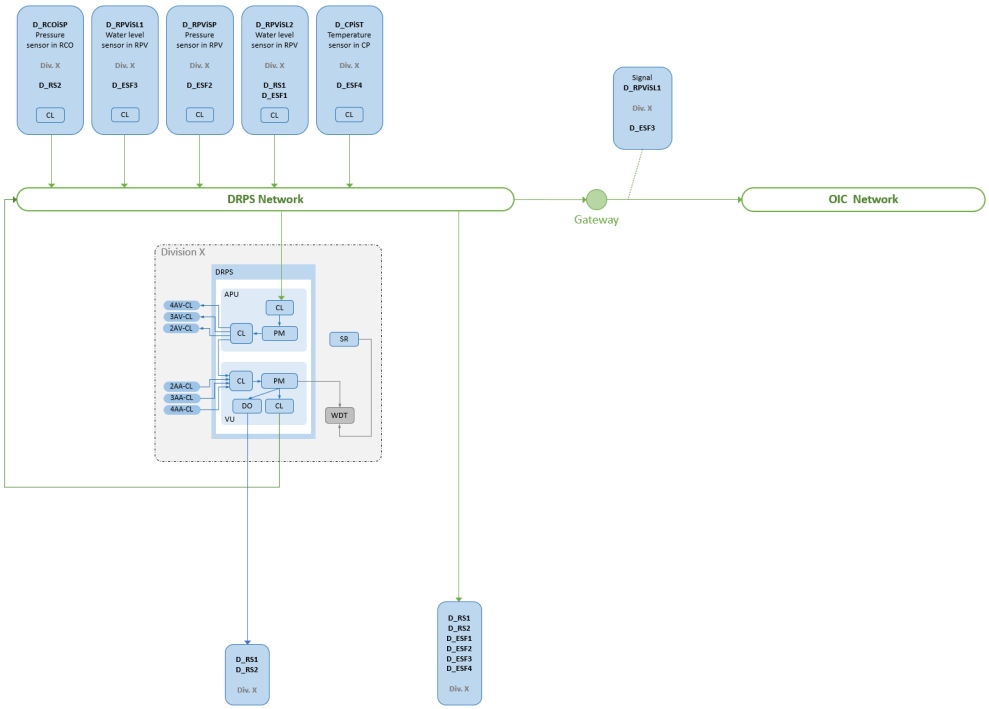


Abb. 4.2 DRPS-Modell einer von vier Redundanzen („Division“) für LMFW

Das Modell des HWBS ist in Abb. 4.3 dargestellt. Im Rahmen des Referenzfalls wird das HWBS als einfache Blackbox behandelt, welches basierend auf den Eingangssignale der Sensoren (z. B. H_RPViSP) dem Bedienpersonal erlaubt, manuelle Auslösesignale[24] zu generieren.

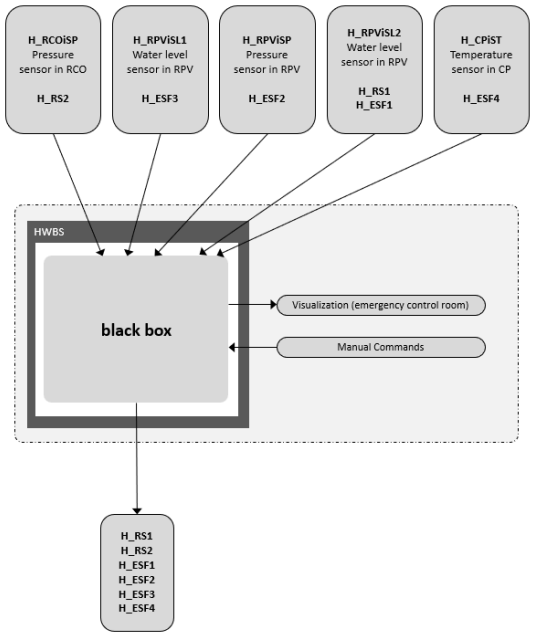


Abb. 4.3 HWBS-Modell für LMFW (einfach redundante Blackbox)

Alle drei Sicherheitsleittechniksysteme (PRPS, DRPS, HWBS) generieren also auf Basis jeweils eigener Sensoren Signale für die verfahrenstechnischen Sicherheitssysteme. Diese Signale werden von den Priorisierungsmodulen (PAC) dieser Sicherheitssysteme weiterverarbeitet (Abb. 4.4). In der Realität würden hierbei von den einzelnen Redundanzen der Sicherheitsleittechniksysteme jeweils entsprechende Redundanzen der verfahrenstechnischen Sicherheitssysteme angesteuert.

Im Referenzfall bzw. der Referenzanlage sind die verfahrenstechnischen Sicherheitssysteme jedoch vereinfacht nur einfach redundant vorhanden[25]. Aus diesem Grund verfügt jedes Sicherheitssystem (ADS, CCW, ECC, EFW, HVA, RHR, SWS) per Definition

[24] Hierbei können in späteren Analysen im Rahmen des Projekts DIGMORE auch menschliche Fehler berücksichtigt werden, diese sind in den Fehlerbaum- und Monte-Carlo-Simulationsmodellen der GRS auch bereits berücksichtigt, allerdings die entsprechenden Wahrscheinlichkeiten in der aktuellen Analysephase von DIGMORE noch auf null gesetzt.

[25] Die höhere Zuverlässigkeit eines realistischerweise eigentlich mehrfach redundanten Systems wird im Referenzfall durch geringere Ausfallwahrscheinlichkeiten der entsprechenden Komponenten indirekt berücksichtig (siehe auch /DIG 24/).

über vier PAC (angesteuert durch jeweils eine Redundanz vom PRPS und DRPS sowie alle durch das einfach redundante HWBS). Der in der Realität zu erwartende höhere Redundanzgrad jedes verfahrenstechnischen Sicherheitssystems wird dabei ersatzweise durch ein Erfolgskriterien ersetzt.

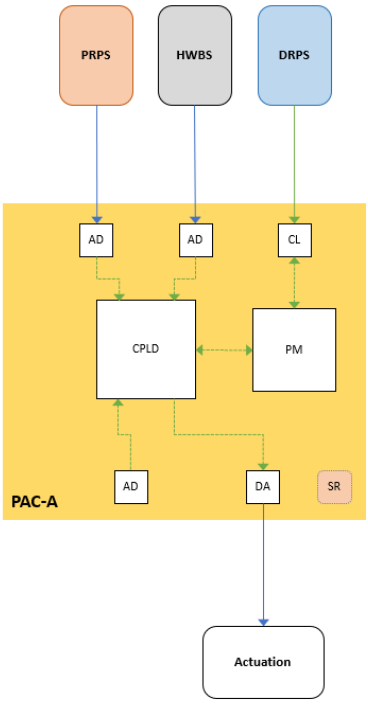


Abb. 4.4 PAC-Modell für LMFW

Abb. 4.5 zeigt repräsentativ komplett die Auslösung der Nachwärmeabfuhr (RHR) im Referenzfall. Entsprechende Bilder für die anderen Sicherheitssysteme würden ähnlich aussehen und sich im Wesentlichen nur in den Sensor- und Signalbezeichnungen unterscheiden. In allen Fällen müssen jeweils mindestens zwei der vier PAC ein Auslösesignal ans verfahrenstechnische Sicherheitssystem schicken, damit dieses im Referenzfall erfolgreich in Betrieb geht (Erfolgskriterium – „Success“[26] in der Abbildung).

[26] Das konkrete Erfolgskriterium für jedes Sicherheitssystem (2oo4 – 2 out of 4, also 2 von 4) legt fest, dass mindestens zwei PAC des jeweiligen Sicherheitssystems ein Auslösesignal erzeugen müssen, damit das Sicherheitssystem erfolgreich in Betrieb geht. Formal werden hierdurch die Sicherheitssysteme als 4x50%-Systeme behandelt, auch wenn diese im Referenzfall eigentlich nur einfach redundant sind.

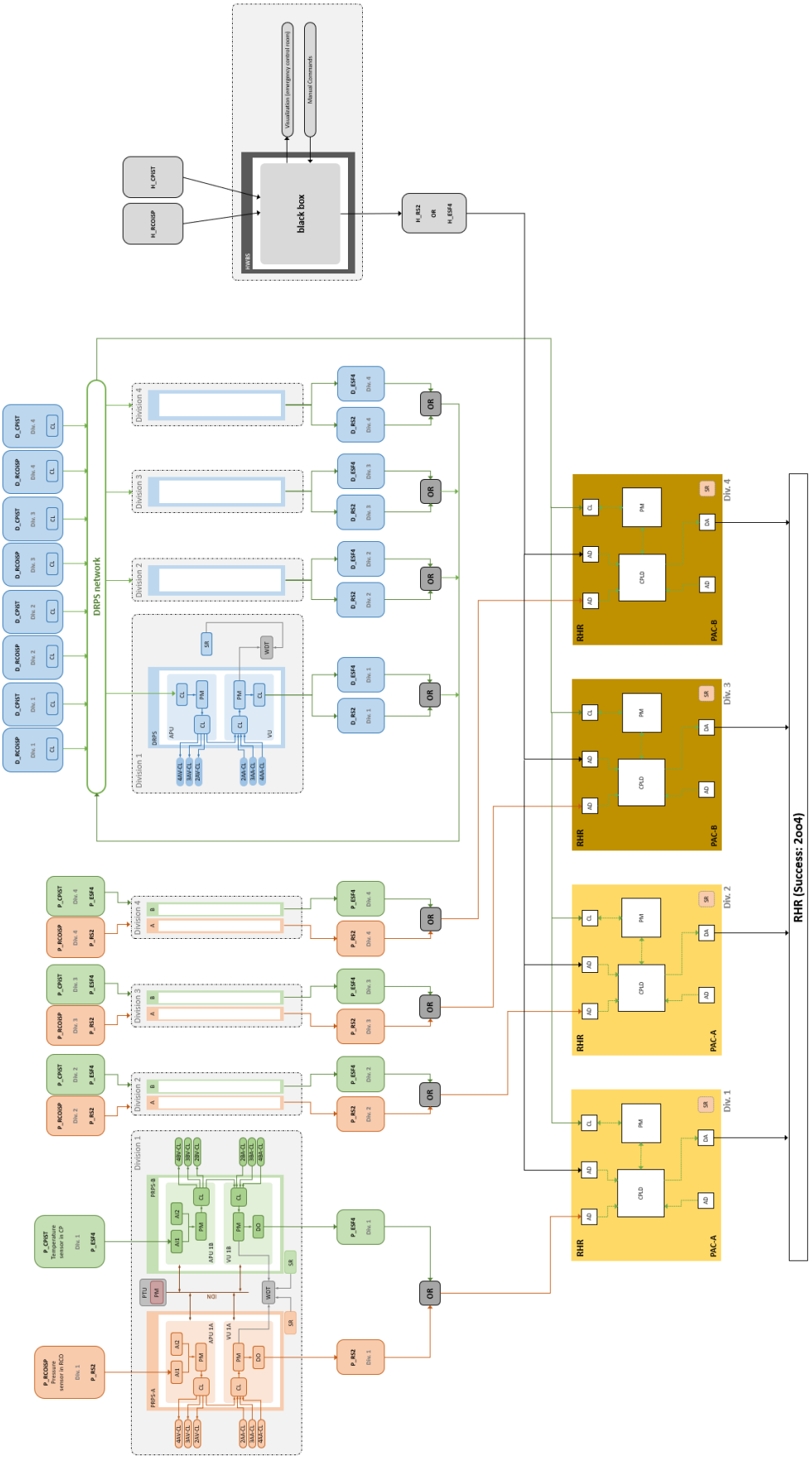


Abb. 4.5 Auslösung der Nachwärmeabfuhr (RHR) bei LMFW im Referenzfall

4.2 Fehlerbaumanalysen

Das GRS-Fehlerbaummodell der Architektur I (Gesamtmodell) für den Fall eines Hauptspeisewasserausfalls (LMFW) im Referenzfall (siehe Abb. 3.2) umfasst insgesamt 275 Basisereignisse, einen Ereignisbaum und 36 Fehlerbäume. Zusätzliche Fehlerbaum-Einzelmodelle der Einzelsysteme (PRPS, DRPS, HWBS, PAC) dienten zusätzlich dem Abgleich mit den entsprechenden Modellen für Monte-Carlo-Simulationen zur Validierung (vergleiche Kapitel 5). Diese zusätzlichen Fehlerbaum-Einzelmodelle entsprechen im grundsätzlichen Aufbau den entsprechenden Fehlerbäumen der Einzelsysteme im Gesamtmodell. Die zusätzlich untersuchten Architekturen im Rahmen dieses Vorhaben (GII, GIII, GIV – siehe Abschnitt 3.2) wurden in eigenen Fehlerbäumen untersucht, welche durch entsprechende Veränderungen am Gesamtmodell gewonnen wurden.

Die Basisereignisse innerhalb der Fehlerbäume wurden für das PRPS und das DRPS auf der Ebene von Modulausfällen erstellt (beispielsweise Ausfälle eines Prozessormoduls, PM), die Basisereignisse des HWBS berücksichtigen neben Ausfällen der Sensoren nur den Gesamtausfall der Hardware des Systems (Blackbox). Für die hochredundanten PRPS und DRPS wurden ausschließlich GVA (als Basisereignisse, vergleiche Abschnitt 4.1), für die PAC neben GVA auch zusätzlich Einzelausfälle berücksichtigt[27]. GVA und Einzelausfälle der PAC wurden ebenfalls auf Modulebene betrachtet (z. B. Ausfälle von CPLD der PAC).

Beispielhaft vermittelt Abb. 4.6 einen Eindruck von der Fehlerbaummodellierung im Rahmen dieses Vorhabens.

[27] Die jeweils vier PAC eines Sicherheitssystems (z. B. ADS) setzen sich aus zwei PAC-A und zwei PAC-B zusammen. Da PAC-A und PAC-B im Referenzfall als diversitär zueinander betrachtet werden, sind PAC-A und PAC-B für (pro Sicherheitssystem) jeweils nur zweifach redundant vorhanden. In diesem Fall werden die Beiträge von Einzelausfällen signifikant.

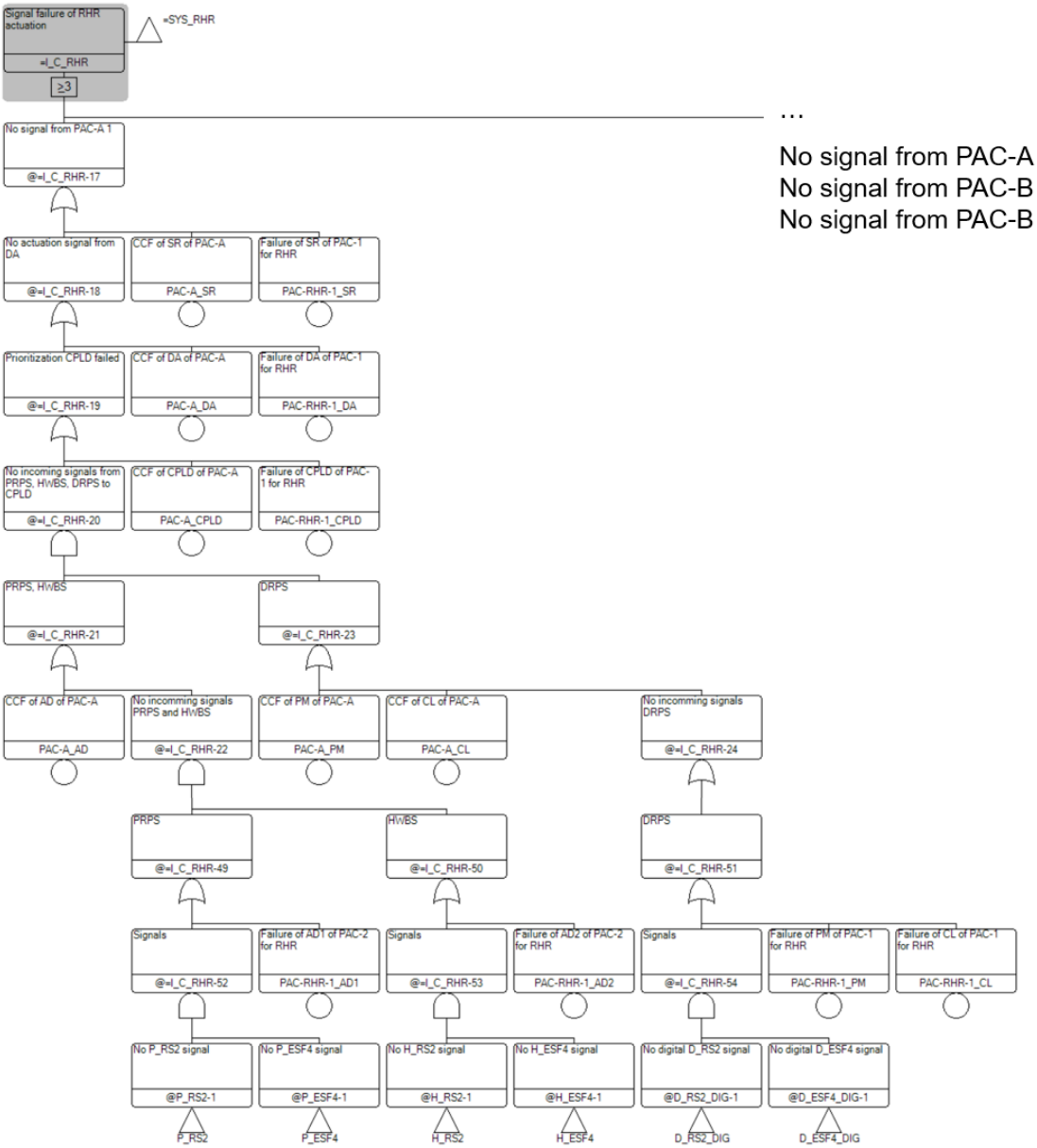


Abb. 4.6 Ausschnitt aus dem Fehlerbaum zur Auslösung der Nachwärmeabfuhr (RHR) bei LMFW für Architektur I

Diese Abbildung zeigt nur ein Viertel des ganzen Fehlerbaums zur Auslösung der Nachwärmeabfuhr (RHR). Wie oben rechts angedeutet, gehören zu diesem auch noch gleichartige Teile zu den Signalen weiterer drei PAC (PAC-A 2, PAC-B 1 und PAC-B 2). Die mit Kreisen gekennzeichneten Gatter sind Basisereignisse, Dreiecke unter einem Gatter kennzeichnen Verbindungen zu weiteren Fehlerbäumen (unten im Bild zu Fehlerbäumen von Signalen aus dem PRPS („P_...“), dem DRPS („D_...“) und dem HWBS („H_...“), oben im Bild zum RHR).

4.3 Ergebnisse

Im Rahmen dieses Vorhabens wurden Fehlerbaumanalysen für die Architekturen I, GII, GIII und GIV (vergleiche Abschnitt 3.2) durchgeführt. Eine Übersicht der dabei gewonnenen Ergebnisse (Häufigkeiten von Kernschäden (Core Damage Frequencies, CDF)) ist in Tab. 4.1 dargestellt.

Tab. 4.1 Core Damage Frequencies (CDF) für die Architekturen I, GII, GIII, GIV

Architektur	SILT-Systeme	CDF [/h]	Bewertung
I	PRPS DRPS HWBS	$5{,}59 \cdot 10^{-5}$	SILT-Systeme haben keinen signifikanten Einfluss auf die CDF
GII	PRPS DRPS	$5{,}59 \cdot 10^{-5}$	SILT-Systeme haben keinen signifikanten Einfluss auf die CDF
GIII	PRPS HWBS	$5{,}75 \cdot 10^{-5}$	SILT-Systeme haben einen geringen Einfluss auf die CDF
GIV	PRPS	$7{,}49 \cdot 10^{-5}$	PRPS hat signifikanten Einfluss auf die CDF
SILT – Sicherheitsleittechnik CDF – Core Damage Frequency			

Für alle betrachteten Architekturen kommt der dominierende Beitrag zur CDF von bestimmten Hardware-Ausfällen der Sicherheitssysteme (RHR und SWS), ein beobachtbarer Anstieg der CDF durch die Sicherheitsleittechnik ist nur für die Architekturen GIII und GIV zu erkennen.

Dies wird noch deutlicher, wenn man die Minimalschnitte[28] zu diesen Fällen betrachtet (Tab. 4.2, Tab. 4.3, Tab. 4.4, Tab. 4.5). Während für Architektur I (mit den Sicherheitsleittechniksystemen PRPS, DRPS, HWBS) Ausfälle in den Sicherheitsleittechniksystemen erst ab der 119. Ausfallkombination (siehe Tab. 4.2) mit keinerlei nennenswertem Beitrag zur CDF zu finden sind, haben Ausfälle der (einzigen) Sicherheitsleittechnik PRPS für die Architektur GIV bereits ab der dritten Kombination einen signifikanten Einfluss auf die CDF.

[28] Minimalschnitte (oder Minimal Cut Sets, MCS) repräsentieren die kleinsten Kombinationen von Basisereignissen, die ausreichen, um das unerwünschte Top-Ereignis zu verursachen. Jeder Minimalschnitt beschreibt somit eine spezifische Pfadkonstellation von Fehlern, die gemeinsam auftreten müssen, damit der (Gesamt-)Systemausfall eintritt.

Tab. 4.2 Minimalschnitte (Minimal Cut Sets, MCS) für Kernschäden (Core Damage, CD) – Architektur I (Auszug)

No.	Frequency	%	Event 1	Event 2	Event 3	Event 4
1	2,399E-05	42,93	~LMFW	=SWS_MP_FR		
2	2,399E-05	42,93	~LMFW	=RHR_MP_FR		
3	1,920E-06	3,43	~S_OIC_PM	=SWS_MP_FR		
4	1,920E-06	3,43	~S_OIC_PM	=RHR_MP_FR		
5	1,200E-06	2,15	~LMFW	=RHR_HX_FR		
…	…	…	…	…		
30	1,736E-09	0,00	~LMFW	PAC-B_DA	PAC-SWS-2_DA	
31	1,736E-09	0,00	~LMFW	PAC-B_DA	PAC-SWS-1_DA	
32	1,736E-09	0,00	~LMFW	PAC-B_DA	PAC-RHR-1_DA	
33	1,736E-09	0,00	~LMFW	PAC-B_DA	PAC-RHR-2_DA	
34	1,736E-09	0,00	~LMFW	PAC-A_DA	PAC-RHR-4_DA	
…	…	…	…	…	…	
119	1,972E-10	0,00	~LMFW	D_VU_CL_IN	H_HW	P_APU_CL
120	1,972E-10	0,00	~LMFW	D_APU_CL_IN	H_HW	P_VU_CL
121	1,972E-10	0,00	~LMFW	D_VU_CL_OUT	H_HW	P_VU_CL
122	1,972E-10	0,00	~LMFW	D_APU_CL_IN	H_HW	P_APU_CL
123	1,972E-10	0,00	~LMFW	D_VU_CL_OUT	H_HW	P_APU_CL
…	…	…	…	…	…	…

~LMFW	Loss of Main Feedwater (Initiating Event)
~S_OIC_PM	Spurious Actuation by Processor Module (PM) of OIC (Initiating Event)
=	Basic Event within Hardware of Safety System (e.g., RHR)
APU	Acquisition and Processing Unit
CL	Communication Link Module
D_	Diverse Reactor Protection System (DRPS)
DA	Digital-to-Analog Converter
FR	Fails to Run (does not start)
H_	Hard-wired Backup System (HWBS)
HX	Heat Exchanger
MP	Main Pump
P_	Primary Reactor Protection System (PRPS)
PAC	Priority and Actuation Control
RHR	Residual Heat Removal System
SWS	Service Water System
VU	Voting Unit
red color	Common Cause Failure (CCF)

Tab. 4.3 Minimalschnitte (Minimal Cut Sets, MCS) für Kernschäden (Core Damage, CD) – Architektur GII (Auszug)

No.	Frequency	%	Event 1	Event 2	Event 3
1	2,399E-05	42,90	~LMFW	=SWS_MP_FR	
2	2,399E-05	42,90	~LMFW	=RHR_MP_FR	
3	1,920E-06	3,43	~S_OIC_PM	=RHR_MP_FR	
4	1,920E-06	3,43	~S_OIC_PM	=SWS_MP_FR	
5	1,200E-06	2,15	~LMFW	=RHR_HX_FR	
6	5,000E-07	0,89	~LMFW	=SWS_MP_FS	
7	5,000E-07	0,89	~LMFW	=RHR_MV_FO	
8	5,000E-07	0,89	~LMFW	=RHR_MP_FS	
…	…	…	…	…	
27	2,380E-09	0,00	~LMFW	D_VU_CL_OUT	P_APU_CL
28	2,380E-09	0,00	~LMFW	D_APU_CL_IN	P_VU_CL
29	2,380E-09	0,00	~LMFW	D_APU_CL_IN	P_APU_CL
30	2,380E-09	0,00	~LMFW	D_APU_CL_OUT	P_VU_CL
31	2,380E-09	0,00	~LMFW	D_APU_CL_OUT	P_APU_CL
32	2,380E-09	0,00	~LMFW	D_VU_CL_IN	P_APU_CL
33	2,380E-09	0,00	~LMFW	D_VU_CL_OUT	P_VU_CL
34	2,380E-09	0,00	~LMFW	D_VU_CL_IN	P_VU_CL
…	…	…	…	…	…

~LMFW	Loss of Main Feedwater (Initiating Event)
~S_OIC_PM	Spurious Actuation by Processor Module (PM) of OIC (Initiating Event)
=	Basic Event within Hardware of Safety System (e.g., RHR)
AD	Analog-to-Digital Converter
AI	Analog Input Module
APU	Acquisition and Processing Unit
CL	Communication Link Module
D_	Diverse Reactor Protection System (DRPS)
DA	Digital-to-Analog Converter
DO	Digital Output Module
FO	Fails to Open (keeps closed)
FR	Fails to Run (does not start)
FS	Fails to Stop (does not stop)
H_	Hard-wired Backup System (HWBS)
MP	Main Pump
MV	Main Valve
P_	Primary Reactor Protection System (PRPS)
PAC	Priority and Actuation Control
RHR	Residual Heat Removal System
SWS	Service Water System
VU	Voting Unit
red color	Common Cause Failure (CCF)

Tab. 4.4 Minimalschnitte (Minimal Cut Sets, MCS) für Kernschäden (Core Damage, CD) – Architektur GIII (Auszug)

No.	Frequency	%	Event 1	Event 2	Event 3
1	2,399E-05	41,74	~LMFW	=RHR_MP_FR	
2	2,399E-05	41,74	~LMFW	=SWS_MP_FR	
3	1,920E-06	3,34	~S_OIC_PM	=SWS_MP_FR	
4	1,920E-06	3,34	~S_OIC_PM	=RHR_MP_FR	
5	1,200E-06	2,09	~LMFW	=RHR_HX_FR	
6	5,000E-07	0,87	~LMFW	=SWS_MP_FS	
7	5,000E-07	0,87	~LMFW	=RHR_MP_FS	
8	5,000E-07	0,87	~LMFW	=RHR_MV_FO	
9	4,042E-07	0,70	~LMFW	H_HW	P_VU_CL
10	4,042E-07	0,70	~LMFW	H_HW	P_APU_CL
11	3,695E-07	0,64	~S_DRPS_PM	=SWS_MP_FR	
12	3,695E-07	0,64	~S_DRPS_PM	=RHR_MP_FR	
13	1,621E-07	0,28	~LMFW	H_HW	P_VU_DO
14	1,621E-07	0,28	~LMFW	H_HW	P_APU_AI
15	1,466E-07	0,25	~LMFW	H_HW	P_APU_PM
16	1,466E-07	0,25	~LMFW	H_HW	P_VU_PM
…	…	…	…	…	…

~LMFW	Loss of Main Feedwater (Initiating Event)
~S_OIC_PM	Spurious Actuation by Processor Module (PM) of OIC (Initiating Event)
~S_DRPS_PM	Spurious Actuation by Processor Module (PM) of DRPS (Initiating Event)
=	Basic Event within Hardware of Safety System (e.g., RHR)
AI	Analog Input Module
APU	Acquisition and Processing Unit
CL	Communication Link Module
DO	Digital Output Module
FO	Fails to Open (keeps closed)
FR	Fails to Run (does not start)
FS	Fails to Stop (does not stop)
H_	Hard-wired Backup System (HWBS)
MP	Main Pump
MV	Main Valve
P_	Primary Reactor Protection System (PRPS)
RHR	Residual Heat Removal System
SWS	Service Water System
VU	Voting Unit
red color	Common Cause Failure (CCF)

Tab. 4.5 Minimalschnitte (Minimal Cut Sets, MCS) für Kernschäden (Core Damage, CD) – Architektur GIV (Auszug)

No.	Frequency	%	Event 1	Event 2	Event 3
1	2,399E-05	32,04	~LMFW	=RHR_MP_FR	
2	2,399E-05	32,04	~LMFW	=SWS_MP_FR	
3	4,879E-06	6,52	~LMFW	P_APU_CL	
4	4,879E-06	6,52	~LMFW	P_VU_CL	
5	1,956E-06	2,61	~LMFW	P_APU_AI	
6	1,956E-06	2,61	~LMFW	P_VU_DO	
7	1,920E-06	2,56	~S_OIC_PM	=SWS_MP_FR	
8	1,920E-06	2,56	~S_OIC_PM	=RHR_MP_FR	
9	1,769E-06	2,36	~LMFW	P_APU_PM	
10	1,769E-06	2,36	~LMFW	P_VU_PM	
…	…	…	…	…	
54	1,736E-09	0,00	~LMFW	PAC-B_DA	PAC-SWS-2_DA
55	1,736E-09	0,00	~LMFW	PAC-B_DA	PAC-RHR-1_AD1
56	1,736E-09	0,00	~LMFW	PAC-A_AD	PAC-SWS-4_DA
57	1,736E-09	0,00	~LMFW	PAC-B_AD	PAC-RHR-2_DA
58	1,736E-09	0,00	~LMFW	PAC-A_AD	PAC-SWS-3_AD1
…	…	…	…	…	…

~LMFW	Loss of Main Feedwater (Initiating Event)
~S_OIC_PM	Spurious Actuation by Processor Module (PM) of OIC (Initiating Event)
=	Basic Event within Hardware of Safety System (e.g., RHR)
AD	Analog-to-Digital Converter
AI	Analog Input Module
APU	Acquisition and Processing Unit
CL	Communication Link Module
D_	Diverse Reactor Protection System (DRPS)
DA	Digital-to-Analog Converter
DO	Digital Output Module
H_	Hard-wired Backup System (HWBS)
MP	Main Pump
P_	Primary Reactor Protection System (PRPS)
PAC	Priority and Actuation Control
RHR	Residual Heat Removal System
SWS	Service Water System
VU	Voting Unit
red color	Common Cause Failure (CCF)

Die Ergebnisse zeigen, dass sich die verschiedenen Sicherheitsleittechniksysteme mithilfe der GRS-Modelle adäquat darstellen lassen. Diese Modelle bieten eine fundierte Basis zur Bewertung der Sicherheitsleittechniksysteme und unterstützen damit das Ziel des Vorhabens, eine entsprechende Bewertungsgrundlage zu schaffen.

Aus dem Vergleich der Ergebnisse für die unterschiedlichen Architekturen lässt sich bereits jetzt schließen, dass durch Verwendung mindestens eines zum primären Reaktorschutzsystem (PRPS) diversitären Sicherheitsleittechniksystems (DRPS oder HWBS) für die Referenzanlage ein signifikanter Zuverlässigkeitsgewinn erreichen lässt.

Hinsichtlich einer genauen Bewertung, wie sich der Einsatz eines HWBS (insbesondere im Vergleich zum Einsatz eines DRPS) auswirkt, wären detailliertere Betrachtungen sinnvoll, in denen insbesondere festverdrahtete Backup-Systeme detaillierter untersucht werden.

Zusätzlich zur Betrachtung der Architekturen, können mit den GRS-Modellen auch noch Bewertungen der Komponenten der einzelnen Sicherheitsleittechniksysteme vorgenommen werden. Repräsentativ sind hierfür die Minimalschnitte für ausgesuchte, gleichartige leittechnische Signale[29] der drei Sicherheitsleittechniksysteme (PRPS, DRPS und HWBS) wiedergegeben (Tab. 4.6, Tab. 4.7, Tab. 4.8).

Aus den Minimalschnitten zu den repräsentativ ausgewählten Signalen (P_ESF1, D_ESF1, H_ESF1) wird ersichtlich, dass die Sensoren jeweils nur eine geringe Bedeutung für Ausfälle von Anregesignale haben. Außerdem sind in der Referenzanlage (speziell für PRPS und DRPS) hauptsächlich Kommunikationsmodule (Communication Link (Modules), CL) für fehlende Anregesignale verantwortlich.

[29] Konkret die Minimalschnitte für die Signale P_ESF1, D_ESF1 und H_ESF1. Die Abkürzung ESF steht hierbei für Engineered Safety Actuation System (ESFAS). Im Referenzfall erzeugen die Sicherheitsleittechniksysteme jeweils insgesamt pro Redundanz sechs Signale (RS1, RS2, ESF1, ESF2, ESF3, ESF4), Kombinationen von einem, zwei oder drei Signalen werden dann von jeweils einer Redundanz eines Sicherheitsleittechniksystems an jeweils ein Priorisierungsmodul (PAC) eines Sicherheitssystems gesendet (vergleiche Abb. 4.5).

Tab. 4.6 Minimalschnitte P_ESF1 (PRPS) (Q = 3,63E-4)

No.	Probability	%	Event 1
1	9,758E-05	26,85	P_VU_CL
2	9,758E-05	26,85	P_APU_CL
3	3,912E-05	10,76	P_VU_DO
4	3,912E-05	10,76	P_APU_AI
5	3,539E-05	9,74	P_APU_PM
6	3,539E-05	9,74	P_VU_PM
7	1,934E-05	5,32	P_RPVISL_2
8	0,000E+00*)	0,00	P_SR

P – Primary Reactor Protection System (PRPS)
APU – Acquisition and Processing Unit
VU – Voting Unit
AI – Analog Input (Module)
CL – Communication Link (Module)
DO – Digital Output (Module)
PM – Processor Module
RPVISL – Water Level Sensor in Reactor Pressure Vessel (RPV)
SR – Subrack
red color – Common Cause Failure (CCF)
*) Hierbei handelt es sich keineswegs um einen Fehler. Im Referenzfall sind sämtliche Ausfälle des Subracks (SR) des PRPS automatisch detektierbar. Da das GRS-Modell für das PRPS (als hochredundantes System) ausschließlich GVA berücksichtigt, treten keine (nicht-detektierte) GVA der SR auf.

Tab. 4.7 Minimalschnitte D_ESF1 (DRPS) (Q = 2,62E-3)

No.	Probability	%	Event 1
1	4,878E-04	18,62	D_VU_CL_IN
2	4,878E-04	18,62	D_RPVISL_2_CL
3	4,878E-04	18,62	D_APU_CL_IN
4	4,878E-04	18,62	D_VU_CL_OUT
5	4,878E-04	18,62	D_APU_CL_OUT
6	7,253E-05	2,77	D_VU_PM
7	7,253E-05	2,77	D_APU_PM
8	1,934E-05	0,74	D_RPVISL_2
9	1,934E-05	0,74	D_SR

D – Diverse Reactor Protection System (DRPS)
APU – Acquisition and Processing Unit
VU – Voting Unit
AI – Analog Input (Module)
CL – Communication Link (Module)
DO – Digital Output (Module)
PM – Processor Module
RPVISL – Water Level Sensor in Reactor Pressure Vessel (RPV)
SR – Subrack
red color – Common Cause Failure (CCF)

Tab. 4.8 Minimalschnitte H_ESF1 (HWBS) (Q = 8,37E-2)

No.	Probability	%	Event 1
1	8,285E-02	99,04	H_HW
2	8,771E-04	1,05	H_RPVISL_2
3	0,000E+00	0,00	HUMAN

H – Hard-wired Backup System (HWBS)
Human – Human Error (not yet included and therefore set to zero)
HW – Hardware (Black Box)
RPVISL – Water Level Sensor in Reactor Pressure Vessel (RPV)

An dieser Stelle wird ausdrücklich noch einmal darauf hingewiesen, dass es sich um Ergebnisse für generische Systeme handelt. Diese sind zwar mit mehreren internationalen Experten abgestimmt worden, sowohl der generische Referenzfall als auch speziell die dabei verwendeten Parameter und die gewonnenen Ergebnisse dürfen aber keinesfalls unkritisch auf reale Fragestellungen unmittelbar übertragen werden.

5 Validierung

Die Validierung der Modellierung des Referenzfalls (und der zusätzlich betrachteten Leittechnikarchitekturen) durch die GRS fand auf zwei unterschiedlichen Ebenen statt.

Zum einen wurden mit Hilfe der Software Matlab /MAT 25/ (inklusive des zusätzlichen Moduls Simulink) Simulationsmodelle der Sicherheitsleittechniksysteme (PRPS, DRPS, HWBS) sowie zusätzlich der Priorisierungsmodule (PAC) und des Reaktorschnellabschaltsystems (RTS) erstellt. Diese Simulationsmodelle wurden danach zur Durchführung von Monte-Carlo-Simulationen verwendet, um die auf diese Weise gewonnenen zusätzlichen Ergebnisse mit denen der Fehlerbaumanalysen vergleichen zu können.

Zum anderen konnten die Ergebnisse speziell zur Architektur I mit bereits vorhandenen Ergebnissen anderer Organisationen verglichen werden, die im Rahmen des Projekts DIGMORE /DIG 25/ bereits entsprechende eigene Modelle erstellt haben.

5.1 Monte-Carlo-Simulationen

Für die Erstellung der Simulationsmodelle, die für Monte-Carlo-Simulationen verwendet wurden, diente die Software Matlab /MAT 25/ inklusive des Zusatzmoduls Simulink. Simulink erlaubt die Erstellung von Simulationsmodellen mit Hilfe von Blockdiagrammen, die in einer grafischen Benutzeroberfläche erstellt werden können. Darüber hinaus ist es möglich Matlab-Simulationsmodelle zu kompilieren und in sogenannte DLL (Direct Link Libraries)[30] umzuwandeln. Diese DLL können dann von anderen Programmen, im Fall dieses Vorhabens eigens erstellte Python-Skripte, verwendet werden.

Abb. 5.1 bis Abb. 5.4 zeigen die Simulink-Modelle für das PRPS, das DRPS, das HWBS sowie die Priorisierungsmodule (PAC). Diese Modelle spiegeln exakt die Verhaltensweisen wider, die auch bei der Erstellung der Fehlerbaummodelle (siehe) angenommen wurden. Insbesondere wurden für die Monte-Carlo-Simulationen, die mit diesen Modellen durchgeführt wurden, dieselben Zuverlässigkeitsparamater wie bei der Fehlerbaummodellierung verwendet.

[30] Eine DLL (Dynamic Link Library) ist eine Datei in Windows-Betriebssystemen, die gemeinsam genutzte Funktionen und Ressourcen wie Code, Daten oder Bibliotheken enthält, die von anderen Programmen genutzt werden können. Sie ermöglicht es, Anwendungen modular zu gestalten, Ressourcen effizient zu teilen und den Speicherbedarf zu reduzieren, da Funktionen zur Laufzeit geladen werden.

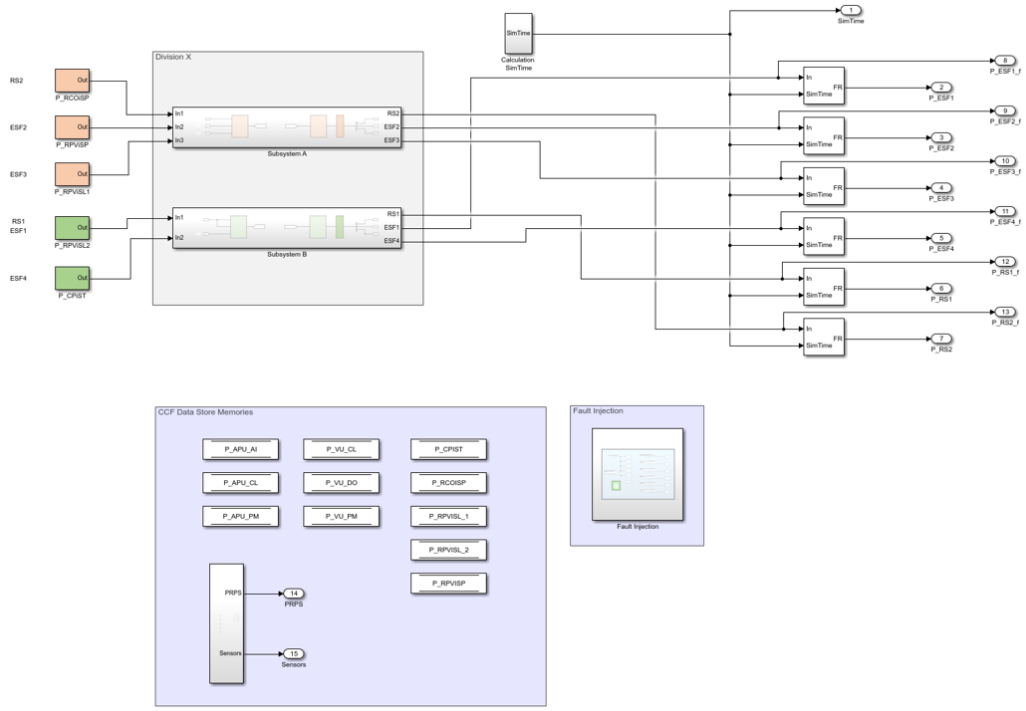


Abb. 5.1 PRPS-Modell für Monte-Carlo-Simulationen

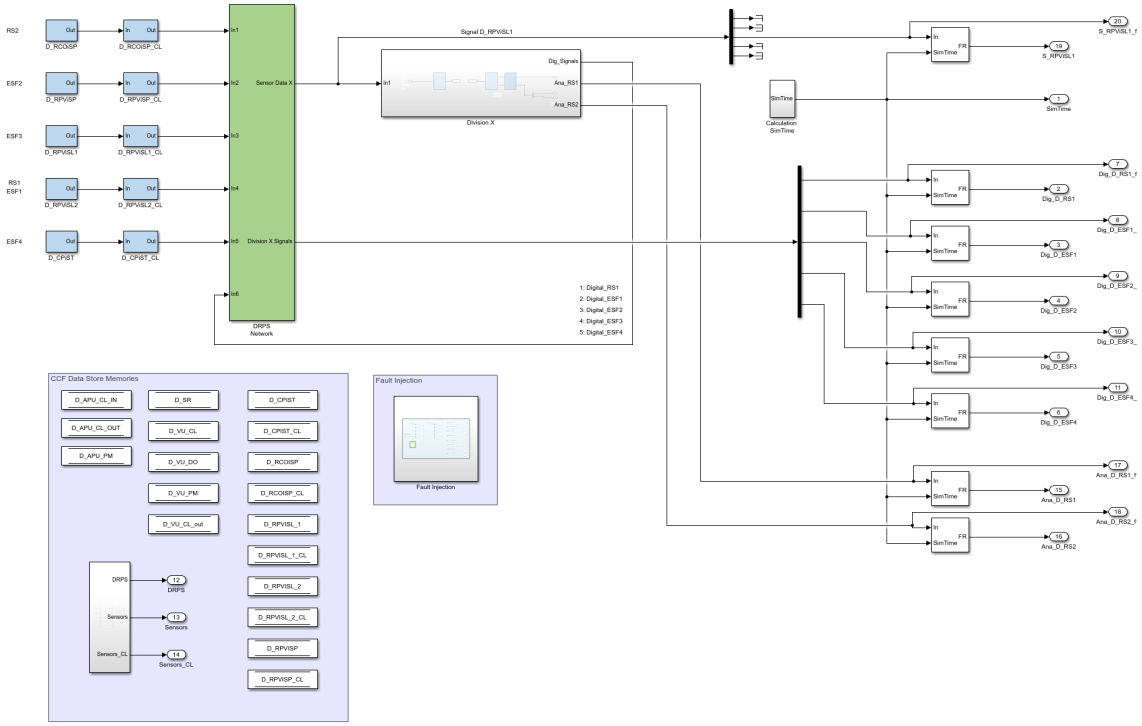


Abb. 5.2 DRPS-Modell für Monte-Carlo-Simulation

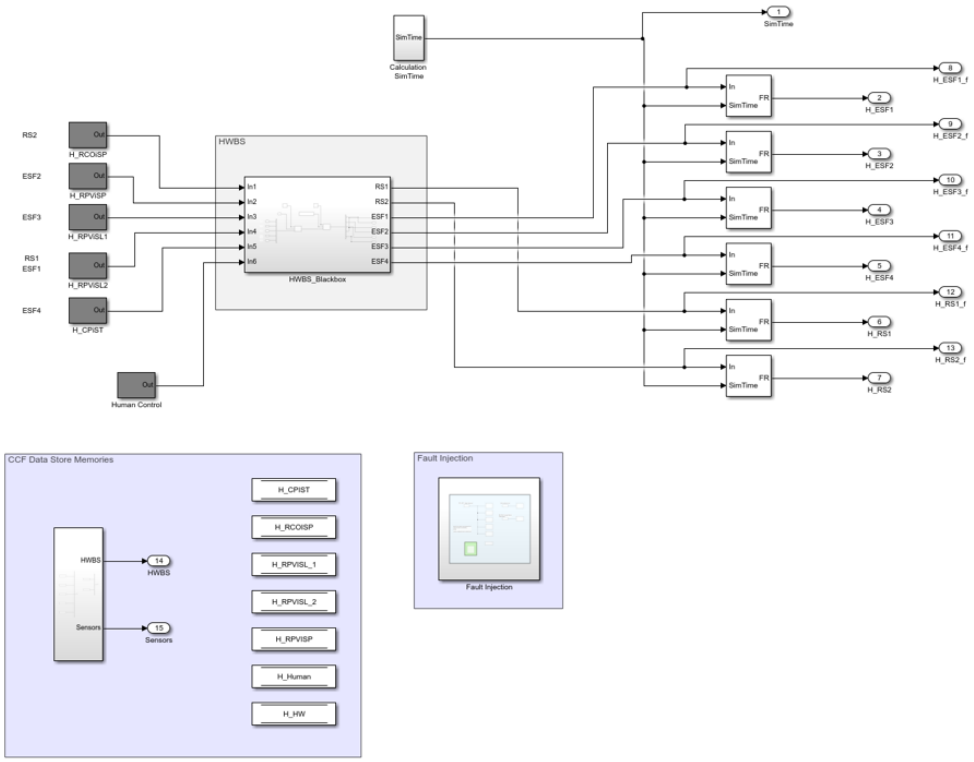


Abb. 5.3 HWBS-Modell für Monte-Carlo-Simulation

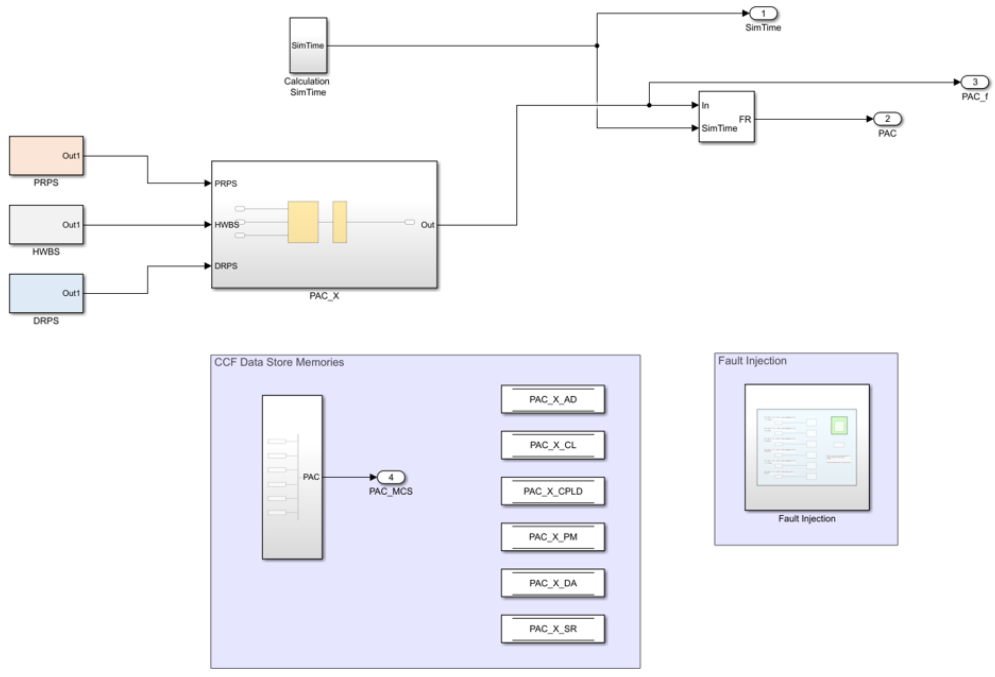


Abb. 5.4 PAC-Modell für Monte-Carlo-Simulation

Da für das PRPS und das DRPS, wie bei der Fehlerbaummodellierung, ausschließlich GVA als mögliche Ausfallarten berücksichtigt wurden, konnte bei deren Modellierung jeweils nur eine einzige Redundanz simuliert werden, ohne hierdurch im Vergleich zur Fehlerbaummodellierung auf Genauigkeit zu verzichten.

Tab. 5.1 Ergebnisse der Fehlerbaumanalysen und Monte-Carlo-Simulationen für die einzelnen Auslösesignale

Signal	Beschreibung	Fehlerbaum	Monte-Carlo
D_ESF1_DIG	No digital D_ESF1 signal	2,62E-03	2,61E-03
D_ESF2_DIG	No digital D_ESF2 signal	2,62E-03	2,62E-03
D_ESF3_DIG	No digital D_ESF3 signal	2,62E-03	2,61E-03
D_ESF4_DIG	No digital D_ESF4 signal	2,62E-03	2,61E-03
D_RS1_ANA	No analog D_RS1 signal (via DO)	2,33E-03	2,31E-03
D_RS1_DIG	No digital D_RS1 signal (via CL)	2,62E-03	2,61E-03
D_RS2_ANA	No analog D_RS2 signal (via DO)	2,33E-03	2,30E-03
D_RS2_DIG	No digital D_RS2 signal (via CL)	2,62E-03	2,61E-03
H_ESF1	No H_ESF1 signal	8,37E-02	8,36E-02
H_ESF2	No H_ESF2 signal	8,37E-02	8,36E-02
H_ESF3	No H_ESF3 signal	8,37E-02	8,36E-02
H_ESF4	No H_ESF4 signal	8,37E-02	8,36E-02
H_RS1	No H_RS1 signal	8,37E-02	8,36E-02
H_RS2	No H_RS2 signal	8,37E-02	8,36E-02
P_ESF1	No P_ESF1 signal	3,63E-04	3,69E-04
P_ESF2	No P_ESF2 signal	3,63E-04	3,69E-04
P_ESF3	No P_ESF3 signal	3,63E-04	3,68E-04
P_ESF4	No P_ESF4 signal	3,63E-04	3,77E-04
P_RS1	No P_RS1 signal	3,63E-04	3,69E-04
P_RS2	No P_RS2 signal	3,63E-04	3,69E-04

Tab. 5.1 vergleicht die mit Fehlerbäumen erlangten Ergebnisse mit solchen, die mit Hilfe von Monte-Carlo-Simulationen gewonnen wurden. Die angegebenen Zahlenwerte sind Wahrscheinlichkeiten für das Versagen bei Anforderung für verschiedene von den Sicherheitsleittechniksystemen generierte Signale. Die mittels Monte-Carlo-Simulationen

gewonnen Werte sind dabei aufgrund begrenzter Simulations-/Rechenzeit etwas ungenauer und streuen ein wenig mehr, dennoch stimmen die Ergebnisse beider Methoden hervorragend überein.

Tab. 5.2 Minimalschnitte P_ESF1 (PRPS), ermittelt mit Monte-Carlo-Simulation

No.	Probability	%	Event 1
1	10,3E-05	28,08	P_VU_CL
2	9,5E-05	25,94	P_APU_CL
3	4,0E-05	10,89	P_APU_PM
4	4,0E-05	10,87	P_VU_PM
5	3,9E-05	10,67	P_VU_DO
6	3,3E-05	9,08	P_APU_AI
7	1,6E-05	4,47	P_RPViSL_2

P – Primary Reactor Protection System (PRPS)
APU – Acquisition and Processing Unit
VU – Voting Unit
AI – Analog Input (Module)
CL – Communication Link (Module)
DO – Digital Output (Module)
PM – Processor Module
RPVISL – Water Level Sensor in Reactor Pressure Vessel (RPV)

Neben den vergleichbaren quantitativen Ergebnissen wie bei den Fehlerbaumanalysen (s. o.), können innerhalb der Monte-Carlo-Simulationen auch qualitative Ergebnisse (z. B. Minimalschnitte von Basisereignissen) gewonnen werden. Hierzu werden während der jeweiligen Simulation jedes Mal, wenn ein Totalausfall des Systems registriert wird, auch die gerade aktive Fehlerkombination (d. h. alle daran beteiligten Einzelausfälle und GVA) aufgezeichnet. Die Analyse dieser aufgezeichneten Fehlerkombinationen nach Beendigung der Simulation erlaubt dann die Bestimmung der (häufigsten[31]) Minimalschnitte, wie repräsentativ in Tab. 5.2 für das Signal P_ESF1 des PRPS dargestellt.

[31] Es gibt hier im Vergleich zur Fehlerbaumanalyse ein paar Dinge zu beachten. So können bei Totalausfall des Gesamtsystems in einer Monte-Carlo-Simulation beispielsweise zufällig auch gerade solche Fehler aktiv sein, ohne die das Gesamtsystem dennoch als ausgefallen gelten würde. Ferner werden in einer (zeitlich begrenzten) Monte-Carlo-Simulation evtl. nicht alle denkbaren Fehlerkombinationen aufgetreten sein, insbesondere wenn diese Fehlerkombinationen nur sehr unwahrscheinlich auftreten. Insgesamt sind hier sehr sorgfältige Analysen notwendig. Weitere Erläuterungen zu dieser Art der Auswertung können beispielsweise in /MUE 21/ nachgelesen werden

Vergleicht man die Ergebnisse in Tab. 5.2 mit den Ergebnissen der entsprechenden Fehlerbaumanalyse (Tab. 4.6), so lässt sich erkennen, dass beide Methoden auch hier (innerhalb erwartbarer Streuungen) zu den gleichen Ergebnissen kommen.

Die Übereinstimmung der Ergebnisse mit verschiedenen Methoden beweist für sich allein noch keine korrekte Modellierung (beispielsweise könnte ein falsches Verständnis des Modellierers in beiden Fällen gleichartig umgesetzt worden sein). Diese Übereinstimmung ist allerdings ein starkes Indiz dafür, dass in beiden Modellen (Fehlerbaummodell und Monte-Carlo-Simulationsmodell) dasselbe System beschrieben wird und dabei höchst wahrscheinlich keine versehentlichen Fehler gemacht wurden.

5.2 Vergleich mit anderen Modellen

Eine weitere, wichtige Validierungsmöglichkeit ist der Vergleich der Ergebnisse mit den Ergebnissen anderer Organisationen, die im Rahmen des Projekts DIGMORE ebenfalls Modelle desselben Referenzfalls erstellen. Hierfür werden in Tab. 5.3 die Ergebnisse für die Frequenz von Kernschäden (Core Damage Frequencies, CDF) sowie die Wahrscheinlichkeiten eines Signalversagens für drei repräsentative Signale verglichen, die von unterschiedlichen Organisationen im Rahmen von DIGMORE in deren Modellen bestimmt wurden.

Tab. 5.3 Vergleich der Ergebnisse verschiedener Organisationen (für Architektur I)

	EDF	**GRS**	**NRG**	**UJV**	**VTT**
CDF [1/h]	5,60E-05	5,59E-05	5,61E-05	5,59E-05	5,60E-05
P_ESF1	5,26E-04	3,63E-04	6,14E-04	7,05E-04	6,49E-04
D_ESF1	4,02E-03	2,62E-03	6,17E-03	4,09E-03	5,84E-03
H_ESF1	8,84E-02	8,37E-02	8,33E-02	8,35E-02	8,33E-02

EDF - Électricité de France, Frankreich
GRS – Gesellschaft für Anlagen- und Reaktorsicherheit, Deutschland
NRG – Nuclear Research and Consultancy Group, Niederlande
UJV – Nuclear Research Institute, Tschechien
VTT – VTT Technical Research Centre of Finland, Finnland

Man beachte hierbei, dass das Projekt DIGMORE /DIG 25/ noch nicht abgeschlossen ist (Stand März 2025) und voraussichtlich noch bis Mitte 2026 weiterläuft. Derzeit befindet sich das Projekt beim Abschluss der ersten Modellierungsphase, einzelne oder mehrere Zahlenwerte der anderen Organisationen können sich daher noch ändern.

Insbesondere werden in den kommenden Monaten auch noch die Unterschiede bei den Modellierungen analysiert und hierdurch die Unterschiede in den Zahlenwerten konkreten Modellierungsentscheidungen zugeordnet (wie dies bereit auch im Vorgängerprojekt DIGMAP /DIG 24/ durchgeführt wurde). Die Streuung der Werte innerhalb vergleichbarer Größenordnung entspricht aber den Erwartungen auf Basis der Erfahrungen in DIGMAP.

Es fällt auf, dass insbesondere die Zahlenwerte der GRS für die Signale der Sicherheitsleittechniksysteme PRPS (P_ESF1) und DRPS (D_ESF1) systematisch etwas kleiner sind[32]. Dies könnte insbesondere eine Folge der vereinfachten Betrachtung ausschließlich von GVA für diese Systeme sein, entsprechende Analysen werden dies in Kürze im Rahmen des Projekts DIGMORE prüfen. Ggf. werden anschließend die Modelle der GRS um Einzelfehler für diese Systeme ergänzt.

Insgesamt stimmen die bisherigen Ergebnisse allerdings gut genug überein, dass auf eine im Grundsatz korrekte Modellierung durch alle Organisationen geschlossen werden kann, die am Projekt DIGMORE teilnehmen. Im Sinne der Entwicklung einer Bewertungsgrundlage, kann die in diesem Vorhaben entwickelte Vorgehensweise daher auch als validiert betrachtet werden.

[32] Außer für die CDF, diese ist von Ausfällen der verfahrenstechnischen Sicherheitssysteme dominiert.

6 Zusammenfassung

Im Rahmen dieses Vorhabens wurden Leittechnikkonzepte neuer Reaktoranlagen eingehend analysiert, um eine Bewertungsgrundlage zu schaffen, die sich gezielt an bewertende Institutionen wie regulatorische Behörden und vergleichbare Organisationen richtet. Ziel war es, diesen Institutionen und der GRS eine systematische Methode zur Verfügung zu stellen, mit der die sicherheitstechnischen Eigenschaften und Risiken moderner Leittechnikarchitekturen und -systeme verlässlich bewertet werden können.

Zentrale Grundlage der Untersuchungen war ein Referenzfall, der als repräsentatives und realitätsnahes System entwickelt wurde, um die Bewertung und Analyse von Leittechnikarchitekturen in einem praxisbezogenen Rahmen zu ermöglichen. Dieser Referenzfall, ein vereinfachtes Modell der Leittechnikarchitektur eines generischen Siedewasserreaktors, wurde von internationalen Experten im Rahmen des OECD/NEA-Projekts DIGMORE in enger Zusammenarbeit entwickelt. Die Konzeption des Referenzfalls wurde maßgeblich durch umfangreiche Recherchen zu bestehenden Leittechnikkonzepten im Rahmen dieses Vorhabens beeinflusst, sodass der Fall eine plausible und relevante Grundlage für die Analysen bietet. Die verschiedenen sicherheitskritischen Systeme der Referenzanlage, beispielweise das automatische Druckentlastungssystem (ADS) oder das Reaktorschnellabschaltsystem (RTS), wurden im Hinblick auf ihre Interaktion mit unterschiedlichen Leittechnikarchitekturen untersucht. Ziel war es, die Auswirkungen dieser Architekturen auf die Sicherheit und Zuverlässigkeit der Anlage zu bewerten.

Im Zuge dieses Vorhabens wurden mehrere Leittechnikarchitekturen und -systeme modelliert, die sich in Komplexität und in weiteren wichtigen Aspekten (z. B. Technologien der Signalübertragung – digital oder analog) unterschieden. Neben der Analyse der Systeme diente der Referenzfall als Testumgebung zur Validierung der entwickelten Bewertungsgrundlagen. Monte-Carlo-Simulationen spielten hierbei eine zentrale Rolle, da sie die Möglichkeit boten, die Zuverlässigkeit und Robustheit der Bewertungen zu validieren. Zudem wurden die Ergebnisse mit den Analysen anderer Organisationen verglichen (die zum Referenzfall im Projekt DIGMORE eigene Modelle entwickeln), um die Plausibilität und Anwendbarkeit der Bewertungsmethodik weiter zu bestätigen.

Die Analysen zeigten beispielsweise, dass digitale Leittechniksysteme zahlreiche Vorteile hinsichtlich Flexibilität, Automatisierung und Ergonomie der Mensch-Maschine-Schnittstellen bieten. Gleichzeitig wurde jedoch deutlich, dass das Risiko von Fehlern

aufgrund gemeinsamer Ursachen (GVA) ein kritischer Punkt bleibt, der einer sorgfältigen Betrachtung bedarf. Um diesen Herausforderungen zu begegnen, werden international Leittechnikarchitekturen mit diversitäre Backup-Systemen entwickelt, die durch redundante und unabhängige Signalübertragungswege sowie z. B. durch festverdrahtete oder digitale Backup-Systeme eine erhöhte Ausfallsicherheit bieten. Durch die Arbeiten im Rahmen dieses Vorhabens wurde die Grundlage geschaffen, um weiterführende vertiefte Untersuchungen zu festverdrahteten oder digitalen Backup-Systemen in verschiedenen Ausführungen durchführen zu können. Ziel ist es, konkrete Empfehlungen zur Minimierung von Risiken und zur Verbesserung der Systemzuverlässigkeit abzuleiten.

Die Ergebnisse des Vorhabens bieten bewertenden Institutionen und der GRS eine wertvolle Grundlage für die objektive und fundierte Beurteilung neuer Leittechnikkonzepte. Durch die systematische Analyse und Validierung des Referenzfalls wurde ein belastbares Werkzeug geschaffen, das die Vergleichbarkeit unterschiedlicher Architekturen ermöglicht und dabei hilft, Schwachstellen frühzeitig zu identifizieren. Im internationalen Kontext trägt dies dazu bei, die Sicherheit und Zuverlässigkeit moderner Reaktoranlagen zu erhöhen und konsistente Standards für die Bewertung von Leittechnikkonzepten zu etablieren.

Abschließend kann festgehalten werden, dass die im Rahmen dieses Vorhabens entwickelte Bewertungsgrundlage nicht nur als Methode zur Beurteilung einzelner Projekte dient, sondern auch als Leitfaden für die Entwicklung sicherheitstechnischer Standards auf internationaler Ebene. Die Kombination aus realitätsnaher Modellierung, methodischer Analyse und umfassender Validierung ermöglicht es bewertenden Institutionen, informierte Entscheidungen zu treffen und die Sicherheit neuer Reaktoranlagen nachhaltig zu fördern.

Im noch laufenden Projekt DIGMORE werden weitere Schritte unternommen, die darauf abzielen, die entwickelte Bewertungsgrundlage zu ergänzen und zu validieren. Dabei spielt die Untersuchung des bestehenden Referenzfalls eine zentrale Rolle, der als repräsentatives, realitätsnahes Beispiel für Leittechnikarchitekturen konzipiert wurde. Dieser Referenzfall wird weiterhin genutzt, um die Sicherheit und Zuverlässigkeit moderner Leittechnikkonzepte zu analysieren und zu bewerten. Insbesondere der Vergleich mit probabilistischen Sicherheitsanalysen (PSA) anderer Organisationen bietet die Möglichkeit, die Konsistenz und Anwendbarkeit der Bewertungsmethodik zu prüfen. Monte-

Carlo-Simulationen dienen ergänzend dazu, die Modelle und Annahmen des Referenzfalls zu validieren und die Robustheit der Ergebnisse unter verschiedenen Bedingungen sicherzustellen.

Ein wichtiger Aspekt, der über das Projekt DIGMORE und dieses Vorhaben hinausreicht, ist die mögliche Entwicklung eines Satzes weiterer Referenzfälle in künftigen Vorhaben. Solche Referenzfälle könnten eine größere Bandbreite verallgemeinerter Leittechnikkonzepte abdecken und als Grundlage dienen, um Anlagenkonzepte zu bewerten, zu denen derzeit keine detaillierten Informationen verfügbar sind. Dies wäre insbesondere für Szenarien relevant, bei denen Herstellerdaten nicht zugänglich sind oder neue Technologien noch nicht umfassend untersucht wurden. Mit solchen verallgemeinerten Konzepten könnte die Bewertungsgrundlage weiter ausgebaut und auf breitere regulatorische Fragestellungen angewendet werden.

Im Rahmen von DIGMORE bleibt es hingegen bei der Analyse des bestehenden Referenzfalls und der darauf basierenden Vergleichsstudien. Die Ergebnisse werden dazu beitragen, die Anwendbarkeit der Bewertungsgrundlage auf internationaler Ebene zu bestätigen und mögliche Verbesserungen oder Erweiterungen für zukünftige Projekte zu identifizieren. Diese Perspektive unterstreicht die Bedeutung der bisher erzielten Fortschritte und zeigt auf, wie die gewonnenen Erkenntnisse in späteren Vorhaben für eine noch umfassendere Bewertung moderner Leittechnikkonzepte genutzt werden könnten. Damit schafft DIGMORE eine Basis, auf der zukünftige regulatorische Ansätze für Anlagenkonzepte aufbauen können, auch wenn diese bislang nur eingeschränkt dokumentiert oder erforscht sind.

Literaturverzeichnis

/ARI 15/ R. Arians, S. Arnold, S. Blum et. al.: *Entwicklung und Einsatz von Analysemethoden zur Beurteilung software-basierter leittechnischer Einrichtungen in deutschen Kernkraftwerken*, GRS-355, März 2015

/ASN 09/ Autorité de Sécurité Nucléaire (ASN): *Recteurs nucléaires à eau sous pression – Projet EPR-Flamanville 3 – Architecture générale du contrôle-commande et des plateformes associées*, Schreiben an die EDF, Oktober 2009

/BEL 18/ M. A. Belonosov et. al.: *Verification on application program generation and loading for safety systems of nuclear power plants based on the reverse engineering method*, Nuclear Energy and Technology 4(4): 223–228, DOI 10.3897/nucet.4.31868, 2018

/BER 10/ E. Berger: *ALS (advanced logic system), an FPGA (field programmable gate array) based safety control system as dissimilar reactor safety system*, Jahrestagung Kerntechnik 2010 der IAEA, Reference Number 43018361, 2010

/BRO 07/ C. Brockhoff: *AP1000 Overview*, ASME O&M Committee Meeting, 25.06.2007

/BRO 96/ S. Brown, J. Rose: *FPGA and CPLD architectures: a tutorial*, in IEEE Design & Test of Computers, Vol. 13, no. 2, 1996

/DIG 15/ NEA/CSNI/WGRISK: *Failure Modes Taxonomy for Reliability Assessment of Digital Instrumentation and Control Systems for Probabilistic Risk Analysis (DIGREL)*, NEA/CSNI/R(2014)16, Februar 2015

/DIG 24/ NEA/CSNI/WGRISK: *Digital I&C PSA – Comparative Application of Digital I&C Modelling Approaches for PSA (DIGMAP)*, NEA/CSNI/R(2021)14, Januar 2024

/DIG 25/ NEA/CSNI/WGRISK: *DIGMORE – A Realistic Comparative Application of DI&C Modelling Approaches for PSA*, bis Juni 2026 laufendes Projekt, 2025

/DIN 22/ DIN EN IEC 61226 VDE 0491-1:2022-09: Kernkraftwerke. Leittechnische Systeme und elektrische Energieversorgungssysteme mit sicherheitstechnischer Bedeutung – Kategorisierung von Funktionen und Klassifizierung von Systemen.

/DRS 25/ https://www.drs.com, zuletzt abgerufen am 09.01.2025

/FRA 22/ Framatome: *SPINLINE - Modular I&C digital platform dedicated to nuclear safety*, Product Sheet A3038-SPINLINE-EN, März 2022

/GEH 09/ GE-Hitachi Nuclear Energy: *Instrumentation and Control Systems – ESBWR Design Control Document*, Tier 2, Chapter 7, 26A6642AW, Revision 6, Juni 2009

/GRS 20/ GRS: *Generische Trends in der Entwicklung und Herstellung der Leittechnik für WWER-Reaktoranlagen*, Technische Notiz GRS-V-4717R01520-22/2020, April 2020

/HAN 05/ H. B. Kim: *National Report on Nuclear Power Plant I&C in the Republic of Korea*, 21st IAEA Meeting of Technical Working Group on Nuclear Power Plant Control and Instrumentation (TWG-NPPCI), Wien, 23. – 25.05.2005

/HEI 10/ M. Heinrich, M. Walter, J. Oldenburg et al.: *Bewertung neuer Reaktorkonzepte und der Übertragbarkeit sicherheitstechnischer Lösungen auf in Betrieb befindliche Anlagen – Band 2*, GRS-A-3649, Dezember 2010

/IAE 18/ International Atomic Energy Agency (IAEA): *Criteria for diverse actuation systems for nuclear power plants*, IAEA TECDOC-1848, 2018

/IAE 24/ International Atomic Energy Agency (IAEA): *Nuclear power reactors in the world*, ISBN 978-92-0-122224-4, Juli 2024

/IBR 14/ W. Z. Ibrahim und H. Sallam: *Instrumentation and control architectures in new NPPs, International Journal of Nuclear Knowledge Management*, Volume 6, No. 4, 2014

/IEC 98/ International Electrotechnical Commission (IEC): *Functional safety of electrical/electronic/programmable electronic safety-related systems*, International Standard IEC 61508, First Edition 1998-12, 1998

/IEE 08/ IEEE Power Engineering Society: *IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations*, IEEE Std 323™-2003 (R2008)- Revision of IEEE Std 323-1983, 2008

/IEE 16/ IEEE Standard Association: IEEE Standard Criteria for Programmable Digital Devices in Safety Systems of Nuclear Power Generating Stations, IEEE Std 7-4.3.2-2016, 2016

/IPS 05/ Invensys Process Systems, Nuclear Solutions: *TRICON: A Field-Proven Triple Modular Redundant (TMR) Digital System for Feedwater Control and Safety Application in Nuclear Power Plants*, WHITE PAPER, 2005

/JUN 07/ I. Jung: *Current Digital Instrumentation and Control Licensing Activities*, 21st IAEA Meeting of Technical Working Group on Nuclear Power Plant Control and Instrumentation (TWG-NPPCI), Wien, 23. – 25.05.2005

/KEP 25/ https://www.khnp.co.kr/eng/index.do, zuletzt abgerufen am 24.02.2025

/KOR 25/ https://www.kns.org/?lang=english, zuletzt abgerufen am 25.02.2025

/KRA 08/ K. Jürgen, R. Roland: *Die Entwicklung der Kernkraftwerkstechnik in Russland*, atw – International Journal for Nuclear Power, Heft 8/9, 2008

/MAT 25/ https://de.mathworks.com/products/matlab.html, zuletzt abgerufen am 22.01.2025

/MHI 07/ Mitsubishi Heavy Industry: *Mitsubishi US-APWR, Digital I&C and Electrical System*, DOE Technical Session, Juni 2007

/MUE 21/ C. Müller, E. Piljugin, P. Gebhardt, J. Shvab: *AnTeS – Entwicklung und Anwendung des Analyse- und Testsystems der GRS*, GRS-648, März 2021

/NEA 18/ OECD/NEA: *Multinational Design Evaluation Programme*, Technical Report TR-APR1400-01, März 2018

/NRC 94/ US NRC: *Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems*, NUREG/CR-6303, Dezember 1994

/NRC 01/ US NRC: *Review of Triconex Corporation*, Topical Reports 7286-545, 7286-546, Revision 1, 2001

/NRC 11/ US NRC: *AP1000 Design Control Document, Revision 19*, ML11171A500, Juni 2011

/NRC 15/ US NRC: *Guidance on Software Reviews for Digital Computer-based Instrumentation and Control Systems*, NUREG-0800/BTP 7-14, 2015

/NRC 04/ US NRC: *Advanced Reactor Licensing: Experience with Digital I&C Technology in Evolutionary Plants*, NUREG/CR-6842, April 2004

/NRC 07/ US NRC: *Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems*, NUREG-0800, BTP 7-19, 2007

/NRC 11/ US NRC: *Westinghouse AP1000 Design Control Document*, ML11171A500, Rev. 19, 2011

/RAS 21/ RASU JSC Products and services catalog, RASU.RU, 2021

/ROD 15/ J. J. Rodríguez-Andina, M.D. Valdés Peña, M. J. Moure: *Advanced Features and Industrial Applications of FPGAs - A Review*, IEEE Transactions on Industrial Informatics, Volume 11, Issue 4, Seiten 853 - 864, 2015

/ROL 10/ Rolls-Royce Civil Nuclear SAS: *Instrumentation and Control*, Technical Sheet 0004/TS/15, 2010

/TRI 11/ Invensys: *TRICON Applications in Nuclear Reactor Protection Systems – Compliance with NRC Interim Guidance ISG-2 & ISG-4, Document No.: NTX-SER-09-10*, Januar 2011

/VNI 17/ VNIIA: System Overview TPTS-NT, T142-08/210-17, Revision 1.0, 2017

/VNI 25/ https://www.vniia.ru/, zuletzt abgerufen am 24.02.2025

/WGR 25/ https://www.oecd-nea.org/jcms/pl_25617/working-group-on-risk-assessment-wgrisk, zuletzt abgerufen am 15.01.2025

/WIK 25/ https://de.wikipedia.org/wiki/EPR_(Kernkraftwerk), zuletzt abgerufen am 10.01.2025

Abkürzungsverzeichnis

ABWR	Advanced Boiling Water Reactor
ADS	Automatic Depressurization System
AEP	Atomenergoprom (Firma)
AI	Analog Input
ALS	Advanced Logic System (Leittechnikplattform)
AP1000	Advanced Passive (Reactor) 1000
APR-1400	Advanced Power Reactor 1400
APU	Acquisition and Processing Unit
APWR	Advanced Pressurized Water Reactor
ATWS	Anticipated Transient Without Scram
BDA	Beyond Design Accident
BLT	Betriebsleittechnik
BTP	Branch Technical Position (der US NRC)
CAN	Controller Area Network
CCF	Common Cause Failure
CCW	Component Cooling Water
CD	Core Damage
CL	Communication Link
CLARISSE	Contrôle Logiciel Automatique Réseau Informatique de Sécurité Sécurisé
Common Q	Common Qualified (Leittechnikplattform)
CPLD	Complex Programmable Logic Device
DAS	Diverse Actuation System
DI&C	Digital Instrumentation and Control
DO	Digital Out
DRPS	Diverse Reactor Protection System
DS&S	Diagnostics, Surveillance, and Safety (Firma)
DTM	Digital Trip Module
E/A	Ein-, Ausgabe
ECC	Emergency Core Cooling
EDF	Électricité de France (Firma)
EDI	Enhanced Digital Input

EFW	Emergency Feedwater System
EICM	Enhanced Intelligent Communications Module
EPR	European Pressurized Reactor oder Evolutionary Power Reactor, heute eigenständiger Markenname
ERO	Enhanced Relay Output (Module)
ESBWR	Economic Boiling Water Reactor
ESFAS	Engineered Safety Features Actuation System
FPGA	Field Programmable Gate Array
FTT	Fault Tolerant Technique
GE	General Electric (Firma)
GVA	Ausfälle aufgrund gemeinsamer Ursache
HDAI	High-Density Analog Input (Module)
HDDI	High-Density Digital Input (Module)
HVA	Heating, Ventilation and Air-Conditioning
HWBS	Hard-Wired Backup System
I&C	Instrumentation and Control
IDN	Intra-Division Network
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
ITC	Isolated Thermocouple
KEPCO	Korea Electric Power Corporation (Firma)
KHNP	Korea Hydro & Nuclear Power (Firma)
KKW	Kernkraftwerk
KNICS	Korean Nuclear Instrumentation and Control System (Leittechnikplattform)
LMFW	Loss of Main Feedwater
LWL	Lichtwellenleiter
MELTAC	Mitsubishi Electric Total Advanced Controller (Leittechnikplattform)
MFW	Main Feedwater
MHI	Mitsubishi Heavy Industries (Firma)
NCM	Network Communications Module
NEA	Nuclear Energy Agency
NERVIA	Nuclear Emergency Response and Vital Instrumentation Architecture

NIS	Nuclear Instrumentation System
NITC	Non-Isolated Thermocouple
NRC	(United States) Nuclear Regulatory Commission
NUMAC	Nuclear Measurement Analysis and Control (Leittechnikplattform)
OECD	Organisation for Economic Co-operation and Development
OIC	Operational I&C
PAC	Prioritization and Actuation Control
PLC	Programmable Logic Controller
PM	Processor Module
PMS	Protection and Safety Monitoring System
PROFIBUS	Process Field Bus
PROFINET	Process Field Network
PRPS	Primary Reactor Protection System
PSA	Probabilistische Sicherheitsanalyse
PTU	Periodical Testing Unit
RESA	Reaktorschnellabschaltung
RHR	Residual Heat Removal
RPS	Reactor Protection System
RS	Reactor SCRAM (RESA)
RT	Reactor Trip
RTS	Reactor Trip System
SAS	Safety Automation System
SBWR	Simplified Boling Water Reactor
SCADE	Safety Critical Application Development Environment
SCRAM	"Safety Control Rod Axe Man" (historische Herleitung) für RESA
SDO	Supervised Digital Output
SER	Safety Evaluation Report
SIL	Safety Integrity Level
SILT	Sicherheitsleittechnik
SoC	System-on-a-Chip
SPINLINE	Système de Protection Intégré et Logiciel Nucléaire Evolutif (Leittechnikplattform)

SPPA	Siemens Power Plant Automation
SR	Subrack
SWS	Service Water System
TMR	Triple Modular Redundancy
TPTS	Technological Process Control System (Leittechnikplattform)
TRICON	Triple Modular Redundant Controller (Leittechnikplattform)
TÜV	Technischer Überwachungsverein
TXS	Teleperm XS (Leittechnikplattform)
VME	Versa Module Eurocard
VNIIA	Russisches Forschungsinstitut für Automatisierung
VNIIEM	Russisches Forschungsinstitut für Elektrotechnik
VU	Voting Unit
W&T	Wissenschaft und Technik
WDT	Watchdog Timer
WWER	Wodo-Wodyanoi Energetichesky Reaktor

Abbildungsverzeichnis

Tabellenverzeichnis

Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH

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

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 978-3-911727-00-6