Entwicklung eines aktualisierten Ansatzes zur Berücksichtigung softwarebasierter Sicherheitsleittechnik in der PSA

GRS - A - 3550

Gesellschaft für Anlagen-
und Reaktorsicherheit
(GRS) mbH

**Technischer Bericht/
Technical Report**

Reaktorsicherheitsforschung-
Vorhabens Nr.:/
Reactor Safety Research-Project No.:
RS1180

Vorhabenstitel / Project Title:
Weiterentwicklung und Erprobung von Methoden und Werkzeugen für probabilistische Sicherheitsanalysen

Development and Test Applications of Methods and Tools for Probabilistic Safety Analyses

Berichtstitel:
Entwicklung eines aktualisierten Ansatzes zur Berücksichtigung softwarebasierter Sicherheitsleittechnik in der PSA

Autor / Authors:
Ewgenij Piljugin,
Joachim Herb

Berichtszeitraum / Publication Date:
August 2010

Anmerkung:

Das diesem Bericht zugrunde liegende F&E-Vorhaben wurde im Auftrag des Bundesministeriums für Wirtschaft und Technologie (BMWi) unter dem Kennzeichen RS1180 durchgeführt.

GRS - A - 3550

Kurzfassung

Im Rahmen des vom Bundesministerium für Wirtschaft und Technologie (BMWi) beauftragten Forschungs- und Entwicklungsvorhabens RS1180 sollen Methoden und Werkzeuge für die Durchführung probabilistischer Sicherheitsanalysen (PSA) weiterentwickelt und für die Anwendung PSA nutzbar gemacht werden. Zu Beginn des Vorhabens war seitens der GRS geplant, die Weiterentwicklung des Konzepts zur probabilistischen Bewertung softwarebasierter digitaler Leittechnik aus einem Forschungs- und Entwicklungsvorhaben des BMU (Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit) fortzusetzen. Hierzu war es erforderlich, die konzeptionellen Ansätze anhand des aktualisierten Standes von Wissenschaft und Technik zu überprüfen. Dementsprechend wurden vertiefte Recherchen zu Methoden der Zuverlässigkeitsbewertung der Hard- und Software einschließlich der Mensch-Maschine-Schnittstelle durchgeführt.

Auf der Grundlage der vorgenannten Recherchen wurde ein neues Konzept zur Modellierung softwarebasierter Sicherheitsleittechnik entwickelt. Im Vorhaben wurde auf den anfangs geplanten Einsatz zustandsraumorientierten Modelle zur Zuverlässigkeitsbewertung dynamischer Wechselwirkungen der Hard- und Software (z. B. Anwendung der Markov-Methodik, Petry-Netze) verzichtet. Bisher konnte weltweit kein deutlicher Fortschritt hinsichtlich Verifizierung und Nachvollziehbarkeit der Quantifizierung zustandsraumorientierter Modellierung komplexer Strukturen softwarebasierter Sicherheitsleittechnik erzielt werden.

Der Modellansatz im neuen Konzept soll eine Plattform für weitere Analysen einer generischen auf der TELEPERM-XS-System basierten Sicherheitsleittechnik bilden, um die Auswirkungen potentieller Fehler der Hard- und Software in einem Kernkraftwerk probabilistisch zu analysieren. Dieses Konzept nutzt weiterhin die Methode traditioneller Fehlerbaumanalyse der Baugruppenausfälle der Leittechnik (Hardware) und sieht die geeigneten Schnittstellen zur Berücksichtigung potentieller Fehler in der Software der Leittechnik vor. Ein geschlossenes Bewertungskonzept liegt nach wie vor weder national noch international vor.

In diesem Konzept ist vorgesehen, die aktuellen Entwicklungen hinsichtlich des Einsatzes diversitärer (dissimilarer) Leittechnik zur Beherrschung der gemeinsam verursachter Ausfälle in der softwarebasierten Sicherheitsleittechnik durch die Modellanpassungen bzw. Variantenuntersuchungen mittels Fehlerbaumtechnik zu berücksichtigen.

Darauf aufbauend soll zukünftig ein Bewertungsschema für den Diversitätsgrad der Hard- und Software erarbeitet werden.

Abstract

In the frame of ´the research and development project RS1180 funded by the Federal German Ministry for Economics and Technology (BMWi) methods and tools for probabilistic safety analysis (PSA) shall be enhanced to be applicable within a PSA. The intention at the beginning of the project was to continue the development of a conceptual approach for probabilistically assessing software based digital instrumentation and control started within another project funded by BMU (German Federal Ministry for The Environment, Nature Conservation and Nuclear Safety). In this context, the concept had to be checked with respect to the actual state-of-the-art. Therefore, in-depth investigations with regard to assessing the reliability of hard- and software including the human machine interface have been carried out.

Based on these inquiries a new concept for modelling software based safety related instrumentation and control has been developed. In the project the originally planned state control oriented models for assessing the reliability assessment of dynamic interactions between hardware and software (e.g. applicability of Markov methodology, Petry nets) has been passed. Up to the time being, considerable progress with respect to verification and traceability of the results from state control oriented modelling of complex safety related instrumentation and control structures have not been observed.

The modelling approach of the new concept shall provide a platform for further analyses of a generic safety related instrumentation and control system based on the TELEPERM-XS system for probabilistic assessment of potential failures in the hardware as well as the software of a nuclear power plant. The concept continues using the methodology of traditional fault tree analysis for instrumentation and control assemblies (hardware). Moreover, it envisages suitable interfaces for considering potential software failures of the instrumentation and control. A complete concept for assessment is nationally as well as internationally still missing.

Within this concept, it is intended to consider recent developments with respect to the application of diverse (dissimilar) instrumentation and control for the control of common cause failures of the software based instrumentation and control by model adjustments and/or analysis of the different alternatives by means of fault tree technique.

Based on these investigations, a scheme for assessing the level of diversity of the hard- and software shall be elaborated in future.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

Im Rahmen des vom Bundesministerium für Wirtschaft und Technologie (BMWi) beauftragten Vorhabens RS1180 sollen Methoden und Werkzeuge für die Durchführung probabilistischer Sicherheitsanalysen weiterentwickelt und für die Anwendung in der PSA nutzbar gemacht werden. Dabei sollen in dem Vorhaben insbesondere die Fragestellungen bearbeitet werden, bei denen aus den unterschiedlichsten Gründen eine erhöhte Dringlichkeit für derartige Untersuchungen und Analysen gegeben ist. Der Einsatz neuer Technologien und die neuen Erkenntnisse aus der Betriebserfahrung können zu neuen Anforderungen an die PSA-Methodik führen.

So ist in den letzten Jahren u. a. zu beobachten, dass digitale, softwarebasierte Automatisierungseinrichtungen die konventionelle Leittechnik in den Kernkraftwerken ersetzen. In absehbarer Zeit werden zunehmend auch sicherheitsrelevante Aufgaben durch softwarebasierte Einrichtungen gelöst.

Unter den Begriffen 'Leittechnik oder Automatisierungseinrichtungen' bezeichnet man die Gesamtheit der Einrichtungen zum Ausführen von Leittechnik-Funktionen zum Messen, Steuern, Regeln, Überwachen, Aufzeichnen und Schützen eines Prozesses oder einer technischen Einrichtung. Typische Einsatzgebiete der Leittechnik sind:

- Prozessleittechnik,
- Kraftwerksleittechnik,
- Netzleittechnik der Energieversorgung,
- Verkehrsleittechnik,
- Leittechnik in der Avionik,
- Fertigungs- bzw. Produktionsleittechnik.

Bereits in der ersten Hälfte des vorigen Jahrhunderts wurden erste leittechnische Einrichtungen mittels Analogtechnik (z. B. Relais, elektrische Messeinrichtungen) realisiert und für einfache Steuerungsfunktionen eingesetzt. In den 60er Jahren lösten festverdrahtete (verbindungsprogrammierte) elektronische Steuerungen zunehmend die Relaistechnik ab, und es wurden Prozessrechner für die Prozessüberwachung eingeführt. Beginnend in den 80er Jahren wurden in den meisten Industriezweigen zunehmend digitale Automatisierungseinrichtungen, zuerst auf der Basis digitaler integrierter Schalt-

kreise (IC) und später auf der Basis der Prozessortechnik (u. a. µP - Mikroprozessor, µC - Mikrocontroller, CPU - Zentrale Verarbeitungseinheiten der Rechner) eingesetzt. Mit dem Einzug der rechnerbasierten Automatisierungssysteme wurden zahlreiche Funktionen der Leittechnik im industriellen Bereich auf der Basis von Software realisiert.

Die softwarebasierte Leittechnik unterscheidet sich in Struktur und Funktionsweise wesentlich von der analogen Leittechnik auf Grund spezifischer Eigenschaften, u. a.:

- Wesentlich höhere Integrationsdichte der Baugruppenschaltkreise der Leittechnik. Die Hersteller elektronischer Baugruppen (Hardware) setzen auf fortschreitende Miniaturisierung von Produkten und auf die Erhöhung der Integrationsdichte zur Verbesserung der Leistungsfähigkeit einzelner Baugruppen (z. B. Multitasking - eine Baugruppe kann eine Vielzahl von Funktionen gleichzeitig ausführen, Einsatz von Co-Prozessoren, interne integrierte Speicherfunktionen).
- Flexibler Einsatz der Leittechnik-Baugruppen durch die Konfiguration- und Anwendungssoftware unter Verwendung einheitlicher Hardware. Damit kann die gleiche Hardware für die Steuerung unterschiedlicher Antriebe (z. B. für Pumpen, Ventile, Funktionsgruppensteuerung z. B zum Start von Notstromdieseln) mit flexibler Konfiguration der Vorrangsteuerung verwendet werden.
- Flexible konfigurierbare Arten der Signal- bzw. Datenübertragung (z. B. LAN-lokale Datennetze (Ethernet), Feldbus-Technik für dezentrale Kommunikation (u. a. CAN-Bus, PROFIBUS)),
- unterschiedliche Architekturen der Signal- bzw. Datenübertragung (u. a. Point-to-Point-, Stern-, Bus- und Ring-Topologien) und deren Kombinationen.

Außerdem haben softwarebasierte leittechnische Einrichtungen in der Regel die erweiterten Möglichkeiten der Fehlerdiagnose und Implementierung einer fehlertoleranten Funktionsweise, d. h. z. B. Fehlermarkierung und- filterung.

Alle o. g. Unterschiede können sowohl das Ausfallverhalten als auch die Auswirkungsbreite von Fehlern (z. B. unerkannte Ausbreitung fehlerhafter Informationen im Netzwerk redundanter Einrichtungen) in der Hard- und Software beeinflussen.

In einem Forschungs- und Entwicklungsvorhaben des Bundesministeriums für Umwelt, Naturschutz und Reaktorsicherheit (SR 2418) hat die GRS bereits einen ersten Ansatz

für eine probabilistische Zuverlässigkeitsbewertung entwickelt /PIL 04/. Die dort durchgeführten Arbeiten zur Zuverlässigkeitsbewertung softwarebasierter Leittechnik haben allerdings gezeigt, dass die konventionelle Methode der Fehlerbaumanalyse der Hardware allein nicht ausreicht, ein nachvollziehbares Ausfallverhalten eines komplexen Leittechniksystems in der PSA zu modellieren, dessen relevanten Funktionen durch Software realisiert sind.

Eine konsequente Behandlung softwarebasierter Leittechnik in probabilistischer Sicherheitsanalyse (PSA) erfordert deshalb weitere Entwicklungsarbeiten in diesem Bereich. Das Ziel der Methodenentwicklung im Vorhaben RS1180 besteht darin, diesen Ansatz zunächst hinsichtlich seiner Realisierbarkeit zu überprüfen und, soweit erforderlich, dem Stand von Wissenschaft und Technik anzupassen. Dabei sollen die zu entwickelnden Methoden zur Zuverlässigkeitsbewertung der digitalen Leittechnik deren spezifische Eigenschaften einschließlich der Software berücksichtigen und belastbare quantitative Aussagen liefern. Auf den Forschungs- und Entwicklungsbedarf zu diesem Thema wird auch in /BMU 05/ hingewiesen.

2 Untersuchungen zum Stand von Wissenschaft und Technik bei Methoden der Zuverlässigkeitsbewertung softwarebasierter Leittechnik

2.1 Allgemeine Betrachtungen zur Einführung softwarebasierter Leittechnik

In der nicht-nuklearen Industrie wird die Leittechnik immer dann als sicherheitsbezogenes System bezeichnet /DIN 09/, wenn dieses zur Ausführung von einer oder mehrerer Sicherheitsfunktionen erforderlich ist. Die Aufgabe von Sicherheitsfunktionen besteht darin das Risiko von Prozessen zu minimieren, von denen Gefahren für Mensch, Umwelt und Sachwerte ausgehen.

Die Anforderungen an die Leittechnik mit Sicherheitsfunktionen sind anwendungsunabhängig in der DIN IEC 61508-Industrienorm /DIN 09/ formuliert. Diese Industrienorm beschreibt sowohl die Art der Risikobewertung als auch die Maßnahmen zur Auslegung entsprechender Sicherheitsfunktionen bezüglich ‘Fehlervermeidung, und ‘Fehlerbeherrschung, und gilt für alle Anwendungen, in denen elektrische, elektronische oder programmierbare elektronische sicherheitsbezogene Systeme zur Ausführung von Sicherheitsfunktionen eingesetzt werden.

Sowohl die Norm DIN IEC 61508 /DIN 09/ als auch die DIN EN 61511-Norm /DIN 05/ schreiben im Wesentlichen folgende Schritte zur Minimierung des Risikos vor:

- Risikodefinition und -bewertung mittels Bestimmung detaillierten Versagenswahrscheinlichkeiten vom Sensor über die Steuerung bis hin zum Antrieb über die gesamte Lebensdauer der Komponenten,
- Festlegung und Umsetzung der Maßnahmen zur Minimierung des Restrisikos,
- Einsatz geeigneter Geräte,
- Wiederkehrende Prüfung der korrekten Einhaltung der Sicherheitsfunktionen.

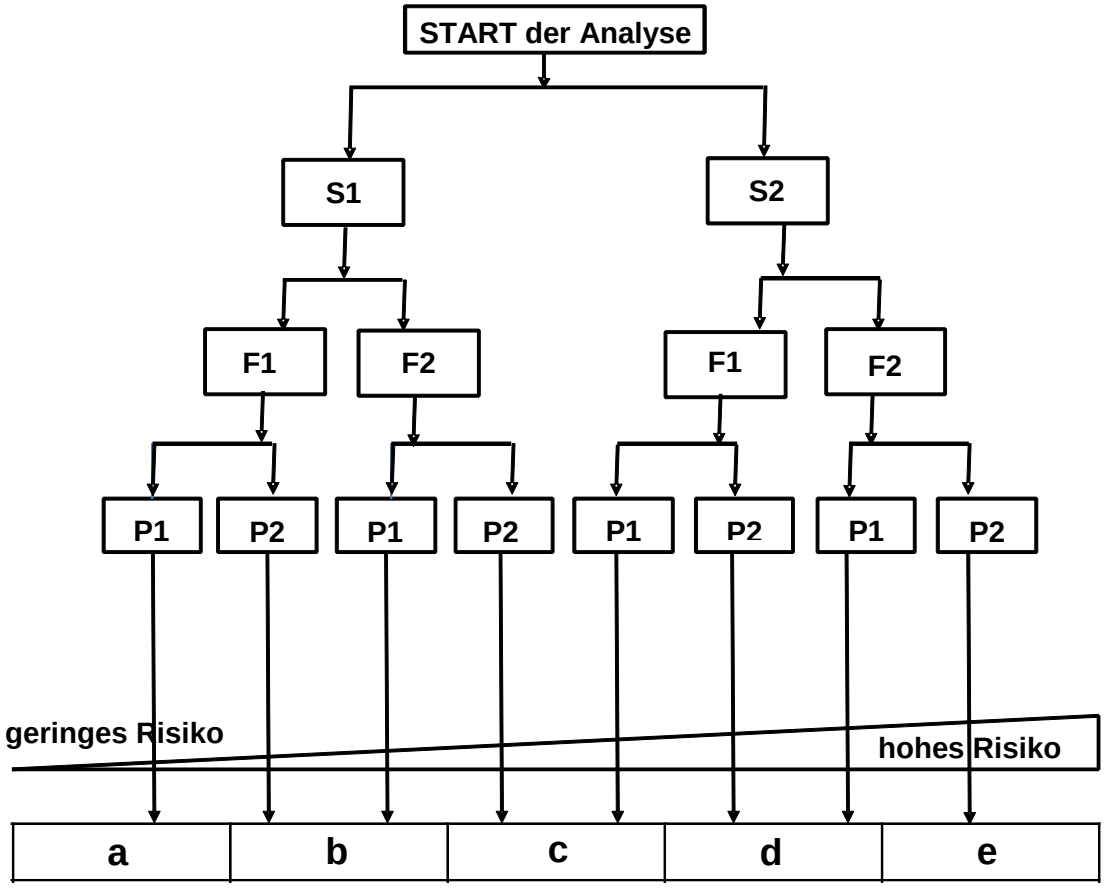
Dabei wird bereits die Anwendung eines probabilistischen Bewertungsansatzes von sicherheitsbezogenen Funktionen (u. a. im Maschinen- und Anlagenbau) durch die Sicherheitsnormen (DIN EN Normen, Typ A: Gestaltungsgrundsätze und Risikobeurteilung für Maschinen und Anlagen) im Rahmen der Gefahrenanalyse gefordert. Dieser Ansatz wurde in den DIN IEC Normen, ausgehend von der IEC 61508 /DIN 09/, auch in den untergeordneten Normen wie IEC 61511 /DIN 05/ (Anlagenbau)

und IEC (EN) 62061 /DIN 06/ (Maschinenbau) umgesetzt. Die Norm DIN EN ISO 13849 /DIN 08/ bietet dazu einen relativ einfachen Ansatz der Risikograph-Methode (vgl. Abb. 2-1) unter Anwendung probabilistischer Kriterien (Wahrscheinlichkeit gefahrbringender Ausfälle pro Stunde) zur Bestimmung des Sicherheits-Integritätslevels (SIL):

- Sicherheits-Integritätslevel 1 - 4:
  Dabei handelt es sich um vier diskrete Stufen zur Spezifizierung der Anforderung für die Sicherheitsintegrität der Sicherheitsfunktionen, wobei der SIL 4 die höchste Stufe der Sicherheitsintegrität und der SIL1 die niedrigste darstellen.

- Sicherheitsintegrität:
  Die Sicherheitsintegrität ist die Wahrscheinlichkeit, dass ein sicherheitsbezogenes System die geforderten Sicherheitsfunktionen unter allen festgelegten Bedingungen innerhalb eines festgelegten Zeitraumes anforderungsgemäß ausführt.

Die Bestimmung der Wahrscheinlichkeit eines risikorelevanten Ausfalls der Hardware (Baugruppe) kann nach dem Berechnungsmodell aus den Normen DIN IEC 62061 oder DIN EN ISO 13849 unter Verwendung der Herstellerdaten (z. B. MTTF – Mittlere Zeit bis zum Ausfall), von Daten aus der Betriebserfahrung (z. B. empirische Ausfallraten) und von Schätzungen (z. B. β-Faktor, als Anteil von Ausfällen, die eine gemeinsame Ursache haben) erfolgen. Für die Software werden in den DIN IEC Sicherheitsnormen gegenwärtig lediglich deterministische Methoden wie z. B. Software-FMEA (*F*ailure *M*ode and *E*ffect *A*nalysis) und qualitative Bewertungskriterien genannt.



S = Schwere der Verletzung
S1 - leichte, reversible Verletzungen
S2 - schwere, irreversible Verletzungen, einschließlich Tod
F = Häufigkeit/Aufenthaltsdauer der Gefährdungsaussetzung
F1 - seltene oder kurze Gefährdungsexposition
F2 - häufige oder dauernde Gefährdungsexposition
P = Möglichkeit zur Vermeidung der Gefährdung oder Begrenzung des Schadens
P1- möglich unter bestimmten Bedingungen
P2 – kaum möglich

Performance Level PL nach EN ISO 13849-1 /DIN 08/	Wahrscheinlichkeit PFH gefahrbringender Ausfälle pro Stunde [t/h]			Sicherheitsintegritäts-level SIL nach DIN-EN/IEC 62061 /DIN 06/
a	10^{-5}	≤ PFH <	10^{-4}	SIL -
b	3×10^{-6}	≤ PFH <	10^{-5}	SIL 1
c	10^{-6}	≤ PFH <	3×10^{-6}	SIL 2
d	10^{-7}	≤ PFH <	10^{-6}	SIL 3
e	10^{-8}	≤ PFH <	10^{-7}	SIL 4

a, b, c, d, e = Ziele des sicherheitsgerichteten Performance Level
Übersicht über Performance Level und Ausfallwahrscheinlichkeiten

Abb. 2-1 Anwendung der Risikograph-Methoden nach DIN EN ISO 13849 /DIN 08/

In kerntechnischen Anlagen unterscheidet man beim Einsatz der Leittechnik zwischen Betriebs- und Sicherheitsleittechnik. Dabei ist die Sicherheitsleittechnik die Leittechnik des Sicherheitssystems und der anderen Systeme mit sicherheitstechnischer Bedeutung /RSK 97/. Für die Sicherheitsleittechnik gelten hinsichtlich Nachweisführung der erforderlichen Zuverlässigkeit in Deutschland zusätzlich die Anforderungen des kerntechnischen Regelwerkes (u. a. KTA-Regeln, RSK-Leitlinien). So wird in /RSK 97/ gefordert, dass bei der Auslegung der Sicherheitsleittechnik der Kategorie 1 (Reaktorschutz) Vorsorge gegen systematische Ausfälle zu treffen ist:

- Es ist nachzuweisen, dass die Sicherheitsleittechnik der Kategorie 1 ihre Aufgaben auch dann erfüllt, wenn zusätzlich zum Störfall ein Zufallsausfall und ein systematischer Ausfall und Folgeausfälle eintreten.
- Ein systematischer Ausfall braucht dabei nicht angenommen zu werden, wenn ausreichende Maßnahmen zu seiner Vermeidung nachgewiesen werden. Während eines Instandhaltungsfalls ist auch ein Störfall zu unterstellen.

Die softwarebasierte digitale Sicherheitsleittechnik wird bereits bei der Modernisierung in- und ausländischer Kernkraftwerke eingesetzt. Neue Reaktoranlagen im Ausland werden generell unter Berücksichtigung des Einsatzes softwarebasierter Leittechnik für praktisch alle Automatisierungsaufgaben ausgelegt (siehe Abb. 2-2 und Abb. 2-3).

In deutschen Kernkraftwerken hingegen kommt softwarebasierte Leittechnik bisher fast ausschließlich in betrieblichen Systemen zum Einsatz, z. B.:

- Prozessrechner zur Beurteilung des Betriebszustandes und zur Aufzeichnung der Prozessparameter,
- Regel- und Begrenzungseinrichtungen für die Durchführung des bestimmungsgemäßen Betriebes der Anlage,
- digitale Messeinrichtungen (u. a. Neutronenflussmessung),
- Steuerung der Brennelementlademaschine
- Turbine: Steuer- und Schutzsysteme

Der Einsatz softwarebasierter Leittechnik mit Sicherheitsfunktion ist in absehbarer Zeit auch in deutschen Kernkraftwerken im Rahmen einer tiefgreifenden Modernisierung der Sicherheitsleittechnik zu erwarten. Die nach dem kerntechnischen Regelwerk (z. B. KTA 3503 /KTA 05/) typ- bzw. eignungsgeprüfte analoge Leittechnik ist einerseits

schwierig zu beschafften und andererseits ist der Instandhaltungsaufwand in der Regel größer.

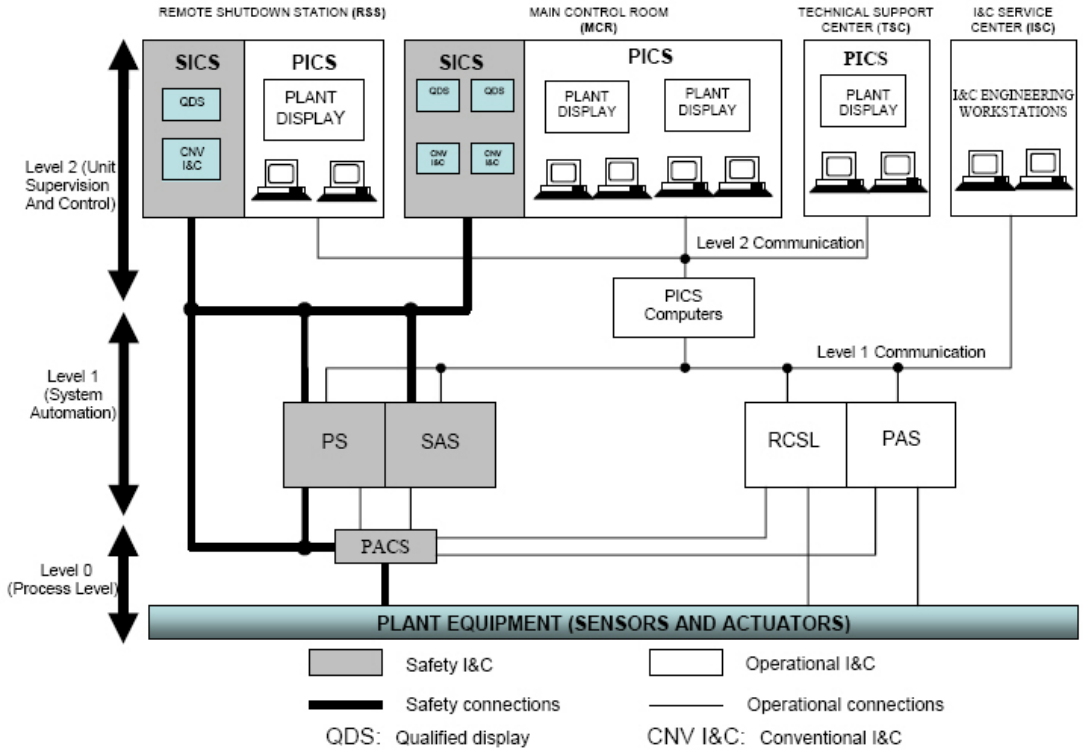


Abb. 2-2 Leittechnikkonzept einer U.S. EPR-Reaktoranlage **/**KOR 09/

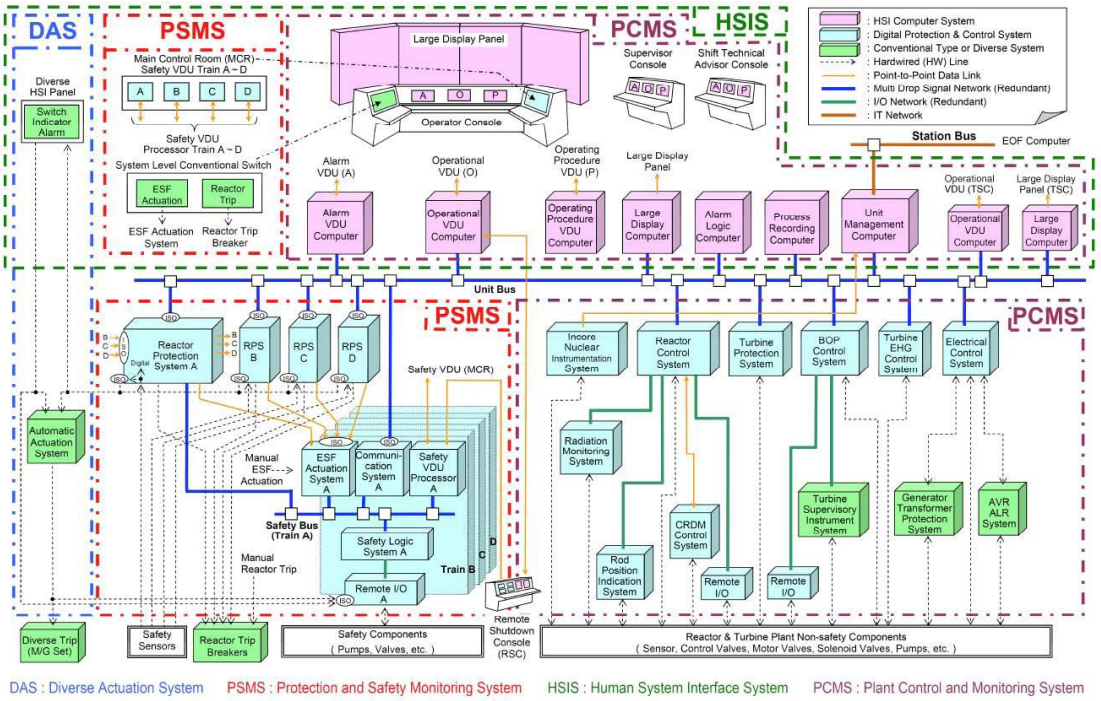


Abb. 2-3 Leittechnikkonzept einer U.S. APWR-Reaktoranlage /KOR 09/

2.2 Übersicht zu Methodenentwicklungen auf dem Gebiet probabilistischer Zuverlässigkeitsbewertung softwarebasierter Automatisierungseinrichtungen

Die bekannten Grundmodelle der Zuverlässigkeits- und Verfügbarkeitsmodellierung technischer Anlagen lassen sich prinzipiell in die Kategorien der kombinatorischen und der zustandsraumorientierten Modelle einteilen. Zur Kategorie der kombinatorischen Methoden zählen die Ereignisbaumanalyse, die Fehlerbaumanalyse und der Risikograph (gemäß Industrienorm DIN EN ISO 13849-1, DIN EN IEC 62061). Zu den zustandsraumorientierten Modellen der Zuverlässigkeitsanalyse zählen das Markov-Netz sowie die stochastischen Petri-Netze.

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

Die wesentlichen Modelle zur Bewertung der Software-Zuverlässigkeit stammen aus einer Phase, die vom Beginn der 70er Jahre bis in die 80er Jahre reicht. In diesem Zeitraum wurde intensiv an dieser Problematik gearbeitet. In der Folge hat sich hinsichtlich der Software-Zuverlässigkeit das Interesse der Industrie vermehrt auf die konstruktive Seite verlagert (fortschrittliche Software-Entwicklungsumgebungen, Standards und Methoden zur Qualitätssicherung der Software), während Software-Zuverlässigkeitsmodelle praktisch nicht mehr weiter entwickelt wurden. Dennoch befanden sich zu Beginn des neuen Jahrhunderts einige Methoden bereits in der Erprobungsphase, die grundsätzlich Potential hatten, einzelne Aspekte softwarebasierter Leittechnik hinsichtlich ihres Ausfallverhaltens zu bewerten /PIL 04/. Dazu zählten:

- statische Methoden wie
  - die Ereignisbaumanalyse,
  - die traditionelle Fehlerbaumanalyse.
- dynamische Methoden, u. a.
  - Markov-Modelle,

- Dynamic Flowgraph Methodology (DFM), Cell-To-Cell-Mapping Technique (CCMT) /ALD 07/,
- Bayesian Analysis Methoden,
- Petri-Netz-Modelle,
- die simulative Analyse der Auswirkungen von Hard- und Softwarefehlern (z. B. Fault Injection Methodology),
- Software-Metriken,
- Black-box methodologies (Schneidewind Model).

Die Methoden und der Anwendungsstand einer PSA sollen es gestatten, die Zuverlässigkeiten sicherheitstechnisch relevanter Systeme eines Kernkraftwerkes im Hinblick auf das Spektrum der zu betrachtenden Anforderungsfälle zu quantifizieren /FAK 05/. Daraus ergeben sich folgende Erfordernisse hinsichtlich Modellierung softwarebasierter Leittechnik:

- Ausreichende Detaillierung des probabilistischen Modells,
- Identifizierung der Fehlerarten der Komponenten softwarebasierter Leittechnik,
- Berücksichtigung der potentiellen Softwarefehler im probabilistischen Modell,
- Modellierung der Abhängigkeiten,
- Zuverlässigkeitskenndaten,
- Bewertung der Unsicherheiten,
- Einfache Integration in das PSA-Modell,
- Berücksichtigung der Personalfehler (HF),
- Nachvollziehbarkeit der Dokumentation und der Ergebnisse.

Eine detaillierte Übersicht über die Methoden auf dem Gebiet der probabilistischen Zuverlässigkeitsbewertung softwarebasierter Automatisierungseinrichtungen wird im Anhang B gegeben.

2.3 Review einer beispielhaften Anwendung traditioneller probabilistischer Methoden

Weitere Impulse bekam die Konzeptentwicklung der GRS aus dem Review einer beispielhaften Anwendung probabilistischer Methoden für die Analyse eines softwarebasierten Leittechniksystems der Speisewasserregelung einer Siedewasserreaktoranlage. Die GRS wurde im Oktober 2008 von der U.S. NRC ersucht, an einem Review des Berichtes des Brookhaven National Laboratory ‘Modeling a Digital Feedwater Control System (DFWCS) Using Traditional Probabilistic Risk Assessment Methods‘ /CHU 08/ teilzunehmen. Die GRS hat die darin vorgestellte Fehlerbaummodellierung der softwarebasierten Leittechnik der Speisewasserregelung in einem Siedewasserreaktor (SWR, englisch: BWR) hinsichtlich der Anwendbarkeit dieser Methode für generische Sicherheitsleittechnik in der PSA analysiert und die Ergebnisse in einer Technischen Notiz (siehe Anhang A) festgehalten.

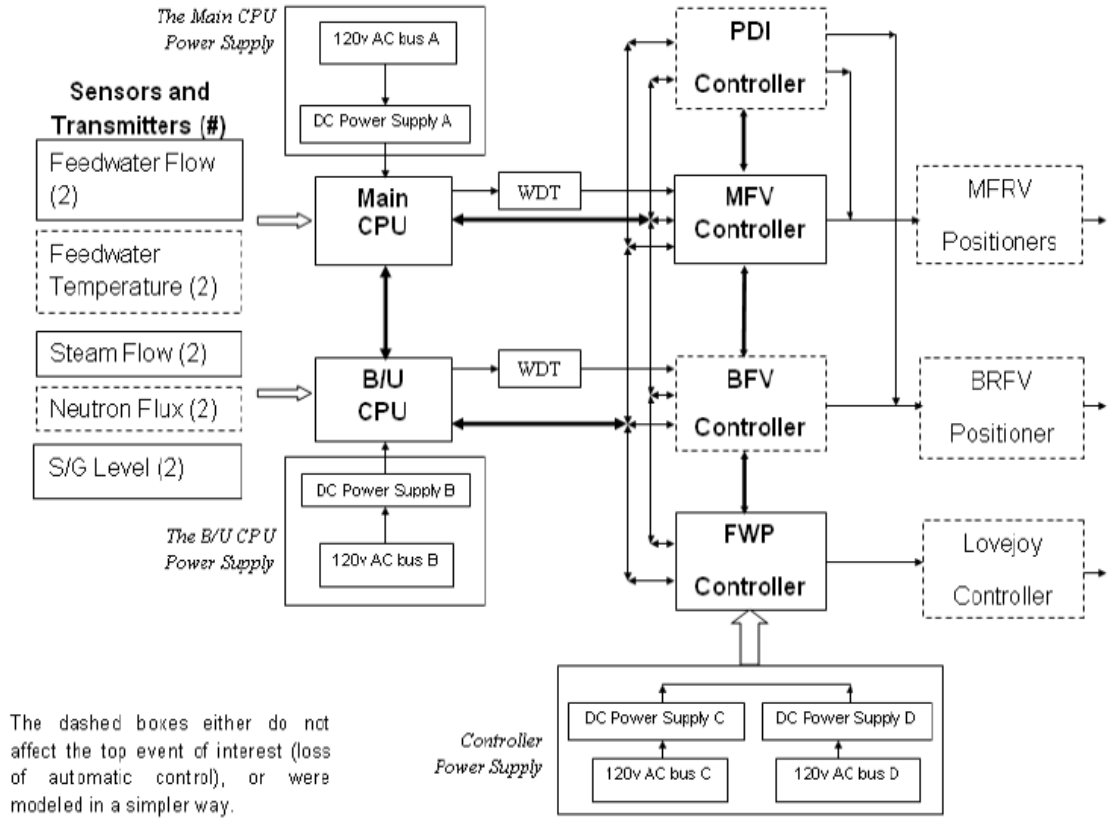


Abb. 2-4 Signalflussdiagramm des DFWCS-Modells der Speisewasserregelung /CHU 08/

Die Modellierung der digitalen Speisewasserregelung (DFWCS) erfolgte in folgenden Schritten:

– Fehlerart- und Effektanalyse (FMEA),

– Markov-Modellierung.

Die Fehlerart- und Effektanalyse (FMEA) der Regeleinrichtung hinsichtlich der Auswirkung auf die Systemfunktion wurde folgendermaßen strukturiert (siehe auch Abb. 2-5):

- System Level FMEA,
- Modul Level FMEA: FMEA-Analyse der Module,
- Detail Level FMEA: FMEA-Analyse wichtiger Komponenten (Baugruppen) der Module (siehe Abb. 2-6).

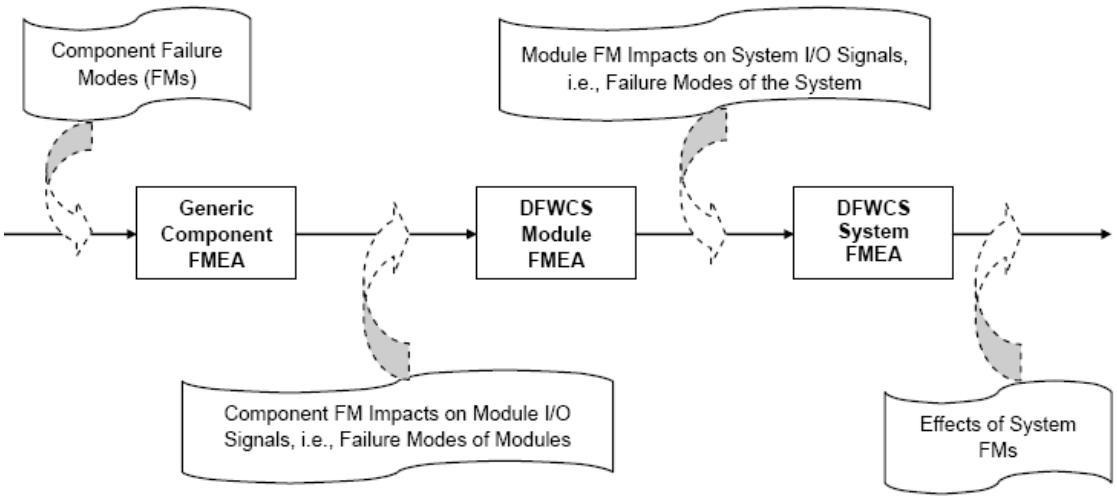


Abb. 2-5 FMEA-Analyse der DFWCS-Regeleinrichtung

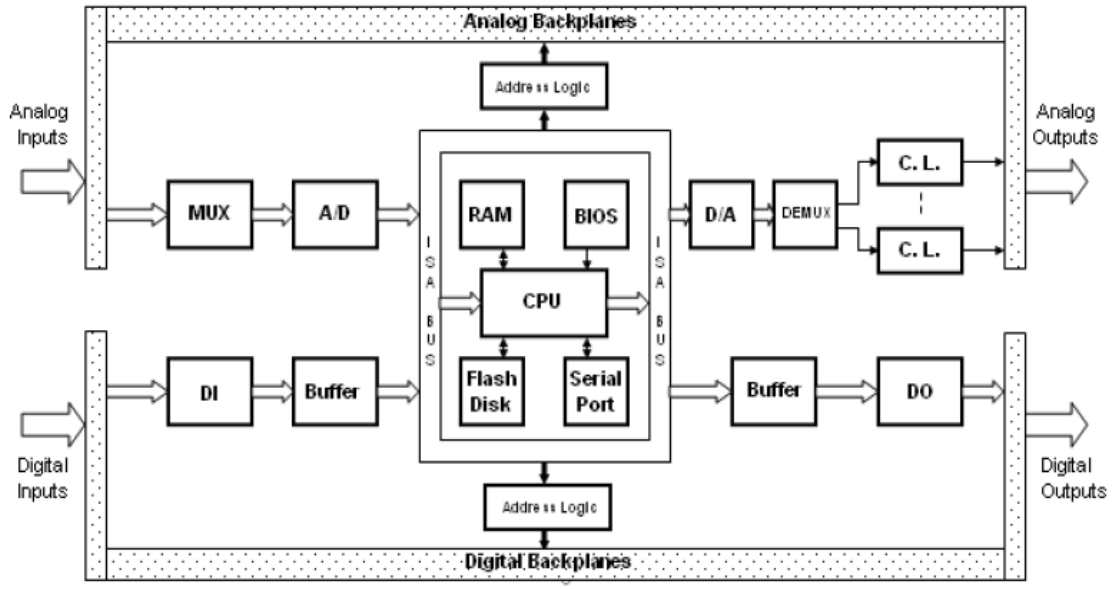


Abb. 2-6 Übersicht über die wichtigen Komponenten eines Moduls der DFWCS-Regeleinrichtung

In der nachfolgenden Tabelle sind beispielhaft die Ergebnisse der Detail-Level-FMEA des Haupt-CPU-Moduls dargestellt.

Tab. 2-1 Beispiele für die FMEA-Durchführung auf Komponentenebene des Haupt-CPU-Moduls

Failure Mode	Failure Mode Detected by		Failure Effects on Main CPU	Does the DFWCS fail?	Comments
	Application Software	WDT			
Software CCF	no	no	undetectable failure	yes	It is assumed that the CCFs of software or hardware will fail the entire system.
Hardware CCF	no	no	undetectable failure	yes	
The software on the main CPU seems to be running normally but sends erroneous output	no	no	undetectable failure	yes	This is considered an undetectable failure of the main CPU and will fail the entire system.
Software halt (CPU stops updating output)	no	yes	WDT detectable failure	no	When the WDT no longer receives a toggling signal, it will cause a fail-over of the main CPU to the back-up CPU provided that the status of the WDT is normal.
The CPU seems to be running normally but sends erroneous output	no	no	undetectable failure	yes	This is considered an undetectable failure of the main CPU and will fail the entire system.
CPU stops updating output	no	yes	WDT detectable failure	no	When the WDT no longer receives a toggling signal, it will cause a fail-over of the main CPU to the back-up CPU provided that the status of the WDT is nor-

Failure Mode	Failure Mode Detected by		Failure Effects on Main CPU	Does the DFWCS fail?	Comments
	Application Software	WDT			
					mal.
Loss of ISA bus	no	yes	WDT detectable failure	no	The input and output of the CPU rely on the ISA bus, and both the application software and the WDT can potentially detect this loss of the ISA bus. However, it is assumed that this CPU failure is detected by the WDT if its status is normal because the application software may be unable to send out any alarm or signal regarding failure of the main CPU due to the loss of both the input and output of the CPU.
Loss of RAM	no	yes	WDT detectable failure	no	Application software has to be loaded into RAM to run it. Thus, the application software cannot run upon a loss of RAM. It is assumed that the WDT can detect the loss of RAM because the software of the main CPU will no longer run and send out toggling signals.
Loss of BIOS	no	no	undetectable failure	yes	The input and output operations of the CPU rely on BIOS routines. However, it is unknown whether a loss of BIOS will cause a complete loss (or a partial loss) of inputs to and outputs from the application software and CPU; hence, the failure is conservatively assumed to be undetectable.
Loss of flash disk	no	no	undetectable failure	yes	The failure effects of a loss of the flash disk that stores software are unknown. The failure is conser-

Failure Mode	Failure Mode Detected by		Failure Effects on Main CPU	Does the DFWCS fail?	Comments
	Application Software	WDT			
					vatively assumed to be undetectable.
Loss of serial port	no	no	continued operation	no	Communication between the main CPU and PDU is via a serial port. From plant information, the CPUs send data to the PDU for display and the setpoint can be changed then is sent to the CPU via the serial port. Apparently setpoints are changed offline. Therefore, a loss of the serial port will not affect main CPU normal operation.
Fail (drift) high or fail (drift) low of current loop device	Signal dependent	no	signal dependent	signal dependent	The current loop is a linear device that may fail high or low, resulting in the associated input or output signal failing high or low. Fail low includes failures of fail to zero. The failure modes of the current loop device cause the associated signal to fail high or low. The main CPU processes different signals differently. For example, failure of level signals will cause the back-up CPU to take over control from the main CPU based on the software logic. Further analysis is needed for individual signals to determine their impacts on the main CPU module and/or the DFWCS.
Fail (drift) or fail (drift) low of voltage signal	Signal dependent	no	signal dependent	signal dependent	The voltage regulator is a major component for the voltage signal input/output. It may fail high or low, and effectively, causes the voltage signals to fail high or low. Again, further analysis of individual signals is needed to determine their impacts on the Main CPU

Failure Mode	Failure Mode Detected by		Failure Effects on Main CPU	Does the DFWCS fail?	Comments
	Application Software	WDT			
					module and/or the DFWCS.
Loss of all signals from multiplexer	yes	no	application software detectable failure	no	Loss of a signals means that the signal fails low. All analog inputs share the multiplexer. This failure mode indicates that all analog signals related to this multiplexer fail low.
Loss of one signal from multiplexer	Signal Dependent	no	signal dependent (application software detectable, undetectable, or continued operation (with latent failure)	signal dependent	The failure mode indicates a loss of a specific analog signal. The responses to this failure depend on the specific signals.
Loss of all signals from demultiplexer	yes (but cannot be corrected by the CPUs)	no	undetectable failure	yes	1. The demultiplexer is similar to the multiplexer. It is shared by all analog outputs. Loss of a signal means that the signal fails low. 2. Based on the system design information, this failure will cause a loss
Loss of one signal from demultiplexer	no	no	signal dependent (undetectable failure or continued operation)	signal dependent	1. The failure mode indicates a loss of a specific analog signal. 2. Responses to this failure depend on the individual signals.

Failure Mode	Failure Mode Detected by		Failure Effects on Main CPU	Does the DFWCS fail?	Comments
	Application Software	WDT			
All 16 bits of A/D converter stuck at zeros or ones	yes	no	application software detectable failure	no	1. Both A/D and D/A converters are linear ICs. The A/D converter is shared by all analog inputs, and its loss will entail the loss of all analog inputs. 2. Stuck at zeros or ones indicates that all analog signals fail low or high. The main CPU software can detect failures of some input signals, and then cause a fail-over.
Random bit failure of A/D converter	no	no	undetectable failure	yes	Although the main CPU software can detect some random failures, they are conservatively assumed to be undetectable and will fail the whole system.
Output of D/A converter fails (drifts) high	yes	no	application software detectable failure	no	1. The D/A converter is shared by all outputs of the main CPU, and its loss will result in a loss of all outputs. 2. This failure will cause a fail-over to the backup CPU by the main CPU application software.
Output of D/A converter fails (drifts) low	yes, (but cannot be corrected by the CPUs)	no	undetectable failure	yes	This failure will cause a loss of automatic control of the DFWCS, defined in this study as a system failure.

Failure Mode	Failure Mode Detected by		Failure Effects on Main CPU	Does the DFWCS fail?	Comments
	Application Software	WDT			
Loss of address logic	no	no	undetectable failure	yes	The address logic also is called a decoder. Although some failures of address logic might be detected by the application software, it is conservatively assumed that a loss of the address logic will result in an undetectable failure of the main CPU and fail the system.
Loss of output buffer	no	yes	WDT detectable failure	no	All digital inputs and outputs rely on buffers. Loss of the output buffer will cause the main CPU to fail to send out a toggling signal to the WDT. A WDT caused fail-over to the backup CPU will be initiated.
Loss of input buffer	no	no	undetectable failure	yes	It is conservatively assumed that a loss of the input buffer causes an undetectable failure (i.e., a toggling signal is still sent to the WDT) and fails the system.
Failure to operate or false operation of solid-state switch	no	signal depen-pen-dent	signal dependent	signal dependent	A solid-state switch carries a digital input or output signal of the main CPU. Ist failure to operate indicates that the digital signal fails to the opposite state. Therefore, based on the normal positions of the solid-state switches defined for each digital signal, the impacts of these failure modes are evaluated using the software and system design information.

Um die Auswirkung der Fehler der Komponenten der DFWCS-Module aus der Detail-Level-FMEA auf die Funktion der Antriebe (Speisewasserventile) zu analysieren, wurde eine spezielle Simulationssoftware eingesetzt. Die Software generierte so lange Fehler aus der Detail-Level-FMEA in der Signalverarbeitung der DFWCS-Regeleinrichtung (Fault Injection Methodology), bis die Ausgangsignale der Regeleinrichtung einen stabilen Zustand erreicht haben(s. Abb. 2-7).

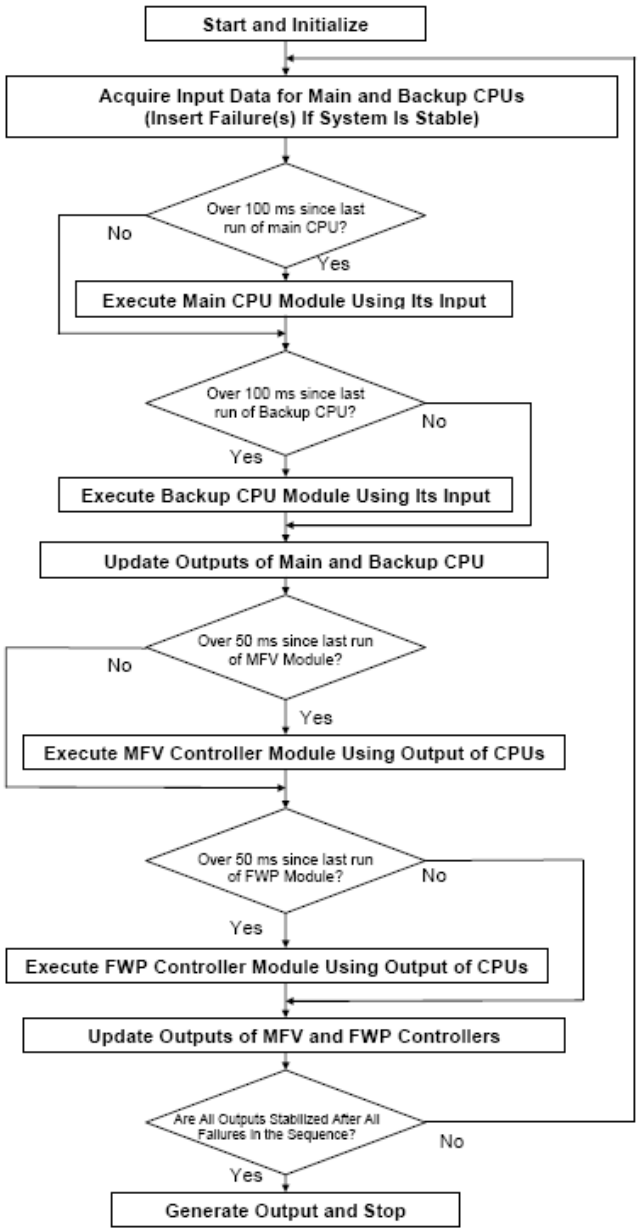


Abb. 2-7 Flussdiagramm des automatisierten FMEA-Tools /CHU 08/

Die Simulationssoftware der FMEA berücksichtigte sowohl den zeitlichen Ablauf als auch die Reihenfolge der Ausfälle. In Simulationen führten einige Kombinationen der Komponentenfehler in einer bestimmten Reihenfolge nicht zum Ausfall der Systemfunktion, aber die gleichen Kombinationen in einer anderen Reihenfolge führten zum Ausfall der Systemfunktion.

Die in /CHU 08/ vorgestellte Methode weist bezüglich der Modellierung der Hardware (u. a. CPU, Speicher, interne Bus-Verbindungen) eine sehr hohen Detailierungsgrad auf. Zur Modellierung der Betriebs- und Fehlerzustände dieser Komponenten wurde die Markov-Methode angewendet. Die Auswirkungen der Fehlerzustände der Komponenten auf die Verfügbarkeit der modellierten Regeleinrichtung wurden mit Hilfe eines automatisierten Werkzeugs bestimmt, das im Wesentlichen auf der Originalsoftware der leittechnischen Einrichtung (DFWCS) basiert.

Aus Sicht der GRS sind folgende Erkenntnisse für die Anwendung traditioneller probabilistischer Methoden für die Analyse softwarebasierter Leittechnik relevant:

- Bei einem hohen Detaillierungsgrad der Modellierung der Hardware sind automatisierte Werkzeuge zur Bestimmung der Auswirkungen von Ausfällen erforderlich. Die analytische Fehlerart- und Effektanalyse wird in diesem Fall sehr umfangreich und schwer durchführbar, da die Reihenfolge von Ausfällen das Ergebnis wesentlich beeinflussen kann.
- Der Rechenaufwand für die Simulation aller Fehlerkombinationen ist schon für das in /CHU 08/ analysierte relativ kleine System mit einer zweifach redundanten Struktur der Signalverarbeitung vergleichsweise hoch.
- Für die entwickelte Methodik besteht noch ein erheblicher Weiterentwicklungsbedarf hinsichtlich:
  - Verifikation und Validierung des verwendeten Werkzeugs zur Simulation des Systemverhaltes,
  - Modellierung gemeinsam verursachter Ausfälle (GVA) der Hard- und Software,
  - Bestimmung der Zuverlässigkeitskenngrößen der Hardware, insbesondere unter Verwendung von Betriebserfahrungen aus der Nuklearindustrie und vergleichbarer Anwendungen,
  - Bestimmung der Unsicherheiten der Modellierung.

2.4 Fazit

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

Eine Untersuchung zum Stand von Wissenschaft und Technik auf dem Gebiet der Methoden der Zuverlässigkeitsbewertung digitaler Leittechnik und deren Anerkennungskriterien für Bewertungen in Kernkraftwerken wurde an der Ohio University im Auftrag der U.S. NRC /ALD 06/ durchgeführt. Tab. 2-2 enthält die Kriterien, die auf der Basis regulatorischer Anforderungen entwickelt wurden.

Tab. 2-2 Anforderungen an die Modellierung

Nr.	Requirement
1	The model must be able to predict encountered and future failures well
2	The model must account for the relevant features of the system under consideration
3	The model must make valid and plausible assumptions
4	The model must quantitatively be able to represent dependencies between failure events accurately
5	The model must be designed so it is not hard for an analyst to learn the concepts and it is not be hard to implement
6	The data used in the quantification process must be credible to a significant portion of the technical community
7	The model must be able to differentiate between a state that fails one safety check and those that fail multiple ones
8	The model must be able to differentiate between faults that cause function failures and intermittent failures
9	The model must have the ability to provide relevant information to users, including cut sets, probabilities of failure and uncertainties associated with the results
10	The methodology must be able to model the interaction of the digital I&C system portions of accident scenarios with non-digital I&C system portions of the scenarios
11	The model should not require highly time-dependent or continuous plant state information

Die Erfüllung der in Tab. 2-2 gestellten Anforderungen wurde für die einzelnen Methoden entsprechend den Kriterien (X – erfüllt Anforderung, 0 – nicht erfüllt, ? – weitere Untersuchungen notwendig) bewertet und in Tab. 2-3 zusammengestellt.

Tab. 2-3 Erfüllung der Anforderungen durch die Methoden

Method	Requirements										
	1	2	3	4	5	6	7	8	9	10	11
Continuous Event Trees	X	X	X	X	0	?	?	X	?	?	0
Dynamic Event Trees	X	X	X	?	X	?	?	?	X	X	0
Markov Models	X	X	X	X	0	?	X	X	?	?	0
Monte Carlo Simulation	X	X	X	X	?	?	?	?	?	?	0
Petri Nets	X	X	X	X	0	?	?	?	?	?	0
Dynamic Flowgraph Methodology (DFM)	X	X	X	?	X	?	?	?	X	X	X
Dynamic Fault Trees	X	?	?	?	X	?	X	?	X	?	X
Event-Sequence Diagram (ESD)	X	X	X	X	0	?	?	?	X	X	0
GO-FLOW, system modeling technology which could be used for the quantitative calculation of reliability analysis	X	?	X	?	0	?	?	?	X	X	X
Bayesian Methodologies	X	?	?	?	0	0	?	?	?	?	X
Test Based Approaches	?	?	X	0	X	?	X	X	?	0	X
Software Metric Based Approaches	0	?	0	0	?	?	X	X	0	0	X
Schneidewind Model, non-homogeneous Poisson process (NHPP) software reliability model	X	?	?	?	?	?	?	?	0	0	X

Aus Tabelle 2-3 ergibt sich, dass z. Z. kein Modell alle Anforderungen erfüllt. Außerdem fällt auf, dass zu vielen Modellen nach Ansicht der Ohio University die Kenntnisse fehlen, um abschätzen zu können, welche die Anforderungen erfüllen.

Auch die internationale Arbeitsgruppe DICRel der OECD/Nuclear Energy Agency (NEA)/CSNI//WGRISK, an der Fachleute der GRS beteiligt waren, hat auf der Basis einer Umfrage in den Mitgliedsländern der OECD/NEA die Bewertungsmethoden ausgewertet und Empfehlungen für die Bewertung digitaler Leittechnik in der PSA erarbeitet /NEA 09/. Die bisherigen Erfahrungen der teilnehmenden Fachinstitutionen

auf dem Gebiet probabilistischer Analyse softwarebasierter Leittechnik hinsichtlich einer Modellierung relevanter Abhängigkeiten softwarebasierter Leittechnik sind in

zusammengefasst.

Tab. 2-4 Erfahrungen internationaler Teilnehmer der DICRel Arbeitsgruppe, hinsichtlich Modellierung relevanter Abhängigkeiten softwarebasierter Leittechnik

		Dependencies of the Digital Instrumentation and Control (DIC) modeled by several participants					
Organisation	**Country**	**Communication functions of the DIC**	**Support functions of the DIC**	**Sharing of hardware of the DIC**	**Fault-tolerance features of the DIC**	**Dynamic interactions of the DIC**	**CCF of the DIC**
VTT Technical Research Centre of Finland	Finland	X	XX	X			XX
IRSN, EDF, AREVA	France	X	X	X	X		X
GRS	Germany	X	XX	XX			X (Hardware)
JNES Japan Nuclear Energy Safety Organisation	Japan						XX
KAERI Korea Atomic Energy Research Institute	Republic of Korea	X			X		XX
HRP Halden Reactor Project	Norway						XX
INER, Institute of Nuclear Energy Research	Taiwan	XX	X	X	X		XX
BNL Brookhaven National Laboratory	USA	X	X	X	X		X
EPRI Electric Power Research Institute	USA		X	X			X
OSU The Ohio State University	USA	X	X	X	X	XX	X

Anmerkung: X – im Modell berücksichtigt, XX – wesentlicher Risiko-Beitrag

Auffallend ist hier, dass dynamische Interaktionen bisher nirgendwo berücksichtigt worden sind und das auch keine Einschätzung über die Höhe des Risikobeitrages besteht. Der CCF (Common Cause Failure) wird allgemein als hohes Risiko angesehen.

Des Weiteren haben die Experten besonders wichtige Aspekte für die zukünftige Methodenentwicklung identifiziert (vgl. Tab. 2-5).

Tab. 2-5 Übersicht wichtiger Aspekte für die zukünftige Methodenentwicklung /NEA 09/

		Most important topics of probabilistic modeling of the digital Instrumentation and Control (DIC)					
Organisation	**Country**	**Identification of failure modes**	**Dependencies of the DIC**	**Coverage by Fault-tolerance features**	**Failure Data (Hardware)**	**Software Failures**	**Human Reliability related DIC**
CNSC Canadian Nuclear Safety Commission	Canada			X			
IRSN, EDF, AREVA	France						X
GRS	Germany		X		X	X	
JNES Japan Nuclear Energy Safety Organisation	Japan					X	
KAERI Korea Atomic Energy Research Institute	Republic of Korea			X		X	X
INER, Institute of Nuclear Energy Research	Taiwan	X				X	
BNL Brookhaven National Laboratory	USA	X			X	X	
OSU The Ohio State University	USA		X				X

Die Verlässlichkeit von Maßnahmen der Verifizierung und Validierung von Software (V&V-Prozess: phasenspezifische Qualitätssicherung der Software) als Garant für fehlerfreie Funktion der Software ist derzeit nicht quantifizierbar, weil hierzu keine nachvollziehbaren Methoden existieren. So sind z. B. die formalen Methoden (u. a. Syntax-, Logikprüfmethoden), welche die Korrektheit von Software nachweisen sollen, für praktische Anwendungen derzeit wenig geeignet. Deshalb hat sich in vielen Industriezweigen bei sicherheitsrelevanten Anwendungen, für die eine sehr hohe Zuverlässigkeit erreicht werden muss, neben Maßnahmen zum Erzielen einer hohen Qualität der Ein-

satz diversitärer (dissimilarer) Einrichtungen mit unterschiedlicher Hard- und Software etabliert.

Die Ergebnisse der umfangreichen Untersuchungen der GRS zum Stand von Wissenschaft und Technik auf dem Gebiet der Zuverlässigkeitsbewertung softwarebasierter Leittechnik haben gezeigt, dass derzeit intensiv und branchenübergreifend nach einer anerkannten Methode hinsichtlich einer quantitativen Bewertung softwarebasierter Leittechnik geforscht wird.

Die Mitarbeit der GRS-Experten in der internationalen DICRel-Arbeitsgruppe (Arbeitsgruppe der OECD-CNSI-WGRisk) hat einige wichtige Erkenntnisse zur Weiterentwicklung des GRS-Konzeptes gegeben:

- Die Ausfälle softwarebasierter Leittechnik werden zurzeit weltweit in der PSA der Kernkraftwerke entweder versuchsweise analysiert (z. B. Verfügbarkeitsanalyse, Simulationsanalyse als Fallstudien) oder auf der Basis von Expertenschätzungen berücksichtigt.
- Die Anwendung dynamischer PSA-Methoden (u. a. Markov-Modell, Bayesian Belief Network (BBN), Dynamic Flowgraph Methodology, Petry-Netze) für eine probabilistische Bewertung softwarebasierter Leittechnik wird seitens der Mehrheit der Fachleute als nicht zielführend angesehen. Einige Ausnahmen stellen spezielle Fragestellungen hinsichtlich der Bewertung der Zuverlässigkeit von Personalhandlungen in Zusammenhang mit der Mensch-Maschine-Schnittstelle softwarebasierter Leittechnik (u. a. Bedienung der Einrichtungen, Instandhaltung) dar.

3 Konzeptentwicklung

3.1 Allgemeine Festlegungen

Auf der Grundlage der Literaturrecherchen (s. Abschnitt 2) sowie einer Analyse der digitalen Leittechnik eines sicherheitsrelevanten Systems im Vorhaben SR 2418 /PIL 04/ wurde ein Konzept zur Modellierung softwarebasierter Sicherheitsleittechnik weiterentwickelt. In diesem Vorhaben wurde auf den anfangs geplanten Einsatz zustandsraumorientierter Modelle zur Zuverlässigkeitsbewertung dynamischer Wechselwirkungen der Hard- und Software (z. B. Anwendung der Markov-Methodik, Petry-Netze) verzichtet, weil bisher weltweit kein Fortschritt hinsichtlich Verifizierung und Nachvollziehbarkeit der Quantifizierung zustandsraumorientierter Modellierung komplexer Strukturen softwarebasierter Sicherheitsleittechnik erreicht wurde.

Seit einigen Jahren wird national und international intensiv über die Bewertbarkeit von gemeinsam verursachten Ausfällen (GVA)im redundanten Reaktorschutzsystem, welches mit softwarebasierter Technik (Rechner-Technik) ausgestattet werden soll, diskutiert. Deshalb gibt es Entscheidungen einiger ausländischer Aufsichtsbehörden, strukturelle und gerätetechnische Maßnahmen in einer diversitären (dissimilaren) Leittechnik (mit unterschiedlicher Soft- und Hardware) für Sicherheitsfunktionen zu fordern. Es zeigt sich bereits, dass konkrete Maßnahmen zur Beherrschung des GVA in der softwarebasierten Leittechnik ganz unterschiedlich sein können /WOO 10/. So gibt es homogene zwei- bzw. dreifach dissimilare Leittechnik-Strukturen für den Reaktorschutz sowie heterogene Leittechnik-Strukturen mit dem Einsatz sogenannter Back-up-Leittechnik-Funktionen.

Das Konzept zur Modellierung softwarebasierter Leittechnik in der PSA soll die aktuellen Entwicklungen hinsichtlich des Einsatzes diversitärer (dissimilarer) Leittechnik zur Beherrschung der gemeinsam verursachten Ausfälle in der softwarebasierten Sicherheitsleittechnik durch Modellanpassungen bzw. Variantenuntersuchungen mittels Fehlerbaumtechnik berücksichtigen.

3.2 Modifizierter Ansatz

Unter Berücksichtigung der o. g. Festlegungen wurde das Konzept zur Modellierung eines softwarebasierten Leittechniksystems in der PSA aus dem BMU-Vorhaben

SR 2418 /PIL 04/ teilweise modifiziert und den neuen Erfordernissen angepasst. Es wurden für die Modellierung folgende Randbedingungen festgelegt:

- Der Modellansatz im neuen Konzept sollte eine Plattform für eine Analyse einer generischen auf dem TELEPERM-XS-System basierendem Sicherheitsleittechnik darstellen, um die Auswirkungen potentieller Fehler der Hard- und Software in einem Kernkraftwerk probabilistisch zu analysieren.

- Das Konzept sollte weiterhin die Methode traditioneller Fehlerbaumanalyse der Baugruppenausfälle der Leittechnik (Hardware) nutzen und die geeigneten Schnittstellen zur Berücksichtigung potentieller Software-Fehler vorsehen.

- Um einen adäquaten Detaillierungsgrad der Fehlerbaummodellierung der Hardware zu erreichen, sollte die Struktur des Modells ausgehend vom unerwünschten Ereignis, durch eine schrittweise Aufgliederung bis auf Basisereignisse mithilfe logischer Verknüpfungen, erfolgen. Die Aufgliederung der Fehlerbäume sollte so erfolgen, dass

  - Basisereignisse keine gemeinsamen funktionellen Abhängigkeiten besitzen bzw. zu verschiedenen verfahrenstechnischen Konsequenzen (z. B. Ausfall redundanter Pumpen und Ausfall gemeinsamer Ölversorgung der Pumpen) führen können,

  - die Eintrittswahrscheinlichkeit von Basisereignissen für die Hardwareausfälle möglichst aus der Betriebserfahrung ermittelbar ist,

  - die relevanten Folgefehler im Modell berücksichtigt werden. Unter Folgefehler werden Ausfälle von Einheiten verstanden, die dadurch verursacht werden, dass sie übergreifenden Einwirkungen als Folge von Ausfällen anderer Einheiten ausgesetzt werden.

Bei der Modellierung der Softwarefehler in einem Fehlerbaummodell ist die Wahl der Detaillierung bzgl. der Software ein zentrales Problem. Hierzu steht kein etablierter Ansatz zur probabilistischen Bewertung der Softwarezuverlässigkeit zur Verfügung. Für die Konzeptentwicklung wurde festgelegt, die Software jedes einzelnen Rechners zunächst in grob skizzierte, auf die Ausfallart orientierte Module (Basiselemente, die Auswirkungen potentieller Softwarefehler repräsentieren sollen) aufzuteilen:

- Module der Anwendungssoftware eines Rechners, die für die Ausführung spezifischer Leittechnik-Funktion (LEFU) zuständig sind; LEFU - Funktion zum Messen, Steuern, Regeln, Überwachen, Aufzeichnen und Schützen eines Prozesses oder einer Einrichtung;
- Betriebssystem-Software eines Rechners: Software, die den Betrieb eines Rechners ermöglicht. Sie verwaltet Betriebsmittel wie Speicher, Ein- und Ausgabegeräte, Datenaustausch und steuert die Ausführung der Anwendungssoftware.

Bei der Konzeptentwicklung soll die Frage beantwortet werden, wie die möglichen funktionalen Abhängigkeiten der unterschiedlichen Software und die Folgefehler im Fehlerbaum korrekt modelliert werden können. So ist es denkbar, dass das Betriebssystem eines Rechners als Folge eines Fehlers der Anwendungssoftware (z. B. Modul LEFU X) versagt. Die weiteren Module (z. B. LEFU Y, Z) dieses Rechners sind funktional vom Betriebssystem abhängig und können demzufolge auch ausfallen. Der o. g. Ansatz sollte helfen, die funktionale Abhängigkeit und die Ausbreitung von Folgefehlern im Fehlerbaummodell zu analysieren.

Die Zielstellung des neuen Ansatzes ist zunächst auf folgende Aspekte der Analyse softwarebasierter Leittechnik in der PSA fokussiert:

- Grundlagen schaffen, um eine ausreichende Detaillierung des probabilistischen Modells softwarebasierter Leittechnik zu definieren,
- Hilfestellung zur Identifizierung der Fehlerarten der Komponenten softwarebasierter Leittechnik zu erarbeiten,
- Eine Plattform für die Untersuchungen zur Berücksichtigung der potentiellen Softwarefehler zu entwickeln,
- Modellierung der Abhängigkeiten unterschiedlicher Strukturen softwarebasierter Leittechnik.

In Abb. 3-1 ist die Struktur der Leittechnik einer Redundanz aus dem Modell im Vorhaben SR 2418 /PIL 04/ dargestellt.

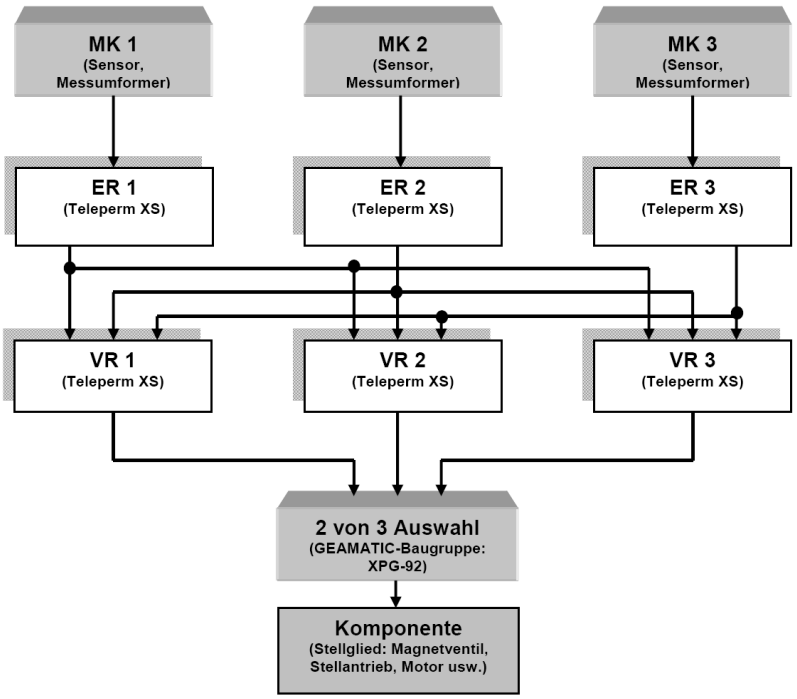


Abb. 3-1 Struktur der Leittechnik einer Redundanz aus dem Modell im Vorhaben SR 2418 /PIL 04/

In Tab. 3-1 sind wesentliche Merkmale des modifizierten Modellansatzes im Vergleich zum Modell aus dem Vorhaben SR 2418 (s. Abb. 3-1, /PIL 04/) dargestellt.

Tab. 3-1 Gegenüberstellung der Modellentwicklung zur Bewertung softwarebasierter Leittechnik

	Konzept aus dem Vorhaben SR 2418 /PIL 04/	**Konzept des aktuellen Modellansatzes**
Probabilistische Analysemethode	traditionelle Fehlerbaummodellierung	traditionelle Fehlerbaummodellierung
Gegenstand der Analyse	Sicherheitsleittechnik einer Referenzanlage: zweisträngiges Notstandssystem einer Siedewasserreaktoranlage (siehe Abb. 3-1)	Sicherheitsleittechnik einer generischen Reaktoranlage: Leittechnik-Funktion eines generischen Reaktorschutzsystems (siehe Abb. 3-2)
Leittechniksystem	TELEPERM XS, 1. Generation	TELEPERM XS, 1. bzw. 2. Generation
Struktur der Leittechnik-Funktionen	2-fache Redundanz: 3 Teilsysteme mit interner 2-von-3-Logik für Steuerung der verfahrenstechnischen Komponenten jedes Stran-	4-fache Redundanz: 2-von-4-Logik für Steuerung der verfahrenstechnischer Komponenten jedes Stranges

	Konzept aus dem Vorhaben SR 2418 /PIL 04/	Konzept des aktuellen Modellansatzes
	ges	
Struktur der Signalverarbeitung in jeder Redundanz bzw. Teilsysteme jeder Redundanz	1. Feldebene: analoge Messwerterfassung) 2. Signalverarbeitung: softwarebasierter Erfassungs- und Verarbeitungsrechner 3. Ansteuerung: analoge Wertungslogik und analoge Antriebssteuerung (GEAMATIC)	1. Feldebene: analoge Messwerterfassung) 2. Signalverarbeitung: softwarebasierter Erfassungs- und Verarbeitungsrechner 3. Ansteuerung: softwarebasierter Voter-Rechner und digitale Antriebssteuerung
Detaillierungstiefe (Hardware)	TXS-Baugruppen, GEAMATIC-Baugruppen (analoge Voter und Antriebssteuerung)	TXS-Baugruppen, digitale programmierbare Antriebssteuerung (u.a. AV42)
Bestimmung der Ausfallart der Hardware	Ergebnisse der Fehlerart- und Auswirkungsanalyse (FMEA), TXS-Betriebserfahrung	Ergebnisse der Fehlerart- und Auswirkungsanalyse (FMEA), generische Betriebserfahrung, Expertenschätzungen
Berücksichtigung der Software	Software ist im Fehlerbaummodell nicht berücksichtigt. Es wurde zunächst ein Ansatz zur Bewertung der Komplexität der Anwendungssoftware entwickelt.	Im Fehlerbaummodell sind Basisereignisse implementiert, die Auswirkung der GVA unterschiedlicher Software (Betriebssystem, Anwendungssoftware) repräsentieren sollen. Die Quantifizierung dieser Basisereignisse sollte zum späteren Zeitpunkt durch Schätzungen auf der Basis der Betriebserfahrungen erfolgen.

Die Modellierung der Fehlerbäume der Sicherheitsleittechnik soll anfangs den Bereich von der Messung der relevanten Parameter bis zur Bildung der Auslösesignale (Steuerung der verfahrenstechnischen Komponenten) umfassen. Das Modell wird unter folgenden Annahmen aufgebaut:

- 4-fach redundante Signalverarbeitung, wobei nur einige typische Ausfälle ausgewählter HW-Komponenten der TXS-Rechner modelliert werden, die für das Top-Ereignis (Ausfall der Anregung oder eine fehlerhafte Anregung) relevant sind.

– Anmerkung: diejenigen Baugruppen, die die Bildung und Ausgabe von Meldungen übernehmen, werden in der Analyse nur dann berücksichtigt, wenn deren Ausfälle Rückwirkungen auf die Funktion der Leittechnik-Funktion bewirken können.

- Verfahrenstechnik der Reaktoranlage wird nicht im Fehlerbaum der Sicherheitsleittechnik modelliert, d. h. nur die relevanten Schnittstellen (Messung, Stellglieder) werden im Modell berücksichtigt.

Die im Konzept festgelegte Struktur der Hardware der generischen Sicherheitsleittechnik ist in Abbildung 3-2 dargestellt.

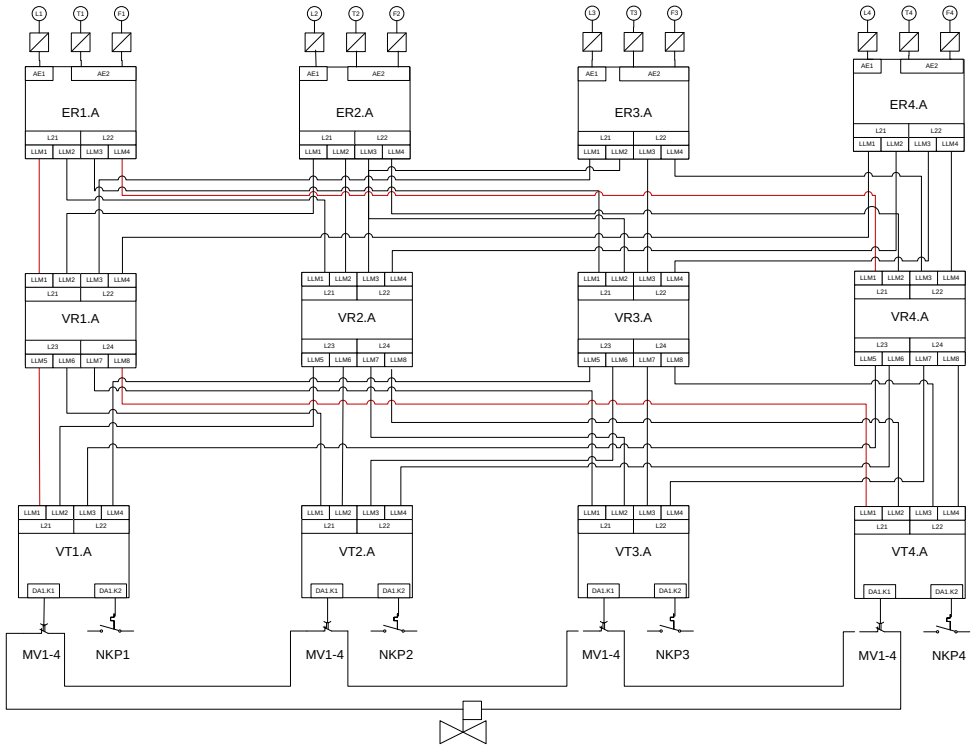


Abb. 3-2 Modell generischer Sicherheitsleittechnik im aktuellen Vorhaben - Struktur der Hardware (Basis: TELEPERM- XS-Leittechnikbaugruppen)

Es werden zunächst nur zwei Leittechnik-Funktionen (LEFU) modelliert:

- LEFU „DDA-FDL“ (Durchdringungsabschluss der FD-Leitungen): Fehler der Ansteuerung der Magnetventile redundanzübergreifend,
- LEFU „NKP EIN“ (Notkühlung): Ausfall der EIN-Ansteuerung einer Notkühlpumpe redundanzbezogen.

Die Leittechnik-Funktionen LEFU „DDA-FDL“ und LEFU „NKP EIN“ werden im Modell durch folgende leittechnischen Einrichtungen realisiert:

- Analogteil in den Redundanzen 1 – 4 (Messgeber, Messumformer, Signalaufbereitung/SAA-Baugruppe werden vereinfacht zu einer Komponente zusammengefasst):
  - Füllstandsmessung im Reaktor L1, L2, L3, L4,
  - Kerntemperaturmessung im Reaktor T1, T2, T3, T4,
  - Frischdampfdurchsatzmessung in den FD-Leitungen F1, F2, F3, F4.
- Erfassungsrechner in den Redundanzen 1 – 4:
  - ER1.A, ER2.A, ER3.A, ER4.A
- Verarbeitungsrechner in den Redundanzen 1 – 4:
  - VR1.A, VR2.A, VR3.A, VR4.A
- Voter-Rechner in den Redundanzen 1 – 4:
  - VT1.A, VT2.A, VT3.A, VT4.A
- Ansteuerung der Stellglieder erfolgt direkt durch die analogen Steuersignale der Voter-Rechner VT1.A – 4.A zur Schaltanlage:
  - redundanzweise für die Notkühlpumpen NKP1, NKP2, NKP3, NKP4,
  - redundanzweise für die Vorsteuerventile des Durchdringungsabschlusses der FD-Leitungen MV1-4 (die Modellierung der Steuerung des Hauptventils soll im Fehlerbaummodell des FD-Systems erfolgen).

Jeder Erfassungsrechner (ER1.A – 4.A) erhält drei analoge Messsignale und führt die Anwendersoftware der Signalbearbeitung (z. B. Funktionspläne der Überwachung der Messbereiche, der Dimensionierung usw.), der Hardware-Funktionspläne (Dispositionspläne der Hardware, Netzwerkpläne) und die Kommunikation zur den Verarbeitungsrechnern (VR1.A – 4.A) aus.

Jeder Verarbeitungsrechner (VR1.A – 4.A) führt die Anwender-Software mit Leittechnik-Funktionen (LEFU „DDA-FDL“ und LEFU „NKP EIN“), der Hardware-Funktionspläne (Dispositionspläne der Hardware, Netzwerkpläne) und die Kommunikation zu den Verarbeitungsrechnern (VT1.A – 4.A) aus.

Jeder Verarbeitungsrechner (VR1.A – 4.A) führt die Anwender-Software mit Leittechnik-Funktionen (logische Funktionen, wie 2-von-4-Logik) und der Hardware-Funktionspläne (Dispositionspläne der Hardware, Netzwerkpläne) aus. Jeder Voter-Rechner (VT1.A – 4.A) steuert durch die analogen Signale der D/A-Ausgabebaugruppe die Relais in der Schaltanlage zum Ein- und Ausschalten der verfahrenstechnischen Komponenten.

Die Steuerung der verfahrenstechnischen Komponenten wird zunächst stark vereinfacht im Modell abgebildet:

- die Ansteuerung der DDA-Magnetventile erfolgt nach Arbeitsstromprinzip, d. h. aktives Signal „1“ am Ausgang eines beliebigen Voters führt zum Anregen des Durchdringungsabschlusses. Das Ausgangssignal „0“ führt zum Entregen der Magnetventile und damit bleibt das DDA-Ventil offen.
- die Steuerung der Notkühlpumpe erfolgt zweikanalig durch zwei aktive 1-Signale: „NKP-Pumpe EIN“ und „NKP-Pumpe AUS“.

3.3 Modellierung der Hardware

3.3.1 Kurzbeschreibung der TXS-Hardware

Die TXS-Leittechnik besteht im Wesentlichen aus vier Grundkomponenten:

- Baugruppenträger (Basis eines Rechenknotens),
- Baugruppen des Funktionsrechners,
- Kommunikationseinrichtungen,
- Peripheriebaugruppen (analoge bzw. digitale Ein- und Ausgabebaugruppen).

In Tab. 3-2 wird eine Übersicht über die TELEPERM-XS-Baugruppen und ihre Funktionen gegeben. In Abb. 3-3 werden die TXS-Baugruppen strukturiert nach ihrer Funktion dargestellt.

Tab. 3-2 Gesamtübersicht der TELEPERM-XS-Baugruppen (s. auch Abb. 3-3)

Typ TXS 1. Gen.	Funktion	Kurzbeschreibung der Baugruppen
Rechnerbaugruppen		
SVE1	Verarbeitungseinheit	Prozessor Intel 80486DX-33, 128 RAM, EPROM und Flash-EPROM-Speicherbereiche, Systemsteuerung, Überwachungseinheit, Timer und Interrupt-Controller, Schnittstellen zum Rückwandbus, Kommunikationsspeicher
SCP1	Kommunikationsprozessor	SVE1 und Datenübertragung-Modul (10 Mbit/s)
SL21	Kommunikationsmodul	Datenübertragung-Modul (1,5 Mbit/s)
SKO1	Kommunikationsmodul	Erweiterung des K32-Busses
SBU1	Buskopplerbaugruppe	Koppelbaugruppe zu SKO1
SBG1	Baugruppenträger	32-Bit-Rückwandbus, Überwachungseinrichtungen, Spannungsversorgung (+5 V, ±15 V), Lüfterzeile, bis drei SBG pro Schrank,
SBG2	Baugruppenträger	dito.
Ein-/Ausgabe-Baugruppen		
S430	Digitaleingabebaugruppe	32 Kanäle mit Optokoppler
S431	Digitaleingabebaugruppe	32 Kanäle mit Optokoppler
S706	Zählerbaugruppen	3 Eingänge
S451	Digitalausgabebaugruppe	32 Kanäle mit Optokoppler
S458	Digitalausgabebaugruppe	16 Kanäle mit Relais
S460	Analogeingabebaugruppe	8 Kanäle potentialgetrennt
SMMU	Messbereichsmodul	
SMMI	Messbereichsmodul	
SMMT	Messbereichsmodul	
S466	Analogeingabebaugruppe	16 Kanäle massebezogen oder 8 Differenzeingänge
S470	Analogausgabebaugruppe	8 Kanäle 0-20 mA (±10 V)
SRB1	Relaisbaugruppe	Zwei Relais mit je 3 potentialgetrennten Wechslerkontakten für DC 24V, 110V, 220V; AC 115V, 230V
SRB2	Relaisbaugruppe	Zwei Relais mit je 3 potentialgetrennten Wechslerkontakten für DC 60V, AC 60V

Typ TXS 1. Gen.	Funktion	Kurzbeschreibung der Baugruppen
Kommunikationsbaugruppen		
SHT1	SINEC H1-Buskoppler	
SHT2	Twin-Transceiver	Schnittstelle für zwei Teilnehmer an SHS1 (elektrisch)
SHO1	optischer Mini-Transceiver	Steckbaugruppe zum externen Anschluss (optisch)
SHO2	optischer Transceivereinschub	Schnittstelle zum Anschluss eines Teilnehmers an SHS1 (optisch)
SLBT	SINEC-L2-Busterminal	
SLLM	Optical Link-Modul	SINEC-L2-Modul mit zwei optischen und zwei elektrischen Schnittstellen
SHS1	Aktiver Sternkoppler	für zwei SINEC-H1-Sterne (optische und elektrische Teilnehmer)
Aufbaukomponenten		
STS42-1 EMV	Standardschrank	
SES72-24	Standardeinspeisung	±24V-Einspeisung, Entkopplung, Absicherung, Verteilung, Einsteckü̈berwachung, Überwachung von Lüfter und der SBG-Temperatur, Schranküberwachung, Störmeldung von den SVE

Ein Baugruppenträger mit den erforderlichen Funktionsbaugruppen bildet einen Rechenknoten. Im TXS-System werden zwei Arten von Rechenknoten eingesetzt:

- Automatikrechner zur Ausführung der Steuerungsfunktionen,
- Melderechner zur Überwachung des Automatikrechners,

Die leittechnischen Funktionen werden zusammen mit den erforderlichen Systemfunktionen als ablauffähige Programme in die schreibgeschützten Flash-EPROM – Speicherbereiche abgelegt und durch Kontrollsummen (CRC) gesichert. Die Programmabarbeitung im Funktionsrechner erfolgt zyklisch.

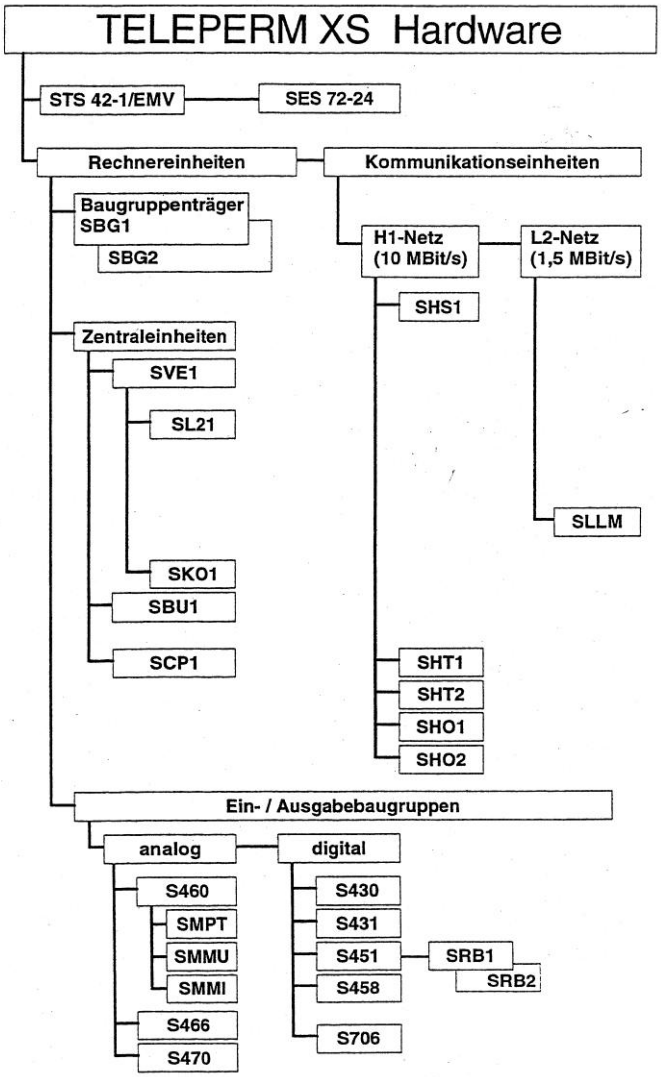


Abb. 3-3 Übersicht der Baugruppen der TELEPERM-XS-Leittechnik der 1. Generation

Die Eingangssignale für leittechnische Funktionen, die auf einem Funktionsrechner implementiert sind und deren Ergebnisse, werden entweder als Telegramme über Kommunikationseinrichtungen oder als Einzeldrahtsignale über Peripheriebaugruppen zur Verfügung gestellt bzw. weitergeleitet. Der interne Signalaustausch des Funktionsrechners erfolgt über den Rückwandbus. Im TXS-System werden ausschließlich nicht programmierbare Peripheriebaugruppen mit galvanischer Entkopplung zum Prozess eingesetzt. Der Zugriff auf die Peripheriebaugruppen durch den Funktionsrechner erfolgt durch baugruppenspezifische Softwaretreiber, wobei die Peripheriebaugruppen grundsätzlich keinen eigenen Zugriff auf den Rückwandbus haben.

Die Datenübertragung zwischen Funktionsrechnern in unterschiedlichen Baugruppenträgern erfolgt über Kommunikationseinrichtungen in folgenden Schritten:

- Schreiben der zu übertragenden Daten in den Dualportspeicher der betroffenen Anschaltbaugruppe durch den Funktionsrechner,
- Serielle Übertragung der Daten über das Netz entsprechend dem verwendeten Protokoll zur Anschaltbaugruppe des Zielsystems,
- Übertragung der Daten in den Dualportspeicher des Ziel-Funktionsrechners durch die Anschaltbaugruppe,
- Lesen der Daten und Überprüfung der Datenintegrität durch den Ziel-Funktionsrechner.

Zur seriellen Datenübertragung stehen zur Verfügung:

- Anschaltbaugruppe (Kommunikationsprozessor) zur Abwicklung des H1-Protokolls (IEEE 802.3),
- Anschaltbaugruppe (Kommunikationsprozessor) zur Abwicklung des L2-Protokolls (DIN 19245),
- Netzwerkkomponenten (u. a. Transceiver, Sternkoppler, Repeater).

3.3.2 Kurzbeschreibung der TXS-Software

Die TELEPERM XS-Software /ARE 06/ unterscheidet sich in der

- Offline-Software (SPACE-Engineering-Software) für die Aufgaben: Projektierung, Verifizierung, Konfiguration, Prüfung und Wartung. Diese Software läuft auf dem Servicegerät und trägt nicht unmittelbar zur Ausführung leittechnischer Funktionen.
- Online-Software zur Ausführung von leittechnischen Funktionen, Kommunikations-funktionen und Online-Selbstüberwachung. Diese Software arbeitet auf den Rechnerbaugruppen des Systems. Die Online-Software (s. Abb. 3-4) ist unterteilt in
  - Betriebssystem-Software,
  - Ablaufsystem- und Anwendersoftware.

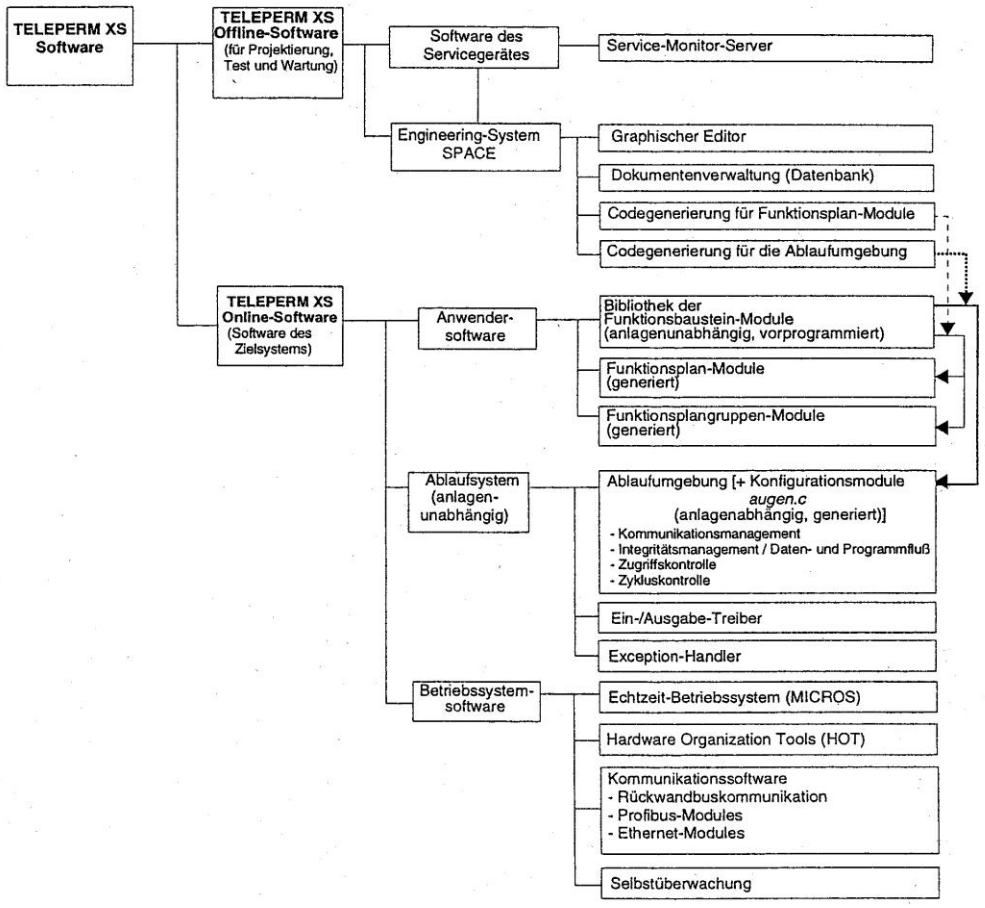


Abb. 3-4 Gesamtübersicht der Software der TELEPERM-XS-Leittechnik

Die Software mit unveränderlichen Daten (Programmcode und nicht veränderbare Parameter) ist im schreibgeschützten Flash-EPROM - Speicherbereich des Funktionsrechners abgelegt. Daten, die geplanten Änderungen unterworfen sind (änderbare Parameter), werden im EEPROM – Schreib-und Lesespeicher redundant abgelegt, während zyklisch änderbare Daten (Signale und Zustandsspeicher) im RAM-Bereich abgelegt werden.

Im TXS-System wird das Echtzeitbetriebssystem MICROS eingesetzt. Ein großer Teil des Betriebssystems bildet die Protokollsoftware für serielle Datenübertragung. Diese läuft auf den Kommunikationsprozessoren SCP1 und SL21 ab und ist damit strikt von Betriebssystemteilen auf den Funktionsrechnern SVE1 getrennt, auf denen die Anwendungsprogramme ablaufen.

Der Kern des Betriebssystems kann bis maximal 16 Tasks verwalten, wobei im Normalbetrieb bis zu drei Tasks (Ablaufumgebung, Bedientask, Selbstüberwachung) aktiv sind. Die Ablaufumgebung wird zyklisch vom Betriebssystem (Millisekunden-Hardware timer) aktiviert und berechnet danach die spezifizierten Anwendungsfunktionen. Der Bedientask wird dann von der Ablaufumgebung aktiviert, wenn diese die zulässigen Anforderungen vom Servicegerät erkannt hat. Nach Bearbeitung der Anforderung deaktiviert sich der Bedientask selbst. Die Selbstüberwachung arbeitet als endlos laufender Hintergrund-Task mit zyklischer Überprüfung der Hardware des Funktionsrechners.

Die Ablaufumgebung ist Bestandteil des Ablaufsystems. Sie liest und prüft alle Eingangsinformationen, steuert die Bearbeitung der Funktionsplan-Module, die Kommunikation, die Ausgabe der Berechnungsergebnisse (Ausgangssignale) an nachgeschaltete Funktionsrechner oder über Peripherie-Baugruppen und stellt eine Bedienschnittstelle der Online - Software auf den Funktionsrechnern zum Servicegerät zur Verfügung:

- Rücksetzen eines Hardware-Timers (Watchdog-Funktion),
- Inkrementieren des Zykluszählers,
- Einlesen der Prozessdaten über Peripheriebaugruppen,
- Einlesen der Telegramme aus dem Dualport-RAM - Speicher,
- Übergabe der Daten an die Funktionsplangruppenmodule,
- Bearbeiten der Funktionsplangruppenmodule, Prüfen der Fehlermeldungen und Setzen der Fehlerstatussignale,
- Ausgabe der Ergebnisse über Peripheriebaugruppen,
- Versenden der Telegramme an andere Funktionsrechner,
- Aktivierung und Deaktivierung der Bedientasks.

Die Ablaufumgebung jedes Funktionsrechners wird durch einen Codegenerator entsprechend der in der Projektierungsdatenbank hinterlegten Informationen konfiguriert. Die verbleibende Rechenzeit jedes Bearbeitungszyklus wird für die Durchführung der zyklischen Selbstüberwachung genutzt. Die zyklische Selbstüberwachung ist eine Softwarekomponente mit der Aufgabe, Fehler in der Leittechnik-Hardware aufzudecken. Meldung und entsprechende Reaktion auf erkannte Fehler werden von der zu-

gehörigen Ablaufumgebung oder in einigen Fällen mit Hilfe spezieller Programme durchgeführt. Die zyklische Selbstüberwachung ist zu diesem Zweck mit einer Schnittstelle zur Ablaufumgebung und zum Exception-Handler ausgestattet. Sie sind grundsätzlich auf allen Prozessorbaugruppen implementiert.

Die Auslegung von Sicherheitssystemen erfolgt derart, dass für die eigentliche Anwenderfunktion nicht mehr als ca. 50 % der in einem Zyklus vorhandenen Rechenzeit benötigt wird, so dass die Selbstüberwachung ebenfalls ca. 50 % der Rechenzeit zur Verfügung hat (Zeitbedarf der Ablaufumgebung wenige Millisekunden). In diesem Fall dauert die vollständige Prüfung der Hardware einer Funktionsrechnerbaugruppe ca. 10 Minuten.

Falls die Ablaufumgebung aufgrund eines Fehlers im Signalfluss nicht ordnungsgemäß terminiert wird, läuft der Watchdog-Timer ab und erzeugt einen Hardware – Interrupt und aktiviert damit eine Fehlerbehandlungsfunktion des Rechners (Exceptionhandler), der den Zustand des Rechners für eine spätere Analyse sichert und den Rechner in einen definierten Fehlerzustand versetzt. In diesem Fehlerzustand sind alle Signalausgaben gesperrt und der Prozessor wird in einer Warteschleife festgehalten. Das Sperren der Signalausgaben kann auf mehrere unterschiedliche Weisen erfolgen und zwar durch explizite Treiberaufrufe und durch ein Hardware-Signal (BASP), über das die Laststromversorgung für die Peripheriebaugruppen weggeschaltet wird.

Die Fehlerbehandlungsfunktion sorgt für die Behandlung und Anzeige von Ausnahmezuständen und ggf. für den geordneten Neustart oder den Dauerstopp der Rechnerbaugruppen mit Rücksetzen der angeschlossenen Ein-/Ausgabebaugruppen in einen definierten Zustand. Fehlermeldungen, die auf der Peripheriebaugruppe erkannt werden (Drahtbruch, Überlauf, Unterlauf), werden von den Treibern derart berücksichtigt, dass die betroffenen Signale mit dem Signalstatus 'fehlerhaft' markiert werden, so dass diese Signale keinen Einfluss auf die weitere Funktionsbearbeitung haben sollen.

Die Anwendersoftware, d. h. der Teil der Online - Software, der die Leittechnik-Funktion realisiert, besteht aus:

- Funktionsbaustein-Modulen, u. a.:
  - qualifizierte Bausteine, die leittechnische Elementarfunktionen wie Grenzwertgeber, Summierer oder Integrierer realisieren sowie

  - logische Funktionen (z. B. AND, OR) und Verknüpfungen (z. B. 2-von-3, 2-von-4).

- Funktionsplan- und Funktionsplangruppen-Module
  - Verknüpfungen von Funktionsbausteinen zu Leittechnik-Funktionsplänen. Für jeden Funktionsplan wird genau ein Softwaremodul generiert (Funktionsplan-Modul). Es enthält die Aufrufe der Funktionsbaustein-Module aller auf einem Funktionsplan verwendeten Funktionsbausteine in einer algorithmisch korrekten Reihenfolge. Das Funktionsplan-Modul gewährleistet die korrekte Parametrierung der Funktionsbaustein-Module und realisiert deren Verschaltung.
  - Alle Funktionsplan-Module, die auf einer einzelnen Funktionsrechnerbaugruppe mit der gleichen Zykluszeit ablaufen, werden zu einem Funktionsplangruppen-Modul verbunden.

Auf den einzelnen Funktionsrechnern werden diese Funktionsplan-Module durch die Ablaufumgebung ausgeführt.

Die Kommunikationsaufgaben des Betriebssystems im Funktionsrechner beschränken sich darauf

- die Kommunikationsprozessoren zu initialisieren und
- auf Daten im RAM-Speicher des Kommunikationsprozessors über den Rückwandbus des Baugruppenträgers oder über die Netzverbindung zuzugreifen.

Die E/A-Treiber sind für den Signalaustausch zwischen den Funktionsplänen und der Peripherie sowie zwischen den verschiedenen Funktionsrechnern erforderlich.

3.3.3 Erfassungsrechner

In jeder Redundanz ist ein Erfassungsrechner vorgesehen, der mit den Verarbeitungseinheiten SVE1, den Kommunikationsprozessoren SCP1 (für H1-Verbindungen für Melderechner), bzw. SL21 (für L2-Verbindungen zu den Verarbeitungsrechnern), SKO1 (Kommunikationsmodul LEBUS), SBU1 (Koppelbaugruppe LEBUS), sowie Ein- und Ausgabebaugruppen für Analog- und Binärsignale bestückt ist. Auf die E/A-Baugruppen sind die Prozessvariablen der entsprechenden Redundanz aufgelegt.

Eine SVE1 (LVXX) ist ausschließlich für die Kommunikation mit den Verarbeitungsrechnern vorgesehen. Sie verteilt alle Signale, bei Analogsignalen nach entsprechender Vorverarbeitung (Messbereichsanpassung) auf die Verarbeitungsrechner in allen Redundanzen. Eine SVE1 (LV42) übernimmt die Abarbeitung der Funktionspläne.

Die SINEC H1 Kommunikationsprozessoren SCP1 sorgen für die Kommunikation zum Melderechner. Eine weitere SVE1 (LVXX) mit Kommunikationsmodul (LKXX) stellt über die Koppelbaugruppe SBU1 (LKXX) die Verbindung zum zweiten Baugruppenträger her.

Innerhalb eines Erfassungsrechners erfolgt die Erfassung und Digitalisierung der Eingangssignale. Jedes Signal ist dabei einer Redundanz (R1 - 4) zugeordnet.

Die nachfolgende Tab. 3-3 stellt alle beteiligten Eingangssignale sowie deren Zuordnung zu Redundanzen und Eingabebaugruppen zusammen.

Tab. 3-3 Eingangssignale der Erfassungsrechner (Analogeingabe-Baugruppe)

Signal Kennzeichen	Parameter	Signalart	Redundanz	Analogsignal-BG	Kanal	Eingabebaugruppe	Kanal
R1_RDB_L 1	Füllstand RDB	analog	1	SAA1		AE621_ER1.A	1
R2_RDB_L 1	Füllstand RDB	analog	2	SAA1		AE621_ER2.A	1
R3_RDB_L 1	Füllstand RDB	analog	3	SAA1		AE621_ER3.A	1
R4_RDB_L 1	Füllstand RDB	analog	4	SAA1		AE621_ER4.A	1
R1_RDB_T 1	Kerntemperatur	analog	1	SAA1		AE621_ER1.A	2
R2_RDB_T 1	Kerntemperatur	analog	2	SAA1		AE621_ER2.A	2
R3_RDB_T 1	Kerntemperatur	analog	3	SAA1		AE621_ER3.A	2
R4_RDB_T 1	Kerntemperatur	analog	4	SAA1		AE621_ER4.A	2
R1_FDL_F 1	FD-Durchsatz FDL	analog	1	SAA1		AE622_ER1.A	3
R2_FDL_F 1	FD-Durchsatz FDL	analog	2	SAA1		AE622_ER2.A	3
R3_FDL_F 1	FD-Durchsatz FDL	analog	3	SAA1		AE622_ER3.A	3
R4_FDL_F 1	FD-Durchsatz FDL	analog	4	SAA1		AE622_ER4.A	3

Die Analogsignale werden erfasst, digitalisiert und nach der Digitalisierung ohne weitere Verarbeitung durch das Netzwerk auf die Verarbeitungsrechner verteilt.

3.3.4 Verarbeitungsrechner

Dem jeweiligen Erfassungsrechner ist in jeder Redundanz ein Verarbeitungsrechner, der über die SINEC L2 Kommunikationsverbindungen die Prozessvariablen von den Erfassungsrechnern aller Redundanzen erhält (LVXX), zugeordnet. Die Verarbeitungsrechner sind mit Verarbeitungseinheiten SVE1, Kommunikationsprozessoren SCP1 (für H1-Verbindungen für Melderechner), bzw. SL21 (für L2-Verbindungen zu den Voter-Rechnern), SKO1 (Kommunikationsmodul LEBUS), SBU1 (Koppelbaugruppe LEBUS), sowie Binärausgaben bestückt.

In dieser Ebene findet in der als „Master“ parametrierten Verarbeitungseinheit (LVXX) die Validierung der Eingangssignale (Bildung von 2. MIN, 2. MAX oder Rechenschaltung) sowie die Signalverarbeitung zur Bildung von Anrege- und Steuersignalen statt. Die hier gewonnenen Rechenergebnisse werden über L2-Verbindungen zu den Voter-Rechnern als Telegramme versendet.

Die Auswahlbausteine (2. MIN, 2.MAX) des Spezifikationswerkzeuges SPACE haben aktive Statusverarbeitung (siehe Tab. 3-4), d. h.

- Erkannt ausgefallene Eingangssignale werden von der weiteren Verarbeitung ausgeschlossen. Damit wird das Ausgangssignal erst dann als fehlerhaft markiert, wenn alle vier Eingangssignale des 2. MAX/2. MIN Bausteines erkannt ausgefallen sind (erkannter Ausfall des Ausgangssignals).
- Das Ausgangssignal wird als unerkannt ausgefallen angesetzt, wenn zwei oder mehr Eingangssignale des 2. MAX/2. MIN Bausteines unerkannt ausgefallen sind. (Dieser Ansatz ist konservativ für:
  - das 2. MAX, wenn noch zwei Eingangssignale intakt sind und die Prozessvariablen während der Transiente ansteigen und
  - das 2. MIN, wenn noch zwei Eingangssignale intakt sind und die Prozessvariablen während der Transiente abfallen.)

Tab. 3-4 Verhalten von 2. MAX/2. MIN-Bausteinen in der Anwendersoftware des Verarbeitungsrechner (VR1-4.A) bei Ausfallkombinationen der Eingänge

Anzahl Eingänge			2. MIN/ 2. MAX
unerkannt ausgefallen	**intakt**	**erkannt ausgefallen**	**Zustand**
-	4	-	intakt
-	3	1	intakt
-	2	2	intakt
-	1	3	intakt
-	-	4	erkannt ausgefallen
1	3	-	intakt
1	2	1	intakt
1	1	2	kontextabhängig
1	-	3	unerkannt ausgefallen
2	2	-	intakt
2	1	1	unerkannt ausgefallen
2	-	2	unerkannt ausgefallen
3	1	-	unerkannt ausgefallen
3	-	1	unerkannt ausgefallen
4	-	-	unerkannt ausgefallen

Die Verarbeitungsrechner erhalten sämtliche Prozessvariablen aus allen Redundanzen. In ihnen findet die Signalverarbeitung für die Leittechnikfunktionen, Module und Submodule statt. Des Weiteren werden die für die Analyse relevanten Ansteuersignale für die Komponenten gebildet und auf die Voter-Rechner mittels Telegrammen (Netzwerk) verteilt.

3.3.5 Voter-Rechner

Die LEFU-Signale der Verarbeitungsrechner werden in den Voter-Rechnern nach der 2-von-4-Auswahllogik verknüpft und die Steuersignale für verfahrenstechnische Komponenten an den Ausgängen der Digitalausgabebaugruppen generiert.

Sobald an einem beliebigen Eingang ein Eingangssignal ansteht („1“-Signal), wird mit einer Zeitverzögerung die „1 von 4“ Meldung aktiviert. In dem Moment, wo ein zweites Signal an den Eingängen des Voters ansteht, wird am Ausgang das Signal „2 von 4“ wirksam und zeitgleich wird die Meldung „1 von 4“ gelöscht.

Tab. 3-5 Ausgangssignale des Voter-Rechners (Binärausgabe-Baugruppe)

Signal-Kennzeichen	Stellglied	Signalart	Red	Ausgabe-BG	Kanal
R1_NKP1_E	NKP EIN	binär	1	DA105_ VT1.A	1
R2_NKP1_E	NKP EIN	binär	2	DA105_VT2.A	1
R3_NKP1_E	NKP EIN	binär	3	DA105_ VT3.A	1
R4_NKP1_E	NKP EIN	binär	4	DA105_ VT4.A	1
R1_NKP1_A	NKP AUS	binär	1	DA105_ VT1.A	2
R2_NKP1_A	NKP AUS	binär	2	DA105_VT2.A	2
R3_NKP1_A	NKP AUS	binär	3	DA105_ VT3.A	2
R4_NKP1_A	NKP AUS	binär	4	DA105_ VT4.A	2
R1_FD-DDA-MV_E	MV EIN	binär	1	DA106_VT1.A	1
R2_FD-DDA-MV_E	MV EIN	binär	2	DA106_VT2.A	1
R3_FD-DDA-MV_E	MV EIN	binär	3	DA106_VT3.A	1
R4_FD-DDA-MV_E	MV EIN	binär	4	DA106_VT4.A	1

3.4 Ausfallmodelle, Daten

3.4.1 Ausfallarten basiert auf der generischen FMEA

Folgende Annahmen wurden auf der Basis der Informationen des Herstellers der TELEPERM-XS-Leittechnik /ARE 06/ für den Signal- bzw. Datenaustausch zwischen den redundanten Rechnern und für die Ansteuerung der Komponenten getroffen:

- Die Erfassungs- und Verarbeitungsrechner in den Redundanzen befinden sich in direkter Kommunikation miteinander, wobei die Telegramme mit Prozessvariablen ausgetauscht werden.
- Die Verarbeitungs- und Voter-Rechner in den Redundanzen befinden sich in direkter Kommunikation miteinander, wobei die Telegramme mit Steuerbefehlen ausgetauscht werden.
- Die Ansteuerung einer verfahrenstechnischen Komponente erfolgt in jeder Redundanz (R1 bis 4) durch die Steuersignale (Digitalsignal-Ausgabe) eines Voter-Rechners (VT1.A – 4.A), wobei auf die Modellierung der Antriebsteuerung (u. a. Vorranglogik, Rückmeldungen) zunächst verzichtet wird.

Für die TELEPERM-XS-Baugruppen wurden generisch ermittelte Ausfalleffekte (s. Tab. 3-6) unterstellt /PIL 04/.

Tab. 3-6 Ergebnisse der generischen Ausfallanalyse der TXS-Hardware

Baugruppe	Fehlerart	Auswirkung	Erkennung
SVE1	Blockierung des Rückwandbusses (RWB)	Ausfall des gesamten Baugruppenträgers und Kommunikation	selbstmeldend
S451, S430, S470 und S466	Blockierung des Rückwandbusses (RWB): konservative Annahme wegen K32-Busanschaltung	Ausfall des gesamten Baugruppenträgers: Rechnerausfall (Ausfallrate λ_{RWB})	selbstmeldend
Digitalausgabebaugruppe S451: Kanäle 1-32	Einzelner Kanalausfall: „Ausgabe 0-Signal bei gefordertem 1-Signal“	abhängig von Funktion	abhängig von Funktion
Digitalausgabebaugruppe S451:	Einzelner Kanalausfall:	abhängig von Funktion	abhängig von Funktion

Baugruppe	Fehlerart	Auswirkung	Erkennung
Kanäle 1-32	„Ausgabe 1-Signal bei gefordertem 0-Signal“		
Baugruppenträger	Ausfall der Stromversorgung, des Busarbiters, des K32-Buses und der Lüfterzeile	Ausfall des gesamten Baugruppenträgers: Rechnerausfall	selbstmeldend
Koppelstrecke LEBUS: SKO1 – SBU1	nicht implementiert	nicht implementiert	nicht implementiert
Das optische Link-Modul SLLM	Ausfall der Kommunikation der Punkt-zu-Punkt Verbindungen	Ausfall der Kommunikation	selbstmeldend
Kommunikationsmodul SL21 (2 Kanäle: 2 Submodule L2)	Ausfall des gesamten Moduls	Ausfall der Kommunikation	selbstmeldend

Begründung: Fehler, die sich nicht durch Störungen der Anschaltung am Rückwandbus auswirken und nicht von den Treibern erkannt werden, sollen durch projektierte Überwachungsfunktionen (Bildung 2. MAX oder 2. MIN, Messsignalvergleiche) erkannt und maskiert werden.

3.4.2 Modellierung der Ausfallarten im Fehlerbaum

Im Modell wurden zunächst die Ausfälle der Hardware-Komponenten der 1. Generation der Teleperm-XS-Leittechnik berücksichtigt. In der nachfolgenden Tab. 3-7 sind die modellierungsrelevanten Ergebnisse der Fehlerart- und Effektanalyse der Hardware zusammengefasst. Die Basisereignisse charakterisieren die Ausfälle, die nicht durch andere Ausfälle verursacht werden. In der Modellierung wird zwischen der selbstmeldenden erkannten Ausfallart (SM-Ausfallart) und der nicht selbstmeldenden unerkannten Ausfallart (NSM-Ausfallart) der Hard- und Software unterschieden.

Die Fortpflanzung der SM- und NSM-Ausfälle in der Signalverarbeitung ist unterschiedlich und muss im Fehlerbaum adäquat berücksichtigt werden.

Tab. 3-7 Übersicht über die Basisereignisse im Fehlerbaummodell (Ausfälle der TXS-Hardware)

Bezeichnung der Komponente FB-Modell #-Redundanz-Nr.	Fehlerart	Effekt / Auswirkung (konservative Annahmen)	Basisereignis für Rechner R1 aus PSA-69 Studie
SVE1_RWB_ER#.A SVE1_RWB_VR#.A SVE1_RWB_VT#.A	Blockierung des Rückwandbuses (RWB) führt zum Ausfall eines gesamten Baugruppenträgers	Rechner liefert keine oder falsche Ausgangssignale an die kommunizierenden Rechner bzw. an die Ansteuerung	VE141_R1_RWB
SVE1_NSM_ER#.A SVE1_NSM_VR#.A SVE1_NSM_VT#.A	Nicht Selbstmeldender (NSM) Ausfall der Verarbeitungseinheit	Rechner liefert keine oder falsche Ausgangssignale an die kommunizierenden Rechner bzw. an die Ansteuerung	VE142_R1_NSM
SVE1_SM_ER#.A SVE1_SM_VR#.A SVE1_SM_VT#.A	Selbstmeldender (SM) Ausfall der Verarbeitungseinheit	Rechner liefert keine oder falsche Ausgangssignale an die kommunizierenden Rechner bzw. an die Ansteuerung	VE142_R1_SM
SCP1_RWB_ER#.A SCP1_RWB_VR#.A SCP1_RWB_VT#.A	Blockierung des Rückwandbuses (RWB) führt zum Ausfall eines gesamten Baugruppenträgers	Rechner liefert keine oder falsche Ausgangssignale an die kommunizierenden Rechner bzw. an die Ansteuerung	CP111_R1_RWB
SL21_SM_ER#.A SL21_SM_VR#.A SL21_SM_VT#.A	Selbstmeldender Ausfall SL21 (gemeinsamer Anteil)	Ausfall der Kommunikation zwischen den SVE führt zum Ausfall der Datenverarbeitung eines Rechners. Rechner liefert keine oder falsche Ausgangssignale an die Wertungslogik oder keine oder falsche Information an kommunizierende Rechner.	L2121G_R1
SLLM_SM_ER#.A SLLM_SM_VR#.A SLLM_SM_VT#.A	Selbstmeldender Ausfall SLLM	Ausfall der Kommunikation zwischen den Rechnern (Punkt-zu-Punkt-Verbindung) Rechner liefert keine oder falsche Ausgangssignale an die Wertungslogik oder keine oder falsche Information an kommunizierende Rechner.	LLM771_R1
S466_RWB_ER#.A	Blockierung des Rückwandbuses (RWB) führt zum Ausfall eines gesamten Baugruppenträgers	Rechner liefert keine oder falsche Ausgangssignale an die Verarbeitungsrechner.	AE001_R1_RWB
S466_SM_ER#.A	Selbstmeldender Ausfall der Analogeingabe-Baugruppe S466	Die Baugruppe liefert falsche oder keine Signale (Prozessvariablen) für die logische Signalverarbeitung des eigenen Rechners.	AE621_R1_G
S451_RWB_VT#.A	Blockierung des Rückwandbuses (RWB) führt zum Ausfall eines gesamten Baugruppenträgers	Rechner liefert keine oder falsche Ausgangssignale an die Antriebsteuerung.	DA101_R1_RWB
S451_SM_G_VT#.A	Selbstmeldender Ausfall Digitalausgabe S451 (gesamt)	Alle Ausgangsignale der Baugruppe an die Antriebsteuerung fallen aus. Hierbei wird die ungünstigste Ausfallrichtung angenommen.	DA105_R1_GES
S451_K1_VT#.A	Ausfall nach '1' eines Kanals (1-32)	Ausgangsignal eines Kanals der Baugruppe zur Wertungslogik fällt nach „1“ aus. Bei der Modellierung wird die ungünstigste Ausfallrichtung angenommen.	DA105_R1_K1
S451_K0_VT#.A	Ausfall nach '0' eines Kanals (1-32)	Ausgangsignal eines Kanals der Baugruppe zur Wertungs-	DA105_R1_K1

Bezeichnung der Komponente FB-Modell #-Redundanz-Nr.	Fehlerart	Effekt / Auswirkung (konservative Annahmen)	Basisereignis für Rechner R1 aus PSA-69 Studie
		logik fällt nach „0“ aus. Bei der Modellierung wird die ungünstigste Ausfallrichtung angenommen.	
SBG1_SM_ER#.A SBG1_SM_VR#.A SBG1_SM_VT#.A	Selbstmeldender Ausfall SBG1	Rechner liefert keine oder falsche Ausgangssignale	BGT_R1
SAA_SM_ER#.A	Selbstmeldender Ausfall Analogsignalbaugruppe SAA1 (gesamt)	Ausfall eines Analogsignals führt zum falschen oder keinem Wert der S466-Analogeingabebaugruppe.	SAA162_R1_G

3.4.3 Zuverlässigkeitskenndaten der TXS-Hardware

Für die Auswertung der anlagenspezifischen Betriebserfahrung mit einem softwarebasierten Leittechniksystem wurde der GRS von einem deutschen Kernkraftwerk die Betriebserfahrung aus den ersten Einsatzjahren eines softwarebasierten Begrenzungssystems zur Verfügung gestellt. Auf dieser Datenbasis wurden die unabhängigen Ausfallraten für die Hardwarebaugruppen (TELEPERM-XS) ermittelt. Die Ausfallraten wurden mit dem nichtinformativen Bayes-Ansatz ermittelt. Die Ergebnisse sind in der nachfolgenden Tab. 3-8 dargestellt:

Tab. 3-8 Anlagenspezifische Auswertung der Hardware TXS-Baugruppen (Stand 2002)

Anlagenspezifische Auswertung der Hardware Baugruppen TELEPERM XS für eine Anlage, Gesamtausfallraten, Beobachtungsintervall 5 Jahre						
Baugruppe	**Funktion**	**Geräte mittlere Anzahl[1]**	**Ereignisse**	**Bezugszeit/ h**	**Median 50%-Fraktil**	**K-Faktor P95/P50**
S431	Digitaleingabe-baugruppe	53,8	**0**	**2394336**	9,50E-08	8,44
S451	Digitalausgabe-baugruppe	66,7	**2**	**2965032**	7,34E-07	2,54
S466	Analogeingabe-Baugruppe	44,8	**1**	**1993440**	5,93E-07	3,30
S470	Analogeingabe-Baugruppe	36,4	**0**	**1623000**	1,40E-07	8,44
SAA1	Analogsignal-baugruppe	1,7	**0**	**75384**	3,02E-06	8,44
SBG1	Baugruppen-träger	37	**5**	**1648128**	3,14E-06	1,90
SBU1	Buskoppler-baugruppe	9	**0**	**400896**	5,67E-07	8,44
SCP1	Kommunikations-prozessor	48	**0**	**2138112**	1,06E-07	8,44
SHO1	opt. Mini-Tranceiver	41	**0**	**1826304**	1,25E-07	8,44
SHO2	Transceiver-einschub	44	**0**	**1959936**	1,16E-07	8,44

Anlagenspezifische Auswertung der Hardware Baugruppen TELEPERM XS für eine Anlage, Gesamtausfallraten, Beobachtungsintervall 5 Jahre						
Bau-gruppe	**Funktion**	**Geräte mittlere Anzahl(1**	**Ereignisse**	**Bezugszeit/ h**	**Median 50%-Fraktil**	**K-Faktor P95/P50**
SHS1	akt. Sternkoppler	4	**0**	**178176**	1,28E-06	8,44
SHT2	Twin-Transceiver	7	**0**	**311808**	7,30E-07	8,44
SKO1	Kommunikations-modul	9	**0**	**400896**	5,67E-07	8,44
SL21	Kommunikations-modul	132	**5**	**5879808**	8,79E-07	1,90
SLLM	opt. Link-Modul	184	**0**	**8196096**	2,78E-08	8,44
SRB1	Relaisbaugruppe	8	**0**	**356.352**	6,38E-07	8,44
SVE1	Verarbeitungs-einheit	129	**0**	**5746176**	3,96E-08	8,44
(1 Die mittlere Gerätezahl berücksichtigt Änderungen in der Anzahl der Geräte im Beobachtungsintervall						

Die Ausfallraten aus der Tab. 3-8 wurden für die Basisereignisse (s. Tab. 3-7) im Fehlerbaum der Sicherheitsleittechnik verwendet.

Tab. 3-9 Zuverlässigkeitskenndaten der TXS-Hardware

BE_NAME	Typ	Vert	Wert_1	Wert_2	TRM_Wert	TI_Wert
AE001_R1_RWB	D	L	4,46E-07	3,00	24,0	
CP111_R1_RWB	D	L	2,34E-07	8,44	24,0	
DA101_R1_RWB	D	L	4,70E-08	3,00	24,0	
VE141_R1_RWB	D	L	4,97E-07	3,00	24,0	
AE621_R1_G	D	L	7,52E-07	3,30	24,0	
BGT_R1	D	L	3,34E-06	1,90	24,0	
DA105_R1_GES	D	L	8,43E-07	2,54	24,0	
L2121G_R1	D	L	9,35E-07	1,90	24,0	
LLM771_R1	D	L	6,10E-08	8,44	24,0	
SAA162_R1_G	D	L	6,63E-05	8,44	24,0	
VE142_R1_NSM	T	L	8,70E-08	8,44	24,0	8736
VE142_R1_SM	D	L	2,62E-06	3,00	24,0	
DA105_R1_K1	D	L	1,06E-08	3,00	24,0	
DA105_R1_K1	T	L	1,06E-08	3,00	24,0	8736

Legende zur Tabelle ‘Zuverlässigkeitskenndaten aus PSA-69-Studie‘:

Spalte		Beschreibung
BE_NAME		Basisereignis (BE) -Bezeichnung im PSA-69-Modell (RiskSpectrum)
BE_TEXT		Beschreibung des Ausfalls (BE) im PSA-69-Modell (RiskSpectrum)
Typ	**P**	Ausfall bei Anforderung (Wahrscheinlichkeit)
Typ	**D**	Fehler selbstmelden
Typ	**M**	Betriebsausfall
Typ	**L**	bei Test entdeckt
PA_Name		Bezeichnung der Komponente im Fehlerbaum-Modell (RiskSpectrum)
Wert_1		Ausfallrate / Wahrscheinlichkeit
Wert_2		Streufaktor
TRM_Name		Parameterbezeichnung für Reparaturzeit im FB-Modell
TRM_Wert		Reparaturzeit (h)
TI_Name		Parameterbezeichnung für Testinterval
TI_Wert		Testinterval (h)

3.5 Fehlerbaummodellierung der Sicherheitsleittechnik

3.5.1 TOP-Ereignisse (Ausfall einer Leittechnik-Funktion)

Das TOP-Ereignis wird erreicht, wenn eine der angeforderten Komponenten nicht in ihre geforderte Stellung gefahren bzw. die Betriebsstellung nicht beibehalten wird. Dieses Ereignis tritt für eine Komponente ein, wenn

- die Wertungsschaltung des Voter-Rechners kein Ausgangssignal „Signal 0“ ausgibt

ODER

- mehr als 2 Verarbeitungsrechner fehlerhaft „0“-Signal bzw. „1“-Signal ausgeben

ODER

- mehr als 2 Verarbeitungsrechner ausfallen.

3.5.2 Ausfälle des Voter-Rechners

Die 2-von-4-Wertungsschaltung des Voters liefert keine (oder fehlerhafte) Ausgangssignale, wenn

- die der Wertungsschaltung zugehörigen Eingangssignale mit den entsprechenden Ausfalleffekten versagen

ODER

bei intakten Eingangssignalen die Wertungsschaltung selbst ausgefallen ist.

3.5.3 Ausfälle von Verarbeitungsrechnern

Ein Verarbeitungsrechner liefert keine (oder fehlerhafte) Ausgangssignale, wenn

- die dem Verarbeitungsrechner zugeordneten Baugruppen mit entsprechenden Ausfalleffekten versagen (Ausfälle von Prozessoren oder Baugruppenträgern, Blockaden des Rückwandbusses), d. h. der Verarbeitungsrechner selbst erkannt oder unerkannt ausgefallen ist.

ODER

- bei intakten Verarbeitungsrechnern die von den Erfassungsrechnern gelieferten Eingangssignale in den Verarbeitungsrechner fehlerhaft sind. Aufgrund der aktiven Statusverarbeitung der im Verarbeitungsrechner realisierten 2. MAX und 2. MIN Validierungsbausteine innerhalb der Signalverarbeitung für die Leittechnikfunktion, muss auch hier zwischen erkannten und unerkannten Ausfällen unterschieden werden.

3.5.4 Signale von den Erfassungsrechnern zum Verarbeitungsrechner

Signale von einem Erfassungsrechner sind für einen Verarbeitungsrechner ***erkannt*** ausgefallen, wenn

- der Erfassungsrechner selbst erkannt ausgefallen ist (als Folge fällt auch die Kommunikation mit dem Verarbeitungsrechner aus)

ODER

- bei intaktem Erfassungsrechner die Kommunikation (Busverbindungen) mit dem Verarbeitungsrechner ausgefallen ist. (Ausfälle von Kommunikationsprozessen oder optischen Link-Modulen)

Signale von einem Erfassungsrechner sind für einen Verarbeitungsrechner ***unerkannt*** ausgefallen wenn,

- der Erfassungsrechner selbst unerkannt ausgefallen ist (unerkannter Ausfall des Zentralprozessors)

ODER

- die Ausgangssignale aus dem Erfassungsrechner sind unerkannt ausgefallen (aufgrund der Verarbeitung von unerkannt ausgefallenen Eingangssignalen).

3.5.5 Ausfälle von Erfassungsrechnern

Ein Erfassungsrechner liefert keine (oder *erkannt fehlerhafte*) Ausgangssignale, wenn

- die dem Erfassungsrechner zugeordneten Baugruppen mit entsprechenden Ausfalleffekten versagen (Ausfälle von Prozessoren oder Baugruppenträgern, Blockaden des Rückwandbusses), d. h. der Verarbeitungsrechner selbst erkannt oder unerkannt ausgefallen ist.

ODER

- die den einzelnen Signalen zugeordneten Eingabebaugruppen erkannt ausgefallen sind.

Ein Erfassungsrechner liefert *unerkannt fehlerhafte* Ausgangssignale, wenn

- der Erfassungsrechner selbst unerkannt ausgefallen ist (unerkannter Ausfall des Zentralprozessors)

ODER

- die den einzelnen Signalen zugeordneten Eingabebaugruppen unerkannt ausgefallen sind.

3.5.6 Ausfälle der Analogsignale

Ein analoger Messkanal liefert *erkannt fehlerhafte* Ausgangssignale, wenn

- die dem Messkanal zugeordneten Baugruppen mit entsprechenden Ausfalleffekten versagen, d. h. der Messkanal selbst erkannt ausgefallen ist.

Ein Messkanal liefert *unerkannt fehlerhafte* Ausgangssignale, wenn

- der Messkanal selbst unerkannt ausgefallen ist (Messsignal eingefroren).

3.5.7 Berücksichtigung des Softwareversagens im Fehlerbaum

3.5.7.1 Ausfall einer Leittechnik-Funktion durch die GVA der Software

Das TOP-Ereignis wird auch dann erreicht, wenn

- GVA der Anwendersoftware aller Erfassungsrechner ER1-4.A_AS_GVA eintritt
  ODER
- GVA der Anwendersoftware aller Verarbeitungsrechner VR1-4.A_AS_GVA eintritt
  ODER
- GVA der Anwendersoftware aller Voter-Rechner VT1-4.A_AS_GVA eintritt
  ODER
- GVA der Betriebssystem-Software aller Erfassungsrechner ER1-4.A_BS_GVA eintritt
  ODER
- GVA der Betriebssystem-Software aller Verarbeitungsrechner VR1-4.A_BS_GVA eintritt
  ODER
- GVA der Betriebssystem-Software aller Voter-Rechner VT1-4.A_BS_GVA- eintritt.

3.5.7.2 Ausfälle von Voter-Rechnern

Ein Voter-Rechner liefert keine oder fehlerhafte Ausgangssignale, wenn

- Anwendersoftware des Voter-Rechners VT1.A_AS_SM (VT2.A_AS_SM, VT3.A _AS_SM, VT4.A_AS_SM) erkannt versagt hat
  ODER
- Anwendersoftware VT1.A_AS_NSM (VT2.A_AS_NSM, VT3.A_AS_NSM, VT4.A_AS_NSM) unerkannt versagt hat
  ODER
- Betriebssystemsoftware des Voter-Rechners VT1.A_BS_SM (VT2.A_BS_SM, VT3.A_BS_SM, VT4.A_BS_SM) erkannt versagt hat
  ODER
- der Voter-Rechner entweder unerkannt oder erkannt ausgefallen ist.

3.5.7.3 Ausfälle von Verarbeitungsrechnern

Ein Verarbeitungsrechner liefert keine (oder *erkannt fehlerhafte*) Ausgangssignale, wenn

- Anwendersoftware des Verarbeitungsrechners VR1.A_AS_SM (VR2.A_AS_SM, VR3.A_AS_SM, VR4.A_AS_SM) erkannt versagt hat
  ODER
- Betriebssystemsoftware des Verarbeitungsrechners VR1.A_BS_SM (VR2.A _BS_SM, VR3.A_BS_SM, VR4.A_BS_SM) erkannt versagt hat
  ODER
- Die Hardware des Verarbeitungsrechners selbst erkannt ausgefallen ist.

Ein Verarbeitungsrechner liefert *unerkannt fehlerhafte* Ausgangssignale, wenn

- Anwendersoftware VR1.A_AS_NSM (VR2.A_AS_NSM, VR3.A_AS_NSM, VR4.A_AS_NSM) unerkannt versagt hat
  ODER
- der Verarbeitungsrechner selbst unerkannt ausgefallen ist.

3.5.7.4 Ausfälle von Erfassungsrechnern

Ein Erfassungsrechner liefert keine (oder *erkannt fehlerhafte*) Ausgangssignale, wenn

- Anwendersoftware des Erfassungsrechners ER1.A_AS_SM (ER2.A_AS_SM, ER3.A_AS_SM, ER4.A_AS_SM) erkannt versagt hat
  ODER
- Betriebssystemsoftware des Erfassungsrechners ER1.A_BS_SM (ER2.A_BS_SM, ER3.A_BS_SM, ER4.A_BS_SM) erkannt versagt hat
  ODER
- die Hardware des Erfassungsrechners selbst erkannt ausgefallen ist.

Ein Erfassungsrechner liefert *unerkannt fehlerhafte* Ausgangssignale, wenn

- Anwendersoftware ER1.A_AS_NSM (ER2.A_AS_NSM, ER3.A_AS_NSM, ER4.A_AS_NSM) unerkannt versagt hat
  ODER
- der Erfassungsrechner selbst unerkannt ausgefallen ist.

3.6 Entwicklung eines neuen Quantifizierungsansatzes

Im Rahmen des BMU-Vorhabens SR2418 /PIL 04/ wurde ein Bewertungsverfahren für die Komplexität der Software entwickelt, in dem die Zuverlässigkeit verschiedener Softwarekomponenten (u. a. verschiedene Module der Anwendungssoftware) eines softwarebasierten Leittechniksystems quantitativ in Beziehung (z. B. über so genannte Komplexitätsmaße) gesetzt werden sollte. Diese Vorgehensweise hat den entscheidenden Nachteil, dass zunächst die Quantifizierung der Zuverlässigkeit eines zu vergleichenden Softwaremoduls erfolgen sollte. Dafür steht ebenfalls keine anerkannte Methode zur Verfügung.

Zur Entwicklung von neuen Ansätzen zur Quantifizierung softwarebasierter Leittechnik wurde die Betriebserfahrung eines auf der TELEPERM-XS-Technik basierten Leittechniksystem ausgewertet, um Erkenntnisse über Umfang und Relevanz der aufgetretenen Fehler in der Ablaufumgebung eines modernen softwarebasierten Leittechniksystems zu gewinnen. Dazu wurden versuchsweise die TELEPERM-XS-Protokoll-

dateien aus acht Jahren Betrieb eines softwarebasierten Begrenzungssystems erfasst und hinsichtlich Umfang und Relevanz der aufgetretenen Meldungen und weiterer Korrelationen (z. B. Zusammenhang mit einer bestimmten TELEPEM-XS-Baugruppe) ausgewertet. Die Idee bei der Auswertung war, die dabei aufgetretenen verschiedenen Fragen in einem allgemeinen Fragenkatalog zusammen zu fassen. Beispielhaft sind folgende Fragen zu nennen:

- Wie wird der Zeitstempel für die Protokolldateien generiert?
- Wann treten abrupte Dateiabbrüche auf?

Durch die Auftragung der Meldungstyp-Häufigkeit in Abhängigkeit ihres Zeitstempels konnten „auffällige“ Tage mit einer besonders hohen Anzahl von Einträgen lokalisiert werden, wodurch weitere Fragen aufgeworfen wurden, wie z. B.:

- Wie kann dieses Verhalten erklärt werden?
- Was ist an diesen Tagen vorgefallen?

Es wurden auch die Meldungen bezogen auf einzelne CPUs untersucht. Aufgrund der uns zur Verfügung stehenden Informationen war es nicht möglich, die aufgetretenen Fragestellungen nachvollziehbar zu klären. Für eine vertiefte Analyse mit Beschaffung der notwendigen Informationen wäre ein erheblicher Aufwand notwendig geworden. Aufgrund der vorliegenden Datenlage sind wir zu der Auffassung gekommen, dass der Versuch aus den Meldungen des Begrenzungssystems Zuverlässigkeitskenngrößen zu generieren nicht zielführend ist.

4 Zusammenfassung und Ausblick

Die aus den Arbeiten zum Stand von Wissenschaft &Technik gewonnenen Erkenntnisse zeigen, dass die methodischen Entwicklungen für eine probabilistische Bewertung softwarebasierter Leittechnik derzeit noch nicht so weit fortgeschritten sind, dass in unmittelbarer Zukunft mit einer Etablierung geeigneter Analyseverfahren gerechnet werden kann. International, insbesondere in den USA werden enorme Anstrengungen (auch finanzielle) unternommen, um dieses Nachweisdefizit zu beheben. Deshalb ergibt sich aus Sicht der GRS auch weiterhin eine dringende Notwendigkeit, die aktuellen Entwicklungen auf diesem Gebiet kontinuierlich zu verfolgen. Daher sollte auch weiterhin versucht werden, eigene Methoden für eine probabilistische Bewertung softwarebasierter Leittechnik einschließlich Ansätzen zur Quantifizierung der durch Softwarefehler verursachten Ausfälle zu entwickeln.

Eine weitere Herausforderung besteht darin, dass gegenwärtig bei nationalen wie auch internationalen Gutachterorganisationen der Einsatz diversitärer (dissimilarer) Sicherheitsleittechnik im nuklearen wie auch im nichtnuklearen Bereich unter Verwendung diversitärer (dissimilarer) Hard- und Software als eine wegweisende Lösung betrachtet wird. Grundprinzip einer solchen, nachfolgend als dissimilar bezeichneter Auslegung ist es, möglichst unähnliche (dissimilare) redundante Einrichtungen vorzusehen, so dass ein gleichzeitiges Versagen mehrerer, zueinander dissimilarer Einrichtungen aus gemeinsamer Ursache verhindert wird.

Die Einführung von Diversität (Dissimilarität) bei der Auslegung digitaler Sicherheitsleittechnik muss adäquat sowohl in der deterministischen als auch in der probabilistischen Sicherheitsbewertung berücksichtigt werden. Wichtige Fragestellungen sind dabei, welche Faktoren bzw. Merkmale für die Bewertung der Diversität (Dissimilarität) der Hard- und Software relevant sind und welchen Beitrag diese Faktoren hinsichtlich der Beherrschung der GVA leisten. Hierzu sind ebenfalls Bewertungsmethoden zu entwickeln.

5 Literatur

/ALD 06/ Aldemir, T., et.al.
Current State of Reliability Modeling Methodologies for Digital Systems and Their Acceptance Criteria for Nuclear Power Plant Assessments, U.S. Nuclear Regulatory Commission, NUREG/CR-6901, February 2006

/ALD 07/ Aldemir, T., et.al.
Dynamic Reliability Modeling of Digital Instrumentation and Control Systems for Nuclear Reactor Probabilistic Risk Assessments, U.S. Nuclear Regulatory Commission, NUREG/CR-6942, October 2007

/ARE 06/ AREVA NP:
Leittechnik TELEPERM XS Systemübersicht, Informationsprospekt, AREVA NP INC., Erlangen, 2006

/BMU 05/ Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit (BMU)
Leitfaden zur Durchführung der ‘Sicherheitsüberprüfung gemäß §19a des Atomgesetzes – Leitfaden probabilistische Sicherheitsanalyse –' für Kernkraftwerke in der Bundesrepublik Deutschland, Bundesanzeiger Nr. 207a vom 03.11.2005

/CHU 08/ Chu, T.L., et.al.
Traditional Probabilistic Risk Assessment Methods for Digital Systems
U.S. Nuclear Regulatory Commission, NUREG/CR-6962, Oktober 2008

/DIN 05/ Deutsche Industrienorm (DIN)
DIN EN 61511: Funktionale Sicherheit - Sicherheitstechnische Systeme für die Prozessindustrie, VDE Verlag, DIN EN 61511(VDE 0810), Mai 2005

/DIN 06/ Deutsche Industrienorm (DIN)
DIN EN 62061: Sicherheit von Maschinen - Funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer Steuerungssysteme (IEC 62061:2005), Beuth Verlag GmbH, Juni 2006

/DIN 08/ Deutsche Industrienorm (DIN)
DIN EN ISO 13849-1: Sicherheit von Maschinen-Sicherheitsbezogene Teile von Steuerungen – Teil 1: Allgemeine Gestaltungsleitsätze, Deutsche Fassung EN ISO 13849, Beuth Verlag GmbH, Dezember 2008

/DIN 09/ Deutsche Industrienorm (DIN)
DIN EN IEC 61508: Funktionale Sicherheit sicherheitsbezogener elektrischer /elektronischer/ programmierbarer elektronischer Systeme. Teil 2: Anforderungen, VDE Verlag, E DIN EN 61508-2 (VDE 0803-2), Juni 2009

/FAK 05/ Facharbeitskreis (FAK) Probabilistische Sicherheitsanalyse für Kernkraftwerke
Methoden zur probabilistischen Sicherheitsanalyse für Kernkraftwerke, Stand: August 2005, BfS-SCHR-37/05, Wirtschaftsverlag NW / Verlag für neue Wissenschaft GmbH, Salzgitter ISSN 0937-4469,
ISBN 3-86509-414-7, Oktober 2005

/KOR 09/ Korsah K., et.al.
Instrumentation and Controls in Nuclear Power Plants: An Emerging Technologies Update, U.S. Nuclear Regulatory Commission, NUREG/CR-6992, Washington, DC, Oktober 2009

/KTA 05/ Kerntechnischer Ausschuss (KTA)
Sicherheitstechnische Regel des KTA: KTA 3503, Typprüfung von elektrischen Baugruppen der Sicherheitsleittechnik, Fassung 11/05, November 2005

/NEA 09/ OECD Nuclear Energy Agency (NEA) Committee on the Safety of Nuclear Installations (CSNI):
Recommendations on Assessing Digital System Reliability in Probabilistic Risk Assessments of Nuclear Power Plants, NEA/CSNI/R(2009)18, Paris, December 2009

/PIL 04/ Piljugin, E., J. Märtz H. Heinsohn, W. Frey
Anpassung und Erprobung von Methoden zur probabilistischen Bewertung digitaler Leittechnik, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH, GRS-A-3258, Garching/Köln, Dezember 2004

/RSK 97/ Reaktorsicherheitskommission (RSK)
RSK-Leitlinien für Druckwasserreaktoren, Verband der Technischen Überwachungs-Vereine e.V. (VdTÜV), Essen, Fassung 01.97, 1997

/WOO 10/ Wood, R. T., et al.
Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems, U.S. Nuclear Regulatory Commission, NUREG/CR-7007, Washington, DC, Februar 2010

Anhang A

Review of the draft NUREG report "Modeling a digital feedwater control system using traditional probabilistic risk assessment methods"

Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH, Schwertnergasse 1,
D-50667 Cologne, Germany.

W. Frey, E. Piljugin, J. Stiller and A. Wielenberg contributed to the review.

1. Introduction

GRS has been asked by the authors to participate in the peer review of the draft NUREG "Modeling a digital feedwater control system using traditional probabilistic risk assessment methods" [1] and to provide an informal review report [2, 3]. A total effort of one man week was suggested. Therefore, the present review is limited in depth and scope, e.g. the mathematical equations have not been verified in detail.

2. General comments

The benchmark study of a probabilistic assessment of a software based digital feedwater control system (DFWCS) presented in the report is a valuable contribution to the international effort to develop and to establish PRA methods for software based digital I&C systems. The general approach taken appears promising and should be further developed and tested by modeling a software based digital reactor protection system (RTS /ESFAS). Such systems pose additional challenges compared to the modeling of the DFWCS considered in the present report, since due to their high degree of redundancy of signal processing a more sophisticated treatment of CCFs appears necessary. The numerical evaluation will also be more demanding. In the course of this work the methods could be advanced and their applicability for general software based I&C systems could be demonstrated.

We recommend that the draft NUREG report should be revised to enhance clarity, accessibility and comprehensibility of the methodology used. A list of general and detailed recommendations that should be considered is included as an appendix. Several of

these recommendations have already been discussed with the authors in the course of the review process [4-9].

3. Specific questions

A list of specific questions was provided for the review. In the following, short answers or comments are provided after citations of the questions (in italic).

1) Is the level of detail of the digital feedwater control system (DFWCS) failure modes and effects analysis (FMEA) and reliability model appropriate for the objectives of the report, as delineated in Section 1.2.1)? Are there any obvious additional failure modes that appear to have been overlooked?

In principle we regard the hierarchical approach (components – modules – system) utilized in this study to be very useful. From our point of view, it depends on the subject of analysis and the availability of reliability data whether the consideration of the very detailed “component”-level is appropriate for a specific module. In the present study this detailed analysis was carried out for independent failures, considering “major components” of the modules, while CCF have been treated on a higher level. This appears reasonable for the present study, given the data sources used (generic reliability data for generic hardware components). For other applications a different level of detail might be appropriate, e.g. if sufficient operating experience is available, which is usually collected on module level. GRS experience shows that generic reliability data should only be used if sufficient operating experience is unavailable, and that failure rates of modules estimated using a FMEA on component level should be validated by operating experience, if available.

2) Does the approach of using the FMEA tool to automatically generate the system failure combinations and using the Markov model to quantify the system failure frequency seem reasonable? Do you believe this approach can be considered a general method for modeling any digital system? What is your opinion about the practicality of solving the complex model of the whole system?

The approach of using the simulation tool to automatically generate combinations of the component failures leading to the top event seems reasonable for the DFWCS system analyzed in the present study. The approach might also be a valuable tool for the quality assessment of a complex system and the deterministic assurance that unavailability is not dominated by few independent failures, which might help to demonstrate

the robustness of the design. It is also conceivable that this kind of simulation tool could be used for the analysis of specific macro-components in the framework of an ET/FT approach.

Whether the approach can be considered a general method for modeling any digital system in PRA can only be assessed by applying it to a large standby system, i.e. RTS/ESFAS systems. These systems are much more complex than the DFWCS system since they are typically composed of multiple trains, implement a large number of I&C functions, use a very large number of signals and have features like self-monitoring, automatic recovery, automatic reconfiguration and network communication. For these systems we expect additional challenges: A more sophisticated treatment of CCFs will be necessary. Probably, not only the order of events, but also the exact timing can be important due to system recovery features like automated reboot of CPU modules. The numerical evaluations will be much more demanding due to the much larger number of states and the expected necessity to evaluate longer paths. We regard these additional challenges to be substantial. Only the actual performance of the analysis will show if they can be met.

For future applications of an automated FMEA tool the verification and validation of the tool will also be an important issue, especially if PRA results are used in regulation.

A topic that was not mentioned in the report is the integration of the results of the Markov model into an existing PRA. This is not trivial since the failure rates/initiating frequencies calculated with the Markov model are time dependent. It should be described how to use them in a plant PRA. Additionally, it should be discussed how probabilities of component failures on demand are transferred into failure rates for the Markov model.

3) Is the approach for assessing probabilistic parameters reasonable? Is the use of failure parameters and raw data reasonable? Do you have any suggestions on how to get better data, including hardware common cause failure data?

The approach to assess the probabilistic parameters appears to be reasonable for the current proof-of-concept study. We cannot judge whether this procedure would meet the relevant US-American requirements. It would, however, not comply with the German PRA guidelines due to a lack of traceability of the data and their applicability to the

specific I&C equipment analyzed and because plant specific operating experience is not considered.

To obtain reliable probabilistic parameter estimates a substantial research effort including the systematic evaluation of operating experience of nuclear and comparable industries appears necessary.

4) In quantifying the Markov model, what is your opinion regarding the truncation of sequences with more than three failures (e.g., do you feel convergence has been adequately demonstrated)? Do you believe there are other more appropriate quantification methods? Do you believe that there are simplified quantification methods that may be adequate?

It has been demonstrated that for the current application the contribution of sequences is quickly decreasing with the number of failures. If a system is composed of highly reliable components such decrease always should occur. For systems like RTS or ESFAS, which have a higher degree of redundancy, this decrease may be expected to appear at a larger number of failures.

Identifying a trend is not sufficient to demonstrate sufficient accuracy of the numerical calculation. To do this, the maximal absolute error should be calculated, which is straightforward: If paths have been evaluated to order N, the maximal absolute error equals the total probability of paths with more than N failures, because for these paths it is not known if the system fails. This, trivially, is equivalent to (1- total probability of paths with N or less failures). Depending on the aim of the analysis sufficient accuracy has been reached when the maximal absolute error or when the maximal relative error (ratio between the total probability of sequences of order N for which the system fails, and maximal absolute error) is small enough, respectively.

The general method of quantification is adequate. We do not believe that there are simpler methods available.

5) What is your opinion regarding the treatment of parameter, modeling and completeness uncertainties? Do you have any recommendations on how to better treat any of these types of uncertainty? Are there any additional sensitivity calculations that you think would be important to perform as part of this proof-of-concept study?

In general, the systematic assessment of all the possible sources of uncertainty in PRA studies is still partly a subject of basic research. The limited analyses presented in this study have to be judged in light of this fact. We would recommend to initially setting the focus on the further development and demonstration of the principal PRA methods before advancing methods of uncertainty analysis.

6) Are the explanations for satisfying the desirable characteristics adequate, acknowledging that as a proof-of-concept study the scope is limited in some areas?

Due to the limitations of this concept study, several of the desirable characteristics are not satisfied. This appears adequate for a pilot study and should be clearly stated.

7) Are the conclusions supported by the information provided in the report? Do you agree with the conclusions and insights? What are your opinions regarding the suggested areas of additional research? Do you have any other suggestions for additional research?

The conclusions in chapter 11 are supported by the information within the report. While we agree with most of the insights, it should be noted that it is not obvious that parallel computing is able to solve the state explosion problem for more complex models. The influence of time ordering is definitely an important feature of digital systems. However, the possibility that timing itself may be essential for digital I&C systems should also be considered. Therefore, we fully agree with the plan to apply the approach to a RTS or ESFAS system.

With regard to the objective of the report there should be a more elaborate comparison between the Markov and the FT/ET approaches.

The discussion given for drifting signals does not explicitly take into account the result of the sensitivity calculation. Without OOR-checking (i.e. the effect of a drifting signal), system unavailability increases significantly. This would merit further investigation.

The areas of additional research in chapter 11.3 cover the important questions of software based digital I&C modeling. We would highlight items 3 to 7, i.e. probabilistic data for hardware failures including CCF and modeling software related failures. We consider the systematic analysis of operating experience to be essential for the advancement of these topics.

4. Conclusion

The PRA method described is a substantial contribution to the research of PRA modeling of software based digital I&C systems. To demonstrate its general applicability an additional benchmark study on a highly redundant digital standby I&C system (RTS or ESFAS) is necessary. The results might be of high importance to the field of PRA methods for software based digital I&C. We expect that in the course of this study the methods will have to be advanced to cope with the potential problems discussed above (CCF modeling, timing, and state explosion). To complement this research project additional research initiatives appear necessary, most importantly on software related failures and on probabilistic data including CCF. The draft NUREG report should be revised to enhance comprehensibility and accessibility.

List of general and detailed recommendations for the revision of the draft NUREG report "Modeling a digital feedwater control system using traditional probabilistic risk assessment methods"

- The description of the top event of the DFWCS failure analysis should be improved. It should be emphasized that both switchover to manual control and wrong control signal are considered in the failure mode "loss of automatic control".
- A principal outline of the procedure for future analyses that takes into account the lessons learnt should be included (for details see [4] and [5]).
- The description of the automated FMEA tool should be revised. The way how the automated FMEA-tool actually propagates the effects of a component failure mode through the different levels of detail and finally decides whether the system is failed or not should be described. It should be stated clearly where and how information from a manual FMEA enters (e.g. in the form of a rule that the CPU module fails if the RAM fails) and which effects are automatically captured by the inclusion of the original system software. The working of the automated tool should also be discussed in relation to the steps and levels shown in figure 3-1. For a better understanding of this procedure it would be beneficial to discuss some non-trivial examples (e.g. a single component failure and two independent failures that fail the DFWCS, for details see [6] and [7]).
- There is no table showing the detailed results of the study (i.e. under which failure combinations of the macro-components the DFWCS fails). While it is unfeasible to present all possible combinations some interesting examples of failure combinations should be shown.
- The methodology used to identify "major components" should be described.
- "Component", "module", and "system" levels should be used systematically and consistently in the whole report. It should always be made clear to which of the different levels a statement applies. "CPU" and "CPU module" should be used consistently to avoid confusion.
- It also should always be made explicit if results presented come from a manual or automated analysis and whether they are preliminary or final.
- The previous 2 remarks especially apply to the tables. E.g. regarding table 3-1 the following problems were identified:

- CCFs are listed as “failure mode”. CCFs are no failure mode. They can have different failure modes.
- It is not entirely clear to which entities the failures relate, despite the table caption stating „component level”. While “The software on the main CPU seems to be running normally but sends erroneous output” must be on module level (unless there is a software component), the others seem to be on component level, despite the fact they are named like failure modes of the module. This is misleading. An additional column showing the component would be helpful.
- It should be clearly stated how failure effects (columns 4 and 5) were determined.

- The description of the treatment of CCFs should be improved. It should be mentioned that CCFs are included in the Markov model as “pseudo-components”.
- The introduction of "CCF-pseudo-components" and the assumption that "any component only fails once with one specific failure mode" are incompatible. This fact should be mentioned and it should be described how this is resolved.
- The discussion of the out of range (OOR) checking in chapter 8.4.4 shows that the reliability decreases significantly when out of range checking is disabled. This shows that the assumption that drifting signals are always OOR is a substantial and non-conservative assumption. This should be discussed.
- References for the analytic solutions of the equations appear to be incomplete. While we cannot point the authors to a specific publication we would be surprised if the method had not been used before.
- It should be mentioned that the failure rates calculated with the Markov model generally are time-dependent, while e.g. equation (1-1) suggests that they are constant. It should be stated that the values in table 8-2 are average rates for t=1 year. Using these average rates in a plant PSA would not necessarily be conservative.
- Generally, limitations of assumptions should be discussed where they are made. E.g. the validity and limitation of the assumption that drifting analog signals eventually reach “out of range high” (OORH) or “out of range low” OORL are not discussed until page 3-14.
- Figure captions and/or descriptions could be improved (see also [4])

References:

[1] T.L. Chu, M. Yue, G. Martinez-Guridi, and J. Lehner
"Modeling a digital feedwater control system using traditional probabilistic risk assessment methods"
Draft of the NUREG/CR-XXXX

[2] Email T.L. Chu to E. Piljugin 2008-10-07

[3] Email T.L. Chu to E. Piljugin 2008-10-08

[4] Email J. C. Stiller to T.L. Chu and G. Martinez-Guridi 2008-12-05 with attached MS-Word document "questionsNuregdiskussionV2.docx" containing the first list of questions and comments.

[5] Email T.L. Chu to J. C. Stiller 2008-12-09 with attached MS-Word document "ResponseToStiller 12-9-2008.doc" containing answers and comments to [2].

[6] Emails J. C. Stiller to T.L. Chu 2008-12-10

[7] Emails T.L. Chu to J. C. Stiller 2008-12-10, with attached MS-Powerpoint presentation "PSA 2008 An Automated Tool for Supporting FMEAs of Digital Systems.ppt".

[8] Email J. C. Stiller to T.L. Chu and Martinez-Guridi 2008-12-11 with attached MS-Word document "questionsNuregdiskussionS2V1.docx" containing the second list of questions and comments.

[9] Email T.L. Chu to J. C. Stiller 2008-12-11, with attached MS-Word document "Answer to GRS regarding FMEA tool.doc" containing answers and comments to [6].

Verteiler

		Exemplare: gedruckte Form	Exemplare: pdf
BMWi			
Referat III B 4		1 x	
GRS-PT/B			
Internationale Verteilung	(FIZ)	40 x	
Projektbegleiter	(stu)	3 x	1 x
GRS			
Geschäftsführung	(wfp, stj)		je 1 x
Bereichsleiter	(erv, paa, prg, rot, stc, ver, zir)		je 1 x
Abteilungsleiter	(som, wil, poi)		je 1 x
Projektleiter	(row)	1 x	1 x
Projektbetreuung	(wal, bna)		1 x
Informationsverarbeitung	(nit)		1 x
Autoren	(hej, pil)	je 1 x	je 1 x
Bibliothek	(Köln)	1 x	
Gesamtauflage:	**Exemplare**	**48**	

Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH

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

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

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

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

www.grs.de